



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE TELECOMUNICACIONES

**INFORME FINAL DEL TRABAJO DE INTEGRACIÓN
CURRICULAR, PROYECTO DE INVESTIGACIÓN**

TEMA:

**“AUDITORIA DE LA SEGURIDAD A LA RED DE
TELECOMUNICACIONES DE NOVA CLÍNICA MODERNA EN BASE
AL MARCO DE CIBERSEGURIDAD DE LA NIST”**

Trabajo de titulación previo a la obtención del título de Ingeniero en Telecomunicaciones

Línea de investigación: Desarrollo, aplicación de software y cibersecurity (seguridad cibernética)

AUTOR:

Latacumba Farinango Marco Fabricio

DIRECTOR:

Ing. Cuzme Rodríguez Fabián Geovanny, MSc

Ibarra, 2024

**UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA**

IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1004108872		
APELLIDOS Y NOMBRES:	LATACUMBA FARINANGO MARCO FABRICIO		
DIRECCIÓN:	SAN ANTONIO DE IBARRA, CALLE EZEQUIEL RIVADENEIRA Y ALEJANDRO PONCE		
EMAIL:	f.latacumba@gmail.com		
TELÉFONO FIJO:	XXXXXXXXXX	TELF. MOVIL	0990656689

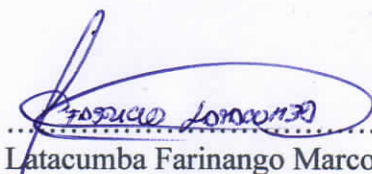
DATOS DE LA OBRA	
TÍTULO:	AUDITORIA DE LA SEGURIDAD A LA RED DE TELECOMUNICACIONES DE NOVA CLÍNICA MODERNA EN BASE AL MARCO DE CIBERSEGURIDAD DE LA NIST
AUTOR (ES):	LATACUMBA FARINANGO MARCO FABRICIO
FECHA: AAAAMMDD	02/12/2024
SOLO PARA TRABAJOS DE INTEGRACIÓN CURRICULAR	
CARRERA/PROGRAMA:	<input checked="" type="checkbox"/> GRADO <input type="checkbox"/> POSGRADO
TÍTULO POR EL QUE OPTA:	INGENIERO EN TELECOMUNICACIONES
DIRECTOR:	ING. CUZME RODRÍGUEZ FABIÁN GEOVANNY. MSC
	ING. DOMÍNGUEZ LIMAICO HERNAN MAURICIO. MSC

AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Latacumba Farinango Marco Fabricio, con cédula de identidad Nro. 1004108872, en calidad de autor (es) y titular (es) de los derechos patrimoniales de la obra o trabajo de integración curricular descrito anteriormente, hago entrega del ejemplar respectivo en formato digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior Artículo 144.

Ibarra, a los 4 días del mes de diciembre de 2024

EL AUTOR:



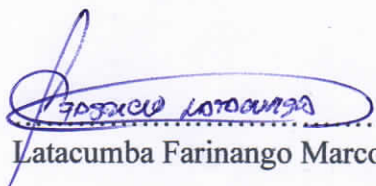
.....
Latacumba Farinango Marco Fabricio

CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 4 días, del mes de diciembre de 2024

EL AUTOR:


Latacumba Farinango Marco Fabricio

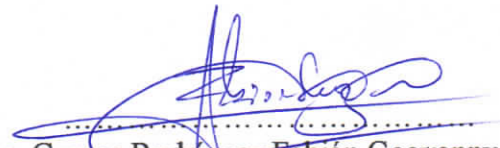
CERTIFICACIÓN DEL DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, 2 de diciembre de 2024

ING. CUZME RODRÍGUEZ FABIÁN GEOVANNY. MSC
DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración Curricular, el mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.



Ing. Cuzme Rodríguez Fabián Geovanny. Msc
C.C.: 1311527012

APROBACIÓN DEL COMITÉ CALIFICADOR

El Comité Calificado del trabajo de Integración Curricular “Auditoria de la seguridad a la red de Telecomunicaciones de Nova Clínica Moderna en base al marco de ciberseguridad de la NIST” elaborado por Latacumba Farinango Marco Fabricio, previo a la obtención del título del Ingeniero en Telecomunicaciones, aprueba el presente informe de investigación en nombre de la Universidad Técnica del Norte:



Ing. Cuzme Rodríguez Fabián Feovanny. Msc
C.C.: 1311527012



Ing. Hernán Mauricio Domínguez Limaico. MSc
C.C: 1002379301

DEDICATORIA

Este trabajo va dedicado con todo mi corazón a mi principal razón de vivir; a mi madre Rosa Matilde Farinango Méndez, pilar fundamental en mi formación personal y profesional, quien siempre ha estado presente incondicionalmente en los buenos y malos momentos con sus sabios consejos, apoyo y confianza en mi capacidad para superar cualquier desafío durante este largo trayecto, por siempre creer en mi y en los objetivos que siempre he plasmado conseguir a lo largo de mi vida forjando siempre mi carácter y valores que hoy por hoy trato de plasmarlos en mi diario vivir.

A mi padre Marco Homero Latacumba Marín por siempre estar al pendiente y apoyarme durante toda mi vida y siempre confiar en el proceso, con su trato afectuoso que siempre ha plasmado en sus hijos.

A mi hermana, mi compañera y amiga de vida Johanna Camila Latacumba Farinango quien con su manera de ser, su amor incondicional y ocurrencias siempre ha logrado plasmar felicidad y alegría dentro de mi corazón y mi ser. Además de ser mi refugio y mi soporte en los momentos amargos que me ha tocado vivir, por siempre ser parte de mis locuras y aventuras que hemos compartimos y que compartiremos durante toda la vida.

Dedicado también para ese ángel de luz que en el cielo está; quien desde que nací y hasta el último día que compartí con él me demostró su infinito amor y sé que hoy por hoy está cuidándome y guiándome en esta nueva etapa profesional, como siempre solía hacerlo. Abuelito esto también va para usted.

Marco Fabricio Latacumba Farinango

AGRADECIMIENTO

En primer lugar agradezco a Dios por permitirme disfrutar el privilegio de estar vivo y tener salud para poder hoy por hoy finalizar este proyecto a fin de culminar con esta etapa de mi vida.

Agradezco con todo mi corazón a mis padres y hermana por el amor y apoyo incondicional a lo largo de mi vida y etapa universitaria, sin ellos nada de esto hubiese sido posible conseguir.

Agradezco a todos mis amigos de colegio, amigos y entrenadores de fútbol, amigos de universidad quienes también han sido parte importante en mi vida por siempre compartir su conocimiento y experiencia que ha contribuido de la mejor manera en mi vida.

Expreso mi más sincero agradecimiento y gratitud a Nova Clínica Moderna y sus dirigentes por abrir en un inicio sus puertas a mi madre y posteriormente permitirme realizar el presente trabajo, al mismo tiempo un agradecimiento especial a la Ingeniera Ximena Andrade por la apertura y al Ingeniero Marcelo Rea por ser guía y apoyo fundamental durante el desarrollo de este proyecto.

A mi tutor de trabajo de titulación MSc. Fabián Cuzme y a mi asesor de trabajo de titulación MSc. Mauricio Domínguez, a quienes agradezco por haber sido una guía fundamental y por haber compartido su conocimiento y experiencia conmigo durante todo este largo trayecto.

Finalmente agradezco a todas las personas que han compartido en mi entorno y siempre han estado para mí y han augurado los mejores deseos durante todo el trayecto de mi carrera

Marco Fabricio Latacumba Farinango

RESUMEN

El presente proyecto se fundamenta en la necesidad de evaluar y brindar políticas, recomendaciones, pautas y directrices que fortalezcan la seguridad de la red de telecomunicaciones de Nova Clínica Moderna, una empresa de prestigio en el sector salud a nivel local y nacional. El objetivo principal fue garantizar la confidencialidad e integridad de datos y sistemas críticos mediante el desarrollo de una auditoría basada en el marco de ciberseguridad de la NIST y la metodología OCTAVE. En base a lo mencionado, el análisis tuvo enfoque en la identificación, valoración y gestión de riesgo asociados a los activos críticos, mediante el desarrollo de política que promuevan la protección de la infraestructura tecnológica de la organización. Basado en la aplicación de la metodología OCTAVE durante el proceso de auditoría, fue posible estructurar un análisis integral de riesgos, identificando posibles vulnerabilidades y proponiendo medidas de protección específicas. Por lo que, se logró realizar un análisis subjetivo proyectado a futuro, en el caso de que se llegara a aplicar dichas políticas, una significativa reducción de los riesgos de los activos críticos, alineándose según las necesidades estratégicas de la organización.

Lo que lleva a la conclusión de que, aunque la empresa cuenta con sólidas bases de seguridad en su red empresarial, la implementación de las políticas recomendadas permitirá fortalecer su infraestructura tecnológica, mejorar su resiliencia antes posibles amenazas. Además, se hace énfasis en la importancia del soporte y colaboración del área de TIC'S, ya que su amplio conocimiento fue clave para el desarrollo de las soluciones alineadas con el contexto organizacional, dejando como aprendizaje importantes experiencias para la aplicación en futuros escenarios profesionales.

Palabras clave: auditoría, ciberseguridad, NIST, OCTAVE, telecomunicaciones, políticas de protección, análisis de riesgos.

ABSTRACT

This project is based on the need to evaluate and provide policies, recommendations, guidelines and directives that strengthen the security of the telecommunications network of Nova Clínica Moderna, a prestigious company in the health sector at local and national level. The main objective was to ensure the confidentiality and integrity of critical data and systems through the development of an audit based on the NIST cybersecurity framework and the OCTAVE methodology. Based on the above, the analysis focused on the identification, assessment and risk management associated with critical assets, through the development of policies that promote the protection of the organization's technological infrastructure. Based on the application of the OCTAVE methodology during the audit process, it was possible to structure a comprehensive risk analysis, identifying possible vulnerabilities and proposing specific protection measures. Thus, a subjective analysis projected into the future was achieved, in the event that such policies were to be applied, a significant reduction in the risks of critical assets, aligned according to the strategic needs of the organization.

This leads to the conclusion that, although the company has solid security foundations in its corporate network, the implementation of the recommended policies will strengthen its technological infrastructure and improve its resilience to possible threats. In addition, emphasis is made on the importance of the support and collaboration of the ICT area, since their extensive knowledge was key to the development of solutions aligned with the organizational context, leaving as learning important experiences for application in future professional scenarios.

Keywords: audit, cybersecurity, NIST, OCTAVE, telecommunications, protection policies, risk assessments.

LISTA DE SIGLAS

ACL. Lista de control de acceso

ANSI. American National Standards Institute

AP. Punto de acceso

CIA TRIAD. Confidentiality, Integrity, Availability Triad

COIP. Código Orgánico Integral Penal

CSF NIST. Cybersecurity Framework del National Institute of Standards and Technology

DDTI. Dirección de Desarrollo Tecnológico e Informático

DNS. Domain Name System

HIS-ERP. Hospital Information System - Enterprise Resource Planning

HIPAA. Health Insurance Portability and Accountability Act

IEEE. Institute of Electrical and Electronics Engineers

IP. Internet Protocol

ISO. International Organization for Standardization

LAN. Local Area Network

LDAP. Lightweight Directory Access Protocol

LIS. Laboratory Information System

LODP. Ley Orgánica de Protección de Datos

MAC. Media Access Control

NIST. National Institute of Standards and Technology

OCTAVE. Operationally Critical Threat, Asset, and Vulnerability Evaluation

ODS. Objetivos de Desarrollo Sostenible

OMS. Organización Mundial de la Salud

ONU. Organización de las Naciones Unidas

PBX. Private Branch Exchange

PEAP. Protected Extensible Authentication Protocol

RIS-PACS. Radiology Information System - Picture Archiving and Communication System

SDN. Software Defined Networking

SNMP. Simple Network Management Protocol

SSH. Secure Shell

SSL/TLS. Secure Sockets Layer/Transport Layer Security

TIC'S. Tecnologías de la Información y la Comunicación

TIA. Telecommunications Industry Association

UTP. Unshielded Twisted Pair

VLAN. Virtual Local Area Network

VPN. Virtual Private Network

VPC. Virtual Personal Computer

VoIP. Voice over Internet Protocol

WAN. Wide Area Network

WAF. Web Application Firewall

WI-FI. Wireless Fidelity

WPA. Wi-Fi Protected Access

ÍNDICE DE CONTENIDOS

1.	CAPÍTULO I. Antecedentes	21
1.1	Tema	21
1.2	Problema	21
1.3	Objetivos	23
1.3.1	Objetivo general.....	23
1.3.2	Objetivos específicos.....	23
1.4	Alcance	24
1.5	Justificación	27
2.	CAPÍTULO II. Fundamento Teórico.....	32
2.1.	Ciberseguridad en las Organizaciones.....	32
2.1.1.	<i>Amenazas en Ciberseguridad</i>	<i>33</i>
2.1.2.	<i>Evolución de las Amenazas Cibernéticas</i>	<i>33</i>
2.1.4.	<i>Riesgos</i>	<i>35</i>
2.1.5.	<i>Impacto</i>	<i>36</i>
2.1.6.	<i>Seguridad Operacional.....</i>	<i>37</i>
2.1.7.	<i>Modelos de Seguridad.....</i>	<i>37</i>
2.1.8.	<i>Ethical Hacking.....</i>	<i>38</i>
2.2.	Auditoría de Seguridad	38
2.2.1.	<i>Tipos de Auditorías de Seguridad.</i>	<i>39</i>
2.2.2.	<i>Herramientas Técnicas para realizar una Auditoría de Seguridad</i>	<i>42</i>
2.3.	Metodologías de una Auditoría de Seguridad.....	43
2.3.1.	<i>OCTAVE</i>	<i>43</i>
2.3.2.	<i>Magerit.....</i>	<i>44</i>
2.3.3.	<i>OSSTMMv3 (Manual de Metodología de Prueba de Seguridad de Código Abierto)</i> <i>45</i>	<i>45</i>
2.3.4.	<i>NIST SP 800-115</i>	<i>46</i>
2.4.	Marco de Ciberseguridad de la NIST.....	47
2.4.1.	<i>Tiers</i>	<i>48</i>
2.4.2.	<i>Profile</i>	<i>49</i>
2.4.3.	<i>Funciones Principales del Marco.....</i>	<i>49</i>
2.5.	Marco Legal Para Procesos de Auditoría de Seguridad de la Información en Ecuador	51
3.	CAPÍTULO III. Análisis de la situación actual de Nova Clínica Moderna.....	55
3.1.	Método de investigación	55
3.1.1.	<i>Estrategias de recolección de datos</i>	<i>56</i>

3.2.	Descripción general de la organización	58
3.1.1.	<i>Estructura organizacional de la empresa</i>	58
3.1.2.	<i>Identificación del nivel de conocimiento de stakeholders acerca de la seguridad actual de la red</i>	60
3.1.3.	<i>Análisis general del Área Tecnológica y de los recursos de telecomunicaciones organizacionales</i>	61
3.2.	Análisis de la infraestructura de Telecomunicaciones	63
3.2.1.	<i>Topología física y lógica</i>	64
3.2.2.	<i>Descripción de los activos críticos que componen la infraestructura de red</i>	67
3.2.3.	<i>Hardware distribuido por áreas en Nova Clínica Moderna</i>	78
3.2.4.	<i>Software y sistemas de información disponible en Nova Clínica Moderna</i>	79
3.3.	Desarrollo de perfil de seguridad actual de los activos críticos de la red de Telecomunicaciones	81
3.3.1.	<i>Aplicación de evaluación de seguridad actual basada en el marco de ciberseguridad de la NIST</i>	82
3.3.2.	<i>Resumen de resultados de la matriz de evaluación</i>	88
3.3.3.	<i>Matriz de valoración de activos críticos de la red de telecomunicaciones de Nova Clínica Moderna</i>	126
3.3.4.	<i>Inventario de amenazas y vulnerabilidades de los activos críticos</i>	130
3.3.5.	<i>Identificación de riesgos a partir de inventario de vulnerabilidades y amenazas</i> 131	
3.3.6.	<i>Matriz de criterio de impacto y probabilidad</i>	136
3.3.7.	<i>Evaluación del nivel de riesgo de los activos críticos de la red de telecomunicaciones de Nova Clínica Moderna</i>	139
4.	CAPÍTULO IV. DESARROLLO DE POLÍTICAS Y PROPUESTA DE IMPLEMENTACIÓN	147
4.1.	Proceso para la creación de políticas de seguridad para la red de Nova Clínica Moderna 147	
4.2.	Diseño de políticas de seguridad	148
4.3.	Procedimiento para implementación de políticas de seguridad como propuesta a Nova Clínica Moderna en base al marco de ciberseguridad de la NIST englobando la Metodología OCTAVE	167
4.4.	Manual de procedimientos de seguridad a la red de Telecomunicaciones de Nova Clínica Moderna	169
4.4.1.	<i>Manual de procedimientos para la protección de datos sensibles</i>	169
4.4.2.	<i>Manual de procedimiento para la gestión de vulnerabilidades e incidentes de ciberseguridad</i>	171
4.4.3.	<i>Manual de procedimientos técnicos para la seguridad de la red</i>	173
4.4.4.	<i>Manual de procedimientos para el control de acceso a los recursos de información críticos</i> 176	

4.5. Simulación de soluciones técnicas propuestas dentro de las políticas de seguridad a la red de Telecomunicaciones de Nova Clínica Moderna	178
4.5.1. Direccionamiento lógico de VLANs	179
4.5.2. Port Security	180
4.5.3. Radius (IEEE 802.1X).....	183
4.5.4. 2FA (Doble factor de autenticación)	189
4.5.5. Certificados digitales SSL/TLS.....	197
4.5.6. VPN IPsec para acceso remoto	205
4.5.7. Sistema de monitorización de redes.....	211
4.5.8. Proxy Transparente	218
4.5.9. Acceso SSH mediante llaves criptográficas	223
4.5.10. Iptables en servidores Linux.....	226
4.5.11. Configuración de seguridad para servidor de VoIP – Elastix.....	227
RESULTADOS Y ANÁLISIS	230
DISCUSIÓN	247
CONCLUSIONES.....	249
RECOMENDACIONES.....	251
REFERENCIAS BIBLIOGRÁFICAS	253
ANEXOS.....	257

ÍNDICE DE TABLAS

Tabla 1 Evolución de ataques cibernéticos.....	34
Tabla 2 Características y patrones de ataques comunes en medios de comunicación social	35
Tabla 3 Niveles de impacto potencial.....	36
Tabla 4 Información derivada de auditorías de ciberseguridad.....	41
Tabla 5 Análisis comparativo de las herramientas automatizadas de auditorías disponibles	42
Tabla 6 Estrategias de recolección de datos	57
Tabla 7 Análisis de dominios ISO 27001 adaptados al proceso de auditoría en Nova Clínica Moderna	60
Tabla 8 Análisis del estado actual del área tecnológica y de los recursos de telecomunicaciones organizacionales.....	62
Tabla 9 Características de conmutadores de Nova Clínica Moderna.....	71
Tabla 10 Características de servidores internos de Nova Clínica Moderna.....	73
Tabla 11 Ubicación de hardware por áreas de Nova Clínica Moderna	78
Tabla 12 Software distribuido por áreas de Nova Clínica Moderna	80
Tabla 13 Resumen de evaluación de la categoría “Gestión de activos”	91
Tabla 14 Resumen de evaluación de la categoría “Evaluación de riesgos”	93
Tabla 15 Resumen de evaluación de la categoría “Estrategia de gestión de riesgos”	95
Tabla 16 Resumen de evaluación de la categoría “Gestión de identidad, autenticación y control de acceso”	97
Tabla 17 Resumen de evaluación de la categoría “Concienciación y capacitación”	99
Tabla 18 Resumen de evaluación de la categoría “Seguridad de los datos”	101
Tabla 19 Resumen de evaluación de la categoría “Procesos y procedimiento de protección de la información”	104
Tabla 20 Resumen de evaluación de la categoría “Mantenimiento”	107
Tabla 21 Resumen de evaluación de la categoría “Tecnología de protección”	109
Tabla 22 Resumen de evaluación de la categoría “Anomalías y eventos”	111
Tabla 23 Resumen de evaluación de la categoría “Monitoreo continuo de la seguridad”.....	113
Tabla 24 Resumen de evaluación de la categoría “Monitoreo continuo de la seguridad”.....	115
Tabla 25 Resumen de evaluación de la categoría “Planificación de respuesta”.....	117
Tabla 26 Resumen de evaluación de la categoría “Comunicación”	119
Tabla 27 Resumen de evaluación de la categoría “Análisis”	121
Tabla 28 Resumen de evaluación de la categoría “Mitigación”	123
Tabla 29 Resumen general de evaluación de la función “Recuperar”.....	125
Tabla 30 Escala de medición del nivel de criticidad de los activos críticos de Nova Clínica Moderna.....	126
Tabla 31 Matriz de valoración de activos críticos de Nova Clínica Moderna.....	127
Tabla 32 Posibles amenazas y vulnerabilidades de los activos críticos de la empresa	130
Tabla 33 Matriz de identificación de riesgos de activos críticos.....	132
Tabla 34 Criterios de impacto de amenazas de los activos críticos.....	136
Tabla 35 Criterios de probabilidad de amenazas de los activos críticos	138
Tabla 36 Matriz de evaluación de riesgos	140
Tabla 37 Tabla de evaluación del nivel de riesgo potencial de los activos críticos	141

Tabla 38 Proceso para la elaboración de políticas de seguridad	147
Tabla 39 Analogía porcentual para la asignación de subred de cada VLAN de Nova Clínica Moderna	179
Tabla 40 Levantamiento de subredes para la red de Nova Clínica Moderna.	180
Tabla 41 Análisis de riesgos residuales para cableado horizontal y vertical dentro de la infraestructura tecnológica	232
Tabla 42 Análisis de riesgos residuales para Routers Firewall dentro de la infraestructura tecnológica.....	234
Tabla 43 Análisis de riesgos residuales para Conmutadores dentro de la infraestructura tecnológica.....	236
Tabla 44 Análisis de riesgos residuales para Equipos Servidores dentro de la infraestructura tecnológica	238
Tabla 45 Análisis de riesgos residuales para Troncal SIP dentro de la infraestructura tecnológica.....	240
Tabla 46 Análisis de riesgos residuales para Troncal analógica (FXO SIP Gateway) dentro de la infraestructura tecnológica.....	242
Tabla 47 Análisis de riesgos residuales para Infraestructura Wireless dentro de la infraestructura tecnológica	244
Tabla 48 Análisis de riesgos residuales para Estaciones de Trabajo dentro de la infraestructura tecnológica	246

ÍNDICE DE FIGURAS

Figura 1 Subfases de la metodología OCTAVE.....	26
Figura 2 Fases de la metodología OCTAVE.....	44
Figura 3 Niveles de implementación del marco	49
Figura 4 Funciones del Framework Core de la NIST	50
Figura 5 Organigrama institucional de CLIMODER S.A	59
Figura 6 Topología actual de Nova Clínica Moderna	66
Figura 7 Cableado Horizontal de Nova Clínica Moderna	68
Figura 8 Cableado vertical de Nova Clínica Moderna	69
Figura 9 Router Firewall Fortigate FG-80E	70
Figura 10 Switch core Aruba Instant On 1930.....	70
Figura 11 Switchs capa de acceso de Nova Clínica Moderna.....	71
Figura 12 Puntos de acceso inalámbricos de la serie Ubiquiti UniFi.....	76
Figura 13 Modelo de router inalámbrico de los consultorios de Nova Clínica Moderna ..	77
Figura 14 Categorías y subcategorías de la función Identificar	83
Figura 15 Categorías y subcategorías de la función Proteger	84
Figura 16 Categorías y subcategorías de la función Detectar	86
Figura 17 Categorías y subcategorías de la función Responder.....	87
Figura 18 Categorías y subcategorías de la función Recuperar	88
Figura 19 Habilitación de Port Security en la interfaz 1/1/5 y asignación de direcciones MAC manualmente	181
Figura 20 Verificación de MAC address en cliente Windows 10.....	182
Figura 21 Verificación de MAC address en cliente VPC	182
Figura 22 Verificación de cliente excedente y rechazado de la interfaz donde se aplicó Port Security	183
Figura 23 Network Policy Server de RADIUS en Windows Server 2019.....	184
Figura 24 Directivas de red de NPS de RADIUS en Windows Server 2019.....	185
Figura 25 Usuario creado dentro de AD siguiendo las directrices de creación de usuario y contraseña robustas.....	185
Figura 26 Habilitación del servicio de configuración automática de redes cableadas	186
Figura 27 Proceso final de autenticación por medio de usuario y contraseña mediante el protocolo 802.1X en una conexión ethernet.....	187
Figura 28 Asignación de dirección IPv4 de la VLAN 10 una vez se autentica el usuario mediante el protocolo 802.1X	188
Figura 29 Visor de eventos de seguridad de Windows Server 2019.....	188
Figura 30 Claves de autenticación de la aplicación Microsoft RDP.....	190
Figura 31 Claves de autenticación de la aplicación Microsoft RDP	191
Figura 32 Comprobación de correcta sincronización con AD de Windows Server 2019	192
Figura 33 Comprobación de correcta sincronización de grupo de usuarios de AD	192
Figura 34 Comprobación de correcta sincronización de grupo de usuarios de AD.....	193
Figura 35 Verificación de usuarios sincronizados con AD y DUO	193
Figura 36 Ingreso de dispositivo móvil para autenticación de 2FA.....	194
Figura 37 Portal de login de usuario mflatacumbaf en Windows 10	195
Figura 38 Portal de autenticación de DUO para usuarios Windows 10.....	195

Figura 39 Notificación de autenticación de 2FA de Duo Mobile para el usuario mflatacumbaf.....	196
Figura 40 Logs de autenticación de los usuarios dentro del portal de administración de DUO	197
Figura 41 Portal de login del sistema de gestión hospitalaria OpenEMR.....	198
Figura 42 Creación de zona de búsqueda directa en el servidor DNS para www.climodersc.com	199
Figura 43 Acceso al sistema de gestión hospitalaria por medio del dominio www.climodersc.com	200
Figura 44 Configuración del archivo makecert.bat dentro de Windows Server 2019	201
Figura 45 Creación y modificación de archivo v3.ext	202
Figura 46 Generación de certificado SSL/TLS auto firmado.....	202
Figura 47 Proceso de instalación del certificado público SSL/TLS.....	203
Figura 48 Configuración de VirtualHost en Apache para redirección de HTTP a HTTPS y habilitación de certificados SSL/TLS.....	204
Figura 49 Certificado SSL/TLS instaurado en servidor web de sistema de gestión hospitalario	205
Figura 50 Creación de grupo de usuarios dentro del router firewall FortiGate.....	206
Figura 51 Proceso de creación de VPN IPsec dentro del router firewall FortiGate.....	207
Figura 52 Selección de interfaz local a la que se va a acceder desde el cliente remoto mediante el uso de la VPN IPsec y creación de rango de direcciones IPv4 para dicha VPN	208
Figura 53 Creación exitosa de la VPN IPsec dentro del router firewall FortiGate	209
Figura 54 Proceso de conexión desde el portal de la aplicación FortiVPN (FortiClient VPN).....	210
Figura 55 Ejemplo de conexión exitosa de manera segura y eficaz hacia un servidor alojado dentro del rango de direcciones de la VLAN de TICS de la empresa.....	211
Figura 56 Portal web de administración de software de monitorización Zabbix	212
Figura 57 Generación de contraseña aleatorio para posterior configuración de email de alertas en el servidor Zabbix.....	214
Figura 58 Configuración de parámetros correspondientes al correo electrónico utilizado para el envío de Triggers de los dispositivos monitoreados por Zabbix	215
Figura 59 Prueba de envío correcto de notificaciones hacia la dirección de correo electrónico	215
Figura 60 Correo de confirmación de sujeto de prueba correctamente configurado dentro de Zabbix hacia la dirección de Gmail ingresada.....	216
Figura 61 Adición de nuevas condiciones según la gravedad que envíen los Triggers por medio de notificaciones de Zabbix hacia el correo electrónico.....	217
Figura 62 Notificación de Triggers generados por Zabbix y notificados por medio de correo	217
Figura 63 Notificación detallada de Triggers generados con parámetros configurados previamente	218
Figura 64 Configuración inicial del proxy web transparente en router FortiGate	219
Figura 65 Selección de perfiles de seguridad para política de proxy web transparente en router FortiGate.	220

Figura 66 Bloqueo de URLs para el filtro web dentro de la política de proxy web transparente.....	221
Figura 67 Creación de política de firewall haciendo uso de modo de inspección basado en proxy.....	222
Figura 68 Comprobación de página bloqueada por medio del uso de proxy transparente web	223
Figura 69 Generación de llave con OpenSSH en cliente Windows 10	224
Figura 70 Administración de llave pública dentro de Windows Server 2019.....	224
Figura 71 Condiciones y restricciones configuradas para el acceso de llaves criptográficas SSH.....	225
Figura 72 Comprobación de acceso a servidor Windows Server2019 mediante uso de llaves criptográficas SSH	225
Figura 73 Tabla de reglas de Firewall para tráfico UDP en servidor de VoIP Elastix.....	227
Figura 74 Tabla de reglas de Firewall para Tráfico TCP en servidor de VoIP Elastix....	228
Figura 75 Cambio de número de puertos configurados por protocolo en el Firewall de Servidor de VoIP Elastix.....	229

1. CAPÍTULO I. Antecedentes

1.1 Tema

Auditoria de la seguridad a la red de Telecomunicaciones de Nova Clínica Moderna en base al marco de ciberseguridad de la NIST

1.2 Problema

En la actualidad múltiples empresas tienen el control de datos e información de clientes y funcionarios, especialmente en clínicas privadas las cuales manejan datos confidenciales en base a pacientes y accionistas de las mismas, en algunos casos pacientes recurrentes que dependiendo el tipo de atención que necesite se llegará a conocer por parte de los administrativos de esta clínica privada, información más a profundidad, enfocándose principalmente a gastos y costos basado a la especialidad que se vaya a tratar. Esto que se menciona puede llegar a ser perjudicial debido a ciertas vulnerabilidades que puede tener la red de Telecomunicaciones del establecimiento privado (U.S. Department of Health & Human Services, 2018).

Es posible recalcar que las clínicas son objetivos atractivos para los ciber atacantes debido a múltiple información de datos médicos sensibles que manejan. Los ataques cibernéticos que pueden sufrir son; ransomware, phishing, malware, entre otros que buscan comprometer la confidencialidad, integridad y disponibilidad de los datos y sistemas de la clínica (Dykstra et al., 2020). Las redes de telecomunicaciones en las clínicas pueden estar sujetas a vulnerabilidades técnicas, humanas, software e infraestructura y de configuración que los ciber atacantes pueden llegar a dañar. Esto podría incluir dispositivos sin parches de seguridad, configuraciones incorrectas, contraseñas débiles o acceso a personas o dispositivos no autorizado a la red. Si la red de telecomunicaciones de la clínica no está adecuadamente protegida, podría haber riesgo de acceso no autorizado a los registros

médicos electrónicos y otros datos confidenciales de los pacientes. Esto puede conducir a violaciones de privacidad y robo de información personal y médica(Rajamaki et al., 2018).

Clínica moderna es una institución médica privada que se encuentra en la ciudad de Ibarra, provincia de Imbabura, la cual presta sus servicios desde 1971. Ahora en la actualidad Nova Clínica Moderna cuenta con un nuevo edificio fundado en Julio de 2005, el cual está compuesto de modernas áreas para hospitalización y con el proyecto de expansión en servicios de imagen, laboratorio y áreas administrativas. Se detalla el área de consulta externa que cuenta con personal especialista altamente calificado con amplia trayectoria y reconocido prestigio, llegando a ser una de las instituciones más reconocidas del norte del país dentro del mercado privado de salud. Hoy en día en cuanto a ciberseguridad se refiere Nova Clínica Moderna no ha tenido registro de ataques o penetraciones a puntos vulnerables a la red debido al constante monitoreo que tiene el área de las TIC's de la empresa.

Nova Clínica Moderna por ser una empresa que ha crecido a lo largo de los años y en base a este crecimiento, y como parte de su enfoque proactivo, busca fortalecer las medidas de ciberseguridad para abordar posibles vulnerabilidades y amenazas en este entorno en constante evolución, como en la actualidad existen intentos de terceros de utilizar el nombre y la imagen de múltiples empresas tanto públicas como privadas, el intento de suplantación de identidad, enviando correos hacia personas externas con el objetivo de engañar y extraer información personal y privada. En la mayoría de los casos las personas reportan este tipo de mal intención a correos y números legítimos de las empresas, llegando a tener una pronta solución por parte del personal de las empresas dando recomendaciones rápidas y sencillas a las personas víctimas de estos fraudes, llegando a evitar conflictos de manera involuntaria tanto a usuarios y empresas.

1.3 Objetivos

1.3.1 Objetivo general

Evaluar el estado de la red de telecomunicaciones de Nova Clínica Moderna mediante una auditoria de seguridad basada en la aplicación del marco de ciberseguridad de la NIST, con el fin de garantizar la confidencialidad e integridad de datos y sistemas críticos de la organización.

1.3.2 Objetivos específicos

- Estudiar la infraestructura de la red de telecomunicaciones de Nova Clínica Moderna y conocer posibles vulnerabilidades que puede llegar a tener en caso de un incidente de ciberseguridad en base a la revisión de fuentes bibliográficas que sustenten el estudio.
- Establecer un conjunto de políticas de alta seguridad en base a una de las funciones principales que conforman el núcleo de la NIST Cybersecurity Framework para ayudar a mejorar la resiliencia fortalecer la línea de defensa ante posibles incidentes en la red
- Verificar los resultados obtenidos una vez se haya desarrollado el conjunto de políticas en la auditoria de la seguridad de la red de telecomunicaciones.

1.4 Alcance

El presente proyecto tiene como enfoque realizar una auditoría a la seguridad de la red de Telecomunicaciones de Nova clínica Moderna, con la finalidad de proponer políticas de ciberseguridad centrada en la función “Proteger” del Framework Core de la NIST, para la implementación de políticas de seguridad como medida de protección de los sistemas de información e infraestructura de la organización. El proyecto busca analizar y mejorar la protección de la red con propuestas de pautas y mejores prácticas proporcionadas por la NIST, con el objetivo de salvaguardar principalmente la confidencialidad, integridad y disponibilidad de datos sensibles de la empresa y mitigar posibles riesgos asociados a la ciberseguridad. Se implementará una investigación aplicada en la que se empleen conocimiento teóricos y conceptuales basados en normativas como referencia a la ya mencionada función “Proteger”, en el campo de la ciberseguridad para abordar y resolver problemas específicos relacionados al tema del proyecto (NIST Cybersecurity Framework, 2021). Se utilizará la metodología OCTAVE la cual se basa en el análisis y gestión de riesgos de la seguridad de una red, basándose en un enfoque práctico y orientado a los objetivos propuestos, centrándose en aspectos de riesgos operativos y prácticas de seguridad que se necesitarán implementar para la red (Alberts et al., 2003). Se revisarán fuentes bibliográficas de estándares y normas que tengan afinidad al marco, para entidades de salud privadas. Se tiene como referencia documentos base para el desarrollo de la investigación, tales como: Publicaciones de la categoría PR (Proteger) de la NIST, documentación oficial de la HIPPA Security Rule. Se presenta una adaptación de las subfases o procesos de la metodología OCTAVE: Investigación aplicada, evaluación de riesgos, diseño de políticas de seguridad, pruebas y validación, propuesta de implementación.

Para la fase de evaluación de riesgos, se realizará una evaluación de riesgos asociados a la red de Telecomunicaciones. Se identificarán posibles amenazas que puedan llegar a ocurrir. Como ataques de hackers, malware o fugas de información. Se analizarán las vulnerabilidades existentes en los sistemas y se evaluará el impacto y la probabilidad de los posibles eventos de seguridad. Principalmente enfocándose en el entorno de la infraestructura de la red, llegando a conocer las condiciones, tiempo de uso, versión, etc. De todos los equipos que trabajan, como también del tipo y modo de operabilidad interna de todos los dispositivos que conforman la red. Cabe recalcar que los datos obtenidos y que con los que se trabajarán dentro de la clínica privada para la elaboración de este proyecto serán netamente confidenciales por lo que se realizará la anonimización de datos, limitaciones y restricciones, para la publicación en el repositorio digital de la universidad.

En la fase de diseño de políticas de seguridad, una vez se ha logrado obtener los datos de la auditoría realizada, para la protección de la red de Telecomunicaciones se utilizará recomendaciones y directrices proporcionadas por la NIST, además de los ya mencionados estándares y normas que tienen relación al marco de ciberseguridad de la NIST, esto implica definir las características técnicas y funcionales de cada control y política, como se involucran dentro de este entorno existente, como se administran y supervisan. Se abordarán los principios más comunes como, por ejemplo: cifrado de datos, control de acceso, gestión de contraseñas, configuración segura de los dispositivos que conforman la red, etc. Estas políticas se adaptan a las necesidades específicas de la clínica y dan soporte para prevenir y mitigar riesgos de seguridad.

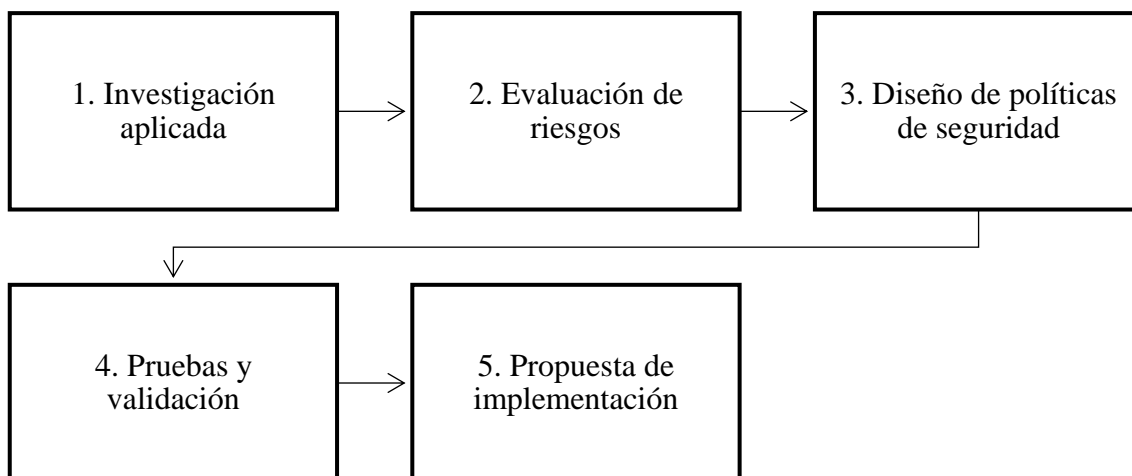
Para la fase de pruebas y validación, se asegurará que las políticas de seguridad desarrolladas y recomendadas para de la red de Telecomunicaciones de Nova Clínica Moderna, contribuyan efectivamente a mejorar la situación actual de la empresa. Estas

políticas serán evaluadas mediante simulaciones en entornos controlados, comprobando su adecuación y eficacia para la protección de la red.

Para la fase de propuesta de implementación se lleva a cabo la recomendación a la empresa de implementar las políticas de seguridad, si de ser el caso se desea aplicar, definidos anteriormente. Se configuran y se despliegan de ser el caso las soluciones tecnológicas que se necesiten como por ejemplo: firewalls, sistemas de detección de intrusos y de prevención de pérdidas de datos. Como también se menciona el establecimiento de las políticas y procedimientos de seguridad que se detallen de manera clara para el personal encargados del área de las Telecomunicaciones de la clínica, como puede ser un extra de capacitaciones sobre buenas prácticas de seguridad.

Figura 1

Subfases de la metodología OCTAVE



1.5 Justificación

El proyecto en cuestión se reduce al simple hecho de la necesidad de realizar un análisis, evaluar y mejorar la seguridad de la red de Telecomunicaciones de Nova Clínica Moderna, la cual nunca ha tenido una auditoría de red ni se han aplicado normas o políticas que regulen un marco de seguridad en su totalidad. La propuesta nace a partir de los avances tecnológicos en el mundo y como influyen hoy en día, principalmente en el enfoque de tecnologías que son vulnerables a ciberataques de una clínica privada que depende cada vez más de la tecnología conectada por medio de las redes de datos locales y a internet, los cuales pueden ser vulnerados desde registros de pacientes y resultados de laboratorios hasta equipos de radiología y ascensores de hospitales. Estas tecnologías dentro de clínicas pueden variar ampliamente: muchos dispositivos médicos son nuevos, pero otros son fabricados por empresas que ya no tienen registros ni actualizaciones en sus sistemas o que se ejecutan con softwares antiguos con enormes vulnerabilidades (Ortega Sáenz, 2020).

Uno de los diecisiete objetivos interrelacionados y ambiciosos que abarcan aspectos sociales, económicos y ambientales de Desarrollo Sostenible (ODS) es el objetivo de industria, innovación e infraestructura la cual fomenta la industrialización sostenible, además de promover la innovación tecnología y el desarrollo de infraestructuras resilientes, también de facilitar el acceso a servicios básicos, fomentar la industrialización inclusiva y la cooperación de alianzas. En el caso de un auditoria de la seguridad de la red de Telecomunicaciones de una clínica privada se hace énfasis a los términos de resiliencia e innovación tecnológica inicialmente en base al análisis de políticas y estrategias gubernamentales. Así demostrar que una resiliencia y una fuerte infraestructura instaurada puede dar soporte a las tecnologías de la red ante un ataque

cibernético y su respuesta o mitigación temprana de los sistemas de seguridad como se propuso en el punto anterior (ONU, 2023).

Se mencionan a los organismos internacionales, siendo la OMS el pilar fundamental el cual detalla lo siguiente: El rápido crecimiento y la expansión de las tecnologías de la información y la comunicación han llevado a un aumento significativo en la dependencia de Internet en muchos aspectos de nuestras vidas, incluida la atención médica. Sin embargo, esta creciente dependencia también ha expuesto a las organizaciones y al personal del área de salud a una serie de desafíos en términos de protección y seguridad en Internet (Organización Mundial de la Salud, 2012). OMS ha estado trabajando en colaboración con los Estados Miembros para abordar estos desafíos y promover la protección y seguridad en Internet en el sector de la salud. Los Estados Miembros de la OMS han reconocido la importancia de garantizar la integridad, confidencialidad y disponibilidad de la información de salud en línea, así como proteger los sistemas y las redes de información contra amenazas cibernéticas. Han implementado una serie de medidas para abordar estos desafíos y mejorar la protección y seguridad en Internet en el sector de la salud. Estas medidas incluyen el desarrollo de marcos normativos y legales para la protección de datos de salud, la implementación de estándares de seguridad cibernética en los sistemas de información de salud, la promoción de la conciencia y la capacitación en ciberseguridad, y la creación de equipos especializados en seguridad cibernética

Un artículo de encuesta publicado por la IEEE menciona que, en una encuesta realizada a 131 audiólogos clínicos, muchos de estos profesionales carecían de experiencia o de fondos para implementar políticas adecuadas de ciberseguridad para prevenir y mitigar amenazas a la seguridad y privacidad. La HIPPA (Ley de portabilidad y responsabilidad de seguros médicos) encontró un despliegue generalizado de seguridad

cibernética que incluye software antivirus e inicios de sesión individuales. Solo el 9,9% de los participantes informaron una violación de datos en 2019, lo cual es significativamente menor que el promedio de las pequeñas empresas y los proveedores de atención médica. Además, solo el 24,4% de los participantes informaron tener un seguro cibernético. Los propietarios de las prácticas médicas tienden a percibir los datos de los pacientes como seguros e improbables de sufrir ataques cibernéticos o violaciones de seguridad. Estos resultados destacan la importancia de la ciberseguridad para proteger la información de salud protegida y mitigar los riesgos. Se enfatiza que los proveedores de atención médica de práctica privada y pequeñas empresas deben tomar medidas prioritarias para adoptar contramedidas que reduzcan los riesgos tanto para los pacientes como para sus propios negocios (Dykstra et al., 2020).

En un artículo publicado por la Drägerwerk AG & Co, empresa que se encarga del desarrollo, producción y comercialización de equipos y sistemas para aplicaciones médicas, de seguridad y buceo, menciona dos casos ocurridos en 2016: El Hollywood Presbyterian Medical Center de Los Ángeles (EE. UU.), un hospital afectado por un ransomware, tuvo que pagar un rescate para liberar sus sistemas informáticos. Según las declaraciones realizadas por el director del hospital, se pagaron 40 bitcoins, con un valor equivalente a unos 15 000 euros en ese momento. Los sistemas afectados volvieron a estar operativos después de una semana de cierre. También el caso cuando los hospitales de Alemania recibieron ataques, se vieron obligados a utilizar métodos del siglo pasado. Los datos de los pacientes se anotaban con papel y bolígrafo, los documentos se enviaban por fax y los pacientes tenían que recoger los resultados de las pruebas en persona, en lugar de recibirlos por correo electrónico (Drägerwerk AG & Co. KGaA, 2017)

La revista científica publicada por el Instituto Tecnológico Superior “Juan Bautista Aguirre” ITSJBA menciona: En el año 2013 Julián Assange anunció al mundo

que la red internet no es privada y que los militares de EEUU pueden observar el tráfico y contenido como alternativa para incidir en la sociedad, además mencionó que Latinoamérica y Centro América no tienen seguridad de privacidad garantizada por el solo hecho de utilizar un canal de comunicaciones de fibra óptica que cruce por USA. El retiro del asilo político al fundador de WikiLeaks fue de mucha controversia para Ecuador, ya que al poco tiempo se reportó un inminente incremento de ataques cibernéticos a entidades públicas y privadas, señalando al Hacker como responsable de tales actos, irrespetando el acuerdo de asilo político. En el año 2019 se anuncia el retiro de asilo político a Julian Assange y desde aquel evento se reportaron 40 millones de ciberataques a sitios web de entidades como el Banco Central, Presidencia, Cancillería, Consejo de la Judicatura, Ministerio del Interior, SRI, IESS, Corte Constitucional del Ecuador, GADS, etc. Ocupando Ecuador el primer lugar de países atacados en el ciberespacio que se ha perpetuado por grupos de Hackers que no estaban de acuerdo con expropiación del asilo político otorgado a Julian Assange.

El caso Assange ha demostrado a las autoridades que el país no estaba preparado para contener los ciberataques, aunque si existe una tenue legislación, las entidades no están debidamente coordinadas siendo esta una debilidad al momento de aplicar políticas de seguridad (Enrique et al., 2020).

En los últimos años, Ecuador ha reconocido la importancia de la ciberseguridad y ha implementado políticas y medidas para hacer frente a las crecientes amenazas cibernéticas. El país se ha comprometido a proteger sus sistemas de información y garantizar la seguridad de la infraestructura digital, incluyendo el ámbito de la salud. Ecuador ha desarrollado políticas de ciberseguridad que abordan varios aspectos clave. Estas políticas se centran en la protección de datos personales y la privacidad, la prevención y detección de incidentes cibernéticos, la colaboración entre entidades

públicas y privadas, la concienciación y capacitación en ciberseguridad, y la promoción de buenas prácticas en el uso de las tecnologías de la información. En el ámbito de la salud, Ecuador ha reconocido la necesidad de proteger la información de salud y garantizar la integridad y confidencialidad de los datos médicos. Se han implementado medidas de seguridad en los sistemas de información de salud, como el uso de cifrado de datos, la autenticación de usuarios y la gestión de accesos (POLÍTICA DE CIBERSEGURIDAD, 2021).

En cuanto a la ley orgánica de protección de datos personales en Ecuador (MINTEL & DINARDAP, 2021). Se mencionan algunos puntos importantes de manera general que tienen relación y abordan relevancia dentro de la auditoría a realizarse:

Se establece los principios de protección de datos relevante en cuanto a la contribución de la investigación para el cumplimiento del cuidado de datos y promover su aplicación en distintas entidades públicas o privadas. Las obligaciones del responsable y encargado de manipular datos de usuarios autorizados en cuanto a fortalecimiento y mejoramiento de la seguridad se refieren. Se menciona además derechos y obligaciones de los custodios de la información de datos personales en cuanto a recomendaciones para las entidades públicas y privadas se refiere con trato más delicado se refiere y en caso de alguna inconsistencia, el reporte a tiempo hacia las autoridades competentes. Y como no menos importante se menciona la seguridad de datos para proteger de acceso no autorizado, pérdidas o filtraciones mediante controles y medidas, al mismo tiempo la notificación de algún incidente a la ARCOTEL y a la autoridad de protección de datos personales ante cualquier incidente que pueda comprometer esta información.

2. CAPÍTULO II. Fundamento Teórico

El ámbito de las telecomunicaciones abarca todas las áreas, desde hardware, software, redes y datos, además es utilizado por las personas para diversas actividades como navegación web, redes sociales y banca. Sin embargo, debido a su importancia, es atracción para delincuentes que pueden cometer delitos cibernéticos, desde piratería informática básica hasta ataques de ransomware, delitos financieros, etc.

2.1. Ciberseguridad en las Organizaciones

Es esencial asegurar la ciberseguridad en diversos sectores, desde pequeñas y medianas empresas hasta las grandes corporaciones. Los marcos según (Dac-Nhuong Le et al., 2018) son el conjunto de mejores prácticas y recomendaciones de ciberseguridad, también conocidos como frameworks, que basados en estándares globales de ciberseguridad, brindan pautas específicas para proteger la seguridad de la información y tener un enfoque adaptable para la protección de las redes de telecomunicaciones, además menciona que la aplicación de políticas y modelos de seguridad son fundamentales en la mayoría de las empresas. (Hasan et al., 2021) menciona que la efectividad de la ciberseguridad se centra en el cumplimiento de un manual de políticas, garantizando la protección de la información de una organización.

Uno de los pilares fundamentales de la ciberseguridad en las organizaciones, según (Mario et al., 2019) se basa en la Confidencialidad, Integridad y Disponibilidad (Triángulo CIA) los cuales abordan los objetivos, estados de información y estrategias para evaluar y proteger sistemas de información y redes de telecomunicaciones. (Qadir & Quadri, 2016) menciona también el enfoque de CIA en puntos estratégicos como: privacidad, identificación, autenticación, autorización y responsabilidad para garantizar la seguridad de una red de telecomunicaciones.

Además, el autor menciona y recomienda que para la creación de políticas en base a la triada CIA, es recomendable adoptar un enfoque de atención prioritaria en áreas específicas como: estudio de la infraestructura de la red, seguridad de la infraestructura de TI, seguridad de aplicaciones de la línea de negocio, educación y cumplimiento de políticas, evaluación y mejora continua.

2.1.1. Amenazas en Ciberseguridad

Una ciber amenaza es la posibilidad de obtener acceso no autorizado, causar daños, interrumpir operaciones, poner en peligro sistemas digitales o redes de telecomunicaciones. Según (Jang-Jaccard & Nepal, 2014) los ciberdelincuentes aprovechan las innovaciones tecnológicas para dirigirse eficientemente a un gran número de víctimas, entre los avances tecnológicos emergentes se destacan amenazas en: redes sociales, la computación en la nube, smartphones y la infraestructura crítica.

2.1.2. Evolución de las Amenazas Cibernéticas

El panorama cibernético ha evolucionado desde el primer ataque informático lanzado en 1971 conocido como “virus Creeper”, hasta las tácticas avanzadas y malware actuales, impulsados por la expansión de la informática y las redes de telecomunicaciones. Haga clic o pulse aquí para escribir texto. (Ervural & Ervural, 2018) describe que los delitos cibernéticos, han avanzado desde ciberataques iniciales hasta tácticas modernas como la cola de paquetes, el escaneo avanzado y la denegación de servicio, anticipando futuros riesgos con el uso de bots, morphing y códigos maliciosos. En la Tabla 1 se desglosa ejemplos de la evolución de ataques cibernéticos por año, tipo de ataque y descripción.

Tabla 1*Evolución de ataques cibernéticos*

Año	Tipo de Ataque	Descripción
1980s	Ataques generales	Ataques menos complejos, menos sofisticados, por ejemplo: Virus de computadora, gusanos de red, ataques de troyanos.
2010s	Ataques Dirigidos	Ataques complejos y relativamente sofisticados, por ejemplo: Exploración avanzada de denegación de servicio (DoS), Packet Spoofing, keylogger.
2020s	Ataques Estratégicos	Ataques sumamente complejos y altamente sofisticados, por ejemplo: Bots, códigos maliciosos, morphing.

Nota: Elaboración propia. Adaptado de (Ervural & Ervural, 2018).

Según (Jang-Jaccard & Nepal, 2014) indica que las redes sociales plantean preocupaciones de seguridad para las empresas, con un 60% temiendo la divulgación de información y un 66% percibiéndolas como amenaza, entre ellas menciona a las tácticas de ingeniería social y cuentas falsas que generan spam y dirigen a usuarios a sitios maliciosos haciéndolos vulnerables. En la Tabla 2 menciona Haga clic o pulse aquí para escribir texto.(Jang-Jaccard & Nepal, 2014) las características y patrones de ataques comunes que se han presentado en los últimos años, por lo que hace énfasis en la necesidad de proteger la privacidad, con propuestas como el cifrado y herramientas de autenticación, buscando garantizar la seguridad de los usuarios.

Tabla 2*Características y patrones de ataques comunes en medios de comunicación social*

Características comunes	Patrones de ataque comunes
Millones de usuarios activos. Se convirtió en parte de la vida diaria de las personas.	Mayor ataque a través del navegador web.
Acceso las 24 horas, los 7 días de la semana desde cualquier lugar y en cualquier momento.	Aumento de los ataques a través de sitios web por medio de ingeniería social.
Los servicios están disponibles a través de una conexión a Internet utilizando navegadores web y aplicaciones.	Aumento de los ataques provenientes de dispositivos que no están basados en PC (por ejemplo, móviles, tabletas, VoIP).
Servicios ofrecidos por muchos dispositivos diferentes, como móviles y tabletas.	Número creciente de ataques más organizados a través de botnet.

Nota: Autoría atribuida a (J. Jang-Jaccard, S. Nepal / Journal of Computer and System Sciences 80 (2014) 973–993)

2.1.3. Infraestructura Crítica

Se entiende por infraestructura crítica a los sistemas, instalaciones y activos vitales para el funcionamiento y estabilidad económica de una organización. (Jang-Jaccard & Nepal, 2014) menciona que un incidente cibernético puede impactar seriamente las operaciones físicas dependientes de una infraestructura crítica. El autor enfatiza amenazas como: terrorismo, sabotaje y desastres naturales, además de la complejidad de la interconexión de redes y la dependencia de sistemas remotos.

2.1.4. Riesgos

Los riesgos de seguridad implican daño a una organización al exponer información al enemigo, (Kosutic, 2021) describe al riesgo como la probabilidad de que una amenaza explote vulnerabilidades y cause consecuencias no deseadas. Se evalúa la probabilidad y el impacto adverso en sistemas de información, afectando la confidencialidad, integridad y disponibilidad, así como las operaciones y activos

2.1.5. *Impacto*

El impacto se refiere a la magnitud del daño causado por la divulgación, modificación, destrucción o pérdida de información de un sistema u organización. La IPS 199 establece tres niveles de impacto potencial que se detalla en la Tabla 3, que pueden ser aplicables y adaptables según el contexto organizacional y el interés particular. (Stine et al., 2008) destaca que para establecer una categoría de seguridad adecuada para un tipo de información simplemente requiere determinar el impacto potencial para cada objetivo de seguridad asociado con el tipo de información específica.

Tabla 3

Niveles de impacto potencial

Impacto Potencial	Definición
Bajo	Efecto adverso limitado en operaciones, activos y personas; puede causar degradación en la capacidad de misión, daño menor a activos, pérdida financiera menor y daño mínimo a individuos.
Moderado	Efecto adverso grave; puede causar degradación significativa en la capacidad de misión, daño significativo a activos, pérdida financiera significativa y daño significativo a individuos sin pérdida de vidas o lesiones graves.
Alto	Efecto adverso severo o catastrófico; puede causar degradación severa o pérdida de capacidad de misión, daño importante a activos, pérdida financiera importante y daño severo o catastrófico a individuos, incluyendo pérdida de vidas o lesiones graves.

Nota: Elaboración propia. Adaptado de (Stine et al., 2008)

2.1.6. Seguridad Operacional

Las operaciones de seguridad buscan comprender y mitigar eventos mediante monitoreo continuo, investigación de incidentes y contramedidas. Identifican indicadores de compromiso, los cuales son señales o pistas que sugieren que un sistema de red puede haber sido comprometido por una actividad maliciosa, gestionan riesgos, escanean vulnerabilidades y realizan análisis forenses. (Daimi & Peoples, 2021) menciona que la seguridad operacional tiene como objetivo primordial la protección de la información no clasificada mediante identificación, control y aplicación de contramedidas basadas en análisis de amenazas, vulnerabilidades y riesgos.

2.1.7. Modelos de Seguridad

Según (Fernandez et al., 2022) los modelos de seguridad guían la protección de datos y sistemas contra amenazas digitales, asegurando la confidencialidad, integridad y disponibilidad de la información. Su comprensión y aplicación son de suma importancia para garantizar la seguridad de los activos de una organización, como ejemplo se tiene: seguridad en la oscuridad, defensa en profundidad, seguridad de perímetro, zero trust, que se detalla más explícitamente a continuación:

a) Seguridad en la oscuridad

El enfoque de seguridad basado en la oscuridad busca mantener en secreto los detalles internos de un sistema para prevenir ataques al limitar el conocimiento de posibles atacantes. (Fernando Maymi & Shon Harris, 2021) recomienda la combinación con otras medidas de seguridad específicos sobre la arquitectura de red.

b) Defensa en profundidad

La estrategia de seguridad por capas aplica medidas de seguridad en todos los niveles de la infraestructura de TI para dificultar ataques y reducir el impacto de violaciones.

(Fernando Maymi & Shon Harris, 2021) menciona que el uso de firewalls para la protección, sistemas de detección de intrusos y cifrado, deben ser implementados desde la periferia de la red hasta dispositivos y aplicaciones, con redundancia para aumentar la resiliencia.

c) Seguridad de perímetro

La estrategia de seguridad perimetral se centra en proteger la frontera de la red con barreras sólidas como firewalls y dispositivos de seguridad. (Fernando Maymi & Shon Harris, 2021) describe como objetivo principal el prevenir el acceso no autorizado y regular el flujo de tráfico, abordando aspectos como control de acceso, sistemas de detección/prevención de intrusiones, VPN, DMZ, y políticas de seguridad con monitoreo.

2.1.8. Ethical Hacking

El hacking ético implica la intrusión autorizada en sistemas para identificar amenazas y vulnerabilidades, con el propósito de mejorar la seguridad y defender contra ataques malintencionados. (Shetty & Shetty, 2019) expone que los hackers éticos utilizan métodos similares a los malintencionados, pero con permisos y estrategias defensivas y ofensivas que se centran en corregir vulnerabilidades descubiertas, debido a que los ataques cibernéticos con el tiempo han llegado a ser más sofisticados y mucho más riesgosos.

2.2. Auditoría de Seguridad

La importancia de una auditoría de seguridad a una red de Telecomunicaciones es crucial ante los riesgos crecientes en un entorno tecnológico cambiante. Las empresas enfrentan amenazas como ciberdelincuencia, violaciones de datos, falta de capacitación del personal, negligencias físicas y posibles desastres naturales en una infraestructura crítica, por lo que recalca la importancia de contar con medidas efectivas ante estas

amenazas. (Stouffer et al., 2015) menciona que una auditoría ayuda a detectar y prevenir violaciones, contribuye al cumplimiento y revela prácticas de alta seguridad por medio de un proceso que evalúa y verifica la protección, eficiencia y confiabilidad de los sistemas de comunicación dentro de una organización.

2.2.1. Tipos de Auditorías de Seguridad.

(Lois et al., 2021) menciona que el objetivo principal dentro de una auditoría es el estudio previo del comportamiento de una red de Telecomunicaciones, descubrir fallos y vulnerabilidades, asegurar el cumplimiento de leyes y políticas empresariales aplicables, mediante la evaluación activa y la documentación del cumplimiento normativo de la información para mantener una infraestructura de comunicación robusta y segura. Dependiendo el enfoque al que se dirija, se abordan algunos ejemplos de tipos de auditoría:

a) Auditoría Interna

(Jadhav, 2023) explica que la auditoría de seguridad de la red interna es una evaluación exhaustiva de la infraestructura interna de una organización para garantizar su seguridad y cumplimiento normativo en las áreas de seguridad del sistema y de la red. En la Tabla 4 se describe el enfoque de la auditoría interna en cuanto a identificar vulnerabilidades y debilidades en dispositivos como: servidores, firewalls y estaciones de trabajo, evaluando la efectividad de los controles de seguridad y las políticas existentes.

b) Auditoría Externa

(Jadhav, 2023) describe que las auditorías externas ofrecen información clave sobre los riesgos de ciberseguridad provenientes de la red del mundo externo para una organización, enfocándose en evaluar y fortalecer los controles de seguridad. Los

auditores externos, con experiencia en diversos sectores, aportan valiosas perspectivas a través de sus evaluaciones y programas de gestión del riesgo empresarial.

c) Auditoría de cumplimiento normativo

El objetivo de esta auditoría es evaluar el cumplimiento de una organización con requisitos legales y normativos en materia de seguridad de red, abarcando leyes de protección de datos, regulaciones internas y estándares internacionales aplicables, menciona (Jadhav, 2023).

d) Auditoría de políticas y procedimientos

La auditoría de políticas y procedimientos revisa y evalúa la implementación, adaptación y actualización de las políticas de seguridad en una organización; como se detalla en la Tabla 4 en el apartado del área de operación de seguridad. Según (Jadhav, 2023) su propósito es aclarar el tratamiento seguro de los elementos de la red de Telecomunicaciones, identificar requisitos para garantizar seguridad y protección, buscando lograr una red estable y segura que satisfaga las necesidades organizativas.

e) Auditoría de controles de acceso

La auditoría de controles de acceso evalúa sistemas y métodos utilizados para controlar el acceso a sistemas y datos organizativos. En la Tabla 4, en el apartado de seguridad de datos, se detallan aspectos como: control de acceso físico, contraseñas, PIN, etc. (Barzilay, 2019) menciona que una auditoría de controles de acceso se evalúa también los tipos de herramientas usadas para la eficiencia de ciberseguridad en la organización, seguridad contra factores humanos y formación para concienciación. .Añade también que su función principal es restringir el uso de recursos solo a usuarios autorizados, definiendo el grado de acceso concedido a cada usuario.

f) Auditoría de gestión de incidentes

La auditoría de gestión de incidentes; según (Barzilay, 2019) evalúa la preparación y respuesta de una organización ante incidentes de seguridad, incluyendo prevención, detección, respuesta y recuperación. Durante este proceso se notifican problemas en la red y se proporcionan recomendaciones de ciberseguridad, fomentando el intercambio de información con el equipo de trabajo con el que se esté colaborando.

La Tabla 4 brinda información proporcionada por estas auditorías sobre seguridad organizativa.

Tabla 4

Información derivada de auditorías de ciberseguridad

Área clave	Enfoque
Seguridad de los datos	Examen de cifrado, control de acceso, seguridad de datos en reposo y transmisiones.
Operación de seguridad	Revisión de los procedimientos, controles y políticas de seguridad.
Seguridad del sistema	Revisión de los procesos de aplicación de parches, endurecimiento, procesos, acceso basado en funciones y gestión de cuentas privilegiadas.
Seguridad de la red	Revisión de los controles de red y seguridad, centro de operaciones de seguridad, infraestructura de telecomunicaciones.
Seguridad física	Revisión del cifrado de discos, datos biométricos, acceso basado en roles, autenticación y otras medidas similares.

Nota: Elaboración propia. Adaptado de (Jadhav, 2023)

2.2.2. Herramientas Técnicas para realizar una Auditoría de Seguridad

La auditoría de seguridad en redes de Telecomunicaciones aborda la protección de activos empresariales mediante herramientas y técnicas específicas. Esto incluye la recopilación de información, el escaneo de puntos débiles, la concientización de riesgos y la investigación forense según (Al-Matari et al., 2018). Haga clic o pulse aquí para escribir texto. La Tabla 5 detalla ejemplos de herramientas que pueden ser utilizadas para evaluar y garantizar las operaciones seguras de la empresa.

Tabla 5

Análisis comparativo de las herramientas automatizadas de auditorías disponibles

Función	Nombre de la Herramienta	Funciones Compatibles	Limitaciones	Sistema Operativo		
				Windows	Linux	Mac
Recopilación de información	NS Lookup	Consulta los servidores DNS.	Requiere formación del personal.	✓	✓	
		Obtiene registros sobre los distintos hosts.				
Escaneado	Nessus	Busca el servidor de correo del sitio web de destino.	Requiere aprender un lenguaje de scripting.	✓	✓	✓
		Explota las vulnerabilidades de la configuración del sistema.				
		Busca vulnerabilidades en los hosts.				

Explotación		Proporciona investigación sobre vulnerabilidades de seguridad.	Sólo requiere un sistema operativo basado en Linux o Windows.		
	Metasploit	Desarrollo de código para atacar la vulnerabilidad.	Capacidades limitadas para la versión gratuita.	✓	✓
Forense			Requiere formación personal.		
	Event log explorer	Una aplicación robusta para examinar interactivamente los registros de sucesos. Fácil acceso a los espacios de trabajo almacenados.	Capacidades limitadas para la versión gratuita.	✓	

Nota: Elaboración propia. Adaptado de (Al-Matari et al., 2018)

2.3. Metodologías de una Auditoría de Seguridad

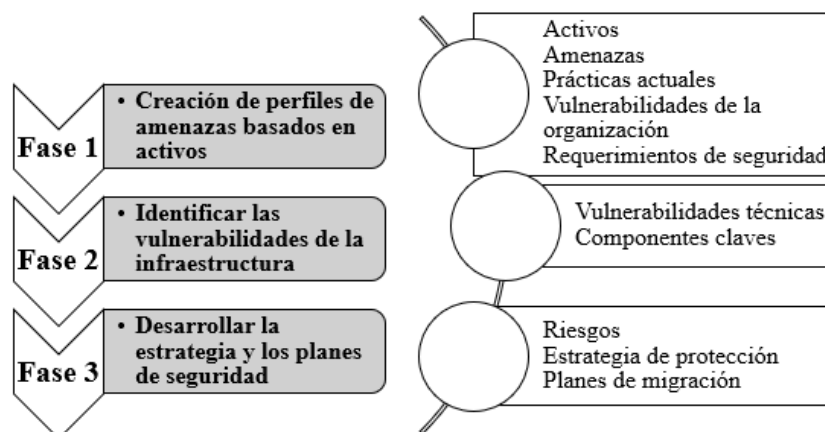
En el ámbito de la seguridad de una organización, una metodología adaptable para una auditoría de redes de Telecomunicaciones proporciona un enfoque sistemático para evaluar la postura de seguridad. (Tomar & Singh, 2021) menciona que este proceso ayuda en la identificación de vulnerabilidades, evaluación de riesgos y recomendaciones para fortalecer la seguridad de la red de la organización.

2.3.1. OCTAVE

OCTAVE mejora la toma de decisiones en la protección de recursos organizativos mediante la evaluación de riesgos basada en la confidencialidad, integridad y disponibilidad. (Pyka & Sobieski, 2012) describe a la metodología con un enfoque sistemático con criterios definidos en tres fases principales y sus procesos tal y como se detallada en la Figura 2. Es esencial para auditorías y se adapta a diversas políticas empresariales, asegurando la protección de la información crítica.

Figura 2

Fases de la metodología OCTAVE



Nota: Elaboración propia. Adaptado de (Pyka & Sobieski, 2012).

2.3.2. Magerit

Magerit; metodología del CSAE (Consejo Superior de Administración Electrónica), según (Tomar & Singh, 2021) guía el análisis de riesgos con fases de determinación de activos, amenazas, medidas de protección, estimación de impacto y evaluación de riesgo. Donde se establecen controles para mitigar, aceptar, eliminar o transferir riesgos; además incluye la recomendación de control en la gestión de seguridad posterior al análisis. A continuación, se enumeran las fases según la metodología Magerit:

1. Identificación de activos, relaciones y valor (Vega et al., 2017, pág. 3).
2. Identificación de amenazas (naturales, industriales, humanas) (Vega et al., 2017, pág. 3).
3. Evaluación de medidas de protección (Vega et al., 2017, pág. 3).
4. Estimación de impacto ante amenazas (Vega et al., 2017, pág. 3).
5. Evaluación de riesgos ponderando impacto y frecuencia (Vega et al., 2017, pág. 3).

6. Establecimiento de controles para mitigar, aceptar, eliminar o transferir riesgos (Vega et al., 2017, pág. 3).

2.3.3. OSSTMMv3 (*Manual de Metodología de Prueba de Seguridad de Código Abierto*)

La Metodología OSSTMMv3 (versión actual del 2010); proporciona una base científica para medir la seguridad mediante pruebas confiables y es usada para la aplicación de auditoría precisa de seguridad operativa, consistente y repetible. (Nabila et al., 2023) señala como objetivo la caracterización precisa de la seguridad operacional y como propósito secundario el brindar lineamientos para auditoría certificada al seguirse correctamente. Estas pautas se rigen para verificar los siguientes requisitos:

1. Definir activos y controles a proteger (Van Den Hout, 2019, pág. 33).
2. Establecer zona de participación (área alrededor de activos) (Van Den Hout, 2019, pág. 33).
3. Identificar el alcance y medibilidad del proceso (Van Den Hout, 2019, pág. 33).
4. Definir interacciones y "vectores" dentro y fuera del alcance (Van Den Hout, 2019, pág. 33).
5. Identificar canales (personal, clientes, físico, lógico, etc.) para pruebas (Van Den Hout, 2019, pág. 33).
6. Determinar el tipo de prueba a realizar (Blind, Double Blink, Gray Box, etc.) (Van Den Hout, 2019, pág. 33).

Cálculo de RAV

(Van Den Hout, 2019) menciona el cálculo de la "Seguridad Real" mediante el Valor de Evaluación de Riesgo (RAV), de acuerdo con la Ec.1, se menciona las variables clave: "Porosidad (OPSEC)" implica visibilidad, acceso y confianza, cruciales para determinar la exposición a riesgos. Los "Controles" como autenticación, resistencia, confidencialidad y privacidad, entre otros, son medidas clave para reforzar la seguridad. Las "Limitaciones", que incluyen vulnerabilidad y debilidad, representan desafíos que pueden afectar la efectividad de estos controles y deben ser cuidadosamente gestionadas para proteger adecuadamente los datos y sistemas. En donde se puede recalcar que cuando $RAV=0$ significa una Seguridad Perfecta, $RAV<0$ significa controles insuficientes y $RAV>0$ significa demasiados controles innecesarios.

$$RAV = \textit{Controles}_{\textit{Actuales}} - \textit{OPSEC} - \textit{limitaciones}$$

Nota: Elaboración propia. Adaptado de Calculadora RAV de OSSTMMv3

(1)

2.3.4. NIST SP 800-115

Esta guía de la NIST adaptable como proceso metodológico, mas no registrada como tal, proporciona una orientación sobre como evaluar controles y medidas de seguridad en sistemas de información. Según (Scarfone et al., 2008) está diseñada para ser utilizada por organizaciones con apoyo de auditores de seguridad internos y externos que desean evaluar la seguridad de los sistemas de información y redes

Los siguientes puntos y componentes claves de esta publicación especial:

- 1. Introducción:** Importancia de pruebas de seguridad (Scarfone et al., 2008, pág. 10-11).

2. **Conceptos:** Planificación, ejecución y post-ejecución (Scarfone et al., 2008, pág. 22-41).
3. **Tipos de evaluaciones:** Vulnerabilidades, pruebas de penetración, control de seguridad (Scarfone et al., 2008, pág. 44-45).
4. **Técnicas de evaluación:** Redes, conexiones inalámbricas, aplicaciones (Scarfone et al., 2008, pág. 62-64).
5. **Selección de la técnica de evaluación adecuada:** Elección según necesidades (Scarfone et al., 2008, pág. 62-64).
6. **Ejecución de la evaluación:** Pasos desde planificación hasta resultados (Scarfone et al., 2008, pág. 62-64).
7. **Informar y comunicar los resultados:** Representación de hallazgos y recomendaciones (Scarfone et al., 2008, pág. 69).
8. **Remediación:** Priorización y corrección de vulnerabilidades (Scarfone et al., 2008, pág. 70-71).
9. **Apéndices:** Incluye plan de prueba, lista de vulnerabilidades, referencias (Scarfone et al., 2008, pág. 74).

2.4. Marco de Ciberseguridad de la NIST.

El Marco de Ciberseguridad de la NIST es un enfoque basado en riesgos compuesto por Core, Tiers y Profiles. El framework core (NIST, 2018) facilita la conexión entre la misión/negocio y la ciberseguridad, siendo integrable con los procesos existentes. Permite expresar requisitos de seguridad, identificar brechas, y considerar la privacidad adaptable en seguridad de redes de Telecomunicaciones. Además, se usa para comparar y mejorar las prácticas de seguridad, fortaleciendo la gestión de riesgos y alineándose con las funciones clave: Identificar, Proteger, Detectar, Responder y Recuperar.

2.4.1. Tiers

La Figura 3 detalla los niveles de implementación del marco (tiers) que indican el enfoque de una organización hacia el riesgo de seguridad de red, con niveles que van desde Parcial hasta Adaptativo. La selección del nivel se basa en las prácticas actuales, el entorno de amenazas, requisitos legales y objetivos organizacionales. La elección busca cumplir con los objetivos, ser factible y reducir el riesgo a niveles aceptables, respaldando decisiones sobre gestión de riesgos y asignación de recursos en redes de Telecomunicaciones (NIST, 2018). A continuación, se describe los niveles (Tier) del framework core de la NIST.

Nivel 1: Parcial - Gestión de riesgos de seguridad ad hoc, conciencia limitada, falta de colaboración externa (NIST, 2018).

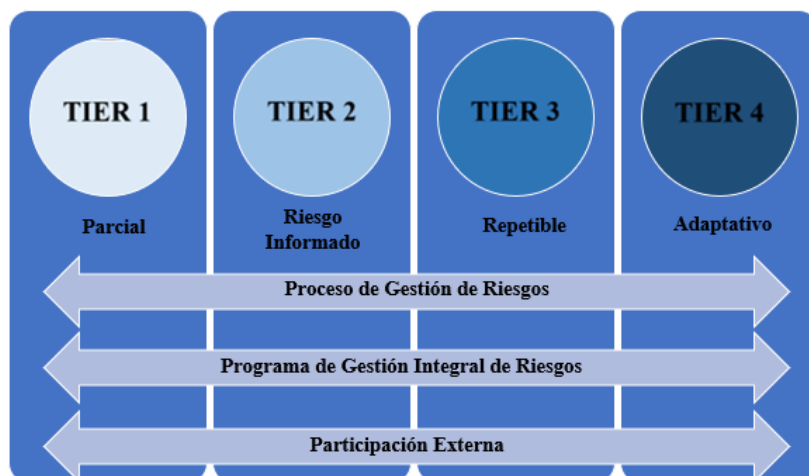
Nivel 2: Riesgo Informado - Prácticas aprobadas, conciencia organizacional, colaboración externa limitada (NIST, 2018).

Nivel 3: Repetible - Prácticas formalizadas, enfoque organizacional, participación externa más completa (NIST, 2018).

Nivel 4: Adaptativo - Adaptación continua, gestión integral, colaboración activa y comprensión avanzada de riesgos (NIST, 2018).

Figura 3

Niveles de implementación del marco



Nota: Autoría atribuida a (NIST, 2018).

2.4.2. Profile

Los perfiles ayudan a las organizaciones a gestionar el riesgo de seguridad, describiendo el estado actual y el deseado. (NIST, 2018) explica detalladamente que los perfiles permiten identificar brechas, desarrollar planes de acción y evaluar recursos necesarios. Además, facilitan la comunicación del riesgo entre organizaciones y la adaptación de funciones según necesidades específicas, dando flexibilidad al enfoque basado en riesgos del marco de seguridad.

2.4.3. Funciones Principales del Marco

El Framework Core ofrece actividades y referencias para lograr resultados clave de seguridad en la red. En la Figura 4, se muestra que no es una lista de verificación, sino un conjunto organizado en funciones (Identificar, Proteger, Detectar, Responder, Recuperar), categorías y subcategorías. Las (NIST, 2018) proporciona referencias informativas de recomendaciones y mejores prácticas basados en estándares comunes en infraestructuras como por ejemplo: ISO/IEC 27001, COBIT, CIS Controls.

Figura 4*Funciones del Framework Core de la NIST*

Identificador único de función	Función	Identificador único de categoría	Categoría
ID	Identificar	ID.AM	Gestión de activos
		ID.BE	Entorno empresarial
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	Proteger	PR.AC	Gestión de identidad y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología protectora
DE	Detectar	DE.AE	Anomalías y eventos
		DE.CM	Vigilancia continua de seguridad
		DE.DP	Procesos de detección
RS	Responder	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
RC	Recuperar	RC.RP	Planificación de recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

Nota: Autoría atribuida a (NIST, 2018)

A continuación, se describe de forma resumida las funciones del marco de ciberseguridad de la NIST:

Identificar: Evaluar la comprensión organizativa actual para gestionar riesgos de seguridad y enfocar esfuerzos en base a una estrategia (NIST, 2011).

Proteger: Implementar salvaguardas de protección para asegurar activos empresariales, incluyendo como ejemplo la Gestión de Identidad y Control de Acceso (Ross et al., 2018).

Detectar: Desarrollar actividades para identificar eventos de amenaza en seguridad, incluyendo como ejemplo posibles Anomalías y Eventos (Dempsey et al., 2011).

Responder: Implementar acciones frente a incidentes, incluyendo como ejemplo la Planificación de respuesta y comunicaciones (Swanson et al., 2010).

Recuperar: Desarrollar actividades para mantener planes de resiliencia y restaurar capacidades afectadas, incluyendo como ejemplo la Planificación de recuperación (Bartock et al., 2016).

2.5. Marco Legal Para Procesos de Auditoría de Seguridad de la Información en Ecuador

El marco legal de la República del Ecuador se sustenta en una serie de leyes y regulaciones que abarcan diversas áreas esenciales para mantener el orden, proteger los derechos individuales y colectivos, regular las actividades sociales y económicas, y promover el desarrollo integral del país.

a) Constitución de la República del Ecuador

La Constitución, como pilar del Estado, establece la organización gubernamental, los derechos y deberes de los ciudadanos. Aborda temas como la justicia, salud, comunicación y trabajo, protege derechos individuales y asegura procesos judiciales justos. Reconoce derechos como la objeción de conciencia, asociación, libertad laboral y la privacidad personal (Asamblea Nacional de la República del Ecuador, 2008).

b) Ley orgánica de Telecomunicaciones

La ley ecuatoriana regula las telecomunicaciones, abarcando el espectro radioeléctrico, servicios y derechos de usuarios y proveedores. Su propósito es fomentar el desarrollo del sector, estimular inversiones y asegurar servicios de calidad (Asamblea Nacional de la República del Ecuador, 2015)

c) Ley orgánica de protección de datos personales (LOPD)

La legislación ecuatoriana regula la protección de datos personales, abordando la recolección, procesamiento y difusión de estos datos, así como los derechos de las personas sobre ellos. Su propósito es salvaguardar la privacidad y derechos fundamentales, fomentar el uso responsable de los datos y establecer un marco protector en Ecuador. (Asamblea Nacional de la República del Ecuador, 2021)

d) Ley Orgánica de Comunicación

La legislación ecuatoriana regula el sector de la comunicación, incluyendo derechos, obligaciones y funcionamiento de los medios, así como la difusión de información. Su propósito es asegurar los derechos de comunicación, promover la comunicación democrática y establecer principios para los servicios comunicacionales en Ecuador (Asamblea Nacional de la República del Ecuador, 2019)

e) Ley de Propiedad Intelectual

La ley establece el marco legal para los derechos de propiedad intelectual, incluyendo derechos de autor, propiedad industrial. Define requisitos, plazos, limitaciones y sanciones, así como procedimientos para la obtención y registro de estos derechos. También considera acuerdos internacionales relevantes para Ecuador, siendo la principal normativa en el país sobre propiedad intelectual (Asamblea Nacional de la República del Ecuador, 2014).

f) Código Orgánico Integral Penal (COIP)

El Código Orgánico Integral Penal (COIP) es la legislación principal de Ecuador para el derecho penal. Se divide en 10 libros que cubren diferentes aspectos, desde disposiciones generales hasta delitos y sistemas procesales. Su objetivo es establecer un

marco integral para la prevención y sanción de delitos, protegiendo los derechos humanos y promoviendo la justicia social (Asamblea Nacional de la República del Ecuador, 2014).

g) Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional

La ley establece reglas y procedimientos para proteger los derechos constitucionales en Ecuador, incluyendo justicia constitucional, garantías jurisdiccionales, y control constitucional. Proporciona marco legal para impugnaciones, hábeas corpus y protección de derechos. Su propósito es asegurar los derechos y la supremacía constitucional en Ecuador (Asamblea Nacional de la República del Ecuador, 2020).

h) Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

La ley establece normas para transacciones electrónicas, firmas, contratos y servicios en línea, buscando validar mensajes electrónicos, promover el comercio en línea y regular las entidades de certificación. En telecomunicaciones, otorga autoridad a reguladores para supervisar la certificación en transacciones seguras (Asamblea Nacional de la República del Ecuador, 2002).

A continuación, se destaca la ley internacional que referencia a la seguridad de la información en el sector de la salud.

HIPPA (Ley de Portabilidad y Responsabilidad del Seguro Médico)

La normativa federal de EE. UU., HIPAA, establece estándares para proteger la información de salud del paciente y prevenir su divulgación sin consentimiento. Según (Moore & Frye, 2019) su objetivo principal es garantizar la privacidad y seguridad de la información médica, facilitando el intercambio electrónico de datos y estableciendo pautas de protección

a) Regla de Privacidad de HIPAA

La Regla de Privacidad de HIPAA establece estándares nacionales americanos para proteger la información de salud, aplicando a planes de salud y proveedores médicos. Requiere confidencialidad, limita divulgaciones sin consentimiento y otorga derechos a las personas sobre su información. Aplica a proveedores de salud y asociados comerciales que manejan información de salud identificable (Office of Civil Rights, 2013).

b) Regla de Seguridad de HIPAA

La Regla de Seguridad de HIPAA establece estándares nacionales americanos para proteger la información de salud electrónica, exigiendo salvaguardias administrativas, físicas y tecnológicas. Se centra en la e-PHI, requiriendo confidencialidad, integridad y detección de amenazas (Office of Civil Rights, 2013).

3. CAPÍTULO III. Análisis de la situación actual de Nova Clínica Moderna

En el siguiente capítulo, se describe de manera concisa la situación actual de la organización a auditar, basándose en el marco de ciberseguridad de la NIST. Se siguen las fases específicas y los procesos de la metodología OCTAVE para detectar posibles amenazas y vulnerabilidades de la organización, con el fin de desarrollar políticas en base a la función proteger del CSF NIST y mejorar la línea de defensa de la estructura de la red de telecomunicaciones de dicha institución. Esto se realizará utilizando los datos proporcionados por el ingeniero líder del área de TIC'S, responsable de la supervisión de la infraestructura de la red de telecomunicaciones, además de visitas in situ a las instalaciones en donde se ubican los dispositivos de comunicación y sistemas de información.

3.1. Método de investigación

Para esta sección, inicialmente se detalla el tipo de investigación a utilizar durante el estudio del análisis de la situación actual de la empresa, dando un enfoque principal a la recopilación de datos por medio de técnicas que faciliten la comprensión del estado vigente y que más se profile al proceso de auditoría de seguridad de la red. Debido a que el presente trabajo se centra en el desarrollo y propuesta de políticas para mejorar la seguridad de la red de la organización, se mencionan a continuación los tipos de investigación más relevantes y efectivos que mejor se adapte a este estudio inicial.

a. Investigación – Acción

Este tipo de investigación tiene un enfoque ideal para la propuesta de políticas de seguridad, ya que permite la adecuación de un ciclo iterativo de planificación, acción, observación y mejora. Siendo de utilidad para asegurar que las políticas propuestas no solo sean teóricamente sólidas, sino también prácticas y efectivas en la operación diaria de la empresa.

b. Investigación descriptiva

Previo al desarrollo de políticas, es importante comprender de manera detallada el estado actual de ciberseguridad en la organización. Esta investigación puede ser de utilidad para documentar las técnicas de configuración actuales, las políticas existentes, y las prácticas de seguridad bajo las que se rige la empresa. Además, proporciona una base sólida para el desarrollo y propuesta de las políticas de seguridad basados en el CSF NIST, asegurando que las nuevas políticas se alineen con las necesidades críticas de la empresa.

c. Investigación mixta

Esta investigación tiene como enfoque adaptable combinar métodos cuantitativos (como la probabilidad de ataques y el impacto potencial) y cualitativos (como la percepción y comprensión de las políticas de seguridad actuales). La investigación mixta proporciona una comprensión holística que puede beneficiar la efectividad del desarrollo de las políticas propuestas asegurando que se aborde tanto la infraestructura crítica de la red como también la concientización del personal.

3.1.1. Estrategias de recolección de datos

Para el desarrollo del trabajo, es crucial seleccionar estrategias o métodos para obtener información adecuada detallada y precisa sobre el estado actual de la seguridad de la red, posibles amenazas y vulnerabilidades, además de los controles existentes. En la Tabla 6 se presentan algunas estrategias para la recolección de datos que pueden ser adaptadas durante el proceso de auditoría de la seguridad de la red en la empresa.

Tabla 6*Estrategias de recolección de datos*

Tipo	Descripción	Propósito
Entrevistas	Desarrollo de entrevistas formales y estructuradas con el personal del área de tecnología de la empresa.	Obtener información específica acerca de la configuración de la red, políticas de seguridad actuales, prácticas operativas.
Cuestionarios y encuestas	Elaboración de cuestionarios dirigidos al líder del área tecnológica de la empresa.	Recopilar datos sobre la conciencia de la seguridad y prácticas diarias de los usuarios de la red.
Observación directa	Observación in situ de prácticas operativas, composición y distribución de equipos y dispositivos que conforman la infraestructura de la red.	Identificar posibles debilidades en las prácticas operativas y conocer las instalaciones por donde se reparten todos los equipos y dispositivos con los que dispone la empresa
Análisis de documentación	Revisión de documentos formales existentes dentro de la empresa que se asemejen o tengan relación a políticas de seguridad o manuales de procedimientos, etc.	Evaluar la alineación de políticas formalizadas con las mejores prácticas y estándares como NIST
Evaluación de vulnerabilidad	Ejecución de pruebas técnicas mediante el uso de herramientas disponibles para la identificación de vulnerabilidades en la red de telecomunicaciones.	Detectar y evaluar posibles debilidades de seguridad en la infraestructura de la red que podrían ser explotadas.

Análisis de Registros	Revisión y análisis de logs y eventos de seguridad de posibles intentos de acceso no autorizado.	Identificar posibles incidentes de seguridad, además de evaluar la efectividad de las medidas actuales de monitoreo.
------------------------------	--	--

3.2. Descripción general de la organización

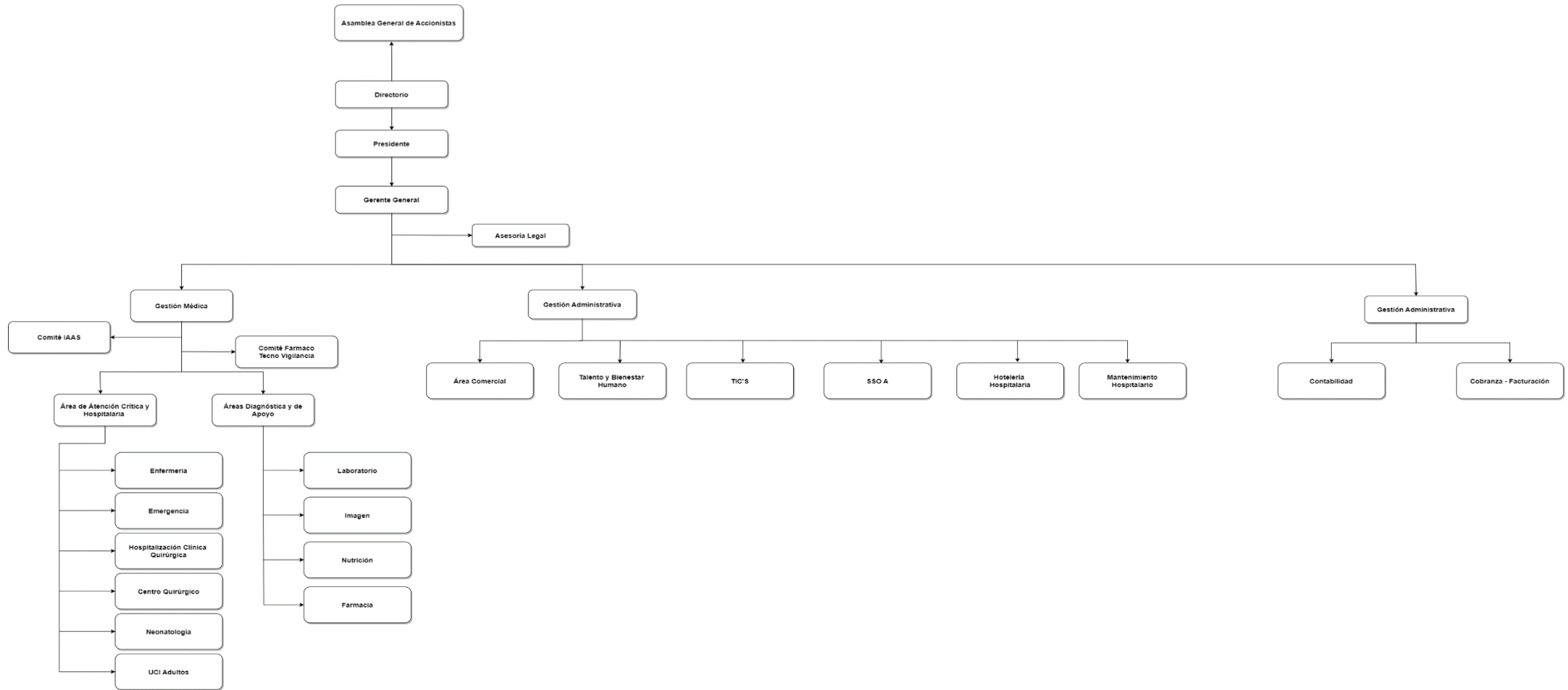
Nova Clínica Moderna es una institución de salud privada ubicada en el norte del país en la ciudad de Ibarra. Cuenta con más de 50 años de experiencia al servicio de la comunidad en el área de la salud con tecnología médica avanzada de última generación. La infraestructura está compuesta por dos torres, liderando el mercado privado de salud con profesionales de prestigio en diferentes especialidades.

3.1.1. Estructura organizacional de la empresa

En cuanto a la estructura organizacional de Nova Clínica Moderna se desglosa jerárquicamente la dirección estratégica y áreas que conforman la organización empresarial de la institución, para el correcto funcionamiento, eficiencia y capacidad para alcanzar sus objetivos estratégicos, en la Figura 5 se evidencia el organigrama institucional.

Figura 5

Organigrama institucional de CLIMODER S.A



Nota: Autoría atribuida a Dirección Estratégica de CLIMODER SA

3.1.2. *Identificación del nivel de conocimiento de stakeholders acerca de la seguridad actual de la red*

La metodología OCTAVE no ofrece instrucciones detalladas sobre medidas y procedimientos diferentes áreas o dominios de una organización durante el proceso de identificación del nivel de conocimiento de seguridad de los stakeholders de la empresa. Por lo tanto, se optó por utilizar y adaptar los dominios de la norma ISO 27001, que facilitan la gestión de la seguridad de la red de Telecomunicaciones de Nova Clínica Moderna en los diversos procesos de la entidad. Estos dominios también permiten al auditor identificar riesgos generales, con el propósito de analizar y desarrollar un plan de acción para mitigarlos; asegurando el adecuado uso, funcionamiento y gestión de la información, en conformidad con los marcos legales pertinentes de la empresa. En la Tabla 7 se muestra una adaptación de dichos dominios; considerando la integridad, disponibilidad y confidencialidad de la información. En el Anexo 1 se evidencia como se recopiló la información mediante una entrevista al líder de área de TIC'S.

Tabla 7

Análisis de dominios ISO 27001 adaptados al proceso de auditoria en Nova Clínica Moderna

Análisis de dominios ISO 27001		
N°	Dominio	Análisis actual
Dominio 1	Liderazgo y compromiso de la dirección	La alta dirección está comprometida con la seguridad de la información en la clínica. Se ha dispuesto la autorización de garantizar la protección adecuada en cuanto ciberseguridad de la red de telecomunicaciones.
Dominio 2	Política de seguridad de la red	Nova clínica moderna, a la fecha, no cuenta con una política de seguridad documentada para la red de telecomunicaciones.
Dominio 3	Roles y responsabilidades de la seguridad de la red	Los roles y responsabilidades específicos del personal del departamento de TIC's incluyen la implementación y

		mantenimiento constante de controles de seguridad en la red, además de la constante comunicación a la alta dirección ante cualquier situación de ciberseguridad que pueda comprometer a la empresa.
Dominio 4	Gestión de activos de la red de Telecomunicaciones	Se tiene identificado los activos críticos de la red y clasificado de manera ad-hoc, mas no se tiene un documento formalizado.
Dominio 5	Control de accesos	Actualmente se controla y gestiona el acceso a los sistemas y datos a través de la red de telecomunicaciones utilizando métodos de autenticación aceptables y autorizaciones adecuadas.
Dominio 6	Seguridad física y del entorno	Actualmente la empresa dispone de una estructurada adecuada para proteger la infraestructura física de la red de telecomunicaciones en los centros de datos y salas de servidores, Además, se controla el acceso físico a los equipos con cerraduras especiales para evitar cualquier acceso no autorizado.
Dominio 7	Seguridad de las operaciones	En Nova Clínica Moderna se mantiene la continuidad operativa de la red de telecomunicaciones por medio procedimientos y controles satisfactorios a cargo del jefe del área de TIC'S
Dominio 8	Relaciones con proveedores	En la actualidad se evalúan y gestionan los riesgos de seguridad asociados con los proveedores de servicios y de equipos de telecomunicaciones de forma ad hoc. Se establecen requisitos de seguridad claros en los contratos con proveedores para garantizar la seguridad de la red.

Nota: Elaboración propia a partir de entrevista realizada a líder de área de TIC'S

3.1.3. Análisis general del Área Tecnológica y de los recursos de telecomunicaciones organizacionales

Durante una de las entrevistas con el líder del área de TIC'S, en el Anexo 2 se evidencia como se llevó a cabo un análisis general del enfoque de supervisión del área tecnológica y de los recursos de telecomunicaciones con los que cuenta Nova Clínica

Moderna. Se discutieron diversos aspectos relacionados a la infraestructura tecnológica del área de dicha empresa como se muestra en la Tabla 8, el rendimiento de los sistemas, así como las necesidades y desafíos presentes de manera general. Indirectamente se llegó a identificar posibles mejoras y soluciones para optimizar el funcionamiento de los recursos informáticos en consonancia con los objetivos organizacionales.

Tabla 8

Análisis del estado actual del área tecnológica y de los recursos de telecomunicaciones organizacionales

Área	Situación Actual
1. Área Tecnológica	El personal del área de TIC'S está formado por un profesional competente y calificado en el campo de la informática y sistemas, lo que les permite llevar a cabo las tareas asignadas de manera efectiva dentro de la empresa.
2. Hardware disponible	<p>El hardware disponible dentro del área cumple con los requisitos necesarios para el correcto funcionamiento de los equipos y dispositivos de las áreas que componen la empresa.</p> <p>La empresa cuenta con UPS individuales por dirección estratégica que salvaguarde los dispositivos en caso de un corte de energía y UPS en áreas críticas de atención médica.</p> <p>El área tecnológica se encarga de la revisión técnica constante en cuanto a equipos y dispositivos como; servidores, switches, AP's, etc. En cuanto a daños en equipos críticos se tiene paquetes de garantía de las empresas proveedoras.</p>
3. Software disponible	<p>El software en ciertos equipos se mantiene actualizados según las necesidades de la empresa y el área. Cuenta con licencias pagadas y autorizadas por sus distribuidores en todos los equipos.</p> <p>En otros casos como servidores, router, switches, AP's, etc. El software se mantiene y se actualiza únicamente dependiendo de la</p>

	necesidad del equipo y en algunos casos se mantiene con el software por defecto.
4. Cableado de la empresa	<p>La empresa cuenta con una topología híbrida haciendo uso de fibra óptica, cables de cobre y cables UTP cat 5,5e,6; revisada y verificada por estándares internacionales.</p> <p>El Tiempo de vida de uso de cableado para conexión entre equipos es verificado y llevado a registro por el jefe de área de TIC's que en caso de tener algún cambio se deberá notificar a los departamentos superiores.</p> <p>La empresa no cuenta con enlaces inalámbricos hacia otras sucursales debido a que es la única matriz en la ciudad.</p>
5. Sistemas de información disponible	<p>Nova Clínica Moderna cuenta con los sistemas de información hospitalaria: HIS-ERP, sistema de laboratorios clínicos LIS y sistemas de gestión de imágenes médicas en entornos radiológicos RIS-PACS.</p> <p>Además, la empresa dispone de una página web, página de Facebook y cuenta en X que sirve de información y consulta para los clientes y personas interesadas acerca de Nova Clínica Moderna, alianzas y servicios que ofrece.</p>

Nota: Elaboración propia a partir de entrevista realizada a líder de área de TIC'S

3.2. Análisis de la infraestructura de Telecomunicaciones

El propósito del siguiente apartado consiste en recopilar toda la información pertinente a la infraestructura de la red de telecomunicaciones de la organización. El objetivo principal fue obtener una comprensión completa del estado actual de la red durante una de las sesiones llevadas a cabo con el líder del área de TIC'S, identificando posibles áreas de mejora para garantizar un rendimiento óptimo y la continuidad operativa de la red.

3.2.1. Topología física y lógica

Topología Física

Para la LAN de Nova Clínica Moderna, es posible evidenciar en la Figura 6, que cuenta con una estructura de una topología de red híbrida que combina la estructura de estrella y cascada, aprovechando las ventajas de ambas configuraciones para crear una red más flexible, escalable y eficiente. Inicialmente, en la topología en estrella los dispositivos están conectados a un switch de core, permitiendo una administración factible y el control de tráfico desde cada punto central. Por otro lado, la topología en cascada añade una dimensión jerárquica de la red, conectando los conmutadores entre sí, por lo que la integración de ambas topologías permite la composición de la topología híbrida.

Dentro del data center de Nova Clínica Moderna se encuentran dos Routers Firewall de la marca Fortinet, de los modelos E80 para tener acceso al servicio de internet y el modelo E50 para la conexión de la troncal de VoIP. Adicionalmente, se encuentran cinco servidores de tipo internos de tipo torre que son de soporte para las operaciones críticas de la red de telecomunicaciones de la empresa y a una troncal analógica de voz gestionada mediante un Gateway GXW410X.

Topología Lógica

En cuanto a la topología lógica de la red se optó por anonimizar la dirección IP con la que trabaja internamente para toda la infraestructura de la red de telecomunicaciones de la empresa, por lo que se utilizó un rango de direcciones de clase B, específicamente la red **172.16.x.x/22**.

Subredes

En base a la información recopilada a partir de una entrevista con el líder del área de TIC's se pudo constatar que la red principal se subdividió en tres subredes de clase B, sin embargo, para la demostración de la topología lógica se va a hacer la adaptación y uso de la división de 3 subredes, 2 de las cuales hacen uso de una máscara /24 y la restante de una máscara /22, cada una con un propósito específico y bien definido que se detalla a continuación.

Subred 1: Red Empresarial Interna (172.16.x.x/24)

Esta subred es de uso exclusivo con una configuración de direcciones IP estáticas, netamente para ciertos activos empresariales críticos de la red, estaciones de trabajo del personal de salud, administrativo y de gestión de Nova Clínica Moderna. Además, para garantizar la seguridad y la confidencialidad de datos e información confidencial de la empresa, esta subred no es visible ni accesible desde las otras subredes.

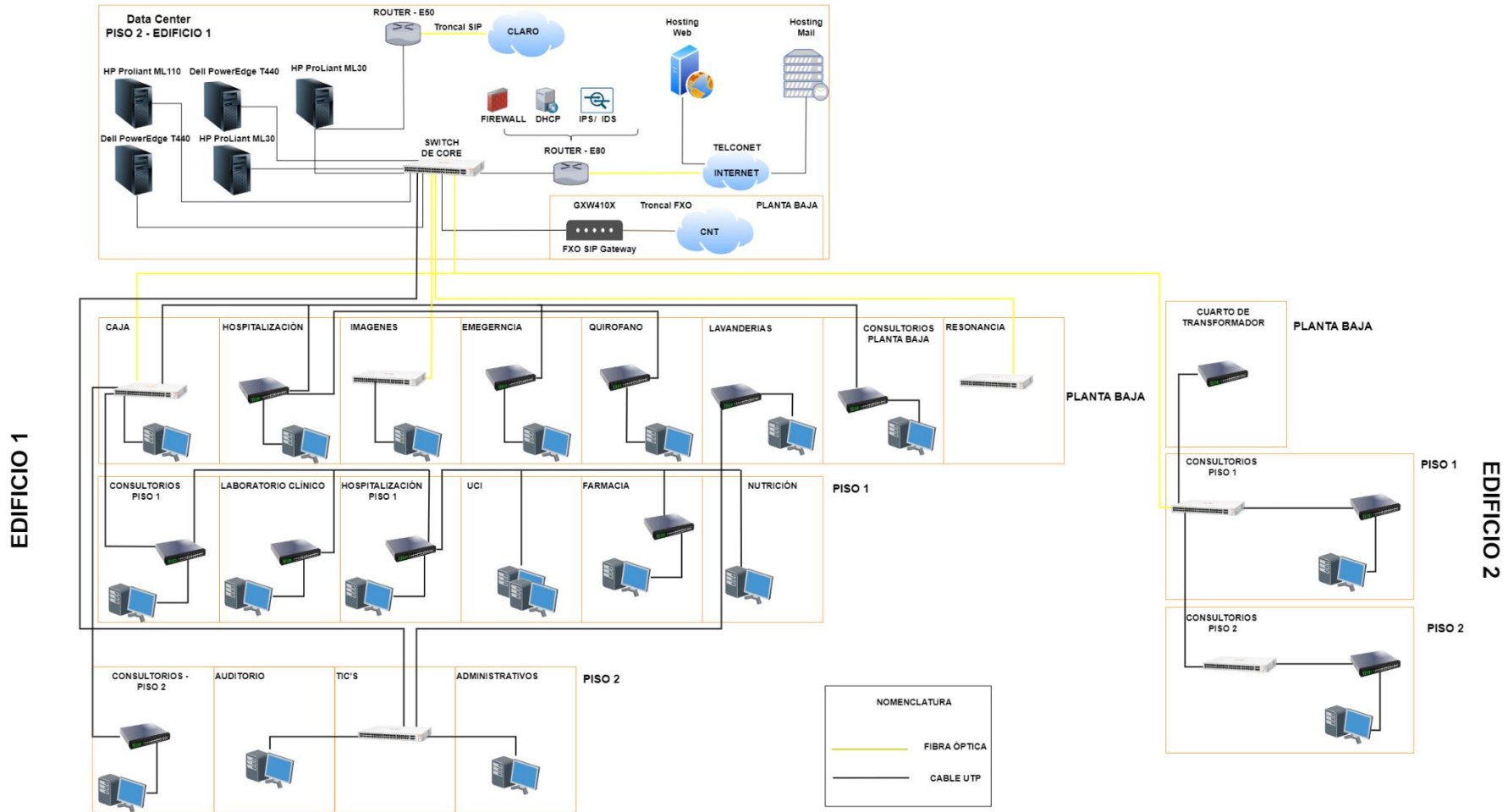
Subred 2: Red DHCP para Personal e Invitados (172.16.x.x/22)

Para esta subred se ha proporcionado una configuración de direcciones IP dinámicas mediante el uso del protocolo DHCP desde el router principal. Esta subred está destinada tanto al personal de la empresa como a los invitados que requieran conectarse temporalmente a la subred con acceso a internet mediante el uso de dispositivos móviles, portátiles, etc.

Subred 3: Red VoIP (172.16.x.x/24)

Para esta subred se ha configurado un rango de direcciones IP estáticas para los dispositivos de telefonía que operan con tecnología VoIP, tanto de la troncal analógica como también de la troncal SIP.

Figura 6
Topología actual de Nova Clínica Moderna



Nota: Autoría propia a partir de entrevista con el líder de área de TIC'S

3.2.2. Descripción de los activos críticos que componen la infraestructura de red

Nova Clínica Moderna cuenta con una variedad de series de equipos y sistemas de información que componen la red actual con la que se desempeñan parte de las tareas de labores diarias de la empresa. Por lo que fue necesario, en una entrevista detallada con el jefe de área de TIC'S y evidenciada en el Anexo 4, recopilar los activos críticos que componen la red de telecomunicaciones y posteriormente con esta información realizar una valoración de manera cuantitativa y cualitativa.

Cableado Horizontal y Vertical

Durante un recorrido a través de las instalaciones de Nova Clínica Moderna en compañía del líder del área de TIC'S se pudo constatar la estructura del cableado horizontal y vertical donde se evidencio el uso principal de cables de par trenzado UTP categoría 5, 5e, 6 y fibra óptica monomodo.

Para el cableado horizontal actualmente la empresa no se rige bajo una norma como tal, pero se evidencia que, cumple un límite de distancia del cableado de no más de 90 m, dejando un margen de otros 10 m del interior de las área de trabajo y del armario de telecomunicaciones de cada piso, además de evidenciar en la Figura 7a faceplates con conectores RJ-45 de voz y datos con cajetines sobrepuestos simples y dobles cerca de las estaciones de trabajo.

En la Figura 7b se evidencia que los cables están guiados y cubiertos por medio del uso de canaletas de plástico en lo referente a cableado horizontal, además de hacer uso de la parte superior al cielo falso de las instalaciones por donde de igual manera se transportan cierta cantidad de cables. Cabe recalcar la observación evidenciada en la Figura 7c, que en algunas áreas de la empresa no se aplican las mencionadas características, por lo que en ciertas zonas de la empresa es complicado saber la

distribución de dicho cableado hacia las estaciones de trabajo, debido al orden incorrecto con el que se encuentran sujetos los cables.

Figura 7

Cableado Horizontal de Nova Clínica Moderna



a)



b)



c)

En lo que respecta al cableado vertical en la Figura 8a y Figura 8b se puede evidenciar al cableado vertical interconectando los conmutadores de cada piso de las 2 torres con los armarios de equipos de telecomunicaciones que se encuentran distribuidos por cada planta. Este cableado cumple con varios de los requisitos en cuanto a distribución y protección se refiere; como el orden y la aseguración de los cables, mediante el uso de canaletas de aluminio, evitando algún daño físico y ayudando a la ventilación adecuada para evitar el sobre calentamiento del cableado.

Figura 8

Cableado vertical de Nova Clínica Moderna



a)



b)

Router Firewall

Nova Clínica Moderna cuenta con dos Fortinet Router Firewall Fortigate; en la Figura 9 se puede evidenciar el modelo FG-80E que actualmente actúa como dispositivo de salida a internet con un plan empresarial, mientras que el modelo FG-50E fue proporcionado como parte del plan de tecnología de voz IP mediante un enlace troncal de telefonía con dicha empresa.

Inicialmente, se recopiló información sobre las características y funcionalidades de los dispositivos en las que incluye; un antivirus integrado, control de aplicaciones, filtro DNS y de correo electrónico, firewall de aplicaciones web (WAF), así como su capacidad de administración de VPN, administración remota, evaluación de la reputación de dominios, y servicios adicionales como FortiExtender y Virus Tracking. Además, se confirmó que estos equipos operan bajo la versión del sistema operativo FortiOS 6.2, garantizando un rendimiento óptimo y protección avanzada.

Figura 9

Router Firewall Fortigate FG-80E



Nota: Autoría atribuida a (Inc, 2021)

Conmutadores

Nova Clínica Moderna cuenta con una línea de switches administrables Aruba Instant On serie 1830 y 1930, en la Tabla 6 se detalla el número de puertos y ciertos estándares con los que trabajan estos equipos de conmutación mencionados. El switch Aruba Instant On 1930, evidenciado en la Figura 10, ocupa un lugar indispensable en la infraestructura de red empresarial actuando como el switch de core, capaz de transportar el tráfico proveniente de las rutas estáticas de los enrutadores, hacia los switches de acceso y a la granja de servidores internos de la empresa que están conectados directamente a este conmutador.

Figura 10

Switch core Aruba Instant On 1930



Nota: Autoría atribuida a (Hewlett Packard Enterprise Development LP, 2022)

En cuanto a los switches de acceso; se cuenta con la serie de conmutadores Aruba Instant 1830 como conmutadores de capa 2 con capacidad para manejar un gran número de puertos y opciones de Power over Ethernet (PoE), facilitando la integración de dispositivos que requieren alimentación eléctrica a través de cable de red. Nova Clínica Moderna dispone además de conmutadores administrables y no administrables de las series; DLink, TP Link y Linksys. En la Figura 11 se evidencia uno de los modelos de conmutador de la marca TP Link con los que trabaja la empresa, y en la Tabla 9 se detalla la serie del modelo, el número de puertos y estándares con los que trabajan estos equipos, utilizados únicamente como switches de acceso ya que facilitan la transferencia de datos entre múltiples dispositivos de las estaciones de trabajo conectados a la red local.

Figura 11

Switchs capa de acceso de Nova Clínica Moderna



Nota: Autoría atribuida a (TP-Link Ecuador)

Tabla 9

Características de conmutadores de Nova Clínica Moderna

Marca / Modelo	Nro de Puertos	Estándares
Aruba Instant On 1930 (Administrable)	48 puertos	IEEE 802.1X IEEE 802.1p IEEE 802.1Q IEEE 802.3x IEEE 802.1D Otros
Aruba Instant On 1830 (Administrable)	24 puertos	IEEE 802.3u IEEE 802.3af/at IEEE 802.3x IEEE 802.3ab

		Otros
TP-Link TL-SF1024D	24 puertos	IEEE 802.3i, IEEE 802.3u IEEE 802.3x
(No administrable)		
D-Link DGS-1210-28	24 puertos	IEEE 802.3 IEEE 802.3u IEEE 802.3ab IEEE 802.3z IEEE 802.3az IEEE 802.3x IEEE 802.3af/at
(Administrable)		
Linksys LGS328PC	24 puertos	IEEE 802.1q IEEE 802.1x IEEE 802.1p
(Administrable)		

Nota: Elaboración propia a partir de entrevista con líder de área de TIC'S

Servidores internos de Nova Clínica Moderna

Nova Clínica Moderna cuenta con alrededor de cinco servidores físicos internos dentro de sus instalaciones ubicados en un Data Center para satisfacer las necesidades operativas de las distintas áreas que conforman la estructura organizacional, en la Tabla 10 se detalla más específicamente las características de los servidores y los servicios montados. Estos servidores de torre desempeñan un papel crucial al proporcionar los recursos tecnológicos necesarios para ejecutar una variedad de tareas, desde el almacenamiento y procesamiento de datos hasta la gestión de aplicaciones y servicios críticos. La distribución dentro de la empresa actualmente garantiza un acceso eficiente y seguro a los recursos informáticos, permitiendo a cada área cumplir con sus labores diarias de manera óptima y sin interrupciones.

Tabla 10*Características de servidores internos de Nova Clínica Moderna*

Servidor	Características	Servicios
HP Proliant ML110 9na Generación	<ul style="list-style-type: none"> - Procesador Intel E52603 V4 de 14 núcleos. - 2 fuentes de alimentación redundantes. - Velocidad de 3.8 GHz y 22 MB de caché. - Memoria de 16 GB de RAM DDR4 ECC. - Unidad de disco duro-SATA/SAS de 3.5 pulgadas de 1 TB de almacenamiento - SO Windows server 2012 R2 	<ul style="list-style-type: none"> - Servidor de archivos SMB - Servicio de consola de antivirus - Sistema contable - Controlador de AP's (Puntos de acceso inalámbricos)
Dell PowerEdge T440	<ul style="list-style-type: none"> - Procesador Intel Xeon Silver 4208 de 28 núcleos - 2 fuentes de alimentación redundantes cada uno - 64 Gb de memoria RAM DDR4 ECC - 2 unidades de disco duro de 2.5 pulgadas de almacenamiento SATA y 2 discos de estado sólido SSD SATA 	<ul style="list-style-type: none"> - Sistema Hospitalario - Base de datos MySQL

Dell PowerEdge T440	<ul style="list-style-type: none"> - Procesador Intel Xeon Silver 4208 de 28 núcleos - 2 fuentes de alimentación redundantes cada uno - 64 Gb de memoria RAM DDR4 ECC - 2 unidades de disco duro de 2.5 pulgadas de almacenamiento SATA y 2 discos de estado sólido SSD SATA 	<ul style="list-style-type: none"> - Sistema de imágenes RX
HP ProLiant ML30 de 9na Generación	<ul style="list-style-type: none"> - Procesador Intel Xeon E3-1220 V5 de 8 núcleos. - Velocidad de 3.5 GHz y 8 MB de caché. - 4 Gb de memoria RAM DDR4 ECC - Un disco SATA de 1 TB de almacenamiento - SO CentOS 8 	<ul style="list-style-type: none"> - Servidor de VoIP Elastix 4.0
HP ProLiant ML30 de 10ma Generación	<ul style="list-style-type: none"> - Procesador Intel Xion E2124 de 6 núcleos - Velocidad de 3.3 GHz y 8 MB de caché. - 16 Gb de memoria RAM DDR4 ECC - 1 TB de disco duro-SATA - SO Windows Server 2019 	<ul style="list-style-type: none"> - Sistema de laboratorio clínico - Base de datos Sybase - Base de datos MySQL

Nota: Elaboración propia a partir de entrevista a líder del área de TIC'S

Troncal SIP

Nova Clínica Moderna actualmente mantiene un contrato de voz empresarial que utiliza el protocolo de señalización SIP (Session Initiation Protocol) para establecer, gestionar y finalizar sesiones de comunicación multimedia (voz, video, mensajes) a través de conexión a internet donde no tiene límite de un número fijo de canales, haciendo dependiente únicamente de la capacidad del ancho de banda disponible en la red IP.

Cuenta con la implementación del servicio PBX Asterisk en un hardware dedicado siendo en este caso en un servidor interno de la empresa donde se alojarán las extensiones internas para los teléfonos IP de las estaciones de trabajo de las diferentes áreas. Cabe recalcar que el tráfico que se genere desde las terminales de VoIP se enviará hacia el Router Firewall Fortigate FG-50E que proporcionó de igual manera la empresa proveedora del servicio.

Troncal Analógica (FXO SIP Gateway)

Nova Clínica Moderna cuenta además con un contrato de telefonía fija empresarial de una troncal que utiliza líneas tradicionales, que comienza desde el punto de demarcación NID (Network Interface Device), hasta la conexión interna con el uso de cables telefónicos con conectores RJ11 hacia un Gateway VoIP de la línea GXW4108, donde se configura el registro de teléfonos IP a utilizar por medio del protocolo SIP, además de configurar las rutas de las llamadas entrantes y salientes en este Gateway. Cuenta con 4 puertos FXO, de los cuales se hace uso únicamente de 2 puertos a los que se conectan los cables telefónicos provenientes del NID, que posteriormente convertirán las señales de las líneas analógicas a señales de VoIP que utilizarán conexión hacia el switch de core de la empresa mediante el uso de cables de par trenzado UTP con

conectores RJ45 para poder conectar únicamente a los teléfonos que hacen uso de esta línea telefónica.

Infraestructura Wireless

En cuanto a la conectividad inalámbrica con la que cuenta Nova Clínica Moderna se mencionan los Wireless AP; Ubiquiti UniFi UAP-AC-LR, UAP-AC-PRO, UAP-nano HD, ilustrados en la Figura 12, repartidos equitativamente por las 3 plantas que dispone cada torre de la empresa. Estos puntos de acceso inalámbricos abarcan el segmento de la subred “invitados” la cual asigna direcciones IP por medio de DHCP y únicamente tiene acceso a internet, además están monitoreados por el software de gestión centralizada UniFi Network Controller montado en uno de los servidores de la empresa. Entre las características más importantes se destaca:

- Configuración sencilla e intuitiva de dispositivos en la red
- Gestión de usuarios y autenticación de dispositivos
- Monitorización y Seguridad

Figura 12

Puntos de acceso inalámbricos de la serie Ubiquiti UniFi



Nota: Autoría atribuida a (UniFi AC Datasheet)

Se menciona, además, dentro de la infraestructura existen routers inalámbricos de la marca TP-Link, modelo TL-WR840N y TL-WR940N, este último ilustrado como ejemplo en la Figura 13. Estos routers inalámbricos se encuentran únicamente en los consultorios de la clínica y tienen acceso privilegiado a limitado personal de la empresa, debido a que este segmento de la red tiene interconexión con los sistemas HIS-ERP, RIS-PACS, LIS, entre otros. Como dato curioso, estos equipos son parte del segmento de la subred “Corporativo”, por lo que la asignación de direcciones IP a estos routers inalámbricos se los realiza de manera manual. Además el SSID de esta subred no está visible para escaneo en dispositivos inalámbricos.

Figura 13

Modelo de router inalámbrico de los consultorios de Nova Clínica Moderna



Nota: Autoría atribuida a (TP-Link Ecuador)

Estaciones de trabajo

Actualmente en Nova Clínica Moderna se manejan alrededor de 46 computadoras de escritorio y laptops repartidas en los departamentos de la empresa respectivamente, además de contar con 47 teléfonos IP para cada departamento. El sistema operativo que predomina en los computadores es Microsoft Windows con versiones y distribuciones que van desde 8.1, 10 y 11; contando con licencia activa y validada respectivamente, además de contar con software de antivirus con licencia premium ESET para cada computador.

En gran parte el personal de la empresa hace uso de herramientas de oficina como son Microsoft Office 2016, Adobe Illustrator, Adobe Photoshop, DaVinci Resolve los cuales también cuentan con licencia activa y válida a la fecha, y dependiendo los departamentos en los que esté trabajando el personal, existen programas o sistemas de los cuales se hacen uso como: HIS-ERP, RIS-PACS y LIS.

3.2.3. *Hardware distribuido por áreas en Nova Clínica Moderna*

El hardware disponible en las distintas áreas de la empresa proporcionó una visión completa de los recursos tecnológicos que respaldan las operaciones diarias de la clínica, abarcando dispositivos de red hasta estaciones de trabajo y dispositivos periféricos. La recopilación de la información se puede evidenciar en el Anexo 5 y en la Tabla 11 se presenta la distribución del hardware disponible en las áreas de toda la Nova Clínica Moderna.

Tabla 11

Ubicación de hardware por áreas de Nova Clínica Moderna

Área	Área de atención crítica y hospitalaria	Diagnóstico y apoyo	Comercial	Talento y bienestar humano	TIC' S	SSO A	Mantenimiento Hospitalario	Contabilidad	Cobranza y facturación	TOTAL
Hardware										
Servidores	0	0	0	0	5	0	0	0	0	5
Routers	0	0	0	0	2	0	0	0	0	2
Conmutadores Administrables	0	2	0	0	1	0	0	0	1	4
Conmutadores No Administrables	11	0	0	0	1	0	0	0	3	15
Gateway VoIP	0	0	0	0	1	0	0	0	0	1
Computadores de Escritorio y Portátiles	24	14	10	1	2	2	1	4	6	46

Puntos de acceso inalámbrico	8	2	3	0	0	0	1	0	2	16
Routers AP consultorios médicos	0	0	0	0	0	0	0	0	0	30
Impresoras	5	6	3	0	1	0	0	1	2	18
Discos Externos	0	1	0	0	1	0	0	0	0	2
Teléfonos IP	23	8	4	1	1	1	0	4	5	47
Cámaras de videovigilancia análogas	17	8	1	0	0	0	0	0	5	32

Nota: Elaboración propia a partir de entrevista con el líder de área de TIC'S

3.2.4. Software y sistemas de información disponible en Nova Clínica Moderna

Nova Clínica Moderna dispone de una infraestructura tecnológica sostenible en el ámbito de software. Entre los componentes clave se mencionan a los Sistemas de Información Hospitalaria (HIS), fundamentales para la integración y gestión exhaustiva de datos clínicos, administrativos y operativos. Estos sistemas están diseñados con una arquitectura técnica sólida que abarca múltiples funcionalidades, además la empresa emplea Sistemas de Planificación de Recursos Empresariales (ERP) que facilitan la gestión de recursos financieros, humanos y materiales. Por otro lado, en el ámbito de laboratorio y diagnóstico por imágenes, se utilizan los Sistemas de Información de Laboratorio (LIS) y los Sistemas de Comunicación y Archivo de Imágenes (PACS), respectivamente, proporcionando soluciones especializadas. Así mismo, los Sistemas de Información de Radiología (RIS); gestionan y administran los procesos de radiología, desde la programación de exámenes hasta la elaboración de informes. Estos sistemas, caracterizados por su capacidad de integración y su enfoque técnico, son esenciales para mejorar la eficiencia operativa, la precisión en el diagnóstico y la calidad de la atención médica en entornos clínicos avanzados.

En la Tabla 12 se caracteriza de manera un poco más detallada al software disponible en Nova Clínica Moderna, donde se muestra la integración de los diferentes sistemas de información mencionado y el desarrollador del software, entre otros aspectos, que son fundamentales para el funcionamiento eficiente y la prestación de servicios de calidad en el ámbito de la atención médica.

Además de los sistemas ya mencionados anteriormente, la empresa emplea otros tipos de software relacionados con el diseño y la ingeniería, los cuales se presentan en la siguiente tabla. Aunque estos programas pueden tener propósitos diferentes, también forman parte de la infraestructura tecnológica de la empresa y contribuyen al desarrollo de sus operaciones diarias.

Tabla 12

Software distribuido por áreas de Nova Clínica Moderna

Software	Tipo	Ubicación / Equipo	Estado de licencia
Sistema HIS-ERP	Sistema Hospitalario	Dell PowerEdge T440	Activo
Sistema RIS-PACS	Sistema de Imágenes RX	Dell PowerEdge T440	Activo
Sistema LIS	Sistema de Laboratorio	HP ProLiant ML30 de 10ma Generación	Activo
Fortiview (FortiOS 6.2)	Gestión de router firewall	Fortinet Fortigate FG-80E	Activo
Aruba Instant On Switch Management	Gestión de red	Aruba Instant On 1930, 1830.	Activo
D-Link Network Assistant	Gestión de red	D-Link DGS-1210-28	Activo
Linksys Smart Switches	Gestión de red	Linksys LGS328PC	Activo
Microsoft Windows	Servidor de archivos SMB	HP Proliant ML110 9na Generación	Activo

ESET Protect	Servicio de consola de antivirus centralizada	HP Proliant ML110 9na Generación	Activo
UniFi Network Controller	Controlador de Wireless AP's	HP Proliant ML110 9na Generación	Activo
Elastix 4.0	Servicio de VoIP PBX	HP ProLiant ML30 de 9na Generación	Activo
Windows 8.1 Windows 10 Windows 11	Sistemas Operativos	Estaciones de Trabajo	Activo
Office 2016	Suite de productividad	Estaciones de Trabajo	Activo
Autocad SolidWorks	Diseño y modelado 3D	Estaciones de Trabajo	Activo
Adobe Illustrator Adobe Photoshop DaVinci Resolve	Diseño gráfico y edición de videos e imágenes	Estaciones de Trabajo	Activo

Nota: Elaboración propia a partir de entrevista con el líder de área de TIC'S

3.3. Desarrollo de perfil de seguridad actual de los activos críticos de la red de Telecomunicaciones

Durante el proceso de auditoría de seguridad a la red de la empresa, es crucial realizar un perfil detallando las amenazas que pueden llegar a enfrentar los activos críticos, pues facilitará mejor la comprensión de los posibles riesgos a los que se está expuesto con el fin de desarrollar estrategias de control y mitigación a futuro, sí está en las posibilidades de la clínica el poder implementarlos. Para cumplir el objetivo de este apartado, se basará en recomendaciones y evaluaciones que brinda el marco de ciberseguridad de la NIST englobando y adaptando al caso la metodología OCTAVE, para identificar, valorar y evaluar los activos críticos; sus posibles riesgos e impactos que, en el peor de los casos, pueda llegar a tener la red de telecomunicaciones.

3.3.1. Aplicación de evaluación de seguridad actual basada en el marco de ciberseguridad de la NIST

Para la aplicación de la matriz de evaluación del marco de ciberseguridad de la NIST fue necesario conocer el nivel actual de seguridad en el que se encuentra la empresa y el nivel objetivo deseado como tentativa, dependiendo de los recursos con los que se cuente, de esta manera perfilar cada función del marco (identificar, proteger, detectar, responder y recuperar) adaptando las categorías y subcategorías del marco los más asimilable a la situación actual de la empresa. Esta matriz cuenta explícitamente con un apartado de evaluación del estado actual, estado objetivo en cuanto a logro y nivel cualitativo y cuantitativo medible de las ya mencionadas categorías y subcategorías. Además de presentar la prioridad de llegar a ese objetivo con una brecha que se valora de la misma manera.

Para este punto, junto al líder del área de TIC'S, se seleccionaron las categorías y las subcategorías del NIST CSF según la información y análisis recopilado que más se apeguen al proceso de auditoría de la red de Telecomunicaciones de la clínica. A continuación, se desglosa de manera más detallada una serie de actividades realizadas en el proceso, a modo de encuesta, para cada función del marco de ciberseguridad que la empresa está cumpliendo a la fecha de realizar este trabajo en lo que respecta la infraestructura y los activos críticos identificados previamente.

A. Función Identificar

Para esta función, se hizo uso de 3 de las 6 categorías, tal y como se evidencia en la Figura 14. Para el inicio de la evaluación, se adoptó la categoría de gestión de activos, la cual lleva a cabo la tarea de identificar y administrar de manera coherente; datos, personal, dispositivos, sistemas e instalaciones en función de su importancia para los objetivos organizativos. En cuanto a la categoría de evaluación de riesgos, se busca comprender y

documentar vulnerabilidades, amenazas e impactos relevantes de los que ya ha sido participe la empresa o posiblemente pueda llegar a enfrentar. Finalmente, la estrategia de gestión de riesgos de ciberseguridad establece prioridades a modo de recomendación referentes al grado de tolerancia que actualmente pueda soportar la empresa en relación con la operatividad de la red.

Figura 14

Categorías y subcategorías de la función Identificar

Función	Categoría	Subcategoría
IDENTIFICAR (ID)	Evaluación de riesgos (ID.RA)	ID.RA-1: Se identifican y se documentan las vulnerabilidades de los activos.
		ID.RA-2: La inteligencia de amenazas cibernéticas se recibe de foros y fuentes de intercambio de información.
		ID.RA-3: Se identifican y se documentan las amenazas, tanto internas como externas.
		ID.RA-4: Se identifican los impactos y las probabilidades del negocio.
		ID.RA-5: Se utilizan las amenazas, las vulnerabilidades, las probabilidades y los impactos para determinar el riesgo.
		ID.RA-6: Se identifican y priorizan las respuestas al riesgo.
Función	Categoría	Subcategoría
IDENTIFICAR (ID)	Gestión de activos (ID.AM)	ID.AM-1: Los dispositivos y sistemas físicos dentro de la organización están inventariados.
		ID.AM-2: Las plataformas de software y las aplicaciones dentro de la organización están inventariadas.
		ID.AM-3: La comunicación organizacional y los flujos de datos están mapeados.
		ID.AM-4: Los sistemas de información externos están catalogados.
		ID.AM-5: Los recursos (por ejemplo, hardware, dispositivos, datos, tiempo, personal y software) se priorizan en función de su clasificación, criticidad y valor comercial.
		ID.AM-6: Los roles y las responsabilidades de la seguridad cibernética para toda la fuerza de trabajo y terceros interesados (por ejemplo, proveedores, clientes, socios) están establecidas.
Función	Categoría	Subcategoría
IDENTIFICAR (ID)	Estrategia de gestión de riesgos (ID.RM)	ID.RM-1: Los actores de la organización establecen, gestionan y acuerdan los procesos de gestión de riesgos.
		ID.RM-2: La tolerancia al riesgo organizacional se determina y se expresa claramente.
		ID.RM-3: La determinación de la tolerancia del riesgo de la organización se basa en parte en su rol en la infraestructura crítica y el análisis del riesgo específico del sector.

Nota: Elaboración Propia. Adaptado de (CSF NIST, 2018)

B. Función Proteger

La evaluación del objetivo del presente trabajo referente a la función proteger, se adoptó las 6 categorías disponibles para esta sección, en la Figura 15 se evidencia el contenido a evaluar. Para la categoría de gestión de identidad, autenticación y control de acceso; el objetivo se centra en limitar el acceso a los activos autorizados y administrar identidades y credenciales que actualmente maneje la empresa.

La categoría de concienciación y capacitación garantiza que el personal comprenda y cumpla con los requisitos de ciberseguridad vigentes y futuros dentro del entorno de las telecomunicaciones. En consecuencia, la categoría de seguridad de los datos implica proteger la confidencialidad, integridad y disponibilidad de la información de la organización.

Para la categoría de procesos y procedimientos de protección de la información, se evalúa la implementación, el mantenimiento y el uso de políticas de seguridad actuales dentro de la organización.

Finalmente, en la categoría de tecnología de protección, se gestiona soluciones técnicas para garantizar la seguridad y capacidad de recuperación de los sistemas y activos ante un posible incidente de ciberseguridad.

Figura 15

Categorías y subcategorías de la función Proteger

Función	Categoría	Subcategoría
PROTEGER (PR)	Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-1: Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.
		PR.AC-2: Se gestiona y se protege el acceso físico a los activos.
		PR.AC-3: Se gestiona el acceso remoto.
		PR.AC-4: Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.
		PR.AC-5: Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red).
		PR.AC-6: Las identidades son verificadas y vinculadas a credenciales y firmadas en las interacciones.
		PR.AC-7: Se autentican los usuarios, dispositivos y otros activos (por ejemplo, autenticación de un solo factor o múltiples factores) acorde al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las organizaciones).
	Concienciación y capacitación (PR.AT)	PR.AT-1: Todos los usuarios están informados y capacitados.
		PR.AT-2: Los usuarios privilegiados comprenden sus roles y responsabilidades.
		PR.AT-3: Los terceros interesados (por ejemplo, proveedores, clientes, socios) comprenden sus roles y responsabilidades.
		PR.AT-4: Los ejecutivos superiores comprenden sus roles y responsabilidades.
		PR.AT-5: El personal de seguridad física y cibernética comprende sus roles y responsabilidades.

PROTEGER (PR)	Seguridad de los datos (PR.DS)	PR.DS-1: Los datos en reposo están protegidos.
		PR.DS-2: Los datos en tránsito están protegidos.
		PR.DS-3: Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.
		PR.DS-4: Se mantiene una capacidad adecuada para asegurar la disponibilidad.
		PR.DS-5: Se implementan protecciones contra las filtraciones de datos.
		PR.DS-6: Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.
		PR.DS-7: Los entornos de desarrollo y prueba(s) están separados del entorno de producción.
		PR.DS-8: Se utilizan mecanismos de comprobación de la integridad para verificar la integridad del hardware.
PROTEGER (PR)	Procesos y procedimientos de protección de la información (PR. IP)	PR. IP-1: Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).
		PR. IP-2: Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas.
		PR. IP-3: Se encuentran establecidos procesos de control de cambio de la configuración.
		PR. IP-4: Se realizan, se mantienen y se prueban copias de seguridad de la información.
		PR. IP-5: Se cumplen las regulaciones y la política con respecto al entorno operativo físico para los activos organizativos.
		PR. IP-6: Los datos son eliminados de acuerdo con las políticas.
		PR. IP-7: Se mejoran los procesos de protección.
		PR. IP-8: Se comparte la efectividad de las tecnologías de protección.
		PR. IP-9: Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de Incidentes y Recuperación de Desastres).
		PR. IP-10: Se prueban los planes de respuesta y recuperación.
		PR. IP-11: La seguridad cibernética se encuentra incluida en las prácticas de recursos humanos (por ejemplo, desaprovisionamiento, selección del personal).
		PR. IP-12: Se desarrolla y se implementa un plan de gestión de las vulnerabilidades.
PROTEGER (PR)	Mantenimiento (PR.MA)	PR.MA-1: El mantenimiento y la reparación de los activos de la organización se realizan y están registrados con herramientas aprobadas y controladas.
	Tecnología de protección (PR.PT):	PR.MA-2: El mantenimiento remoto de los activos de la organización se aprueba, se registra y se realiza de manera que evite el acceso no autorizado.
PROTEGER (PR)	Tecnología de protección (PR.PT):	PR.PT-1: Los registros de auditoría o archivos se determinan, se documentan, se implementan y se revisan en conformidad con la política.
		PR.PT-2: Los medios extraíbles están protegidos y su uso se encuentra restringido de acuerdo con la política.
		PR.PT-3: Se incorpora el principio de menor funcionalidad mediante la configuración de los sistemas para proporcionar solo las capacidades esenciales.
		PR.PT-4: Las redes de comunicaciones y control están protegidas.
		PR.PT-5: Se implementan mecanismos (por ejemplo, a prueba de fallas, equilibrio de carga, cambio en caliente o "hot swap") para lograr los requisitos de resiliencia en situaciones normales y adversas.

Nota: Elaboración Propia. Adaptado de (CSF NIST, 2018)

C. Función Detectar

Para la evaluación de esta función, se adoptó las 3 únicas categorías disponibles en esta sección, evidenciada en la Figura 16. Esta función implica identificar actividad anómala y comprender su impacto potencial que puede afectar de una u otra manera la operatividad de la empresa. El propósito de estas categorías se centra en el establecimiento y gestión de una base de referencia, tanto para las operaciones de la red

de telecomunicaciones, como para el análisis de posibles eventos que detectables y para comprensión de los métodos de ataque a los que se puede enfrentar la empresa.

Finalmente, se monitorea continuamente la seguridad del sistema y de los activos para detectar posibles eventos de seguridad cibernética. Además, se mantienen actualizados los procesos y procedimientos de detección para asegurar la identificación de eventos anómalos, definiendo roles y deberes, probando procesos y comunicando información relevante de manera efectiva.

Figura 16

Categorías y subcategorías de la función Detectar

Función	Categoría	Subcategoría
DETECTAR (DE)	Anomalías y Eventos (DE.AE)	DE.AE-1: Se establece y se gestiona una base de referencia para operaciones de red y flujos de datos esperados para los usuarios y sistemas.
		DE.AE-2: Se analizan los eventos detectados para comprender los objetivos y métodos de ataque.
		DE.AE-3: Cos datos de los eventos se recopilan y se correlacionan de múltiples fuentes y sensores.
		DE.AE-4: Se determina el impacto de los eventos.
		DE.AE-5: Se establecen umbrales de alerta de incidentes.
	Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-1: Se monitorea la red para detectar posibles eventos de seguridad cibernética.
		DE.CM-2: Se monitorea el entorno físico para detectar posibles eventos de seguridad cibernética.
		DE.CM-3: Se monitorea la actividad del personal para detectar posibles eventos de seguridad cibernética.
		DE.CM-4: Se detecta el código malicioso.
		DE.CM-5: Se detecta el código móvil no autorizado.
		DE.CM-6: Se monitorea la actividad de los proveedores de servicios externos para detectar posibles eventos de seguridad cibernética.
		DE.CM-7: Se realiza el monitoreo del personal, conexiones, dispositivos y software no autorizados.
		DE.CM-8: Se realizan escaneos de vulnerabilidades.
	Procesos de Detección (DE. DP)	DE. DP-1: Los roles y los deberes de detección están bien definidos para asegurar la responsabilidad.
		DE. DP-2: Las actividades de detección cumplen con todos los requisitos aplicables.
DE. DP-3: Se prueban los procesos de detección.		
DE. DP-4: Se comunica la información de la detección de eventos.		
DE. DP-5: los procesos de detección se mejoran continuamente.		

Nota: Elaboración Propia. Adaptado de (CSF NIST, 2018)

D. Función Responder

En consecuencia al proceso de evaluación, se adaptó las 5 categorías disponibles dentro de esta función, evidenciada en la Figura 17, donde se detalla específicamente la respuesta a los incidentes de seguridad cibernética la cual implica la ejecución y el mantenimiento de procesos y procedimientos de respuesta, así como la coordinación con partes interesadas internas y externas. Además, se lleva a cabo un análisis para garantizar

una respuesta eficaz y apoyar las actividades previas a la recuperación tras un incidente de ciberseguridad, seguido de actividades para evitar la expansión del evento, mitigar sus efectos y solucionar estos posibles incidentes.

Figura 17

Categorías y subcategorías de la función Responder

Función	Categoría	Subcategoría
RESPONDER (RS)	Planificación de la Respuesta (RS.RP)	RS.RP-1: El plan de respuesta se ejecuta durante o después de un incidente.
	Comunicaciones (RS.CO)	RS.CO-1: El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta.
		RS.CO-2: Los incidentes se informan de acuerdo con los criterios establecidos.
		RS.CO-3: La información se comparte de acuerdo con los planes de respuesta.
		RS.CO-4: La coordinación con las partes interesadas se realiza en consonancia con los planes de respuesta.
		RS.CO-5: El intercambio voluntario de información se produce con las partes interesadas y externas para lograr una mayor conciencia situacional de seguridad cibernética.
	Análisis (RS.AN)	RS.AN-1: Se investigan las notificaciones de los sistemas de detección.
		RS.AN-2: Se comprende el impacto del incidente.
		RS.AN-3: Se realizan análisis forenses.
		RS.AN-4: Los incidentes se clasifican de acuerdo con los planes de respuesta.
		RS.AN-5: Se establecen procesos para recibir, analizar y responder a las vulnerabilidades divulgadas a la organización desde fuentes internas y externas (por ejemplo, pruebas internas, boletines de seguridad o investigadores de seguridad).
	Mitigación (RS.MI)	RS.MI-1: Los incidentes son contenidos.
		RS.MI-2: Los incidentes son mitigados.
		RS.MI-3: Las vulnerabilidades recientemente identificadas son mitigadas o se documentan como riesgos aceptados.

Nota: Adaptado de (CSF NIST, 2018)

E. Función Recuperar

Por último, la función recuperar la cual se compone de 3 categorías que se evidencia en la Figura 18. Explica la recuperación tras incidentes de seguridad cibernética, la cual implica la ejecución y continuidad de procesos para restaurar sistemas o activos afectados. Se coordinan actividades de restauración con partes internas y externas, incluyendo la gestión de relaciones con el personal de la empresa y la comunicación con todas las partes interesadas.

Figura 18

Categorías y subcategorías de la función Recuperar

Función	Categoría	Subcategoría
RECUPERAR (RC)	Planificación de la recuperación (RC.RP)	RC.RP-1: El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.
	Mejoras (RC.IM)	RC.IM-1: Los planes de recuperación incorporan las lecciones aprendidas.
	Comunicaciones (RC.CO)	RC.IM-2: Se actualizan las estrategias de recuperación.
		RC.CO-1: Se gestionan las relaciones públicas.
		RC.CO-2: La reputación se repara después de un incidente.
	RC.CO-3: Las actividades de recuperación se comunican a las partes interesadas internas y externas, así como también a los equipos ejecutivos y de administración.	

Nota: Adaptado de (CSF NIST, 2018)

3.3.2. Resumen de resultados de la matriz de evaluación

Junto al líder de área de TIC'S se discutió y analizó minuciosamente la cualificación de las categorías que más se asemejaban al enfoque operativo de la red de telecomunicaciones de Nova Clínica Moderna en base a las 5 funciones a manera de referencia, teniendo un enfoque principal en la función proteger, la cual engloba uno de los objetivos específicos a trabajar en desarrollo del presente proyecto, en el Anexo 6 se evidencia la recopilación de la evaluación realizada dentro de la empresa.

Para la evaluación de cada categoría y subcategoría se realizó el cálculo matemático porcentual del nivel de logro actual de seguridad en la empresa, el nivel de logro como tentativa a futuro y el porcentaje de la brecha que existe para alcanzar la meta que se desea de la siguiente manera:

Nivel 1 (Parcial): Equivalente al 25% de cumplimiento del objetivo según la subcategoría que se esté evaluando.

Nivel 2 (Riesgo Informado): Equivalente al 50% de cumplimiento del objetivo según la subcategoría que se esté evaluando.

Nivel 3 (Repetible): Equivalente al 75% de cumplimiento del objetivo según la subcategoría que se esté evaluando.

Nivel 4 (Adaptable): Equivalente al 100% de cumplimiento del objetivo según la subcategoría que se esté evaluando.

A continuación, se presenta como ejemplo el cálculo de los resultados obtenidos de la categoría “Gestión de activos” y sus respectivas subcategorías:

La categoría “ID. AM” cuenta con seis subcategorías, cada una con un valor comprendido entre 1 a 4 según su nivel de valoración, siendo 4 el nivel máximo para cada subcategoría. Para lograr un cumplimiento del 100% en dicha categoría, se debe realizar la sumatoria total de las seis subcategorías con su valor máximo de 4, obteniendo como final un valor total de 24. Esto significa que un puntaje de 24 representa el cumplimiento del 100% total del objetivo dentro de la categoría “ID.AM”.

Una vez se entiende esta lógica matemática, se procede a tomar como ejemplo la valoración de la categoría “ID.AM” en la empresa como se muestra en la Ec. 2, de la siguiente manera:

$$ID.AM-1(4) + ID.AM-2(4) + ID.AM-3(2) + ID.AM-4(4) + ID.AM-1(3) + ID.AM-1(2) = 19/24 \quad (2)$$

Por consiguiente se tiene a realizar una regla de 3 simple como se muestra en la Ec. 3, donde:

Logro máximo total = 24

Logro actual = 19

Logro porcentual máximo = 100

Logro porcentual actual = X

$$X = \frac{\text{Logro porcentual máximo} \times \text{Logro actual}}{\text{Logro máximo total}} = \frac{100 \times 19}{24} = 79,17\% \quad (3)$$

Por ende, se llega a entender que la empresa actualmente en la categoría “ID.AM” cumple el 79,17 del máximo objetivo de las subcategorías. Se recalca además la similitud

de cálculo que se debe realizar para el porcentaje del objetivo deseado, que para esta categoría se plantea lograr a futuro el cumplimiento del 91,67% del máximo objetivo de dichas subcategorías. Finalmente, en cuanto al cálculo del porcentaje de la brecha de alcance para lograr el objetivo deseado únicamente se realiza un cálculo de resta entre el objetivo deseado y el estado actual, como se muestra en la Ec. 4, de la siguiente manera:

$$\begin{aligned} \text{Brecha} &= \text{Objetivo deseado} - \text{Logro de estado actual} = 91,67\% - \\ &79,17\% = \mathbf{12,50\%} \quad (4) \end{aligned}$$

Por lo que se concluye que la empresa actualmente en la categoría “Gestión de Activos (ID.AM)” logra un estado actual del 79,17% teniendo como tentativa lograr alcanzar el 91,67% del objetivo propuesto con una brecha de alcance del 12,50%. A continuación, se desglosa la valoración cada una las categorías y subcategorías correspondientes a las 5 funciones del marco de ciberseguridad de la NIST para el desarrollo de este trabajo.

a) Categoría “Gestión de activos” - Función Identificar

El análisis de resultados revela que la empresa ha alcanzado un estado adaptativo (Nivel 4) en el registro de dispositivos físicos (ID.AM-1), plataformas de software (ID.AM-2) y sistemas de información (ID.AM-4). Demostrando un alto grado de madurez en la gestión de los activos mencionados previamente, con ciertas políticas formalizadas y procesos establecidos. Sin embargo, existen áreas con una posible mejora a futuro, dependiendo de las posibilidades que tenga la empresa. En la Tabla 13 se evidencia el resumen de la evaluación de esta categoría con un logro de estado actual del 79,17%, considerando un objetivo deseado del 91,67% con una brecha de prioridad del 12,50%. Esto demuestra un alto nivel de madurez de la empresa en la gestión de activos de telecomunicaciones, sin embargo, debe continuar fortaleciendo ciertas áreas.

Tabla 13

Resumen de evaluación de la categoría “Gestión de activos”

Categoría	Subcategoría	Estado actual		Objetivo deseado		Prioridad	
		Logro	Nivel	Logro	Nivel	Brecha	Prioridad
Gestión de activos (ID.AM): Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.	ID.AM-1: Los dispositivos y sistemas físicos dentro de la organización están inventariados.	Adaptable	4	Adaptable	4	0	Objetivo alcanzado
	ID.AM-2: Las plataformas de software y las aplicaciones dentro de la organización están inventariadas.	Adaptable	4	Adaptable	4	0	Objetivo alcanzado
	ID.AM-3: La comunicación organizacional y los flujos de datos están mapeados.	Riesgo Informado	2	Repetible	3	1	Baja
	ID.AM-4: Los sistemas de información externos están catalogados.	Adaptable	4	Adaptable	4	0	Objetivo alcanzado
	ID.AM-5: Los recursos (por ejemplo, hardware, dispositivos, datos, tiempo, personal y software) se priorizan en función de su clasificación, criticidad y valor comercial.	Repetible	3	Adaptable	4	1	Baja
	ID.AM-6: Los roles y las responsabilidades de la seguridad cibernética para toda la fuerza de trabajo y terceros interesados (por ejemplo, proveedores, clientes, socios) están establecidas.	Riesgo Informado	2	Repetible	3	1	Baja
Resumen de la categoría "ID-AM: Gestión de activos"		%Logro	79,17%	%Objetivo	91,67%	12,50%	%Prioridad

Nota: Elaborado a partir de entrevista con el líder de área de TIC'S. Adaptado de (CSF NIST, 2018)

b) Categoría “Evaluación de riesgos” – Función identificar

Para el siguiente apartado se evidencia que la empresa ha logrado un nivel repetible (Nivel 3) para la subcategoría ID.RA-2, donde la empresa entiende de manera clara y concisa la información acerca de amenazas cibernéticas a partir de foros y fuentes bibliográficas, con un objetivo de alcanzar el nivel adaptativo (Nivel 4). En las subcategorías, como la identificación y documentación de vulnerabilidades (ID.RA-1) y amenazas (ID.RA-3), actualmente se encuentran en estado de riesgo informado (Nivel 2) con un objetivo de alcanzar el nivel repetible (Nivel 3).

Para las subcategorías; ID.RA-4, ID.RA-5 e ID.RA-6, donde se determina el riesgo utilizando amenazas, vulnerabilidades, probabilidades e impactos, se evidencia mayores necesidades de mejora. Estas subcategorías actualmente se encuentran en un estado parcial (Nivel 1) y tienen una brecha de uno a dos niveles para alcanzar el estado deseado (Nivel 2 y 3), lo que sugiere una prioridad media para la mejora. En la Tabla 14 se constata que la empresa tiene un grado de manejo por debajo de la media del 50% en cuanto a la gestión de riesgos se refiere, con un logro actual del 41,67% y con un objetivo deseado del 70,83%, teniendo como brecha el 29,17% para alcanzar este perfil como tentativa a futuro, debido a que existen varias áreas críticas que requieren atención para mejorar la postura general frente algún incidente de ciberseguridad.

Tabla 14

Resumen de evaluación de la categoría "Evaluación de riesgos"

Categoría	Subcategoría	Estado actual		Objetivo deseado		Prioridad	
		Logro	Nivel	Logro	Nivel	Brecha	Prioridad
Evaluación de riesgos (ID.RA): La organización comprende el riesgo de seguridad cibernética para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.	ID.RA-1: Se identifican y se documentan las vulnerabilidades de los activos.	Riesgo Informado	2	Repetible	3	1	Baja
	ID.RA-2: La inteligencia de amenazas cibernéticas se recibe de foros y fuentes de intercambio de información.	Repetible	3	Adaptable	4	1	Baja
	ID.RA-3: Se identifican y se documentan las amenazas, tanto internas como externas.	Riesgo Informado	2	Repetible	3	1	Baja
	ID.RA-4: Se identifican los impactos y las probabilidades de riesgo del negocio.	Parcial	1	Riesgo Informado	2	1	Baja
	ID.RA-5: Se utilizan las amenazas, las vulnerabilidades, las probabilidades y los impactos para determinar el riesgo.	Parcial	1	Repetible	3	2	Media
	ID.RA-6: Se identifican y priorizan las respuestas al riesgo.	Parcial	1	Riesgo Informado	2	1	Baja
Resumen de la categoría "ID-RA: Evaluación de riesgos"		%Logro	41,67%	%Objetivo	70,83%	29,17%	%Prioridad

Nota: Elaborado a partir de entrevista con el líder de área de TIC'S. Adaptado de (CSF NIST, 2018)

c) Categoría “Estrategia de gestión de riesgos” – Función identificar

Para la siguiente categoría es notorio evidenciar que la empresa actualmente se encuentra en un nivel parcial (Nivel 1) en todas las subcategorías evaluadas dentro de la estrategia de gestión de riesgos. En la Tabla 15, se evidencia que todas las subcategorías evaluadas tienen como tentativa lograr alcanzar el nivel de riesgo informado (Nivel 2), como objetivo a futuro, teniendo una brecha baja de un nivel para cada caso llegar a cumplir estas expectativas.

En resumen, la empresa tiene una exigencia significativa de mejorar en lo posible su estrategia de gestión de riesgos, debido a que actualmente tiene el nivel más bajo en la escala de evaluación de las subcategorías con un 25% de los objetivos logrados, y aunque la prioridad sea baja de un 25% para alcanzar un nivel medio del 50%, la empresa requiere una atención continua para lograr un nivel de madurez más alto y mejorar su perfil de ciberseguridad a futuro.

Tabla 15

Resumen de evaluación de la categoría “Estrategia de gestión de riesgos”

Categoría	Subcategoría	Estado actual		Objetivo deseado		Prioridad	
		Logro	Nivel	Logro	Nivel	Brecha	Prioridad
Estrategia de gestión de riesgos (ID.RM): Se establecen las prioridades, restricciones, tolerancias de riesgo y suposiciones de la organización y se usan para respaldar las decisiones de riesgos operacionales.	ID.RM-1: Los actores de la organización establecen, gestionan y acuerdan los procesos de gestión de riesgos.	Parcial	1	Riesgo Informado	2	1	Baja
	ID.RM-2: La tolerancia al riesgo organizacional se determina y se expresa claramente.	Parcial	1	Riesgo Informado	2	1	Baja
	ID.RM-3: La determinación de la tolerancia del riesgo de la organización se basa en parte en su rol en la infraestructura crítica y el análisis del riesgo específico del sector.	Parcial	1	Riesgo Informado	2	1	Baja
Resumen de la categoría "ID-RM: Estrategia de gestión de riesgos"		%Logro	25,00%	%Objetivo	50,00%	25,00%	%Prioridad

Nota: Elaborado a partir de entrevista con el líder de área de TIC'S. Adaptado de (CSF NIST, 2018)

**d) Categoría “Gestión de identidad, autenticación y control de acceso” –
Función proteger**

Por otro lado se tiene el resumen de la cualificación obtenida de la función proteger. En la Tabla 16, se evidencia que la empresa ha logrado un nivel repetible (Nivel 3) en lo que se refiere a la gestión del acceso físico (PR.AC-2), acceso remoto (PR.AC-3) y protección de integridad de la red (PR.AC-5), que tienen como objetivo alcanzar un nivel adaptativo (Nivel 4). Sin embargo, para las subcategorías; emisión y verificación de credenciales (PR.AC-1), la gestión de permisos (PR.AC-4), y la autenticación según el riesgo (PR.AC-7) actualmente se encuentran en estado de riesgo informado (Nivel 2), con una tentativa de lograr alcanzar el nivel repetible (Nivel 3).

En resumen, la empresa requiere mejorar la gestión y verificación de credenciales, fortalecer el acceso físico y remoto a los activos de telecomunicaciones de la empresa, optimizar la gestión de permisos y autorizaciones implementando principios de privilegio mínimo, aumentar la protección de la integridad de la red por medio de la segmentación, etc. Por lo que acorde a lo mencionado anteriormente, se evidencia que se ha logrado el 60,71% del objetivo actual de la evaluación, teniendo como tentativa aproximada al 85,71% de objetivos en proceso a futuro y una prioridad baja del 25% para avanzar en la mejora de las áreas evaluadas dentro de esta categoría, lo que permitirá alcanzar mayores niveles de madurez en las prácticas de seguridad y protección de la infraestructura de la empresa.

Tabla 16

Resumen de evaluación de la categoría "Gestión de identidad, autenticación y control de acceso"

Categoría	Subcategoría	Estado actual		Objetivo deseado		Prioridad	
		Logro	Nivel	Logro	Nivel	Brecha	Prioridad
Gestión de identidad, autenticación y control de acceso (PR.AC): El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	PR.AC-1: Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.	Riesgo Informado	2	Repetible	3	1	Baja
	PR.AC-2: Se gestiona y se protege el acceso físico a los activos.	Repetible	3	Adaptable	4	1	Baja
	PR.AC-3: Se gestiona el acceso remoto.	Repetible	3	Adaptable	4	1	Baja
	PR.AC-4: Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.	Riesgo Informado	2	Repetible	3	1	Baja
	PR.AC-5: Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red).	Repetible	3	Adaptable	4	1	Baja
	PR.AC-6: Las identidades son verificadas y vinculadas a credenciales y afirmadas en las interacciones.	Riesgo Informado	2	Repetible	3	1	Baja
	PR.AC-7: Se autentican los usuarios, dispositivos y otros activos (por ejemplo, autenticación de un solo factor o múltiples factores) acorde al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las organizaciones).	Riesgo Informado	2	Repetible	3	1	Baja
Resumen de la categoría "PR.AC: Gestión de identidad, autenticación y control de acceso"		%Logro	60,71%	%Objetivo	85,71%	25,00%	%Prioridad

Nota: Elaborado a partir de entrevista con el líder de área de TIC'S. Adaptado de (CSF NIST, 2018)

e) Categoría “Concienciación y capacitación” – Función proteger

En lo que concierne a la concienciación y capacitación del personal de Nova Clínica Moderna adaptado a la matriz de evaluación, se evidenció para todas las subcategorías de este apartado que actualmente se mantienen en riesgo informado (Nivel 2), teniendo como tentativa a futuro necesidades clave como la mejora de concienciación y capacitación general de todo el personal de la empresa (PR.AT-1) para lograr alcanzar un nivel adaptativo (Nivel 4), además se menciona el fortalecimiento de la comprensión de roles y responsabilidades entre los usuarios privilegiados, ejecutivos y personal del área de TIC'S (PR.AT-2, PR.AT-4, PR.AT-5) para lograr alcanzar un nivel repetible (Nivel 3), por último se descarta la mejora de la subcategoría PT.AT-3 que menciona mantener el nivel alcanzado en la concienciación y comprensión de roles para terceros dentro la empresa.

En la Tabla 17, se resume que la empresa actualmente ha logrado el 50% de los objetivos que plantea esta categoría, teniendo como tentativa alcanzar un 75% de los objetivos definidos en el proceso, por lo que se tiene una brecha del 25% como prioridad de mejora para esta categoría. Esto permitirá un enfoque al área de mejora en cuanto a concienciación del personal de la empresa se refiere, garantizando una mejor protección de la infraestructura tecnológica y de los activos de la empresa.

Tabla 17

Resumen de evaluación de la categoría “Concienciación y capacitación”

Categoría	Subcategoría	Estado actual		Objetivo deseado		Prioridad	
		Logro	Nivel	Logro	Nivel	Brecha	Prioridad
Concienciación y capacitación (PR.AT): El personal y los socios de la organización reciben educación de concienciación sobre la seguridad cibernética y son capacitados para cumplir con sus deberes y responsabilidades relacionados con la seguridad cibernética, en conformidad con las políticas, los procedimientos y los acuerdos relacionados al campo.	PR.AT-1: Todos los usuarios están informados y capacitados.	Riesgo Informado	2	Adaptable	4	2	Media
	PR.AT-2: Los usuarios privilegiados comprenden sus roles y responsabilidades.	Riesgo Informado	2	Repetible	3	1	Baja
	PR.AT-3: Los terceros interesados (por ejemplo, proveedores, clientes, socios) comprenden sus roles y responsabilidades.	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo alcanzado
	PR.AT-4: Los ejecutivos superiores comprenden sus roles y responsabilidades.	Riesgo Informado	2	Repetible	3	1	Baja
	PR.AT-5: El personal de seguridad física y cibernética comprende sus roles y responsabilidades.	Riesgo Informado	2	Repetible	3	1	Baja
Resumen de la categoría "PR-AT: Concienciación y capacitación"		%Logro	50,00%	%Objetivo	75,00%	25,00%	%Prioridad

Nota: Elaborado a partir de entrevista con el líder de área de TIC'S. Adaptado de (CSF NIST, 2018)

f) Categoría “Seguridad de los datos” – Función proteger

Para el siguiente apartado, se evidencia una cualificación igualitaria de las subcategorías; capacidad y disponibilidad (PR.DS-4), protección contra filtraciones de datos (PR.DS-5) y comprobación de la integridad del software y sistemas de información de la empresa (PR.DS-6) actualmente en estado parcial (Nivel 1), teniendo como tentativa lograr alcanzar un estado objetivo repetible (Nivel 3) o de riesgo informado (Nivel 2) respectivamente.

Por consiguiente, las subcategorías; gestión de activos durante eliminación o traslado (PR.DS-3) y clasificación de los entornos de desarrollo y de producción (PR.DS-7), actualmente se encuentran en un estado de riesgo informado (Nivel 2) y como tentativa a futuro pretende alcanzar un estado objetivo repetible (Nivel 3) enfocándose en la mejora de la gestión formal de los activos críticos durante una eliminación o traslado, así mismo, con la mejora y optimización de los entornos de desarrollo (área de TIC’S) a comparación del entorno de producción de la empresa. Finalmente, se destaca a las subcategorías de protección de datos en reposo y transporte (PR.DS-1, PR.DS-2 y PR.DS-8) que actualmente se encuentran en un estado repetible (Nivel 3), con tentativa a mantenerse en dicho nivel debido a que actualmente se utiliza hardware y software sustentable para proteger la operatividad diaria de la empresa, rigiéndose a constantes actualizaciones, de ser el caso se requiera.

En la Tabla 18, se resume que se ha logrado el 50% de los objetivos que recomienda el framework, con un 68,75% de los objetivos propuestos a futuro, con una brecha del 18,75% de prioridad para alcanzar estas metas, en caso de abordar estas mejoras, permitirá mejorar la seguridad de los datos que se manejan dentro y fuera de la infraestructura de la red de telecomunicaciones de la empresa.

Tabla 18

Resumen de evaluación de la categoría “Seguridad de los datos”

Categoría	Subcategoría	Estado actual		Objetivo deseado		Prioridad	
		Logro	Nivel	Logro	Nivel	Brecha	Prioridad
Seguridad de los datos (PR.DS): La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	PR.DS-1: Los datos en reposo están protegidos.	Repetible	3	Repetible	3	0	Objetivo alcanzado
	PR.DS-2: Los datos en tránsito están protegidos.	Repetible	3	Repetible	3	0	Objetivo alcanzado
	PR.DS-3: Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.	Riesgo Informado	2	Repetible	3	1	Baja
	PR.DS-4: Se mantiene una capacidad adecuada para asegurar la disponibilidad.	Parcial	1	Riesgo Informado	2	1	Baja
	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.	Parcial	1	Repetible	3	2	Media
	PR.DS-6: Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.	Parcial	1	Riesgo Informado	2	1	Baja
	PR.DS-7: Los entornos de desarrollo y prueba(s) están separados del entorno de producción.	Riesgo Informado	2	Repetible	3	1	Baja
	PR.DS-8: Se utilizan mecanismos de comprobación de la integridad para verificar la integridad del hardware.	Repetible	3	Repetible	3	0	Objetivo alcanzado
Resumen de la categoría "PR-DS: Seguridad de los datos"		%Logro	50,00%	%Objetivo	68,75%	18,75%	%Prioridad

Nota: Elaborado a partir de entrevista con el líder de área de TIC'S. Adaptado de (CSF NIST, 2018)

**g) Categoría “Procesos y procedimientos de protección de la información” –
Función proteger**

Para el siguiente apartado se realizó mayor énfasis de atención debido a que contiene la mayor cantidad de subcategorías disponibles en la función. Se evidencia que para las subcategorías; PR. IP-1, PR. IP-9, PR. IP-10 y PR. IP-11 actualmente se encuentran en un estado parcial (Nivel 1) crítico con una tentativa de alcanzar un estado objetivo de riesgo informado (Nivel 2) teniendo una brecha baja para lograr esta meta.

Por otro lado, para las subcategorías; PR. IP-3, PR. IP-5, PR. IP-6, PR. IP-7, PR. IP-8 y PR. IP-12, actualmente se encuentran en un estado de riesgo informado (Nivel 2), con tentativa de alcanzar un estado objetivo repetible (Nivel 3) de igual manera con una brecha baja para de un nivel para llegar a cumplir con las metas. Por consiguiente, las subcategorías PR. IP-2 y PR. IP-4 se encuentran al momento en un estado repetible (Nivel 3), siendo los más altos en cuanto a la evaluación realizada y teniendo como tentativa para PR. IP-2 mantenerse dentro de ese estado actual con un objetivo alcanzado, mientras que para PR. IP-4 se provee poder alcanzar el estado adaptable (Nivel 4) con una brecha baja de prioridad para cumplir con la meta.

Por lo tanto, para las subcategorías PR. IP-1 y PR. IP-3 recomienda el framework la implementación y mantenimiento de configuraciones base de sistemas y procesos de control más robustos para gestionar mejor los sistemas y seguridad. En cuanto a las subcategorías PR. IP-4 y PR. IP-10, es necesario realizar, examinar y probar constantemente las copias de seguridad, así como los planes de respuesta y restauración para mantener la integridad y disponibilidad de la información. En cuanto a PR. IP-5 y PR. IP-6, se indica la creación y cumplimiento de políticas formalmente para el entorno operativo de la red de telecomunicaciones.

Del mismo modo para PR. IP-7 y PR. IP-8 es necesario continuar mejorando la efectividad de las tecnologías de protección actualmente utilizadas. Además, para PR. IP-9 y PR. IP-10, se recomienda desarrollar y gestionar planes de respuesta a posibles incidentes, así también, planes de recuperación ante desastres naturales y cibernéticos, para asegurar la continuidad operativa de la empresa y la recuperación rápida ante algún incidente. Por otra parte, para la subcategoría PR. IP-11, la empresa no tiene como requisito el incluir la ciberseguridad como parte de recursos humanos por lo que se descarta la necesidad de mejorar el nivel de esta sección.

Finalmente, se recomienda el desarrollo e implementación de un plan de gestión de vulnerabilidades para la identificación, evaluación y mitigación de riesgos de manera proactiva. En la Tabla 19, se evidencia que para esta categoría actualmente la empresa tiene un logro del 45,83%, teniendo como tentativa lograr un objetivo del 66,67% con una brecha del 20,83% como prioridad para alcanzar esta meta a futuro si está en las posibilidades de la empresa.

Tabla 19

Resumen de evaluación de la categoría “Procesos y procedimiento de protección de la información”

Categoría	Subcategoría	Estado actual		Objetivo deseado		Prioridad	
		Logro	Nivel	Logro	Nivel	Brecha	Prioridad
Procesos y procedimientos de protección de la información (PR.IP): Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	PR.IP-1: Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).	Parcial	1	Riesgo Informado	2	1	Baja
	PR.IP-2: Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas.	Repetible	3	Repetible	3	0	Objetivo alcanzado
	PR.IP-3: Se encuentran establecidos procesos de control de cambio de la configuración.	Riesgo Informado	2	Repetible	3	1	Baja
	PR.IP-4: Se realizan, se mantienen y se prueban copias de seguridad de la información.	Repetible	3	Adaptable	4	1	Baja
	PR.IP-5: Se cumplen las regulaciones y la política con respecto al entorno operativo físico para los activos organizativos.	Riesgo Informado	2	Repetible	3	1	Baja
	PR.IP-6: Los datos son eliminados de acuerdo con las políticas.	Riesgo Informado	2	Repetible	3	1	Baja
	PR.IP-7: Se mejoran los procesos de protección.	Riesgo Informado	2	Repetible	3	1	Baja

	PR.IP-8: Se comparte la efectividad de las tecnologías de protección.	Riesgo Informado	2	Repetible	3	1	Baja
	PR.IP-9: Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de Incidentes y Recuperación de Desastres).	Parcial	1	Riesgo Informado	2	1	Baja
	PR.IP-10: Se prueban los planes de respuesta y recuperación.	Parcial	1	Riesgo Informado	2	1	Baja
	PR.IP-11: La seguridad cibernética se encuentra incluida en las prácticas de recursos humanos (por ejemplo, desaprovisionamiento, selección del personal).	Parcial	1	Parcial	1	0	Objetivo alcanzado
	PR.IP-12: Se desarrolla y se implementa un plan de gestión de las vulnerabilidades.	Riesgo Informado	2	Repetible	3	1	Baja
Resumen de la categoría "PR-IP: Procesos y procedimientos de protección de la información"		%Logro	45,83%	%Objetivo	66,67%	20,83%	%Prioridad

Nota: Elaborado a partir de entrevista con el líder de área de TIC'S. Adaptado de (CSF NIST, 2018)

h) Categoría “Mantenimiento” – Función proteger

En la Tabla 20, es posible evidenciar las 2 únicas subcategorías disponibles dentro de esta sección, donde PR.MA-1 actualmente se encuentra en un estado repetible (Nivel 3) con el objetivo alcanzado, donde el mantenimiento y revisión constante de los activos de telecomunicaciones de la empresa actualmente se encuentran registrados formalmente, lo que recomienda mantener estos principios y garantizar el uso de herramientas certificadas y controladas.

En segundo lugar se evidencia la subcategoría PR.MA-2, que en la actualidad se encuentra en un estado parcial (Nivel 1), con tentativa de lograr un estado objetivo repetible (Nivel 3) con una brecha de 2 niveles de media para conseguir su meta como máximo, debido a que el mantenimiento remoto de los activos de la organización requieren de una mejora significativa por medio de la implementación de procesos para la aprobación, registro y control de manera mucho más rigurosa de los activos, garantizando evitar cualquier acceso no autorizado.

En resumen, la empresa se encuentra en un estado actual del 50% de logro sobre el 100%, con la finalidad de alcanzar un estado objetivo del 75% con una brecha del 25% de prioridad para cumplir las metas establecidas.

Tabla 20

Resumen de evaluación de la categoría "Mantenimiento"

Categoría	Subcategoría	Estado actual		Objetivo deseado		Prioridad	
		Logro	Nivel	Logro	Nivel	Brecha	Prioridad
Mantenimiento (PR.MA): El mantenimiento y la reparación de los componentes del sistema de información y del control industrial se realizan de acuerdo con las políticas y los procedimientos.	PR.MA-1: El mantenimiento y la reparación de los activos de la organización se realizan y están registrados con herramientas aprobadas y controladas.	Repetible	3	Repetible	3	0	Objetivo alcanzado
	PR.MA-2: El mantenimiento remoto de los activos de la organización se aprueba, se registra y se realiza de manera que evite el acceso no autorizado.	Parcial	1	Repetible	3	2	Media
Resumen de la categoría "PR-MA: Procesos y procedimientos de protección de la información"		%Logro	50,00%	%Objetivo	75,00%	25,00%	%Prioridad

Nota: Elaborado a partir de entrevista con el líder de área de TIC'S. Adaptado de (CSF NIST, 2018)

i) Categoría “Tecnología de protección” – Función proteger

En la Tabla 21 se muestra para las subcategorías; Auditoría y registro de archivos (PR.PT-1) y mecanismos de capacidad (PR.PT-5), que actualmente se encuentran en un estado parcial (Nivel 1) con un nivel de brecha para lograr alcanzar un estado de riesgo informado como objetivo deseado. Por otro lado, las categorías; protección de medios extraíbles (PR.PT-2), principio de privilegios mínimos (PR.PT-3), protección y control de la red de telecomunicaciones (PR.PT-4), actualmente se encuentra en un estado de riesgo informado (Nivel 2) con tentativa de lograr alcanzar un estado repetible (Nivel 3) de igual manera con una brecha de un nivel de por medio.

En resumen, para conseguir estos niveles de madurez en cuanto a tecnología de protección se refiere, la empresa debe enfocarse en la implementación y optimización de sistemas de control y registro, mecanismo de resiliencia, protección de medios externos conforme a las políticas de la organización, configuración basada en privilegios mínimos para el personal proporcionando solo necesidades esenciales y énfasis en la protección de la red de telecomunicaciones contra accesos no autorizados y otras amenazas. Además, se revela un logro actual del 40%, teniendo como objetivo lograr un 65% de mejora con una brecha del 25% como prioridad para alcanzar esta meta.

Tabla 21

Resumen de evaluación de la categoría “Tecnología de protección”

Categoría	Subcategoría	Estado actual		Objetivo deseado		Prioridad	
		Logro	Nivel	Logro	Nivel	Brecha	Prioridad
Tecnología de protección (PR.PT): Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y la capacidad de recuperación de los sistemas y activos, en consonancia con las políticas, procedimientos y acuerdos relacionados.	PR.PT-1: Los registros de auditoría o archivos se determinan, se documentan, se implementan y se revisan en conformidad con la política.	Parcial	1	Riesgo Informado	2	1	Baja
	PR.PT-2: Los medios extraíbles están protegidos y su uso se encuentra restringido de acuerdo con la política.	Riesgo Informado	2	Repetible	3	1	Baja
	PR.PT-3: Se incorpora el principio de menor funcionalidad mediante la configuración de los sistemas para proporcionar solo las capacidades esenciales.	Riesgo Informado	2	Repetible	3	1	Baja
	PR.PT-4: Las redes de comunicaciones y control están protegidas.	Riesgo Informado	2	Repetible	3	1	Baja
	PR.PT-5: Se implementan mecanismos (por ejemplo, a prueba de fallas, equilibrio de carga, cambio en caliente o “hot swap”) para lograr los requisitos de resiliencia en situaciones normales y adversas.	Parcial	1	Riesgo Informado	2	1	Baja
Resumen de la categoría "PR-PT: Tecnología de protección"		%Logro	40,00%	%Objetivo	65,00%	25,00%	%Prioridad

Nota: Elaborado a partir de entrevista con el líder de área de TIC'S. Adaptado de (CSF NIST, 2018)

j) Categoría “Anomalías y eventos” – Función detectar

Para la evaluación referente a las categorías de la función detectar, se inició con la categoría de “anomalías y eventos”, la cual cuenta con 5 subcategorías que pueden ser evidenciados en la Tabla 22. En primer lugar, para las subcategorías; marco de referencia para la gestión y operación de la red (DE.AE-1), integración y análisis de antecedentes de eventos (DE.AE-3), evaluación de impacto de los eventos (DE.AE-4) y niveles de alerta ante incidentes (DE.AE-5), la empresa cualifica un estado actual de riesgo informado (Nivel 2) con una tentativa de lograr un estado repetible (Nivel 3) como objetivo deseado, separado de una brecha de un nivel y en el caso de la subcategoría DE.AE-4, se provee mantenerse dentro de ese nivel, debido a que no han existido situaciones que comprometan el impacto de eventos de ciberseguridad hacia la operatividad de la empresa.

Por otro lado, se tiene a la subcategoría; análisis de eventos detectados (DE.AE-2) en un estado actual repetible (Nivel 3) con un provisorio mantenimiento de ese nivel, ya que el líder de área de TIC’S de la empresa manifiesta estar al corriente de eventos suscitados en toda la infraestructura tecnológica de la red de Telecomunicaciones de la empresa en base al análisis y revisión constante y del soporte de fuentes que sustentan actualizaciones recurrentes a posibles eventos cibernéticos que puedan suscitarse dentro de la empresa.

En resumen, para esta categoría la empresa actualmente tiene un logro del 55% de los objetivos, con una tentativa de lograr una mejora de hasta el 70%, separado una brecha de 15% de prioridad para alcanzar esta meta de mejora a futuro. Por medio del establecimiento de bases de referencia más robustas, la mejora de comprensión de los eventos que se susciten o puedan suscitarse.

Tabla 22

Resumen de evaluación de la categoría “Anomalías y eventos”

Categoría	Subcategoría	Estado actual		Objetivo deseado		Prioridad	
		Logro	Nivel	Logro	Nivel	Brecha	Prioridad
Anomalías y Eventos (DE.AE): se detecta actividad anómala y se comprende el impacto potencial de los eventos.	DE.AE-1: Se establece y se gestiona una base de referencia para operaciones de red y flujos de datos esperados para los usuarios y sistemas.	Riesgo Informado	2	Repetible	3	1	Baja
	DE.AE-2: Se analizan los eventos detectados para comprender los objetivos y métodos de ataque.	Repetible	3	Repetible	3	0	Objetivo alcanzado
	DE.AE-3: Los datos de los eventos se recopilan y se correlacionan de múltiples fuentes y sensores.	Riesgo Informado	2	Repetible	3	1	Baja
	DE.AE-4: Se determina el impacto de los eventos.	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo alcanzado
	DE.AE-5: Se establecen umbrales de alerta de incidentes.	Riesgo Informado	2	Repetible	3	1	Baja
Resumen de la categoría "DE-AE: Anomalías y Eventos"		%Logro	55,00%	%Objetivo	70,00%	15,00%	%Prioridad

Nota: Elaborado a partir de entrevista con el líder de área de TIC'S. Adaptado de (CSF NIST, 2018)

k) Categoría “Monitoreo continuo de la seguridad” – Función detectar

Para la siguiente sección es posible evidenciar que cuenta con 8 subcategorías, donde; escaneo de vulnerabilidades (DE.CM-8), actualmente cuenta con un estado parcial (Nivel 1) siendo el más crítico en cuanto a la evaluación de esta categoría, sin embargo, la empresa tiene como objetivo alcanzar un estado repetible (Nivel 3) con una brecha de 2 niveles de prioridad media. Por otro lado, se tiene las subcategorías; monitoreo de la red (DE.CM-1), monitoreo del entorno físico (DE.CM-2), monitoreo de la actividad del personal (DE.CM-3), monitoreo de terceros dentro de la empresa (DE.CM-6), monitoreo de dispositivos personales no autorizados (DE.CM-7) y detección de aplicaciones móviles no autorizadas (DE.CM-5), actualmente se encuentran estado de riesgo informado (Nivel 2) con una tentativa de lograr alcanzar un estado repetible (Nivel 3) en algunas secciones y en otras tantos mantenerse en dicho nivel actual, debido a que para la implementación de nuevos mecanismos conllevaría tiempo y cierta inversión por parte de la empresa, que de momento no considera prioritario.

Finalmente, se tiene la subcategoría; detección de código malicioso (DE.CM-4) actualmente en un estado repetible (Nivel 3) con la tentativa de mantenerse en ese nivel, debido a que, en secciones anteriores del documento se mencionó el uso de softwares de seguridad informática dentro de la empresa.

En resumen, en la Tabla 23 se constata que la empresa actualmente ha logrado un 50% de los objetivos que plantea esta categoría, con una tentativa de alcanzar el 65,63% de la meta con una brecha del 15,63% de prioridad para avanzar en los niveles de madurez, mediante el monitoreo continuo de la seguridad, la implementación de escaneos regulares de vulnerabilidades, el monitoreo de la red y la actividad que realiza el personal con múltiples dispositivos personales, además de asegurar que los invitados dentro de la empresa con dispositivos no autorizados sean monitoreados adecuadamente

Tabla 23

Resumen de evaluación de la categoría “Monitoreo continuo de la seguridad”

Categoría	Subcategoría	Estado actual		Objetivo deseado		Prioridad	
		Logro	Nivel	Logro	Nivel	Brecha	Prioridad
Monitoreo Continuo de la Seguridad (DE.CM): El sistema de información y los activos son monitoreados a fin de identificar eventos de seguridad cibernética y verificar la eficacia de las medidas de protección.	DE.CM-1: Se monitorea la red para detectar posibles eventos de seguridad cibernética.	Riesgo Informado	2	Repetible	3	1	Baja
	DE.CM-2: Se monitorea el entorno físico para detectar posibles eventos de seguridad cibernética.	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo alcanzado
	DE.CM-3: Se monitorea la actividad del personal para detectar posibles eventos de seguridad cibernética.	Riesgo Informado	2	Repetible	3	1	Baja
	DE.CM-4: Se detecta el código malicioso.	Repetible	3	Repetible	3	0	Objetivo alcanzado
	DE.CM-5: Se detecta el código móvil no autorizado.	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo alcanzado
	DE.CM-6: Se monitorea la actividad de los proveedores de servicios externos para detectar posibles eventos de seguridad cibernética.	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo alcanzado
	DE.CM-7: Se realiza el monitoreo del personal, conexiones, dispositivos y software no autorizados.	Riesgo Informado	2	Repetible	3	1	Baja
	DE.CM-8: Se realizan escaneos de vulnerabilidades.	Parcial	1	Repetible	3	2	Media
Resumen de la categoría "DE-CM: Monitoreo Continuo de la Seguridad"		%Logro	50,00%	%Objetivo	65,63%	15,63%	%Prioridad

Nota: Elaborado a partir de entrevista con el líder de área de TIC'S. Adaptado de (CSF NIST, 2018)

l) Categoría “Procesos de detección” – Función detectar

Para la última categoría de la función detectar, se tiene 5 subcategorías de evaluación adaptables al proceso de auditoría, donde; definición de roles y responsabilidades (DE.DP-1), procesos de detección (DE.DP-3) y comunicación de detección de eventos (DE.DP-4), actualmente se encuentran en un estado parcial (Nivel 1), con la posibilidad de superar un nivel a estado de riesgo informado (Nivel 2), teniendo una brecha baja un nivel de distancia para lograr este objetivo. Por otro lado, la subcategoría; cumplimiento de los requisitos de detección de amenazas, actualmente se encuentra en un estado de riesgo informado (Nivel 2) con el propósito de alcanzar un estado repetible (Nivel 3) como objetivo deseado con una brecha de alcance baja.

Finalmente, se tiene a la subcategoría; mejoras continuas en los procesos de detección (DE.DP-5), actualmente y de mantenerse en un estado repetible (Nivel 3), siendo la sección con mayor puntaje de evaluación ya que previamente en el documento se menciona y resalta que la empresa cuenta con hardware y software sostenible certificado, además de mencionar la alta capacidad del líder del área de TIC'S de mantenerse en constante actualización de la información que se genera diariamente dentro de la infraestructura tecnológica de la empresa.

En la Tabla 24, se resume que la empresa ha alcanzado el 40% de sus objetivos que propone esta sección, con una tentativa de alcanzar el 60 % de los objetivos totales y una brecha de conseguir esta meta del 20% de prioridad para avanzar en los niveles de madurez de los procesos de detección, por lo que la empresa debe formalizar la clasificación de roles y responsabilidades en cuanto a ciberseguridad se refiere, verificar regularmente los procesos de detección de amenazas y vulnerabilidades que se utilizan actualmente en la infraestructura tecnológica.

Tabla 24

Resumen de evaluación de la categoría "Monitoreo continuo de la seguridad"

Categoría	Subcategoría	Estado actual		Objetivo deseado		Prioridad	
		Logro	Nivel	Logro	Nivel	Brecha	Prioridad
Procesos de Detección (DE.DP): Se mantienen y se aprueban los procesos y procedimientos de detección para garantizar el conocimiento de los eventos anómalos.	DE.DP-1: Los roles y los deberes de detección están bien definidos para asegurar la responsabilidad.	Parcial	1	Riesgo Informado	2	1	Baja
	DE.DP-2: Las actividades de detección cumplen con todos los requisitos aplicables.	Riesgo Informado	2	Repetible	3	1	Baja
	DE.DP-3: Se prueban los procesos de detección.	Parcial	1	Riesgo Informado	2	1	Baja
	DE.DP-4: Se comunica la información de la detección de eventos.	Parcial	1	Riesgo Informado	2	1	Baja
	DE.DP-5: los procesos de detección se mejoran continuamente.	Repetible	3	Repetible	3	0	Objetivo alcanzado
Resumen de la categoría "DE-DP: Procesos de Detección"		%Logro	40,00%	%Objetivo	60,00%	20,00%	%Prioridad

Nota: Elaborado a partir de entrevista con el líder de área de TIC'S. Adaptado de (CSF NIST, 2018)

m) Categoría “Planificación de respuesta” – Función responder

Se evalúa a la función responder como cuarta función que conforma el núcleo del framework, donde, para la primera categoría únicamente se evidencia la única subcategoría; ejecución de plan de respuesta (RS.RP-1) que actualmente cuenta con un estado de riesgo informado (Nivel 2), con el objetivo deseado de alcanzar un estado repetible (Nivel 3), siendo de prioridad baja para la empresa lograr esta meta.

En la Tabla 25, se revela un resumen general de la categoría evaluada, donde, la empresa ha logrado el 50% de los objetivos planteados, sin embargo, pretende alcanzar un 75% de mejora de madurez y para lograr estos objetivos se interpone una brecha del 25% como prioridad. Esto en conjunto con la mejora de un plan de respuesta a incidentes cibernéticos, asegurando que los procedimientos se lleven a cabo de manera efectiva; tanto, durante y después de que ocurra un incidente de ciberseguridad, lo que incluye el establecimiento de protocolos claros y la capacitación del personal para que sepan cómo actuar en estos casos.

Tabla 25

Resumen de evaluación de la categoría "Planificación de respuesta"

Categoría	Subcategoría	Estado actual		Objetivo deseado		Prioridad	
		Logro	Nivel	Logro	Nivel	Brecha	Prioridad
Planificación de la Respuesta (RS.RP): Los procesos y procedimientos de respuesta se ejecutan y se mantienen a fin de garantizar la respuesta a los incidentes de seguridad cibernética detectados.	RS.RP-1: El plan de respuesta se ejecuta durante o después de un incidente.	Riesgo Informado	2	Repetible	3	1	Baja
Resumen de la categoría "RS-RP: Planificación de la Respuesta"		%Logro	50,00%	%Objetivo	75,00%	25,00%	%Prioridad

Nota: Elaborado a partir de entrevista con el líder de área de TIC'S. Adaptado de (CSF NIST, 2018)

a) Categoría “Comunicación” – Función responder

En cuanto al análisis de resultados de la función responder la cual se compone de 5 subcategorías, donde; el conocimiento de roles y responsabilidades (RS.CO-1), informe de incidentes (RS.CO-2), difusión de información en base a los planes de respuesta (RS.CO-3) y colaboración por parte de stakeholders (RS.CO-4) tienen el nivel de calificación más bajo, estado parcial (Nivel 1), debido a que dentro de la empresa actualmente no se maneja de manera formal una comunicación acerca de un incidente de ciberseguridad, dando únicamente una respuesta ad-hoc que en caso de ocurrir, el responsable de una solución o comunicación es el líder de área de TIC'S sin la guía de un protocolo o sistema de gestión de seguridad. Por lo que, a mediano o largo plazo se prevé alcanzar un estado de riesgo informado (Nivel 2), gestionando dichos planes en donde se garantice que el personal de Nova Clínica Moderna entienda de la mejor manera sus roles y responsabilidades dentro de la empresa por medio de capacitaciones y simulaciones de incidentes. Así también, se involucre a los stakeholders de la organización por medio de la coordinación interna con la guía de planes de respuesta elaborados y formalizados.

Por otro lado, se tiene la única subcategoría; intercambio voluntario de información (RS.CO-5) que mantiene un estado de riesgo informado (Nivel 2), debido a que es complicado llegar a concientizar a terceros y proveedores relacionados a la empresa, por lo que se considera mantener ese estado como objetivo máximo alcanzado.

En resumen, en la Tabla 26, es posible evidenciar que la empresa ha logrado el 30% de los objetivos que plantea esta categoría, y como tentativa tiene alcanzar el 50 % de los objetivos con una brecha del 20% de prioridad para garantizar la mejora de madurez de esta categoría.

Tabla 26

Resumen de evaluación de la categoría “Comunicación”

Categoría	Subcategoría	Estado actual		Objetivo deseado		Prioridad	
		Logro	Nivel	Logro	Nivel	Brecha	Prioridad
Comunicaciones (RS.CO): Las actividades de respuesta se coordinan con las partes interesadas internas y externas (por ejemplo, el apoyo externo de organismos encargados de hacer cumplir la ley).	RS.CO-1: El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta.	Parcial	1	Riesgo Informado	2	1	Baja
	RS.CO-2: Los incidentes se informan de acuerdo con los criterios establecidos.	Parcial	1	Riesgo Informado	2	1	Baja
	RS.CO-3: La información se comparte de acuerdo con los planes de respuesta.	Parcial	1	Riesgo Informado	2	1	Baja
	RS.CO-4: La coordinación con las partes interesadas se realiza en consonancia con los planes de respuesta.	Parcial	1	Riesgo Informado	2	1	Baja
	RS.CO-5: El intercambio voluntario de información se produce con las partes interesadas externas para lograr una mayor conciencia situacional de seguridad cibernética.	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo alcanzado
Resumen de la categoría "RS-CO: Comunicaciones"		%Logro	30,00%	%Objetivo	50,00%	20,00%	%Prioridad

Nota: Elaborado a partir de entrevista con el líder de área de TIC'S. Adaptado de (CSF NIST, 2018)

b) Categoría “Análisis” – Función responder

La evaluación de esta categoría adaptada al proceso de auditoría de la empresa reveló que la subcategoría; clasificación de incidentes (RS.AN-4) actualmente se encuentra en un estado parcial (Nivel 1) debido a que en toda la vida empresarial no se ha registrado algún tipo de incidente cibernético, sin embargo, con la evolución de las amenazas a lo largo de los años, la empresa prevé alcanzar un estado de riesgo informado (Nivel 2) como tentativa de mejora de la madurez del análisis a estos incidentes.

Por otro lado, para las subcategorías; análisis forense (RS.AN-3) y procesos para vulnerabilidades (RS.AN-5), al momento se encuentran en un estado de riesgo informado (Nivel 2) con el propósito de alcanzar un estado repetible (Nivel 3), por medio del fortalecimiento de análisis forense digital y protocolos de respuesta en caso de llegar a tener un incidente y afecte la operatividad de los activos críticos de la red de telecomunicaciones de la empresa. Además, es de suma necesidad crear, verificar y mantener procesos formales para receptar, analizar y responder a posibles vulnerabilidades que puedan suscitarse dentro de la empresa.

Finalmente, para las subcategorías; análisis de las alertas de detección (RS.AN-1) y evaluación del efecto de impacto ante incidentes (RS.AN-2), actualmente tiene una valoración media – alta en un estado repetible (Nivel 3), con el objetivo de mantener ese estado actual mediante el soporte de sistemas de detección para asegurar la identificación y pronta respuesta ante posibles incidentes de ciberseguridad, como también mantener el entendimiento formal de posibles consecuencias que pueden suscitarse y sus posibles medidas adecuadas para mitigar los riesgos. En resumen, en la Tabla 27, se constata que la empresa ha logrado el 55% de los objetivos de la categoría, con una tentativa de lograr alcanzar el 70% de cumplimiento a estos objetivos con una brecha del 15% de prioridad que separa de lo que actualmente se cualifica.

Tabla 27

Resumen de evaluación de la categoría "Análisis"

Categoría	Subcategoría	Estado actual		Objetivo deseado		Prioridad	
		Logro	Nivel	Logro	Nivel	Brecha	Prioridad
Análisis (RS.AN): Se lleva a cabo el análisis para garantizar una respuesta eficaz y apoyar las actividades de recuperación.	RS.AN-1: Se investigan las notificaciones de los sistemas de detección.	Repetible	3	Repetible	3	0	Objetivo alcanzado
	RS.AN-2: Se comprende el impacto del incidente.	Repetible	3	Repetible	3	0	Objetivo alcanzado
	RS.AN-3: Se realizan análisis forenses.	Riesgo Informado	2	Repetible	3	1	Baja
	RS.AN-4: Los incidentes se clasifican de acuerdo con los planes de respuesta.	Parcial	1	Riesgo Informado	2	1	Baja
	RS.AN-5: Se establecen procesos para recibir, analizar y responder a las vulnerabilidades divulgadas a la organización desde fuentes internas y externas (por ejemplo, pruebas internas, boletines de seguridad o investigadores de seguridad).	Riesgo Informado	2	Repetible	3	1	Baja
Resumen de la categoría "RS-AN: Análisis"		%Logro	55,00%	%Objetivo	70,00%	15,00%	%Prioridad

Nota: Elaborado a partir de entrevista con el líder de área de TIC'S. Adaptado de (CSF NIST, 2018)

c) Categoría “Mitigación” – Función responder

Por consiguiente, los resultados de la evaluación de esta categoría reflejan el objetivo máximo alcanzado y el mantenimiento de los estados actuales en todas sus subcategorías; mitigación y documentación de vulnerabilidades (RS.MI-1) actualmente se encuentra y mantiene en un estado de riesgo informado (Nivel 2), mientras que; control de incidentes (RS.MI-1) y mitigación de incidentes (RS.MI-2), actualmente se encuentran cualificados en un estado repetible (Nivel 3) más avanzado a la subcategoría mencionada anteriormente, de igual manera con el objetivo máximo alcanzado y con la expectativa de mantener ese nivel.

En resumen, se evidencia en la Tabla 28, que la empresa ha logrado el 66,67% de los objetivos que se plantean en esta sección sin brecha ni prioridad, debido a que se ha alcanzado, de momento, el objetivo deseado, por lo que se debe enfocarse en garantizar la consistencia de mitigación con la que cuenta, documentando regularmente las posibles vulnerabilidades que se puedan encontrar, manteniendo y mejorando las prácticas de mitigación a posibles incidentes de ciberseguridad.

Tabla 28

Resumen de evaluación de la categoría "Mitigación"

Categoría	Subcategoría	Estado actual		Objetivo deseado		Prioridad	
		Logro	Nivel	Logro	Nivel	Brecha	Prioridad
Mitigación (RS.MI): Se realizan actividades para evitar la expansión de un evento, mitigar sus efectos y resolver el incidente.	RS.MI-1: Los incidentes son contenidos.	Repetible	3	Repetible	3	0	Objetivo alcanzado
	RS.MI-2: Los incidentes son mitigados.	Repetible	3	Repetible	3	0	Objetivo alcanzado
	RS.MI-3: Las vulnerabilidades recientemente identificadas son mitigadas o se documentan como riesgos aceptados.	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo alcanzado
Resumen de la categoría "RS-MI: Mitigación"		%Logro	66,67%	%Objetivo	66,67%	0,00%	%Prioridad

Nota: Elaborado a partir de entrevista con el líder de área de TIC'S. Adaptado de (CSF NIST, 2018)

d) Resumen general de la función “Recuperar”

Para finalizar con la última función se realiza un resumen general que arrojó la evaluación de esta función, debido a que, como se mencionó anteriormente la empresa no ha tenido en el transcurso de su vida operativa algún tipo de incidente de ciberseguridad, por lo que no existe actualmente ningún tipo de política, plan de recuperación o haya tenido que recurrir al soporte de personal externo para solucionar catástrofes o eventos de riesgo que se hayan suscitado y hayan comprometido a los activos críticos de la red de telecomunicaciones.

Por lo que, en la Tabla 29, se evidencia que la mayoría de las subcategorías están actualmente en un nivel bajo de estado parcial (Nivel 1), con una tentativa de poder alcanzar un objetivo de riesgo informado (Nivel 2), mediante la coordinación de recomendaciones formales de planes de recuperación en conjunto con los stakeholders de la empresa. Este enfoque tiene como objetivo prevenir y, en caso de que ocurra una actividad riesgosa que comprometa la operatividad de la red de telecomunicaciones, se garantice una respuesta rápida y efectiva, asegurando la continuidad operativa de la red.

En resumen, la empresa con los recursos que cuenta actualmente ha logrado un 27,77 de objetivos que propone esta función, sin embargo, con el soporte de esta auditoría y en conjunto a ideas compartidas con el líder de área de TIC'S se ha propuesto como objetivo, sí la empresa a futuro llegara a acceder, pueda alcanzar el 50% de los objetivos deseados, teniendo una brecha del 22,22% de prioridad de conseguir una mejora respecto las metas que propone dicha función

Tabla 29

Resumen general de evaluación de la función "Recuperar"

Categoría	Subcategoría	Estado actual		Objetivo deseado		Prioridad	
		Logro	Nivel	Logro	Nivel	Brecha	Prioridad
Planificación de la recuperación (RC.RP): Los procesos y procedimientos de recuperación se ejecutan y se mantienen para asegurar la restauración de los sistemas o activos afectados por incidentes de seguridad cibernética.	RC.RP-1: El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.	Parcial	1	Riesgo Informado	2	1	Baja
	Resumen de la categoría "RC-RP: Planificación de la recuperación"		%Logro	25,00%	%Objetivo	50,00%	25,00%
Mejoras (RC.IM): La planificación y los procesos de recuperación se mejoran al incorporar en las actividades futuras las lecciones aprendidas.	RC.IM-1: Los planes de recuperación incorporan las lecciones aprendidas.	Parcial	1	Riesgo Informado	2	1	Baja
	RC.IM-2: Se actualizan las estrategias de recuperación.	Parcial	1	Riesgo Informado	2	1	Baja
Resumen de la categoría "RC-IM: Mejoras"		%Logro	25,00%	%Objetivo	50,00%	25,00%	%Prioridad
Comunicaciones (RC.CO): Las actividades de restauración se coordinan con partes internas y externas (por ejemplo, centros de coordinación, proveedores de servicios de Internet, propietarios de sistemas de ataque, víctimas, otros CSIRT y vendedores).	RC.CO-1: Se gestionan las relaciones públicas.	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo alcanzado
	RC.CO-2: La reputación se repara después de un incidente.	Parcial	1	Riesgo Informado	2	1	Baja
	RC.CO-3: Las actividades de recuperación se comunican a las partes interesadas internas y externas, así como también a los equipos ejecutivos y de administración.	Parcial	1	Riesgo Informado	2	1	Baja
Resumen de la categoría "RC-CO: Comunicaciones"		%Logro	33,33%	%Objetivo	50,00%	16,67%	%Prioridad

Nota: Elaborado a partir de entrevista con el líder de área de TIC'S. Adaptado de (CSF NIST, 2018)

3.3.3. *Matriz de valoración de activos críticos de la red de telecomunicaciones de Nova Clínica Moderna*

Antes de poder valorar los riesgos de un activo crítico de la red de telecomunicaciones de Nova Clínica Moderna, se debe conocer su valor cualitativo y cuantitativo, sin embargo, por sensibilidad y privacidad de los datos referentes al valor monetario tangible de estos activos de la empresa, únicamente se presentará una matriz donde se captura que tan importante para la organización representa la confidencialidad, integridad y disponibilidad, englobando y adaptando la guía de perfiles de activos de información con la metodología OCTAVE y la función “Proteger” del marco de ciberseguridad de la NIST. Por ende, se muestra en la Tabla 30 una escala cualitativa y cuantitativa del nivel de criticidad (importancia) del activo dentro de la empresa adaptadas al proceso de auditoría y en conjunto con el líder de área de TIC’S se llegó a la conclusión de lo siguiente.

Tabla 30

Escala de medición del nivel de criticidad de los activos críticos de Nova Clínica Moderna

Nivel de criticidad del activo	Valor numérico
Muy bajo	1
Bajo	2
Medio	3
Alto	4
Muy alto	5

Por consiguiente, en la Tabla 31 se evidencia a los activos críticos, la descripción de la confidencialidad, integridad y disponibilidad, como su nivel de criticidad y las categorías de la función antes mencionadas que más se adapten al objetivo planteado en el proyecto. Valorando y perfilando cualitativamente a los activos críticos de la empresa que, según la metodología OCTAVE, también se aplicará posteriormente a los posibles riesgos e impactos que puedan llegar afectar a la operatividad de la red

Tabla 31*Matriz de valoración de activos críticos de Nova Clínica Moderna*

Activo Crítico	Disponibilidad	Confidencialidad	Integridad	Nivel de criticidad	Categorías de la función “Proteger” del NIST CSF
Routers Firewall	La disponibilidad es de vital importancia para el acceso seguro a la red y para la protección contra amenazas externas, garantizando que la red se mantenga accesible y segura en todo momento	Debe existir control de acceso a la red y protección de la información sensible a terceros con acceso no autorizado, previniendo espionaje y la exfiltración de datos.	Se debe asegurar que las políticas y configuración del firewall no se alteren maliciosamente.	Muy Alto (5)	PR.AC, PR.AT, PR. IP, PR.PT
Conmutadores	Gestionan y garantizan la comunicación efectiva entre los dispositivos conectados a la red.	Controlan el tráfico de la red y deben estar protegidos contra acceso no autorizado, manteniendo la privacidad y seguridad de la información que se transmite.	La integridad de los conmutadores garantiza que las configuraciones y el tráfico de la red no sean alterados, asegurando la operatividad de la red.	Alta (4)	PR.MA
Servidores Internos	Alojan y aseguran que las aplicaciones y datos críticos médicos estén	El almacenamiento de información médica es sensible y confidencial	La integridad de la información y datos almacenados en los	Alta (4)	PR.DS, PR. IP, PR.MA

	disponibles únicamente para las operaciones diarias del personal autorizado	que debe estar siempre protegido del mismo personal y de terceros no autorizados.	servidores deben estar protegidos contra alteraciones no autorizadas y deben mantener constantemente un correcto estado.		
Cableado horizontal y Vertical	Disposición del medio físico por el cual se transmite la información de toda la red, garantizando que la comunicación interna de la red sea constante	Protección contra accesos no autorizados y escuchas que traten de manipular todo el tipo de cable utilizado, asegurando que la información que se transmite no sea interceptada.	Evitar pérdidas o la corrupción de los datos durante su transmisión, garantizando que lleguen a su destino de manera íntegra y sin interrupciones por alguna manipulación física.	Muy Alto (5)	PR.MA
Troncal SIP	Esencial para la comunicación sobre voz IP, por ende, se debe asegurar que las comunicaciones de voz deben estar operativas y accesibles para el personal interno de la empresa	La comunicación por VoIP puede integrar información sensible en tiempo real que deber estar protegida de escuchas no autorizados	Es de suma importancia garantizar que la comunicación por VoIP que se realice dentro, hacia el exterior y que provenga a la empresa, no sea interceptada ni modificada.	Media (3)	PR.DS
Troncal analógica	Importante para comunicaciones	Únicamente usuarios autorizados y para ciertos	Mantener en correcto estado la troncal	Media (3)	PR.DS, PR.PT

	tradicionales de voz dentro y fuera de la empresa, debido a que clientes conocen el número tradicional con el que inició la empresa	procesos deben poder acceder y modificar datos de la troncal, mediante la implementación de seguridad física.	analógica, evitando que ninguna persona modifique o intercepte los datos, debido a la susceptibilidad de las señales analógicas a interferencia o ruido.		
Infraestructura Wireless	La red debe mantener la operatividad y accesibilidad para las subredes dedicadas al personal, garantizando que todos los dispositivos puedan conectarse a la red en cualquier momento	Las redes inalámbricas deben estar protegidas ante posibles vulnerabilidades, únicamente el personal capacitado debe poder acceder o modificar los datos transmitidos a través de la red.	Los datos transmitidos a través de la red deben cifrarse para evitar la manipulación incorrecta de la información dentro de la empresa.	Alto (4)	PR.DS, PR.PT
Estaciones de trabajo	Disponibilidad de los computadores de las estaciones de trabajo en todo momento para garantizar la productividad continua del personal de la empresa y el funcionamiento de procesos empresariales	Protección de la información sensible que se maneja en las estaciones de trabajo, como datos de clientes o propiedad intelectual, de accesos no autorizados.	Garantizar que los datos almacenados y manipulados en las estaciones de trabajo no sean alterados de manera malintencionada o accidental, garantizando la confiabilidad de la información	Muy Alto (5)	PR. IP, PR.AC, PR.AT, PR.DS, PR.PT

Nota: Autoría propia a partir de entrevista con el líder del área de TIC'S. Adaptado de (CSF NIST, 2018)

3.3.4. *Inventario de amenazas y vulnerabilidades de los activos críticos*

En consecuencia, de las categorías y subcategorías identificadas por cada función según el CSF de la NIST, para continuar con el desarrollo de la evaluación, en una reunión con el jefe de área de TIC'S se identificaron las vulnerabilidades y amenazas más cruciales para los activos críticos de Nova Clínica Moderna ya identificados previamente e ilustrados en la Tabla 32, tomando únicamente como referencia un activo crítico para la identificación de amenazas y vulnerabilidades generales, debido a que en el apartado de identificación de riesgos se desglosara la información completa de todos los activos de la empresa.

Una vulnerabilidad se considera como una debilidad o fallo que puede poner en riesgo la seguridad de la información comprometiendo la disponibilidad, integridad o confidencialidad de estos activos ante terceros mal intencionados. Por otro lado, una amenaza se considera como la acción de sacar provecho a una vulnerabilidad para comprometer la seguridad de los ya mencionado activos. Para una mejor comprensión de la Tabla 30, se ha designado identificativos tanto para los activos, vulnerabilidades y amenazas de la siguiente manera; **Activo crítico:** (Ac), **Vulnerabilidad:** (V), **Amenaza:** (A). Y en cuanto al número de activo en relación con su vulnerabilidad y amenaza, se tiene como ejemplo lo siguiente; **Nº Vulnerabilidad y Nº Activo crítico:** V1 – Ac1, **Nº Amenaza y Nº Activo crítico:** A1 – Ac1.

Tabla 32

Posibles amenazas y vulnerabilidades de los activos críticos de la empresa

Activo crítico (Ac)	ID	Vulnerabilidad (V)	ID	Amenaza (A)
	V1 – Ac1	Cableado expuesto a daños físicos	A1 – Ac1	Daño accidental o intencional al cableado

Cableado Horizontal y Vertical	V3 – Ac1	Falta de protección contra sobrecargas eléctricas	A3 – Ac1	Daño por sobretensión eléctrica
	V5 – Ac1	Falta de etiquetado adecuado de los cables	A5 – Ac1	Dificultad en la identificación de los cables

3.3.5. Identificación de riesgos a partir de inventario de vulnerabilidades y amenazas

En esta etapa, el objetivo es identificar los riesgos con los activos que componen la infraestructura de la red de telecomunicaciones, así como analizar el entorno operativo para determinar la probabilidad de un incidente de ciberseguridad y posteriormente su impacto potencial en la organización.

El riesgo resulta de la identificación conjunta de una amenaza y una vulnerabilidad, este proceso utiliza el inventario de activos y el catálogo de vulnerabilidades y amenazas descritas en la sección anterior. En la Tabla 33, se identificaron los riesgos que más se relacionen al proceso de auditoría, que posteriormente serán evaluados para evitar su materialización, previniendo la pérdida de información o daños a los elementos físicos de la infraestructura de la red, así mismo, se evaluarán los riesgos debido a que pueden ser internos o externos, simples o complejos.

Tabla 33

Matriz de identificación de riesgos de activos críticos

Activo Crítico (Ac)	ID	Vulnerabilidad (V)	ID	Amenaza (A)	ID	Riesgo (R)
Cableado Horizontal y Vertical	V1 – Ac1	Cableado expuesto a daños físicos	A1 – Ac1	Daño accidental o intencional al cableado	R1-Ac1	Interrupción del servicio debido a daño físico en el cableado
	V2 – Ac1	Falta de protección contra sobrecargas eléctricas	A2 – Ac1	Daño por sobretensión eléctrica	R2-Ac1	Daños a Equipos Conectados por Sobretensión Eléctrica
	V3 – Ac1	Falta de etiquetado adecuado de los cables	A3 – Ac1	Dificultad en la identificación de los cables	R3-Ac1	Retrasos en el mantenimiento e identificación y solución de problemas
Fortinet Routers Firewall	V1 – Ac2	Parches de actualización no aplicadas	A1 – Ac2	Explotación de vulnerabilidades conocidas	R1-Ac2	Acceso no autorizado y robo de información
	V2 – Ac2	Puerto de administración expuesto	A2 – Ac2	Acceso no autorizado al puerto de administración	R2-Ac2	Modificación no autorizada de la configuración del firewall
	V3 – AC2	Falta de políticas de firewall no implementadas	A3 – Ac2	Manipulación sin restricciones de recursos de la red interna	R3-Ac2	Exposición y posible pérdida de datos críticos o

						confidenciales de la empresa
Conmutadores	V1 – Ac3	Falta de segmentación de la red	A1 – Ac3	Propagación de amenazas a través de la red	R1-Ac3	Propagación de malware o ataques a todos los segmentos de la red
	V2 – Ac3	Ausencia de autenticación de dispositivos	A2 – Ac3	Inserción de dispositivos no autorizados	R2-Ac3	Acceso no autorizado a la red y sistemas
	V3 – Ac3	Configuración por defecto no segura	A3 – Ac3	Acceso no autorizado a la red	R3-Ac3	Compromiso de la red y de los datos en transmisión
Equipos Servidores	V1 – Ac4	Falta de parches de seguridad	A1 – Ac4	Explotación de vulnerabilidades conocidas	R1-Ac4	Infiltración de terceros y pérdida de datos
	V2 – Ac4	Acceso físico no restringido al área de los servidores	A2 – Ac4	Acceso no autorizado a los servidores	R2-Ac4	Robo de información y daños físicos a los equipos
	V3 – Ac4	Configuración inadecuada de los permisos de archivos	A3 – Ac4	Modificación no autorizada de archivos	R3 -Ac4	Alteración de los sistemas y pérdida de integridad
Troncal SIP	V1 – Ac5	Configuración insegura del SIP	A1 – Ac5	Interceptación de las comunicaciones	R1-Ac5	Pérdida de confidencialidad de las comunicaciones
	V2 – Ac5	Falta de encriptación de las comunicaciones SIP	A2 – Ac5	Escucha ilegal de las	R2-Ac5	Manipulación de datos de voz

		comunicaciones SIP				
Troncal Analógica	V3 – Ac5	Implementación defectuosa de reglas de firewall	A3 – Ac5	Acceso no autorizado a los servicios SIP	R3-Ac5	Compromiso de la integridad del sistema de VoIP
	V1 – Ac6	Firmware desactualizado o corrupto	A1 – Ac6	Interrupción de las comunicaciones	R1-Ac6	Posible pérdida de conectividad y fallos en las comunicaciones
	V2 – Ac6	Ciclos extensos de mantenimiento del hardware	A2 – Ac6	Fallo de hardware durante el uso	R2-Ac6	Riesgo de interrupción del servicio y fallos operativos debido a la falta de mantenimiento.
Infraestructura Wireless	V1 – Ac7	Falta de autenticación adecuada por parte del personal	A1 – Ac7	Suplantación de identidad en las conexiones inalámbricas	R1-Ac7	Falsificación de Identidad en conexiones inalámbricas
	V2 – Ac7	Asignación defectuosa de privilegios para la red invitados	A2 – Ac7	Acceso no autorizado de usuarios invitados	R2-Ac7	Implantación de virus de manera remota
	V3 – Ac7	Mantenimiento insuficiente de hardware y actualización de firmware	A3 – Ac7	Posibles fallos mecánicos	R3-Ac7	Interrupción de Operaciones por Fallo Mecánico

Estaciones de trabajo	V1-A8	Mal uso de usuarios en las estaciones de trabajo	A1 – Ac8	Robo de credenciales	R1-Ac8	Acceso no autorizado a datos confidenciales o sistemas críticos
	V2-A8	Falta de reguladores de voltaje en estaciones de trabajo	A2 – Ac8	Daños permanentes en los componentes de hardware debido a variaciones de voltaje	R2-Ac8	Fallos mecánicos de los computadores afectando la continuidad del negocio
	V3-A8	Conexión de dispositivos USB	A3 – Ac8	Introducción de malware o robo de datos mediante dispositivos USB infectados	R3-Ac8	Perdida de información sensible a través de malware

Nota: Autoría propia a partir de mesa de trabajo con el líder de TIC'S de Nova Clínica Moderna

3.3.6. *Matriz de criterio de impacto y probabilidad*

Impacto y probabilidad son dos criterios esenciales en la gestión de riesgos que permiten evaluar y priorizar los riesgos potenciales en una organización. Al comprender estos conceptos, se puede gestionar de mejor manera la seguridad y la continuidad operativa.

Criterio de Impacto

El criterio de impacto se refiere a la gravedad de las consecuencias si un riesgo se materializa y se determina cuánto daño podría causar un evento no deseado a la organización. El impacto se suele clasificar en categorías cualitativas (bajo, medio, alto) o cuantitativas (escala de 1 a 5, por ejemplo). Un impacto alto indica consecuencias severas, como interrupciones significativas en las operaciones, disminución del rendimiento de la red o pérdida de reputación por parte de los clientes. En la Tabla 34, se ilustra de mejor manera el criterio de impacto que se adaptará posteriormente a la evaluación de riesgo de los activos críticos de la empresa.

Tabla 34

Criterios de impacto de amenazas de los activos críticos

Impacto	Nivel	Descripción
Operatividad	Crítico	Interrupción total de los servicios críticos de la red con la paralización de la operatividad.
	Alto	Interrupción severa de servicios críticos de la red por más de 24 horas
	Medio	Interrupción significativa de servicios críticos de la red entre 4 y 24 horas
	Bajo	Interrupción moderada de servicios críticos de la red entre 1 a 4 horas

	Irrelevante	Interrupción mínima de servicios críticos de la red por menos de 1 hora
Reputación	Crítico	Daño significativo a la reputación con repercusión nacional
	Alto	Daño significativo a la reputación con repercusión a nivel regional
	Medio	Daño significativo a la reputación con repercusión a nivel provincial
	Bajo	Daño significativo a la reputación con repercusión interno local
	Irrelevante	Daño insignificante sin repercusión externa
Rendimiento	Crítico	Disminución drástica del rendimiento operativo de la red, afectando su viabilidad en toda la empresa
	Alto	Disminución significativa del rendimiento operativo de la red, afectando múltiples áreas de la empresa
	Medio	Disminución moderada del rendimiento operativo de la red, afectando ciertas áreas específicas de la empresa
	Bajo	Disminución ligera del rendimiento operativo de la red con impacto limitado y recuperable con ajustes menores
	Irrelevante	Disminución irrelevante del rendimiento operativo de la red, fácilmente recuperable

Criterio de Probabilidad

El criterio de probabilidad se refiere a la posibilidad de que un riesgo se materialice, a su vez se entiende que es la frecuencia con la que se espera que ocurra un evento no deseado. En la Tabla 35 se evidencia que la probabilidad también se clasifica en categorías cualitativas (muy baja, baja, media, alta, muy alta) o cuantitativas (porcentajes o escalas numéricas). Una alta probabilidad indica que es muy probable que el evento ocurra en un futuro cercano.

Tabla 35

Criterios de probabilidad de amenazas de los activos críticos

Probabilidad	Descripción	Puntuación
Muy Alta	Es casi seguro que el evento ocurra (80% - 100%)	5
Alta	Probablemente el evento ocurra (60% - 80%)	4
Media	Puede ocurrir el evento en algún momento (40% - 60%)	3
Baja	Es poco probable que el evento ocurra (20% - 40%)	2
Muy Baja	Es improbable que el evento ocurra (0% - 20%)	1

La evaluación del impacto y la probabilidad se combina para determinar el nivel de riesgo total, y ayuda a priorizar los riesgos y tomar decisiones informadas sobre dónde enfocar los recursos y esfuerzos de mitigación.

3.3.7. Evaluación del nivel de riesgo de los activos críticos de la red de telecomunicaciones de Nova Clínica Moderna

En el apartado previo, se explicó que el impacto revela las consecuencias que se derivan cuando una amenaza se concreta. En la Ec.5, se explica como el nivel de riesgo se estima cuantitativamente, calculándose como el producto del impacto (es decir, las consecuencias) vinculado a una amenaza (evento), y la probabilidad de que dicha amenaza ocurra.

$$\mathbf{Nivel\ de\ Riesgo = Impacto * Probabilidad} \quad (5)$$

Por ende, se trata de estipular la gravedad del riesgo mediante el uso de una matriz de calor que se presentó previamente, donde se engloba la probabilidad e impacto, definiendo 4 zonas; zona de riesgo baja, moderada, alta y crítica. De acuerdo con (Cauja Altamirano, 2024), en la Tabla 36 se muestra la matriz de riesgos que permitirá comprender, según las zonas de calor, la zona del riesgo que más atención debe tener.

Tabla 36*Matriz de evaluación de riesgos*

Probabilidad		Impacto				
		Irrelevante	Bajo	Medio	Alto	Crítico
		1	2	3	4	5
Muy Alta	5	Moderado	Moderado	Alto	Extremo	Extremo
Alta	4	Bajo	Moderado	Alto	Extremo	Extremo
Media	3	Bajo	Moderado	Moderado	Alto	Extremo
Baja	2	Bajo	Bajo	Moderado	Alto	Extremo
Muy Baja	1	Bajo	Bajo	Moderado	Moderado	Alto

Zona de riesgo “Baja”: Aceptar el riesgo

Zona de riesgo “Moderada”: Evaluar posibilidad de asumir riesgo

Zona de riesgo “Alta”: Implementar estrategias de mitigación para reducir el riesgo

Zona de riesgo “Extrema”: Imprescindible reducir el riesgo a través de medidas robustas de mitigación.

Nota: Autoría propia. Adaptado de (Cauja Altamirano, 2024)

Este análisis se realiza de forma cualitativa, estableciendo una comparación que examina la probabilidad de que un riesgo ocurra en relación con su impacto. Así, se describe cómo identificar los riesgos utilizando niveles predeterminados de impacto y probabilidad.

El cálculo se efectuó multiplicando el valor de prioridad del criterio de evaluación por el valor de impacto asignado, seguido de la suma de estos valores. Finalmente, en la Tabla 37, se evidencia el resumen para cada activo crítico, identificando el riesgo más potencial, el criterio, e valor del impacto y la zona de riesgo a la que más se asemeja la cualificación.

Tabla 37

Tabla de evaluación del nivel de riesgo potencial de los activos críticos

Activo Crítico	Riesgo Potencial	Criterio De impacto	Probabilidad	Valor de Impacto	Puntuación	Zona de Riesgo
Cableado Horizontal y Vertical	Interferencia electromagnética Reducción significativa de la eficiencia en las comunicaciones y transferencia de datos.	Rendimiento	Baja (2)	Medio (3)	6	Moderado
	Conexiones no autorizadas. Percepción negativa de la empresa en cuanto a la seguridad de transmisión de datos.	Reputación	Baja (2)	Medio (3)	6	Moderado
	Fallo del Cableado Interrupciones en los servicios de red y la operatividad de los sistemas dependientes.	Operatividad	Baja (2)	Alto (4)	8	Alto
	Configuración defectuosa.	Rendimiento	Muy Baja (1)	Medio (3)	3	Moderado

Fortinet Routers Firewall	Exposición o posible acceso no autorizado a segmentos internos críticos de la red.					
	Políticas de firewall insuficientes frente a accesos a recursos y servicios no autorizados.	Reputación	Baja (2)	Alta (4)	8	Alto
	Saturación de recursos de router firewall. Retraso de actividades operativas de la red.	Operatividad	Muy Baja (1)	Medio (3)	3	Moderado
Conmutadores	Sobrecarga de Tráfico. Disminución de la velocidad de transferencia de datos.	Rendimiento	Baja (2)	Medio (3)	6	Moderado
	Intrusión en la Red mediante conexiones ethernet no autorizadas. Percepción de inseguridad en los servicios de la empresa.	Reputación	Baja (2)	Medio (3)	6	Moderado

	Fallo de los Conmutadores. Retraso de ejecución de servicios y operaciones de la red.	Operatividad	Baja (2)	Alto (4)	8	Alto
Equipos Servidores	Configuración defectuosa. Interrupciones y disminución de eficiencia de servicios.	Rendimiento	Baja (2)	Medio (3)	6	Moderado
	Brechas de Seguridad expuestas, debido a la exposición de acceso físico no autorizado al área de servidores.	Reputación	Baja (2)	Medio (3)	6	Moderado
	Interrupciones de Servicio. Paralización de operaciones dependientes de los servidores.	Operatividad	Baja (2)	Critico (5)	10	Extremo
Troncal SIP	Congestión de Red. Reducción en la calidad y velocidad de las comunicaciones de voz.	Rendimiento	Baja (2)	Medio (3)	6	Moderado

	Interceptación de Llamadas Percepción negativa de la seguridad de las comunicaciones.	Reputación	Baja (2)	Medio (3)	6	Moderado
	Interrupción del Servicio de Voz. Afectación de las operaciones que dependen de las comunicaciones de voz.	Operatividad	Baja (2)	Alto (4)	8	Alto
Troncal Analógica (FXO SIP Gateway)	Interferencias en la Comunicación.	Rendimiento	Media (3)	Bajo (2)	6	Moderado
	Reducción en la calidad de las llamadas.					
	Manipulación no Autorizada. Riesgo de daños, pérdida de conectividad y fallos en las comunicaciones	Reputación	Muy Baja (1)	Bajo (2)	2	Baja
	Fallo del Sistema de Comunicaciones. Paralización de servicios que	Operatividad	Baja (2)	Medio (3)	6	Moderado

	dependen de las comunicaciones telefónicas.					
Infraestructura Wireless	Interferencias de Señal inalámbrica. Interrupción de la red inalámbrica	Rendimiento	Baja (2)	Medio (3)	6	Moderado
	Falta de autenticación de usuarios en la red con posible pérdida de datos sensibles	Reputación	Baja (2)	Alto (4)	8	Alto
	Falta de mantenimiento de hardware y software de equipos. Afectación de operaciones que dependen de la conectividad inalámbrica.	Operatividad	Baja (2)	Medio (3)	6	Moderado
Estaciones de trabajo	Pérdida de conectividad debido a interrupciones en la red o por instalación de software malicioso que comprometa el	Rendimiento	Baja (2)	Medio (3)	6	Moderado

rendimiento de los computadores.

Acceso no autorizado a las estaciones de trabajo, fuga de datos sensibles debido falta de seguridad como contraseñas débiles o falta de autenticación en los computadores.

Reputación

Baja (2)

Alto (4)

8

Alto

Fallos de hardware debido a picos de voltaje o fallo de software que afecte la operatividad de las estaciones de trabajo.

Operatividad

Baja (2)

Medio (3)

6

Moderado

Nota: Autoría propia a partir de mesa de trabajo con el líder del área de TIC'S. Adaptado de (NIST, 2012)

4. CAPÍTULO IV. DESARROLLO DE POLÍTICAS Y PROPUESTA DE IMPLEMENTACIÓN

Para el desarrollo del siguiente capítulo se tiene como referencia los resultados obtenidos durante el proceso de auditoría de seguridad realizado a la red de telecomunicaciones de Nova Clínica Moderna, donde se elaborará un conjunto de políticas de seguridad en base al marco de ciberseguridad de la NIST, con enfoque en la función proteger establecido como parte de los objetivos específicos del presente proyecto.

4.1. Proceso para la creación de políticas de seguridad para la red de Nova Clínica Moderna

En base a (CSF NIST, 2018) para el proceso de elaboración de políticas de seguridad y adaptando las subfases de la metodología OCTAVE, se consideran las siguientes fases mostradas en la Tabla 38.

Tabla 38

Proceso para la elaboración de políticas de seguridad

Fase	Proceso	Descripción
1	Revisión de Normas y Estándares	Analizar las normativas y estándares relevantes (NIST Special Publications, etc.) que deben ser considerados para la elaboración de las políticas.
2	Resultados de evaluación de Riesgos	Tomar como referencia el resultado de evaluación de riesgos específicos de la infraestructura de la red de la organización.

3	Identificación de Necesidades Específicas	de Determinar las necesidades particulares de la red de la organización basadas en los resultados de la evaluación de riesgos.
4	Integración de Recomendaciones del CSF NIST	de Incorporar las recomendaciones del marco de ciberseguridad de NIST para el desarrollo de políticas robustas y efectivas.
5	Desarrollo de Políticas de Seguridad	de Redactar políticas de seguridad específicas que aborden las vulnerabilidades y amenazas identificadas.
6	Validación y Revisión de Políticas	de Analizar y verificar mediante una mesa de trabajo que las políticas desarrolladas brinden una proyección de mejora a futuro a la seguridad de la red de telecomunicaciones de la empresa.

Nota: Adaptado de (CSF NIST, 2018)

4.2. Diseño de políticas de seguridad

Para el desarrollo de las políticas de seguridad a la red de Telecomunicaciones de Nova Clínica Moderna, se tomó como referencia y guía las plantillas de políticas que brinda SANS Institute, teniendo como relevancia el desarrollo de las etapas de creación, revisión y propuesta de implementación que se socializara con el líder del área de TIC'S de Nova Clínica Moderna por lo que se presentan a detalle los datos informativos para comenzar con su elaboración.



Estamos aquí por su salud

Título:	Manual de políticas de seguridad para la red de Telecomunicaciones de Nova Clínica Moderna en base al marco de ciberseguridad de la NIST con enfoque en la función “Proteger”.	
Versión:	1.0	
Autor:	Marco Fabricio Latacumba Farinango	
Director de proyecto:	Ing. Fabián Geovanny Cuzme Rodríguez. Msc	
Beneficiario:	Área de TIC’S de Nova Clínica Moderna	
Dirección:	Víctor Gómez Jurado y Avenida Mariano Acosta, Ibarra, Ecuador	
Colaborador:	Líder de área de TIC’S de Nova Clínica Moderna	
Revisado por:	Tutor:	Fecha de revisión: 21-09-2024
	Líder de área de TICS:	Fecha de revisión: 26-09-2024
Aprobado por:	Directorio de Nova Clínica Moderna:	Fecha de aprobación:
Alcance:	Las siguientes políticas desarrolladas están sustentadas a partir del estudio de situación actual de la empresa auditada, así como también de la recopilación de fuentes bibliográficas	

	y del marco de ciberseguridad de la NIST; donde se considera el establecimiento de políticas con enfoque en aspectos generales de la organización, como también de la parte técnica para la infraestructura de la red y aplicaciones.
Aplicación:	Las políticas de seguridad desarrolladas se proponen a criterio de disponibilidad en caso de que la empresa lo requiera y esté al alcance de sus posibilidades para su implementación. Por otro lado, de no existir solución a ciertos problemas con las políticas de seguridad propuestas, el líder del área de TIC'S de la empresa tendrá la potestad para encontrar la solución del problema, además de modificar o anular estas políticas.
Glosario de Términos	
<p>Acceso: La capacidad de un usuario para interactuar con un sistema o recurso.</p> <p>ACL (Listas de Control de Acceso): Conjunto de reglas que definen qué usuarios o sistemas pueden acceder a ciertos recursos en una red.</p> <p>Autenticación: Proceso de verificar la identidad de un usuario o dispositivo.</p> <p>Autenticación de Dos Factores (2FA): Método que requiere dos formas de verificación para acceder a un sistema.</p> <p>Backup: Copia de seguridad de datos o sistemas para protegerlos ante pérdidas o daños.</p> <p>Cifrado: Proceso de convertir datos en un formato que solo puede ser leído por quienes tienen la clave.</p> <p>Confidencialidad: Garantía de que la información es accesible solo para quienes están autorizados.</p> <p>Control de Acceso: Políticas y mecanismos que limitan el acceso a los recursos.</p>	

Ciberseguridad: Prácticas y tecnologías diseñadas para proteger sistemas, redes y datos de ataques y accesos no autorizados.

Datos en Reposo: Información almacenada en un sistema que no está en uso activo.

Datos en Tránsito: Información que se está transmitiendo a través de una red.

Dispositivos Finales: Equipos que se utilizan para acceder a la red, como computadoras, teléfonos móviles y tabletas.

Firewall: Sistema de seguridad que controla el tráfico de red entrante y saliente.

Identificación: Proceso de reconocer a un usuario o dispositivo antes de permitir el acceso.

Integridad: Garantía de que los datos no han sido alterados o manipulados de manera no autorizada.

Intrusión: Acceso no autorizado a un sistema o red.

Malware: Software malicioso diseñado para causar daño o acceder a sistemas sin permiso.

Monitoreo: Proceso de supervisar sistemas y redes para detectar actividades sospechosas.

Privilegios de Acceso: Niveles de acceso otorgados a diferentes usuarios o grupos en un sistema.

Protocolo RADIUS: Protocolo para la autenticación, autorización y contabilización de acceso a redes.

Red VLAN (Red de Área Local Virtual): Segmento lógico de una red que permite separar el tráfico.

Resiliencia: Capacidad de un sistema para recuperarse de fallos o ataques.

Servidor LDAP: Protocolo de acceso a directorios que se utiliza para almacenar y gestionar información sobre usuarios y grupos.

TLS: Protocolos de seguridad que cifran datos transmitidos a través de la red.

VPN (Red Privada Virtual): Conexión segura que permite acceder a una red privada a través de Internet.

Vulnerabilidad: Debilidad en un sistema que puede ser explotada por un atacante.

Zabbix: Herramienta de monitoreo para supervisar la integridad y el rendimiento de la infraestructura tecnológica.

1. Seguridad General

Art. 1 El siguiente documento publica el manual de políticas de seguridad a la red de telecomunicaciones, con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de los recursos que componen la red de Nova Clínica Moderna, además de proteger la información confidencial de activos críticos, empleados, socios y clientes; de acciones ilegales o perjudiciales que pudieran llegar a afectar la operatividad, reputación y rendimiento de la red de la empresa.

Art. 2 El presente documento permite realizar un seguimiento para asegurar que las políticas de seguridad de la red de telecomunicaciones de la empresa sean establecidas, implementadas correctamente, y que se lleve a cabo su revisión y actualización conforme sea necesario.

Art. 3 El cumplimiento de las normas y procedimientos de este manual es obligatorio para todo el personal, por lo que son responsables de seguir los criterios de estas políticas y actuar conforme a los valores y lineamientos de seguridad de la información de la empresa.

Art. 4 Los sistemas relacionados con internet, intranet, extranet, en donde se incluyen equipos informáticos, cableado de red, software, hardware, dispositivos finales, etc. Pertenecientes a Nova Clínica Moderna, deben usarse con fines éticos y profesionales durante las operaciones diarias de la empresa.

Art. 5 La alta gerencia o delegados como talento humano, gestión de calidad en conjunto con el líder del área de TIC'S, serán los responsables y encargados de socializar y guiar al personal en el cumplimiento de las políticas de seguridad para conservar la operatividad de los activos críticos que componen la red de la empresa, en base a las directrices del estándar NIST Special Publication 800-50.

Art. 6 Se deberá tomar en cuenta o hacer partícipe al área de TIC'S, para la gestión de nuevos proyectos que se realicen dentro de la empresa, con el fin de analizar y evaluar posibles riesgos inherentes relacionados a la seguridad de la red de telecomunicaciones.

Art. 7 El área de TIC'S se encargará de capacitar al personal de la empresa por lo menos una vez cada año en cuanto a riesgos y amenazas de ciberseguridad emergentes, de esta manera mantendrá informado al personal sobre recomendaciones y buenas prácticas de ciberseguridad, en base a las directrices del estándar NIST Special Publication 800-16.

Art. 8 El área de TIC'S deberá realizar auditorías internas a la red periódicamente o en el caso de que pueda existir alguna modificación con la versión del documento del conjunto de políticas que se maneja actualmente.

2. Control y gestión de acceso a nivel físico

Art. 9 Asegurar el acceso a áreas restringidas donde se almacenen los activos críticos que componen la red de Telecomunicaciones de Nova Clínica Moderna (como Data Center, Salas de energía y UPS, armarios de distribución de telecomunicaciones, cableado horizontal y vertical, entre otros), mediante el uso de controles de acceso biométrico y cerraduras electrónicas las 24 horas del día brindando únicamente acceso a personal autorizado del área de TIC'S, en base a las directrices del estándar NIST Special Publication 800-116 Rev. 1.

Art. 10 En caso de que el líder del área de TIC'S se ausente de la empresa y se requiera el acceso de un delegado a dicha área, deberá notificar con mínimo de un día de anticipación mediante una solicitud formal de autorización firmada, misma que deberá ser aprobada por la alta gerencia de la empresa.

Art. 11 Para el acceso temporal de visitantes dentro de Nova Clínica Moderna, se deberá implementar la emisión de credenciales temporales y la supervisión constante de dichos visitantes por un contacto interno durante su permanencia en la empresa.

Art. 12 Se prohíbe realizar actos indebidos dentro del Data Center tales como tomar fotos de la zona, fumar, ingerir bebidas de cualquier tipo o realizar cualquier tipo de acto que pueda perjudicar la operatividad de los equipos que se encuentran dentro del Data Center.

Art. 13 En caso de que exista soporte, mantenimiento preventivo o correctivo de proveedores y personal externo para ciertos equipos tecnológicos de la empresa, se deberá comprobar las credenciales emitidas por Nova Clínica Moderna para el acceso a la empresa, a su vez el líder del área de TICS deberá supervisar en todo momento las actividades que realice dicho personal, además de dejar constancia de dicho soporte realizado en guías de servicio físicas o sistemas digitales, en base a las directrices del estándar NIST Special Publication 800-116 Rev. 1.

Art. 14 El Data Center deberá contar con un sistema de ventilación adecuado, un sistema de backup de energía, un sistema contra incendios, además de realizar mantenimientos periódicos para asegurar la integridad y disponibilidad de los equipos y servicios que se encuentran alojados dentro del Data Center, en base a las directrices del estándar NIST Special Publication 800-34 Rev. 1.

Art. 15 Implementar sistemas de videovigilancia y monitoreo en tiempo real dentro de la empresa para la supervisión constante del acceso a áreas restringidas.

Art. 16 La empresa debe mantener un registro detallado de las entradas y salidas a las áreas restringidas donde se almacenen los activos de telecomunicaciones, incluyendo la identificación de las personas y los tiempos de acceso.

3. Control y gestión de acceso a nivel lógico

Art. 17 El área de TIC'S estará encargado de gestionar formalmente la creación de perfiles, identificación de usuarios, contraseñas, claves de acceso y privilegios de acceso según el usuario correspondiente que este definido conforme a las funciones o cargos y políticas internas de la empresa, en base a las directrices del estándar NIST Special Publication 800-63B. Este proceso deberá tener validez y soporte desde su creación y registro inicial hasta su etapa de eliminación o desactivación en el caso de que ya no tenga ciertos tipos de acceso privilegiados o abandone la empresa.

Art. 18 Para todo el personal de Nova Clínica Moderna que requiera acceso mediante autenticación a los sistemas de información de la empresa u otros servicios críticos.

Deberán seguir el siguiente formato para la creación de nombres de usuario:

- Inicial del primer nombre
- Inicial del segundo nombre (En caso de homónimos)
- Primer apellido
- Inicial del segundo apellido

Ejemplo: Si el nombre completo es Marco Fabricio Latacumba Farinango, el nombre de usuario será: mflatacumbaf. En caso de existir similitud tanto con las iniciales del primer, segundo nombre, primer apellido e inicial del segundo apellido, se deberá colocar un número al final del nombre de usuario como distintivo y poder evitar confusiones con los nombres de usuario. Ejemplo: mflatacumbaf1, mflatacumbaf2, mflatacumbaf3, etc.

Art. 19 Las contraseñas de usuario del personal de Nova Clínica Moderna deben tener una longitud mínima de 8 caracteres y una mezcla de letras mayúsculas, minúsculas, números y caracteres especiales, en base a las directrices del estándar de la NIST Special Publication 800-63B.

Art. 20 Se debe limitar como máximo a 5 números de intentos de inicio de sesión con claves incorrectas a los sistemas información y demás servicios críticos que tenga acceso el personal de Nova Clínica Moderna.

Art. 21 En caso de que exista la necesidad del cambio de privilegios de usuario, deberá ser reportado y notificado al líder del área de TIC'S previamente autorizado por el área a cargo de regular este proceso.

Art. 22 Todos los perfiles de usuario y sus privilegios de la empresa serán revisados anualmente para asegurar que estén alineados con las responsabilidades actuales, aplicando y removiendo accesos innecesarios. Ante cambios de rol o bajas se deberá realizar una depuración a corto plazo, ajustando o desactivando accesos según el nivel de privilegio que se designe a dicho usuario.

Art. 23 El establecimiento de redes virtuales de área local (VLANs) debe basarse en las directrices del estándar de la NIST Special Publication 800-215, para cada área de Nova Clínica Moderna con el objetivo de limitar la comunicación entre ellas y garantizar que solo los usuarios autorizados puedan acceder a los recursos de su VLAN correspondiente.

Art. 24 El acceso a internet provisto a clientes y pacientes de Nova Clínica Moderna será asignada a una VLAN de invitados en otro puerto del router, garantizando que el tráfico de los usuarios externos esté aislado del tráfico de la red interna de la empresa, protegiendo así los servicios críticos y sistemas de información sensibles a accesos no autorizados.

Art. 25 La infraestructura Wireless y las conexiones Ethernet deben hacer uso del protocolo de autenticación IEEE 802.1X para los dispositivos de la red corporativa de la empresa y del protocolo RADIUS, en base a las directrices del estándar de la NIST Special Publication 800-53 Revision 5, para el proceso de verificación de credenciales del personal de Nova Clínica Moderna que acceda a la red corporativa donde se alojan los servicios críticos de la empresa con el fin de evitar accesos no autorizados.

Art. 26 El uso de 2FA (Autenticación de dos factores), en base a las directrices del estándar de la NIST Special Publication 800-63B, debe ser obligatorio para añadir una capa adicional de seguridad al requerir que el personal de la empresa proporcionen no solo sus credenciales, sino también un segundo factor de autenticación, como un dispositivo móvil mediante el uso de aplicaciones como (DUO, authenticator, entre otros), de esta forma conceder acceso a una cuenta, sistema de información o servicio crítico de la red.

Art. 27 Se deberá implementar Port Security, en base a las directrices del estándar de la NIST Special Publication 800-53 Revision 5, en los puertos de acceso de los conmutadores con el fin de proteger a la red empresarial contra accesos no autorizados, permitiendo un número limitado de direcciones MAC para los dispositivos finales.

Art. 28 Se deberá implementar Listas de control de acceso (ACLs) en el router de la empresa donde se manejan las VLANs para regular el tráfico entre las diferentes áreas, garantizando que el tráfico esté segmentado de forma lógica y que el acceso entre VLANs se controle exhaustivamente, protegiendo los recursos críticos y minimizando la posible propagación de posibles amenazas entre segmentos de la red.

Art. 29 El acceso a equipos y sistemas críticos mediante el uso del protocolo SSH debe realizarse en lo posible con llaves criptográficas para su autenticación, en base a las directrices de los estándares de la NIST Special Publication 800-57 Parte 1 y NIST

Special Publication 800-131A Revision 2, deshabilitando el uso de contraseñas para minimizar el riesgo de accesos no autorizados, garantizando una autenticación robusta en dichos sistemas críticos de la red empresarial.

Art. 30 Los servidores Linux deben tener configurado y habilitado reglas IPtables, en base a las directrices del estándar de la NIST Special Publication 800-41 Revision 1, para controlar y filtrar el tráfico de red de acuerdo con configuraciones de privilegio mínimo, limitando los intentos de conexión, restringiendo el acceso solo a los puertos y direcciones IP estrictamente necesarios.

Art. 31 Para todas las conexiones remotas que desee establecer el líder del área de TICS fuera de las instalaciones de la empresa a la red interna, deben realizarse a través de una conexión VPN, en base a las directrices del estándar de la NIST Special Publication 800-46 Revision 2, por lo que deberá ser configurada en el router firewall haciendo uso de la aplicación FortiToken Mobile y FortiClient VPN para la autenticación segura de la conexión siguiendo las directrices del Art. 26.

Art. 32 Para el servidor de VoIP (Elastix) y para el Gateway de VoIP analógico se deberá asignar extensiones con contraseñas personalizadas, siguiendo las directrices de los artículos 18 y 19, únicamente para el personal que haga uso del servicio de VoIP de la red empresarial.

Art. 33 Todo el tráfico de VoIP deber ser encaminado a través de una VLAN dedicada de voz configurada en el router dedicado al servicio de VoIP proporcionado por el proveedor de dicho servicio, por lo que estará aislada de las otras VLANs en la red empresarial.

Art. 34 Toda configuración de reglas de firewall en los servidores de VoIP (Elastix) y en el dispositivo FXO SIP Gateway debe realizarse manualmente, garantizando el control del tráfico y de la seguridad, en base a las directrices del estándar NIST SP 800-

41 Revision 1. Esto incluye bloquear accesos no autorizados, permitir únicamente conexiones y protocolos necesarios para el funcionamiento de VoIP, protegiendo los servicios contra amenazas y posibles ataques.

4. Protección de datos

Art. 35 Los algoritmos de cifrado simétrico deben seguir las directrices del estándar de la NIST Special Publication 800-131A Revision 2 con AES o parcialmente compatibles con dicho estándar de cifrado avanzado en la mayoría de los sistemas críticos de la empresa en su posibilidad para el cifrado de datos en reposo y en tránsito.

Art. 36 Los algoritmos de cifrado asimétrico deben seguir las directrices del estándar NIST Special Publication 800-131A Revision 2, en cuanto al uso de la criptografía RSA en la mayoría de los sistemas críticos de la empresa en su posibilidad para la protección de la confidencialidad, autenticidad e integridad de la información sensible.

Art. 37 La familia de algoritmos de HASH deberá ser implementada basándose en las directrices del estándar FIPS PUB 180-4 para la mayoría de los sistemas de información críticos de la empresa asegurando que todas las entradas de datos sean verificadas mediante un proceso de hashing seguro antes de su almacenamiento o transmisión.

Art. 38 Todos los servidores que utilicen protocolos criptográficos SSL/TLS deben hacer uso de certificados firmados por una autoridad de certificación (CA), en base a las directrices del estándar de la NIST SP 800-131A Revision 2.

Art. 39 Toda la información almacenada en la red empresarial deberá clasificarse según el nivel de sensibilidad o normativa aplicable: pública, interna, confidencial o restringida a la cual solo el personal con autorizaciones específicas podrá acceder, manejar o transferir dicha información.

Art. 40 La empresa deberá hacer uso de tecnologías Data Loss Prevention (DLP) para la protección de la información sensible en base a las directrices del estándar NIST Special Publication 800-122, a fin de prevenir fugas de datos y garantizar únicamente al personal autorizado el acceso a la información crítica que se maneje internamente, asegurando que las herramientas de DLP monitoreen, detecten y bloqueen cualquier intento no autorizado de transferir o compartir datos confidenciales fuera de la red corporativa, en cumplimiento con las políticas de seguridad y normativas de la empresa.

Art. 41 La implementación de una política de proxy en el router firewall de la empresa deberá basarse las directrices del estándar de la NIST Special Publication 800-41 Revision 1, lo que permitirá filtrar y bloquear el acceso a contenido inapropiado y no autorizado, incluyendo sitios web de pornografía, violencia, dark web o cualquier otro contenido que no se considere adecuado o productivo para el ambiente laboral.

Art. 42 Las reglas del IDS/IPS del router firewall FortiGate deberán ser actualizadas semestralmente para reflejar posibles amenazas emergentes y ante cualquier alerta generada será analizada por el área de TICS, asegurando el monitoreo continuo del tráfico para detectar y prevenir intrusiones a la red interna de la empresa.

Art. 43 La aplicación de WAF (Firewall de Aplicaciones Web) debe ser configurada y administrada dentro del router a fin de proteger las aplicaciones web de la empresa contra amenazas como inyecciones SQL, XSS, etc. Revisando regularmente sus registros para detectar actividades sospechosas y proteger la información confidencial de la empresa.

5. Gestión y monitoreo de activos

Art. 44 El área de TIC'S se encargará de inventariar de manera correcta los activos críticos de la red de telecomunicaciones, asegurando su adecuada clasificación, registro

y monitoreo, así como realizar chequeos periódicos para verificar el estado y la seguridad de dichos activos.

Art. 45 Todos los dispositivos de cómputo de las estaciones de trabajo de la empresa deben tener una licencia premium de antivirus y actualizada que asegure la protección de la información, realizando un escaneo periódico para confirmar que los archivos de los equipos de cómputo estén libres de virus y protegidos contra ataques de software o malware malicioso, en base a las directrices del estándar NIST Special Publication 800-53 Rev. 5.

Art. 46 El área de TIC'S será responsable de monitorear los equipos de red, sistemas de información, tráfico de red, anomalías y eventos con el fin de mantener la seguridad de la infraestructura tecnológica y de los recursos de la empresa.

Art. 47 Se debe implementar un sistema de monitorización de redes, diseñado para supervisar la integridad, el rendimiento y la disponibilidad de los recursos tecnológicos, incluyendo servidores, máquinas virtuales, aplicaciones, servicios, bases de datos y sitios web, en base a las directrices del estándar NIST Special Publication 800-137. Para la recolección de datos desde ciertos dispositivos de la red, se recomienda el uso SNMPv3, que proporcionan características mejoradas de seguridad y gestión de la información, garantizando así una supervisión efectiva y segura de la infraestructura tecnológica.

Art. 48 Con el fin de optimizar el rendimiento de la red inalámbrica y reducir interferencias, el área de TIC'S se encargará de realizar escaneos de frecuencia en los AP para minimizar conflictos con otras redes y dispositivos cercanos, además de aplicar mapeos de calor para evaluar la cobertura e intensidad de señal en distintas áreas de la empresa, garantizando una cobertura estable y segura.

Art. 49 El área de TIC'S gestionará y administrará los puertos lógicos de los equipos y servicios de la infraestructura tecnológica por lo que deberá realizar un censo de puertos completo a la LAN de la empresa con el fin de cerrar puertos de servicios que no estén en uso dentro de la red empresarial, asegurando que solo los puertos necesarios estén abiertos, en base a las directrices del estándar NIST Special Publication 800-41 Rev. 1.

Art. 50 De ser viable, se debe cambiar los números de puertos de servicios estándar a puertos no estándar o comunes. Esta práctica, aunque no debe considerarse una solución de seguridad, puede ayudar a ofuscar la vulnerabilidad de estos puertos conocidos ante atacantes.

Art. 51 Se debe mantener las versiones de software y hardware de los sistemas y servicios críticos en caso de que estas no soporten una actualización o mantenimiento debido a propiedades y características específicas con las actualmente opera la empresa. De no ser el caso, se deberá tener actualizado el software y hardware en lo posible a las versiones más actuales de los equipos y dispositivos que conforma la infraestructura tecnológica de la empresa, en base a las directrices del estándar NIST Special Publication 800-40 Rev. 4.

Art. 52 El área de TIC'S será responsable de gestionar el control de las instalaciones de software en los equipos de la red de la empresa. En caso de que existan nuevas versiones de software, se deberá realizar pruebas de actualización para validar el correcto funcionamiento y operatividad de los sistemas y servicios críticos de la red.

Art. 53 Cuando la empresa necesite adquirir recursos tecnológicos (software o hardware) de proveedores externos, se deberá constatar que sean avalados y certificados por empresas y compañías registradas en el mercado tecnológico nacional

e internacional. Además de tener la autorización de las autoridades competentes de Nova Clínica Moderna y el aval técnico del área de TIC'S.

Art. 54 Para el entorno clínico y las exigencias de conectividad y rendimiento, se debe adoptar los estándares ANSI/TIA-568.2-D, que ofrecen especificaciones mejoradas para cableado seguro y de alta velocidad, y ISO/IEC 11801, que se enfoca en la infraestructura de cableado para edificios y entornos industriales.

Art. 55 La infraestructura del data center de Nova Clínica Moderna debe cumplir con estándares TIER II proporcionando redundancia en componentes críticos como UPS, generadores de respaldo, sistemas de enfriamiento y almacenamiento de datos, garantizando una disponibilidad del 99.741%. El diseño debe alinearse con las certificaciones internacionales de mejores prácticas de resiliencia definidas por el TIA-942 para entornos de salud.

Art. 56 Todas las estaciones de trabajo deben contar con reguladores de voltaje o unidades de suministro ininterrumpido (UPS) para mitigar los efectos de picos y fluctuaciones de voltaje que puedan dañar los equipos o afectar la continuidad de operaciones en la empresa, en base a las directrices del estándar ISO/IEC 27002.

Art. 57 Las estaciones de trabajo deben mantener un correcto orden del cableado proveniente de los armarios de telecomunicaciones, de esta manera se evitará los riesgos de daños físicos ocasionados por agua, residuos, polvo, interferencias electromagnéticas, con el objetivo de garantizar la seguridad del funcionamiento de las estaciones de trabajo.

6. Al personal de Nova Clínica Moderna

Art. 58 La información generada y almacenada en los sistemas y servicios críticos de Nova Clínica Moderna que contengan información confidencial tanto de la empresa como de clientes, debe ser manejada con total responsabilidad y confidencialidad,

cumpliendo la normativa vigente y no debe ser divulgada por ningún motivo a terceros a menos que la ley lo solicite.

Art. 59 Todo el personal de Nova Clínica Moderna está obligado a notificar o reportar de manera inmediata al área de TIC'S sobre cualquier tipo de actividad inusual o evento sospechoso de seguridad que se detecte en sus estaciones de trabajo.

Art. 60 El personal de la empresa será responsable de salvaguardar los activos de la red que estén bajo su supervisión y deberá reportar de inmediato cualquier tipo de riesgo relacionado con el robo, pérdida o divulgación no autorizada de la información de los recursos pertenecientes a la empresa.

Art. 61 En caso de detectar la presencia de malware o cualquier tipo de virus en algún dispositivo de las estaciones de trabajo, el personal de Nova Clínica Moderna deberá notificar al área de TIC'S y desconectar de inmediato el equipo de la red corporativa, incluyendo cables y conexiones inalámbricas, para prevenir su propagación. Posteriormente, el equipo afectado deberá permanecer aislado hasta que el área de TIC'S realice un análisis exhaustivo, identifique la amenaza y aplique medidas de recuperación y protección necesarias.

Art. 62 El personal de Nova Clínica Moderna deberán mantener de manera responsable y confidencial el mecanismo de control de acceso a los servicios informáticos (Usuario/Contraseña) brindados por parte del área de TIC'S, cumpliendo el reglamento interno.

Art. 63 Bajo ninguna circunstancia, el personal de la empresa deberá exponer a la vista pública las credenciales de acceso a los sistemas y servicios críticos de la red, ya sea mediante notas en monitores, escritorios, paredes u otros lugares visibles, a fin de preservar la seguridad y confidencialidad de la información.

Art. 64 En caso de que un usuario del personal de Nova Clínica Moderna olvide su contraseña o bloquee su cuenta de acceso a alguno de los sistemas de información, deberá notificar al área de TIC'S para su posterior asignación de una clave nueva o desbloqueo de cuenta.

Art. 65 En caso de que un usuario del personal necesite el uso de un dispositivo nuevo dentro de la empresa y quiera acceder a la red que conecta con los sistemas informáticos, deberá notificar previamente al líder de área de TIC'S para su previa revisión y aprobación de ingreso del nuevo dispositivo.

Art. 66 En caso de daño, pérdida o robo de un equipo perteneciente a la infraestructura de telecomunicaciones de la empresa, el personal afectado deberá notificar de manera inmediata al área de TICS, a fin de que se tomen las respectivas medidas correctivas necesarias y se garantice la seguridad de la red y los recursos corporativos.

Art. 67 Los dispositivos móviles y computadores portátiles de los empleados deberán tener un sistema operativo con licencia válida, además deberán estar actualizados y parchados a sus versiones más actualizadas en el caso que deseen integrar estos dispositivos a la red de Nova Clínica Moderna, con previa revisión y autorización del líder del área de TICS, caso contrario estos dispositivos podrán acceder únicamente a la red de invitados con privilegios mínimos.

Art. 68 El uso del correo electrónico empresarial debe ser usado únicamente para fines profesionales acorde a la función designada, que beneficien a Nova Clínica Moderna, manteniendo la ética y moral que caracteriza a la empresa.

Art. 69 Todo el personal de Nova Clínica Moderna deberá informar de inmediato al área de TICS si recibe correos electrónicos no deseados, sospechosos o que soliciten información personal o confidencial, con el fin de prevenir posibles fraudes o estafas atentando contra la protección de la seguridad de la información de la empresa.

Art. 70 El personal de Nova Clínica Moderna tiene prohibido el uso del correo electrónico empresarial para el envío, recepción o distribución de con contenido impropio, difamatorio, ilícito o que infrinja cualquier normativa interna de la empresa. Caso contrario, la autoridad competente tomará las medidas disciplinarias correspondientes, incluyendo, pero no limitándose a sanciones laborales sujetas al reglamento interno, si fuese necesario.

Art. 71 El personal de Nova Clínica Moderna deberá comunicar a los usuarios que la información referente a los servicios y productos que oferta clínica está disponible únicamente a través de los canales oficiales designados por la empresa, como sitio web, redes sociales autorizadas y cualquier otro medio de comunicación previamente aprobado, asegurando que los clientes reciban únicamente información precisa y verificada sobre los servicios de la empresa.

Art. 72 El personal de Nova Clínica Moderna que tenga la responsabilidad de adquirir, recibir o manejar datos personales de los clientes que vayan a hacer uso de los servicios de la empresa, deberá asegurarse que dichos clientes firmen previamente un acuerdo de autorización o consentimiento para el uso y tratamiento de sus datos personales conforme a la ley de protección del Ecuador, además de especificar los fines para los cuales se utilizará dicha información garantizando siempre los principios contemplados en dicha ley.

4.3. Procedimiento para implementación de políticas de seguridad como propuesta a Nova Clínica Moderna en base al marco de ciberseguridad de la NIST englobando la Metodología OCTAVE

Una vez se ha desarrollado el conjunto de políticas de seguridad, se procede a desarrollar una serie de pasos para seguir una ruta de procedimientos para la implementación de políticas en base al marco de ciberseguridad de la NIST.

- 1. Priorización y alcance:** La empresa definirá sus objetivos y prioridades más importantes, con esta información, se tomará decisiones estratégicas sobre la implementación de medidas de ciberseguridad y se determina el alcance de los sistemas y activos que respaldan las operaciones empresariales.
- 2. Orientación:** La empresa debe identificar los sistemas y activos críticos que componen su red, así como los requisitos normativos y el enfoque de riesgo general. Posteriormente, consulta múltiples fuentes bibliográficas para identificar las amenazas y vulnerabilidades que podrían afectar esos sistemas y activos críticos.
- 3. Perfil actual y perfil deseado:** Inicialmente la empresa desarrolla un perfil actual que especifica cuales resultados de categorías y subcategorías del núcleo del marco se tiene alcanzado hasta la fecha actual, lo que proporcionará una base de referencia para futuros procesos de aplicación. Luego, la empresa crea un perfil objetivo, con el fin de evaluar las categorías y subcategorías del marco que definen los resultados deseados en ciberseguridad, considerando también el apoyo de las partes interesadas dentro de la empresa, como también partes externas, clientes, socios empresariales, etc.

- 4. Evaluación de riesgos:** Es posible guiarse por el proceso de gestión de riesgos de la organización o por actividades anteriores de evaluación de riesgos. La organización examina su entorno operativo para determinar la probabilidad de un incidente de ciberseguridad y su posible impacto. Es importante que la empresa identifique riesgos emergentes y esté al tanto de información sobre amenazas de ciberseguridad, tanto internas como externas, para comprender mejor el riesgo asociado con posibles eventos de seguridad cibernética.
- 5. Determinar, analizar y priorizar brechas:** La empresa evaluará las diferencias entre su perfil actual y su perfil objetivo para identificar la brecha de alcance para el mejoramiento de seguridad de la red. Posteriormente, se desarrolla un plan de acción priorizando cubrir las brechas de seguridad encontrados, considerando factores como costos, beneficios, etc. La empresa deberá identificar los recursos necesarios, como financiamiento y personal de apoyo para poder implementar el plan, por lo que los perfiles facilitaran decisiones para implementar planes sobre actividades de ciberseguridad y la gestión de riesgos.
- 6. Implementar un plan de acción:** Finalmente la empresa decide qué medidas seleccionar para dar solución o soporte a las brechas identificadas y adapta sus prácticas de ciberseguridad actuales para alcanzar el perfil objetivo, basándose en referencias informativas que brinda el marco de ciberseguridad, pero la empresa deberá seleccionar las normas, directrices y prácticas específicas que mejor se adapten a sus necesidades. De esta manera se engloba procedimientos y buenas prácticas de ciberseguridad en la empresa con el soporte de políticas que protejan la red de telecomunicaciones y sus principales activos críticos.

4.4. Manual de procedimientos de seguridad a la red de Telecomunicaciones de Nova Clínica Moderna

Como parte adicional del proceso de elaboración del conjunto de políticas de seguridad a la red de telecomunicaciones de Nova Clínica Moderna, se realiza el desarrollo y propuesta de los siguientes manuales de procedimientos de seguridad con instrucciones y procesos que la empresa debe establecer para alcanzar un nivel objetivo adecuado de seguridad detallando los pasos específicos a seguir para proteger sus activos críticos de la red, incluyendo también la protección del personal.

4.4.1. Manual de procedimientos para la protección de datos sensibles

	Manual de procedimientos de seguridad para la red de telecomunicaciones de Nova Clínica Moderna	
Versión:	1.0	
Autor:	Marco Fabricio Latacumba Farinango	
Director de proyecto:	Ing. Fabián Geovanny Cuzme Rodríguez. Msc	
Beneficiario:	Área de TIC'S de Nova Clínica Moderna	
Dirección:	Víctor Gómez Jurado y Avenida Mariano Acosta, Ibarra, Ecuador	
Colaborador:	Líder de área de TIC'S de Nova Clínica Moderna	
Revisado por:	Tutor:	Fecha de revisión:
		21-09-2024
	Líder de área de TICS:	Fecha de revisión:

		24-10-2024
Nombre:	Procedimiento para la protección de datos sensibles	
Objetivo:	Garantizar la confidencialidad, integridad y disponibilidad de los datos críticos y personales que disponga la empresa en base a los principios de la ley orgánica de protección de datos personales del Ecuador.	
Alcance:	El siguiente manual establece las pautas para proteger los datos sensibles, definiendo medidas de seguridad para su almacenamiento, manejo y acceso, con el fin de asegurar su confidencialidad y evitar filtraciones.	
1.	Realizar la identificación, clasificación y protección de datos sensibles y críticos dentro de la empresa mediante la implementación de un sistema DLP (Data Loss Prevention).	
2.	Implementar el cifrado de datos en tránsito y en reposo para los datos críticos de la empresa.	
3.	Establecer controles para el acceso a datos sensibles, garantizando que solo el personal autorizado de la empresa pueda acceder a la información crítica en base al formato el Anexo 17.	
4.	Realizar auditorías periódicas de las actividades del personal de la empresa entorno a la correcta manipulación de los datos sensibles de los sistemas de información de la empresa.	
5.	Asegurar el consentimiento adecuado tanto de los clientes como de los empleados de la empresa para la recopilación y el	

	uso de sus datos personales mediante acuerdos de confidencialidad dentro de la organización.
6.	Capacitar a empleados de la empresa sobre las mejores prácticas de la protección y privacidad de datos sensibles.
7.	Revisar y actualizar regularmente las políticas de protección de los datos críticos para asegurar su efectividad y cumplimiento.

4.4.2. Manual de procedimiento para la gestión de vulnerabilidades e incidentes de ciberseguridad

	Manual de procedimientos de seguridad para la red de telecomunicaciones de Nova Clínica Moderna	
Versión:	1.0	
Autor:	Marco Fabricio Latacumba Farinango	
Director de proyecto:	Ing. Fabián Geovanny Cuzme Rodríguez. Msc	
Beneficiario:	Área de TIC'S de Nova Clínica Moderna	
Dirección:	Víctor Gómez Jurado y Avenida Mariano Acosta, Ibarra, Ecuador	
Colaborador:	Líder de área de TIC'S de Nova Clínica Moderna	
Revisado por:	Tutor:	Fecha de revisión: 21-09-2024
	Líder de área de TICS:	Fecha de revisión: 24-10-2024

Nombre:	Procedimiento para la gestión de vulnerabilidades
Objetivo:	Identificar, evaluar y encontrar posibles soluciones a vulnerabilidades de seguridad en los sistemas, aplicaciones y recursos físicos de la red de la empresa
Alcance:	Establecer procedimientos para identificar, evaluar y gestionar vulnerabilidades e incidentes de ciberseguridad, asegurando una respuesta efectiva y documentación adecuada.
Actividad	Descripción
1.	Definir a la persona encargada de autorizar y verificar la documentación acerca de la gestión de vulnerabilidades en sistemas de información, aplicaciones, dispositivos de la empresa elaborada por el área de TIC'S de Nova Clínica Moderna.
2.	Realizar escaneos periódicos de vulnerabilidades de sistemas y aplicaciones críticos de la red.
3.	Evaluar el impacto y posible probabilidad en caso de que existan vulnerabilidades en la red.
4.	Priorizar las vulnerabilidades para su corrección basado en su nivel de criticidad.
5.	Documentar y reportar las vulnerabilidades encontradas y las posibles acciones a ejecutar para poder prevenirlas o mitigarlas, siguiendo el formato del Anexo 16.
6.	Colaborar con proveedores externos y profesionales en el área de ciberseguridad para garantizar el tiempo de solución de los riesgos

	de las vulnerabilidades encontradas en la red de la empresa, siguiendo el tiempo estimado en el Anexo 15.
7.	Estar actualizado con amenazas emergentes y vulnerabilidades reportadas de fuentes bibliográficas y publicaciones que puedan afectar los recursos de la red de la empresa
8.	Capacitar al personal técnico y demás personal de la empresa en la identificación y remediación de posibles vulnerabilidades encontradas en la red de la organización.

4.4.3. *Manual de procedimientos técnicos para la seguridad de la red*

	Manual de procedimientos de seguridad para la red de telecomunicaciones de Nova Clínica Moderna	
Versión:	1.0	
Autor:	Marco Fabricio Latacumba Farinango	
Director de proyecto:	Ing. Fabián Geovanny Cuzme Rodríguez. Msc	
Beneficiario:	Área de TIC'S de Nova Clínica Moderna	
Dirección:	Víctor Gómez Jurado y Avenida Mariano Acosta, Ibarra, Ecuador	
Colaborador:	Líder de área de TIC'S de Nova Clínica Moderna	
Revisado por:	Tutor:	Fecha de revisión: 21-09-2024
	Líder de área de TICS:	Fecha de revisión:

		24-10-2024
Nombre:	Procedimientos técnicos para la seguridad de la red	
Objetivo:	Proteger la infraestructura de la red de la empresa contra accesos no autorizados, ataques y otros riesgos de seguridad.	
Alcance:	Definir procedimientos técnicos para garantizar la seguridad de la red, incluyendo configuraciones de firewall, gestión de acceso, monitoreo de tráfico y protección ante incidentes en la red.	
Actividad	Descripción	
1.	Definir a la persona encargada de autorizar y verificar la documentación acerca de la protección de la seguridad de la red elaborada por el área de TIC'S de Nova Clínica Moderna.	
2.	En base a auditorías internas realizadas previamente analizar y definir cuál de las soluciones cumplen con los requisitos que más se adaptan a la protección de la seguridad de la red de la empresa	
3.	Realizar la solicitud y recibir la aprobación para la ejecución de los procesos técnicos de protección para la seguridad de la red de la empresa, siguiendo el formato del Anexo 14.	
3.1.	Implementar segmentación de red para limitar el acceso entre diferentes segmentos mediante el uso de VLANS distribuidas estratégicamente por departamentos o secciones de la empresa.	

3.2.	Implementar Port Security en los puertos de los conmutadores que conecten con los servicios críticos de la empresa, limitando el número de direcciones MAC de las estaciones de trabajo.
3.3.	Utilizar métodos de autenticación y cifrado robusto para redes inalámbricas (WPA3, RADIUS) y autenticación 802.1X tanto para conexiones inalámbricas como para conexiones ethernet.
3.4.	Uso de factor de autenticación de 2 pasos (2FA) para los usuarios que se autenticuen y que hagan uso de aplicaciones y servicios críticos de la red empresarial.
3.5.	Establecer servidor de monitoreo de la red para registrar y notificar el estado de los parámetros y servicios de la red, servidores, conmutadores, routers y hardware de red.
3.6.	Uso de redes privadas virtuales (VPN) IPsec para el acceso remoto seguro fuera de la red hacia la red interna de la empresa.
3.7.	Implementar políticas de proxy transparente para la red, excluyendo el acceso a sitios web con categorías y contenido inapropiado.
3.8.	Implementar el acceso remoto SSH haciendo uso de claves criptográficas, mejor conocido como autenticación SSH basada en claves.
3.9.	Implementación de certificados digitales SSL/TLS emitidos por parte de una autoridad certificadora autorizada, en servicios web.
3.10.	Configuración de WAF (Firewall de aplicaciones web) en routers Fortigate para la protección de aplicaciones web para filtrar y monitorear el tráfico HTTP, bloqueando ataques como inyecciones SQL, cross-site scripting (XSS), entre otros exploits.

3.11.	Mantener la actualización del firmware de la mayoría de los dispositivos de la red y aplicar parches de seguridad.
4.	Verificar que las soluciones técnicas mejoren la protección y operatividad de la red a comparación a procesos anteriores.
5.	Realizar un informe detallado de las soluciones aplicadas a la red para la documentación final del manual de procedimientos técnicos.

4.4.4. Manual de procedimientos para el control de acceso a los recursos de información críticos

	Manual de procedimientos de seguridad para la red de telecomunicaciones de Nova Clínica Moderna	
Versión:	1.0	
Autor:	Marco Fabricio Latacumba Farinango	
Director de proyecto:	Ing. Fabián Geovanny Cuzme Rodríguez. Msc	
Beneficiario:	Área de TIC'S de Nova Clínica Moderna	
Dirección:	Víctor Gómez Jurado y Avenida Mariano Acosta, Ibarra, Ecuador	
Colaborador:	Líder de área de TIC'S de Nova Clínica Moderna	
Revisado por:	Tutor:	Fecha de revisión: 21-09-2024
	Líder de área de TICS:	Fecha de revisión: 24-10-2024
Nombre:	Procedimiento para el control de acceso a los recursos de información críticos.	

Objetivo:	Establecimiento de medidas de protección para garantizar únicamente el acceso de usuarios autorizados a sistemas de información y datos críticos de la red
Alcance:	El siguiente manual define el control de acceso seguro a los recursos de información críticos mediante políticas de autenticación y autorización, protegiendo la confidencialidad e integridad de los recursos tecnológicos.
Actividad	Descripción
1.	Definir a la persona encargada de autorizar y verificar la documentación acerca de la administración de identidades y accesos elaborada por el área de TIC'S de Nova Clínica Moderna.
2.	Realizar un control de registro del personal interno o externo que accede al área y recursos de TIC'S de la empresa en base al formato del Anexo 18.
3.	Realizar auditorías periódicas para revisar cuentas de usuarios activas y sus privilegios, pertenecientes al personal de la empresa.
4.	Asegurar la asignación necesaria de privilegios a los usuarios de la empresa que hagan uso principalmente de los sistemas de información y datos críticos de la red para realizar sus funciones operativas, en base a los formatos de los Anexos 11 y 12.
5.	Realizar el proceso de revocación de accesos de usuarios cuando un empleado cambie de rol o abandone la empresa, además de llevar un control detallado de equipos prestados fuera de la empresa siguiendo el formato del Anexo 13.

6.	Revisar y actualizar periódicamente las políticas de gestión de acceso para acoplarse a nuevas amenazas y vulnerabilidades en la red.
7.	Realizar capacitaciones periódicas para todos los empleados sobre la importancia y necesidad de la gestión de accesos y mejores prácticas dentro de la empresa.
8.	Establecer un procedimiento para informes de reportes y gestión de incidentes de seguridad relacionados a accesos no autorizados.

4.5. Simulación de soluciones técnicas propuestas dentro de las políticas de seguridad a la red de Telecomunicaciones de Nova Clínica Moderna

En el siguiente apartado se demuestra en simulación las políticas técnicas; Art. 23, Art. 25, Art. 26, Art. 27, Art. 29, Art. 30, Art. 31, Art. 34, Art. 38, Art. 41 y Art. 46 como parte del proceso de verificación de políticas técnicas en entornos controlados (GNS3), asemejando y simulando en lo posible, la mayor parte de dispositivos y equipos que conforman la red de Telecomunicaciones de Nova Clínica Moderna, con el objetivo de demostrar que dichas políticas técnicas propuestas anteriormente, buscan optimizar y reforzar la seguridad de la red empresarial, garantizando la protección de los datos sensibles y la seguridad operativa del sistema ante posibles amenazas o vulnerabilidades.

4.5.1. *Direccionamiento lógico de VLANs*

En base a las directrices que recomienda seguir el estándar de la NIST Special Publication 800-115, se realiza la creación de 9 VLANs en el router firewall FortiGate en base a las áreas operativas de Nova Clínica Moderna haciendo uso de VLSM (Variable Length Subnet Mask) con el fin de optimizar el uso de direcciones IP, evitando el desperdicio de espacio de red, facilitando al administrador la implementación de medidas de seguridad y la contención de broadcast de la LAN. Para llevar a cabo este proceso de segmentación, se ha tomado en cuenta el número de hosts usados actualmente por cada área, además de la reserva de espacio en cada subred para la inclusión de futuros hosts, garantizando así la escalabilidad y flexibilidad de la red a largo plazo.

Para poder segmentar la red para las 9 VLANs se realizó subnetting a partir de la dirección IPv4 clase C 192.168.0.0/24, en la Tabla 39 se toma la siguiente analogía matemática donde; según el número de hosts actuales por área, se adapta la subred con su máscara para que abarque las direcciones IPv4 y tenga disponibilidad para el ingreso de más dispositivos a futuro, además se hace la analogía porcentual actual de uso de cada subred y el porcentaje disponible para dichas asignaciones de futuras direcciones IP.

Tabla 39

Analogía porcentual para la asignación de subred de cada VLAN de Nova Clínica Moderna

ID VLAN	NOMBRE	N° Hosts actuales	Red	Porcentaje de uso actual de direcciones IPv4	N° Hosts disponibles a futuro	Porcentaje disponible para futuros hosts
10	ATENCIÓN CRÍTICA Y HOSPITALARIA	40	192.168.0.0/26	64,51%	22	35,49%
20	DIAGNÓSTICO Y APOYO	20	192.168.0.64/27	66,66%	10	33,34%
30	COMERCIAL	13	192.168.0.96/27	43,33%	17	56,67%
40	TICS	10	192.168.0.128/27	33,33%	20	66,67%
50	COBRANZA – FACTURACIÓN	10	192.168.0.160/27	33,33%	20	66,67%
60	CONTABILIDAD	5	192.168.0.192/28	35,71%	9	64,29%
70	SSO A	2	192.168.0.208/29	33,33%	4	66,67%

80	TALENTO HUMANO	1	192.168.0.216/29	16,66%	5	83,34%
90	MANTENIMIENTO Y HOTELERIA HOSPITALARIA	1	192.168.0.224/29	16,66%	5	83,34%

Por ende, en la Tabla 40 se detalla el ID de la VLAN, el número de hosts disponibles, IP de red, máscara de red, primer host, último host y dirección de broadcast.

Tabla 40

Levantamiento de subredes para la red de Nova Clínica Moderna.

VLAN	Hosts disponibles	IP de subred	Máscara	1er Host	Último Host	Broadcast
10	64	192.168.0.0/26	255.255.255.192	192.168.0.1	192.168.0.62	192.168.0.63
20	30	192.168.0.64/27	255.255.255.224	192.168.0.65	192.168.0.94	192.168.0.95
30	30	192.168.0.96/27	255.255.255.224	192.168.0.97	192.168.0.126	192.168.0.127
40	30	192.168.0.128/27	255.255.255.224	192.168.0.129	192.168.0.158	192.168.0.159
50	30	192.168.0.160/27	255.255.255.224	192.168.0.161	192.168.0.190	192.168.0.191
60	14	192.168.0.192/28	255.255.255.240	192.168.0.193	192.168.0.206	192.168.0.207
70	6	192.168.0.208/29	255.255.255.248	192.168.0.209	192.168.0.214	192.168.0.215
80	6	192.168.0.216/29	255.255.255.248	192.168.0.217	192.168.0.222	192.168.0.223
90	6	192.168.0.224/29	255.255.255.248	192.168.0.225	192.168.0.230	192.168.0.231

De esta manera la segmentación de la red mediante VLANs fortalece la seguridad de la red al aislar el tráfico entre subredes lógicas, limitando el acceso no autorizado y reduciendo el riesgo de propagación de ataques. Además de permitir aplicar políticas de seguridad en el router firewall específicas a cada segmento, mejorar el control de acceso, la detección de anomalías y una respuesta más rápida ante incidentes, así optimizando y protegiendo los recursos críticos de la red empresa.

4.5.2. Port Security

En base al estándar de la NIST Special Publication 800-53 Revision 5 y siguiendo las recomendaciones y directrices, se tiene como política técnica demostrada en simulación; Port Security en un switch versión ArubaOS-CX Virtual.10.10.1000, siendo un mecanismo importante para el fortalecimiento de la seguridad de la red, permitiendo el control y protección de puertos de los conmutadores a frente a accesos no autorizados, restringiendo el número de dispositivos que pueden llegar a conectarse a un puerto en

específico, además de limitar el número de direcciones MAC autorizadas y bloqueando aquellas que no estén registradas.

En la Figura 19, se demuestra la implementación de port security en la interfaz 1/1/5 misma a la que se ha designado como puerto de acceso para la VLAN 10 (Atención crítica y hospitalaria), además de limitar el acceso a 2 clientes (client-limit 2) estáticos por medio de su MAC address ingresadas manualmente, para la demostración se hizo uso de un cliente Windows 10 y un VPC de GNS3.

Figura 19

Habilitación de Port Security en la interfaz 1/1/5 y asignación de direcciones MAC manualmente

```

interface 1/1/5
  no shutdown
  no routing
  vlan access 10
  port-access port-security
  enable
  client-limit 2
  mac-address 00:50:79:66:68:01
  mac-address 0c:1a:7a:2c:00:00

```

```

Port Security Client Status Details
-----
Authorized-Clients  Type  Port
-----
0c:1a:7a:2c:00:00   static  1/1/5
00:50:79:66:68:01   static  1/1/5
switch# show port-access port-security interface 1/1/5 port-statistics

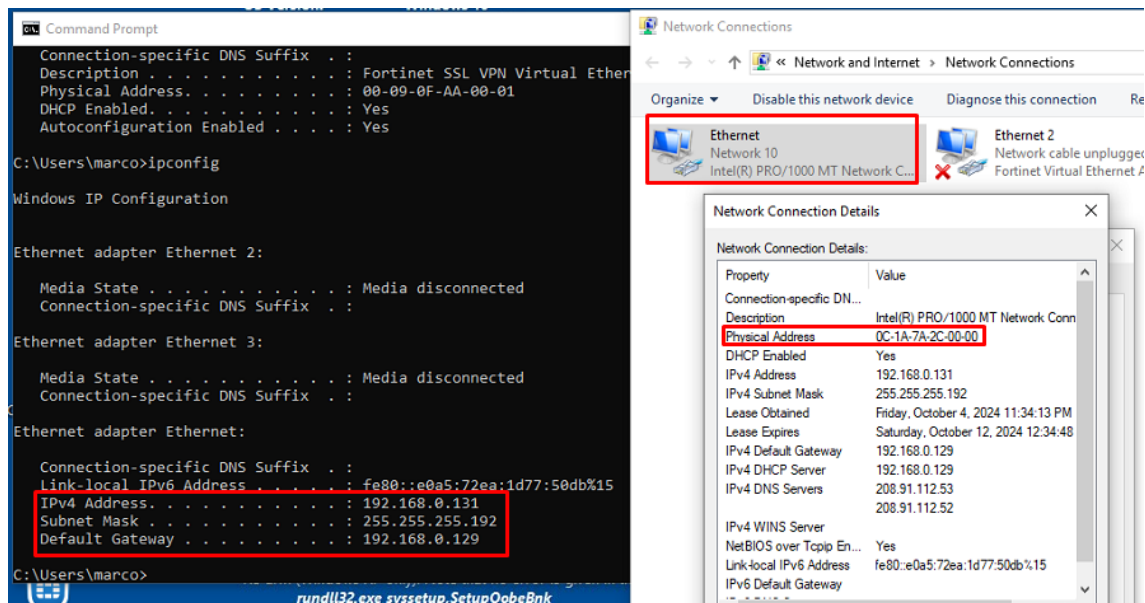
Port 1/1/5
=====
Client Details
-----
Number of authorized clients      : 2
Number of sticky authorized clients : 0

```

Por consiguiente, en la Figura 20 se realiza la verificación de la dirección MAC del cliente Windows 10, ya autorizado en el puerto 1/1/5 configurado como puerto de acceso para la VLAN 10.

Figura 20

Verificación de MAC address en cliente Windows 10



Además se realiza la verificación de la dirección MAC del cliente VPC como se muestra en la Figura 21.

Figura 21

Verificación de MAC address en cliente VPC

```
PC1> dhcp
DDORA IP 192.168.0.132/26 GW 192.168.0.129

PC1> show ip

NAME       : PC1[1]
IP/MASK    : 192.168.0.132/26
GATEWAY    : 192.168.0.129
DNS        : 208.91.112.53 208.91.112.52
DHCP SERVER : 192.168.0.129
DHCP LEASE  : 604798, 604800/302400/529200
MAC        : 00:50:79:66:68:01
LPORT      : 20098
RHOST:PORT : 127.0.0.1:20099
MTU        : 1500
```

Finalmente se realiza la comprobación de que únicamente 2 clientes con MAC estáticas previamente configuradas en la interfaz del conmutador, tengan el acceso autorizado a dicha interfaz, mediante la conexión de un tercer cliente el cual no podrá acceder a la interfaz 1/1/5 del conmutador tal y como se demuestra en la Figura 22.

Figura 22

Verificación de cliente excedente y rechazado de la interfaz donde se aplicó Port Security

```
Client limit exceeded violation status
```

Port	Violation	Violation-Count
1/1/1	No	0
1/1/2	No	0
1/1/3	No	0
1/1/5	Yes	1
1/1/6	No	0
1/1/7	No	0

```
switch#
```

```
PC2> dhcp
DDD
Can't find dhcp server

PC2> show ip
NAME       : PC2[1]
IP/MASK    : 0.0.0.0/0
GATEWAY    : 0.0.0.0
DNS        :
MAC        : 00:50:79:66:68:03
LPORT     : 20018
RHOST:PORT : 127.0.0.1:20019
MTU        : 1500

PC2>
```

4.5.3. Radius (IEEE 802.1X)

IEEE 802.1X es aquel protocolo de acceso a puertos para proteger redes mediante el uso de un mecanismo de autenticación basada en cliente, servidor y un punto intermedio. Este tipo de método de autenticación es sumamente útil en infraestructuras Wireless y para conexiones ethernet en donde los autenticadores son los conmutadores de capa 3 debido a sus capacidades de enrutamiento y manejo de tráfico entre diferentes subredes, crucial para entornos donde se utiliza RADIUS para la autenticación. Existen tres componentes básicos durante la autenticación 802.1X:

- **Solicitante:** Cliente de una estación de trabajo puede ser inalámbrico o que pueda soportar entrada conexión ethernet.
- **Autenticador:** Punto de acceso Wi-Fi, Puerto de conmutador.
- **Servidor de autenticación:** Base de datos de autenticación, servidor RADIUS.

Para la demostración y ejemplo de implementación de dicha política, basándose en directrices y recomendaciones del estándar de la NIST Special Publication 800-53 Revision 5; se realiza el uso, configuración y levantamiento de un servidor RADIUS en Windows Server 2019, siendo uno de los servidores asemejados a uno del entorno de la empresa actualmente. Este servidor RADIUS, como se evidencia en la Figura 23, está

integrado dentro de una característica conocida como NPS (Network Policy Server) la cual es una implementación que permite la autenticación, autorización y contabilidad (AAA) de los usuarios que intentan acceder a una red, soportando varios métodos de autenticación donde el cliente y el servidor han negociado un canal seguro como: EAP (Extensible Authentication Protocol), siendo este último el usado debido a que es un marco que admite métodos de autenticación más robustos como EAP-TLS, EAP-MSCHAPv2, PEAP, etc. Mismo que posteriormente cifrará la contraseña del usuario utilizando un algoritmo de hash como SHA 256, SHA 512 asegurando que la contraseña no se transmita en texto plano a través de la red ya que en caso de una autenticación correcta, se puede establecer un canal seguro con cifrado simétrico AES para asegurar el intercambio de datos.

Figura 23

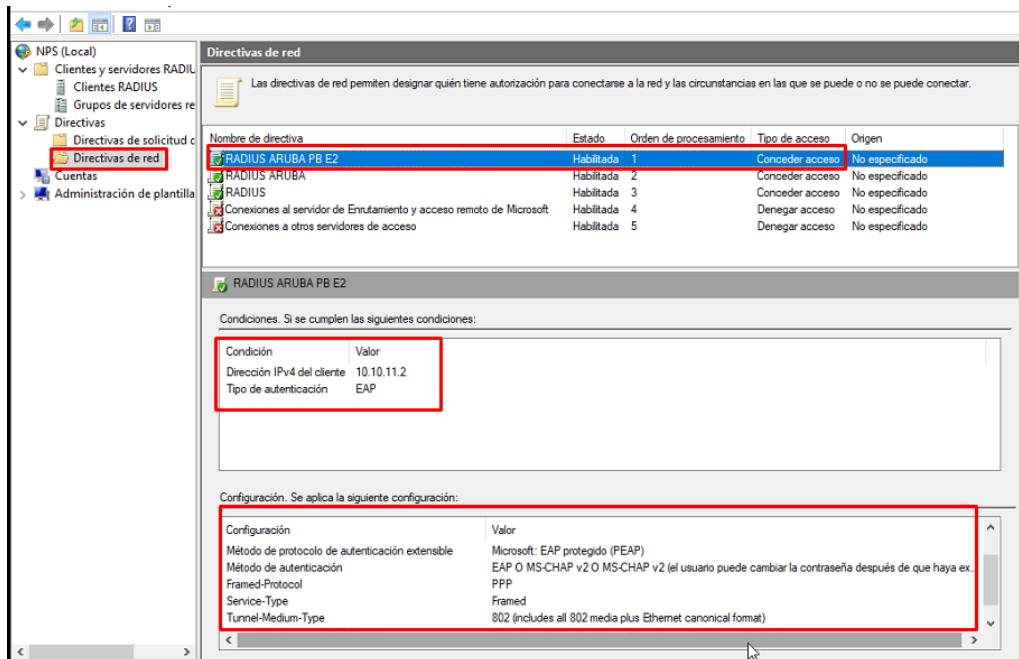
Network Policy Server de RADIUS en Windows Server 2019



En caso de que un usuario se autentique con éxito, NPS decide si se tiene nivel de autorización necesario para acceder a la red o ciertos recursos como se evidencia en la Figura 24, basándose en políticas de red que pueden estar bajo un grupo de usuarios, ubicación, dispositivo de origen, método de autenticación, etc.

Figura 24

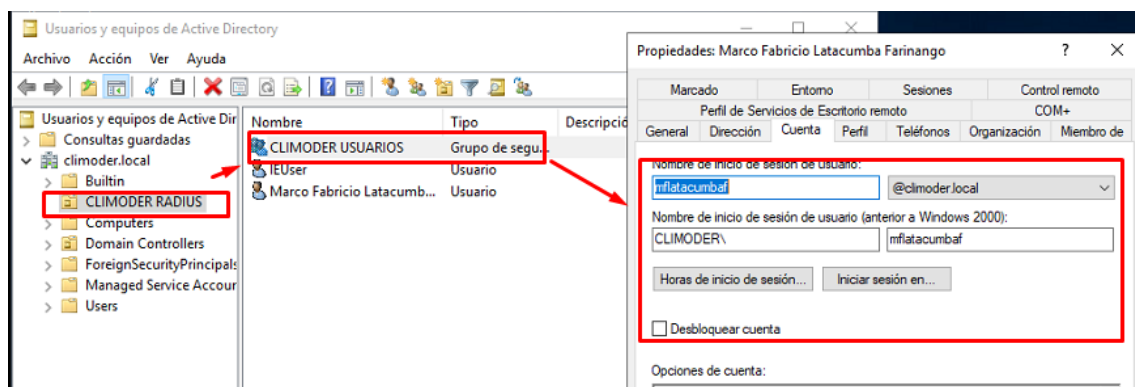
Directivas de red de NPS de RADIUS en Windows Server 2019



Se realiza el énfasis para esta práctica y demostración donde NPS se integra con Active Directory evidenciado en la Figura 25, lo que lleva a utilizar la base de datos de AD para la autenticación de usuarios y la aplicación de políticas de grupo LDAP, facilitando la gestión centralizada de credenciales y políticas de acceso según los privilegios del usuario.

Figura 25

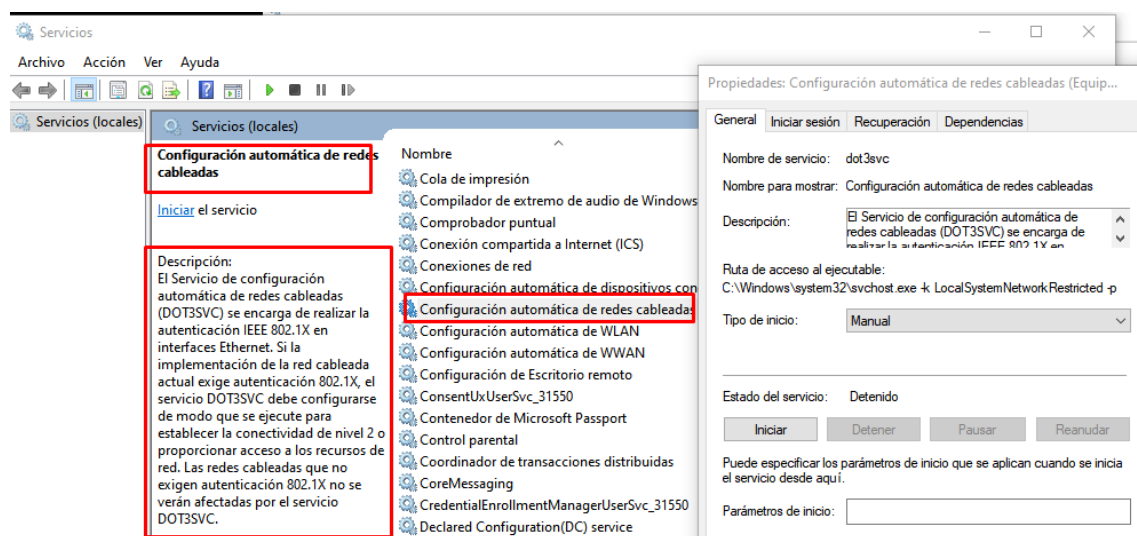
Usuario creado dentro de AD siguiendo las directrices de creación de usuario y contraseña robustas



Posteriormente el NAS (Network Access Server) el cual es un dispositivo de red que un usuario trata de usar para conectarse, en este caso un switch que actúa como cliente RADIUS, recibiendo la solicitud EAPOL (Extensible Authentication Protocol Over LAN), protocolo que permite transmitir mensajes EAP en una red ethernet durante el proceso de autenticación 802.1X desde el dispositivo del usuario siendo este ejemplo Windows 10, hasta el switch o punto de acceso. Cabe recalcar la aclaración de que se deberá activar el servicio local de configuración automática de redes cableadas que se encarga de realizar la autenticación en interfaces ethernet, como se evidencia en la Figura 26.

Figura 26

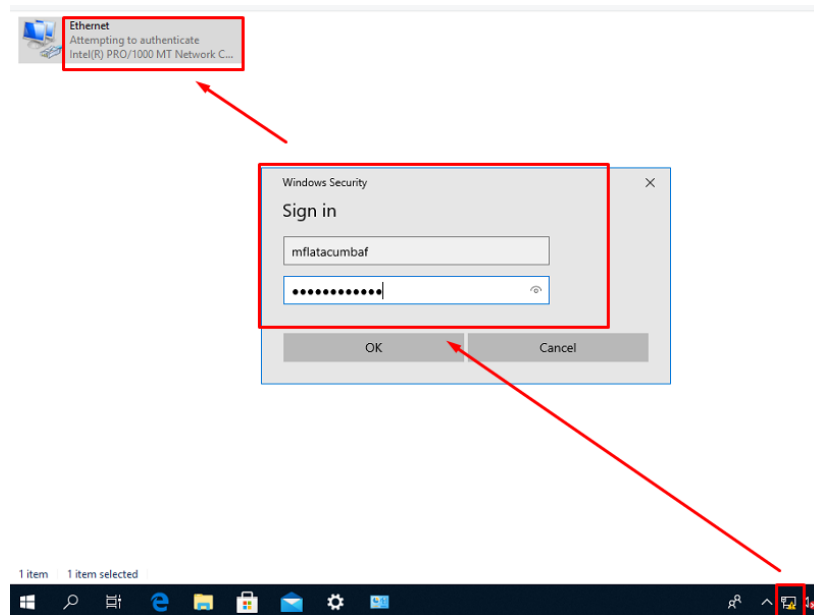
Habilitación del servicio de configuración automática de redes cableadas



Finalmente se realiza el proceso de autenticación con un usuario y contraseña almacenada en la base de datos de AD de Windows Server 2019 y haciendo uso del protocolo RADIUS para un usuario Windows 10, como se evidencia en la Figura 27.

Figura 27

Proceso final de autenticación por medio de usuario y contraseña mediante el protocolo 802.1X en una conexión ethernet



Se evidencia en la Figura 28 la correcta autenticación y posterior asignación de dirección IPv4 en una de las VLANs configuradas en el Router Firewall Fortigate, además de verificar en el visor de eventos de Windows Server 2019 la correcta autenticación del usuario en el NAS (Network Access Server) con un ID de evento 6272, evidenciado en la Figura 29, haciendo detalle y redundancia en los protocolos de autenticación que se han usado para establecer la conexión del usuario final.

Figura 28

Asignación de dirección IPv4 de la VLAN 10 una vez se autentica el usuario mediante el protocolo 802.1X

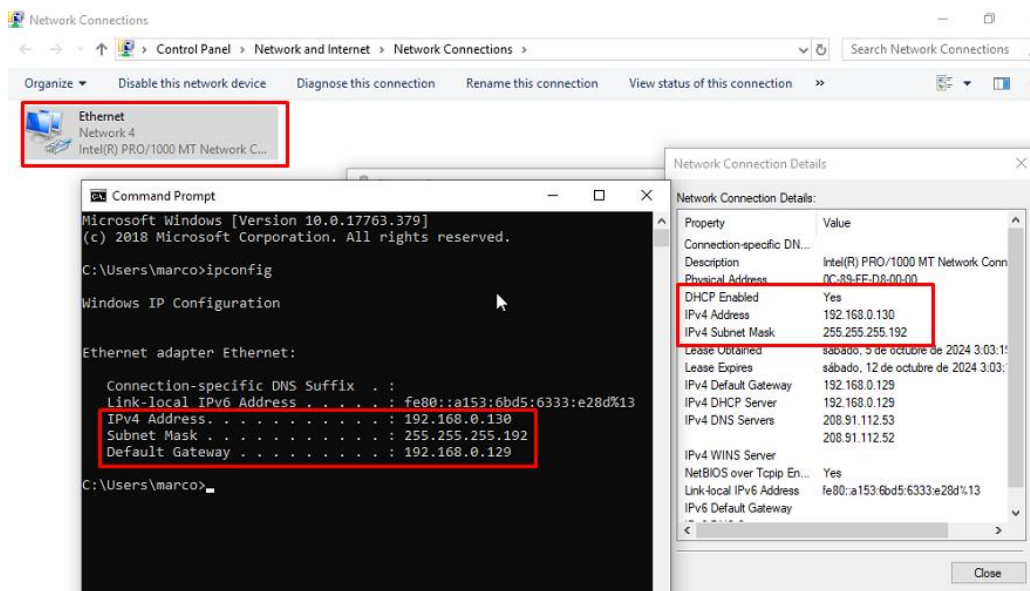
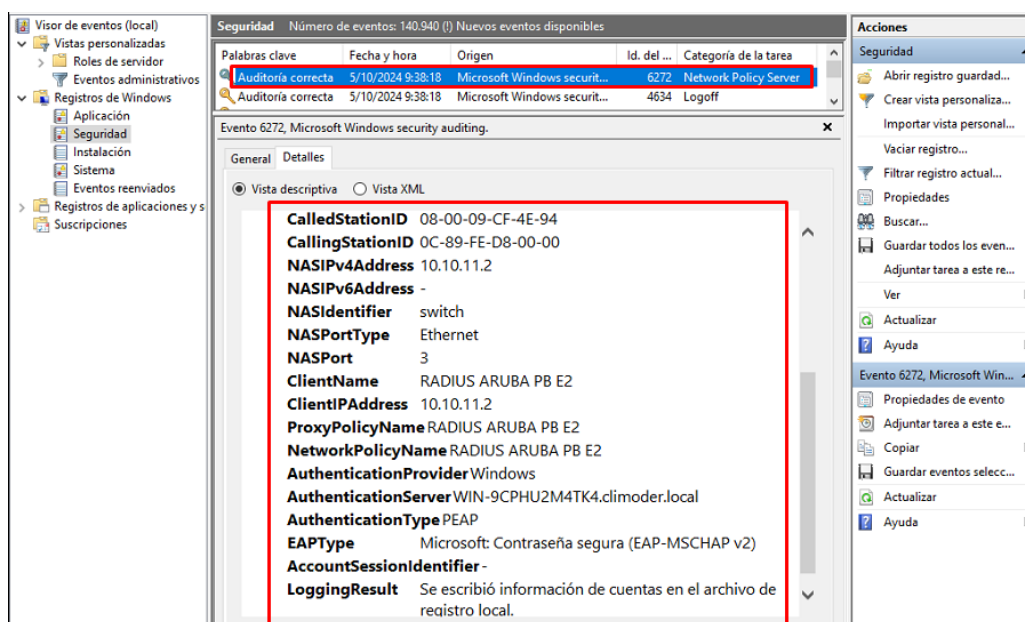


Figura 29

Visor de eventos de seguridad de Windows Server 2019



4.5.4. 2FA (Doble factor de autenticación)

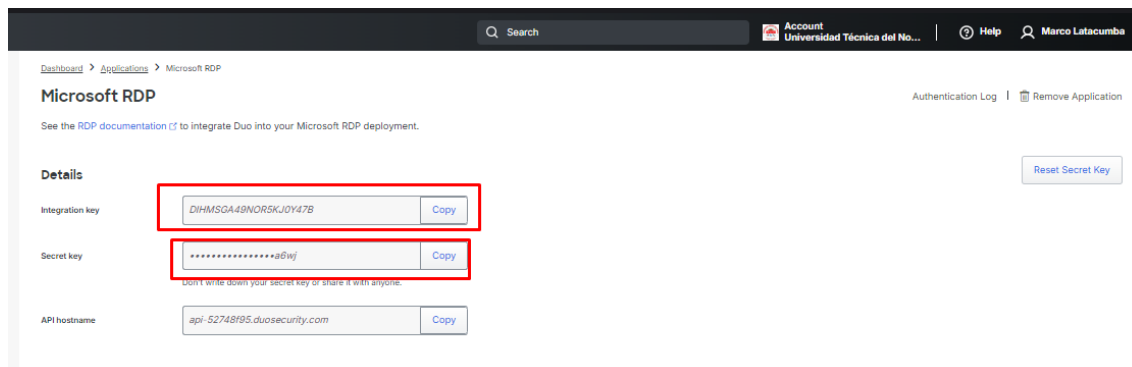
En base a las directrices y recomendaciones del estándar de la NIST Special Publication 800-63B, se toma como ejemplo y configuración para la demostración de la política de autenticación de doble factor 2FA al sistema de autenticación de múltiple factor (MFA) DUO by CISCO la cual proporciona seguridad Zero-Trust (cero confianza) simplificada dando protección a todas las aplicaciones e información confidencial de la empresa. Duo permite la protección de múltiples aplicaciones de diferentes marcas de empresas tecnológicas para diferentes servicios, lo cual lo hace un sistema sostenible para la autenticación de múltiple factor.

Para el ejemplo de demostración se realizará la implementación de este sistema en usuarios que accedan a los escritorios de Windows 10 en las estaciones de trabajo, debido a que los SO operativos de la línea de Microsoft son mayormente usados dentro de la empresa. Esta configuración requerirá que los usuarios después de ingresar su nombre de usuario y contraseña tengan que aprobar un segundo factor de autenticación mediante una notificación push en sus dispositivos móviles registrados, un código enviado por SMS, o el uso de un token de autenticación, garantizando una capa adicional de seguridad, protegiendo el acceso al sistema operativo y los recursos corporativos.

Inicialmente se necesitará seleccionar la aplicación que se desea aplicar 2FA siendo en este caso Windows RDP para poder autenticar usuarios y contraseñas de portales de login en estaciones de trabajo de SO Microsoft. En la Figura 30 se observa que DUO proporciona tres credenciales esenciales: Intregation Key(ikey), Secret Key (skey) y API Hostname, necesarias para que la aplicación pueda comunicarse de manera segura con los servicios de DUO y realizar 2FA.

Figura 30

Claves de autenticación de la aplicación Microsoft RDP



Una vez aclarado el punto de las claves de autenticación, se procede a instalar DUO Authentication Proxy en Windows Server 2019 el cual actúa como intermediario entre el servidor de autenticación y el servicio de DUO para proporcionar la autenticación de segundo factor (2FA), este actúa como puente entre el servidor local (Active Directory) y DUO Cloud para gestionar la autenticación de doble factor. En la Figura 31 se evidencia como el proxy verifica las credenciales de los usuarios del servidor local Active Directory que contiene la base de datos de usuarios y contraseñas, una vez que las credenciales son verificadas correctamente por el proxy hacia el servidor local, este procede a comunicarse con los servidores de DUO en la nube para solicitar el segundo factor de autenticación (2FA).

Figura 31

Claves de autenticación de la aplicación Microsoft RDP

The screenshot shows the Duo Authentication Proxy Manager interface. At the top, it indicates the service is running, with an uptime of 01:03:05 and version 6.4.1. There are buttons for 'Restart Service' and 'Stop Service'. The main area is split into two panes: 'Configure: authproxy.cfg' and 'Output'.

```

Configure: authproxy.cfg
26
27 [AD_server_auto]
28 ikey=DIN2F0YYQXPKCMXYZ7L7
29 skey=H1YgzhIAQsoaiV2Xvku4M8a2K6c3MiD532KnmK8y
30 api_host=api-52748f95.duosecurity.com
31 radius_ip_1=192.168.0.227
32 radius_secret_1=FLatacumba12.
33 ;failmode=safe
34 client=ad_client
35 port=1812
36
37
38 [cloud]
39 ikey=DIZVNNYP822K3G5ECKFM
40 skey=zNaq6wppJKPs2WC4uuQKHYQmoBwjJ8dwRajtDE0q
41 api_host=api-52748f95.duosecurity.com
42
43 ; Uncomment the service_account_username and service_
44 ; Then, enter your Active Directory service account u
45
Output
[info] The RADIUS Server has no connectivity problems.
[info] -----
[info] Testing section 'cloud' with configuration:
[info] {'api_host': 'api-52748f95.duosecurity.com',
[info]   'ikey': 'DIZVNNYP822K3G5ECKFM',
[info]   'skey': '*****[40]'}
[info] The Cloud connection has no connectivity
[info] problems.
[info] -----
[info] SUMMARY
[info] No issues detected

The results have also been logged in C:\Program
Files\Duo Security Authentication
Proxy\log\connectivity_tool.log

Checking updates for Duo Authentication Proxy...
[info] No updates detected. Your Duo Authentication
Proxy is up to date.
  
```

Si todo está correctamente configurado será necesario comprobar la sincronización en el portal web de DUO del proxy de autenticación como se evidencia en la Figura 32. Adicionalmente se procede a verificar la sincronización de los controles de AD donde evidenciamos la confirmación de tener 2 grupos y uno de ellos es “CLIMODER USUARIOS” que contiene 3 usuarios como se observa en la Figura 33 y Figura 34.

Figura 32

Comprobación de correcta sincronización con AD de Windows Server 2019

← Back to Authentication Proxies

Authentication Proxy 1

Details

Name: Authentication Proxy 1
This name will only appear in the Duo Admin Panel.

Description:

0 / 512

Hostname: WIN-9CPHU2M4TK4

Status: Connected to Duo

Version: 6.4.1

Operating System: Windows

[Save](#)

Directory Sync Connections

Active Directory and OpenLDAP connections used for user syncs and admin syncs. [View all directory sync connections.](#)

Status	Name	Type	Servers	Base DN	In use?
✓	AD Sync Connection1	Active Directory	192.168.0.227:389	DC=climoder,DC=local	Used by 1 sync

Figura 33

Comprobación de correcta sincronización de grupo de usuarios de AD

Account Universidad Técnica del No... | Help | Marco Latacumba

Dashboard > Users > Directory_Sync > AD Sync

AD Sync

Rename 5 days left [Delete Directory Sync](#) No Changes

Import Duo user names and other information directly from your on-premises Active Directory. [Learn more about syncing users from Active Directory](#)

Sync Controls

Sync status
Scheduled to automatically synchronize every 12 hours, next around 10:00 PM -05
[Pause automatic syncs](#)

[Sync Now](#)

✓ Sync complete. Synced 3 users and 2 groups.

Troubleshooting ▾

Active Directory Connection

✓ Connected to Duo

AD Sync Connection1
192.168.0.227:389

[Edit connection](#)
[Change connection](#)

Figura 34

Comprobación de correcta sincronización de grupo de usuarios de AD

Sync Controls Delete Directory Sync No Changes

Groups

These groups and their users will be imported from your on-premises Active Directory

Acceso compatible con versiones anteriores de Windows 2000
 CLIMODER USUARIOS

Active Directory Connection

Connected to Duo
 AD Sync Connection1
 192.168.0.227:389
[Edit connection](#)
[Change connection](#)

En el apartado de Dashboard, en la Figura 35, es posible evidencia que los usuarios del grupo “CLIMODER USUARIOS” están listos para ser autenticados por medio de 2FA de DUO en los logs de inicio de sesión de las estaciones de trabajo de Windows 10 para este ejemplo simplificado.

Figura 35

Verificación de usuarios sincronizados con AD y DUO

Dashboard > Users

Users Directory Sync | Import Users | Bulk Enroll Users | Add User

Need to activate a replacement phone? [Learn more about Reactivating Duo Mobile](#).

3 Total Users
 0 Not Enrolled
 0 Inactive Users
 0 Trash
 0 Bypass Users
 0 Locked Out

Select (0) ... Export Search

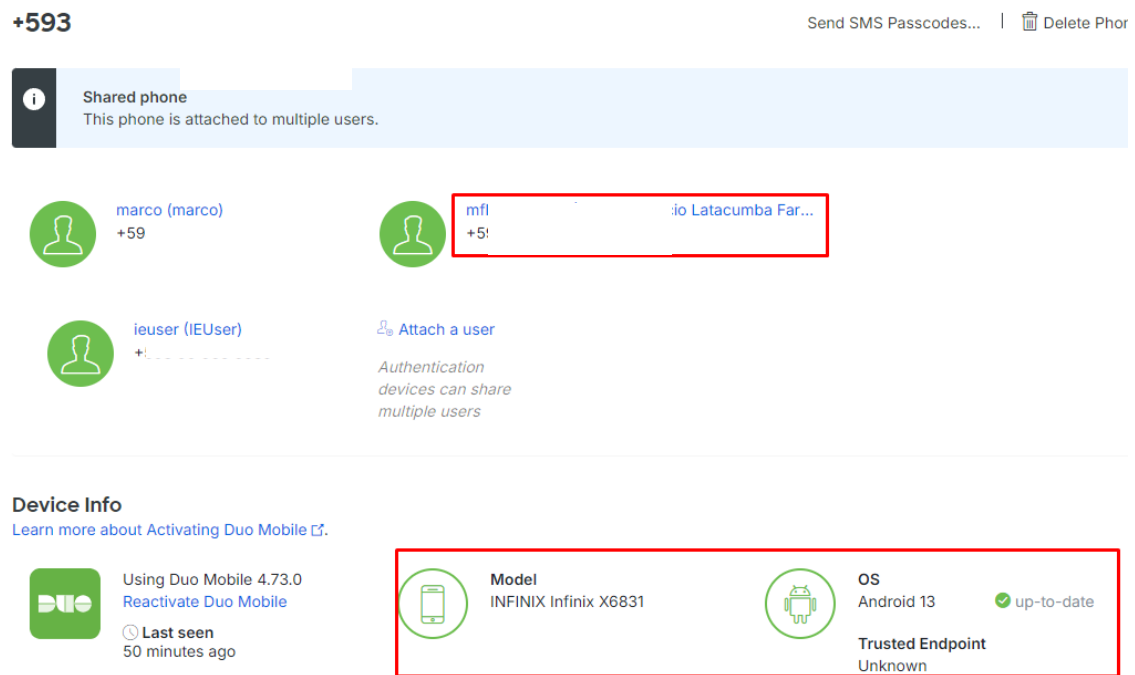
Username	Name	Email	Phones	Tokens	Status	Last Login
<input type="checkbox"/> mflatacumbaf	Marco Fabricio Latacumba Farinango		1		Active	5 de oct. de 2024 11:23
<input type="checkbox"/> marco	marco		1		Active	30 de sep. de 2024 14:23

Por consiguiente se realiza la implementación de los dispositivos que se usará como dispositivo de autenticación 2FA para el o los usuarios que se deseen ingresar como se evidencia en la Figura 36, en este caso de ejemplo práctico se enganchó a los 3 usuarios

pero se debe sincronizar únicamente un número de celular como dispositivo para cada usuario

Figura 36

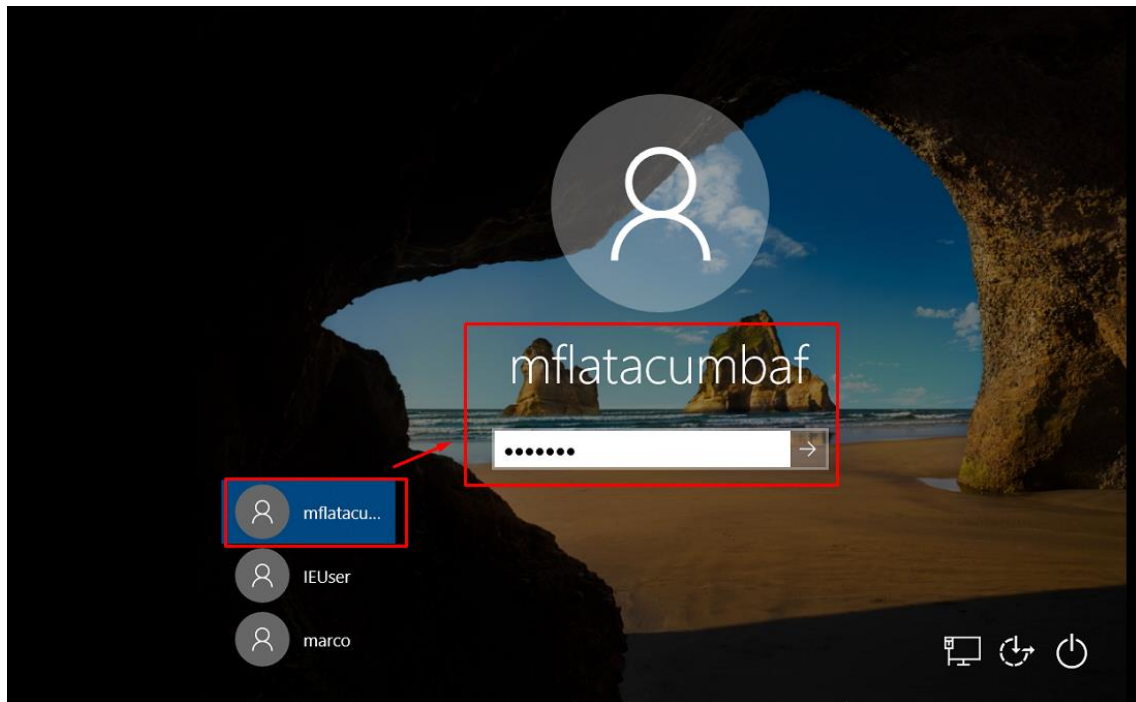
Ingreso de dispositivo móvil para autenticación de 2FA



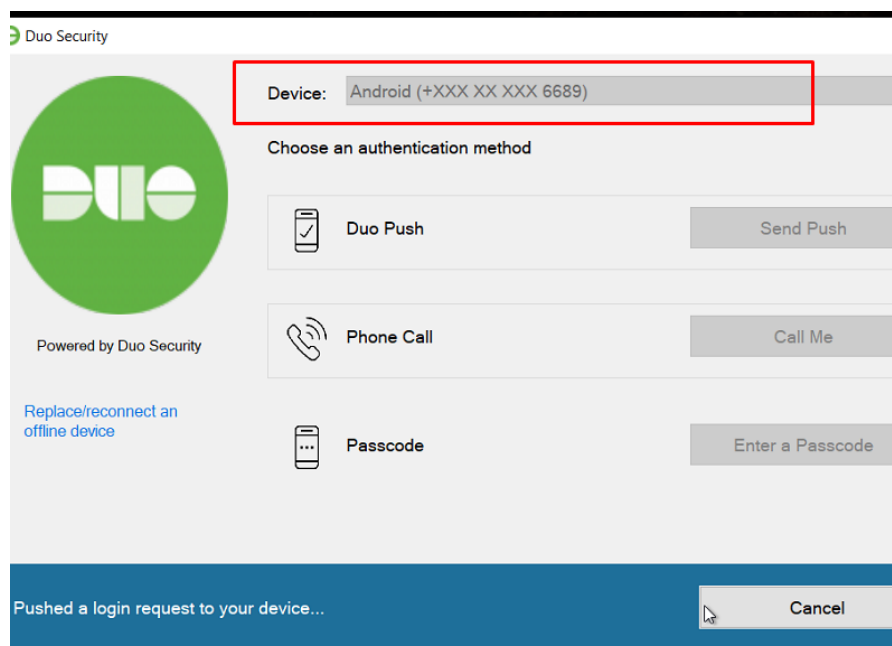
Finalmente se tiene la comprobación de todo el proceso realizado por medio de un ingreso mediante credenciales al login de inicio de sesión de una estación de trabajo con Windows 10, evidenciado en la Figura 37. Posteriormente se tiene la notificación de 2FA tanto en la pantalla de login de inicio de sesión de Windows 10 el cual nos pide autenticar por medio del dispositivo registrado dentro del portal de administración de DUO y así mismo se enviará la notificación al dicho dispositivo como se muestra en la Figura 38.

Figura 37

Portal de login de usuario mflatacumbaf en Windows 10

**Figura 38**

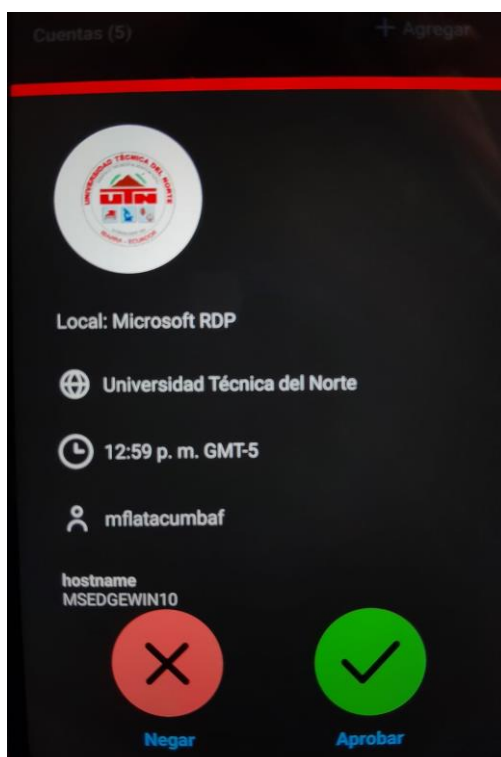
Portal de autenticación de DUO para usuarios Windows 10



Como se mencionó anteriormente la notificación de inicio de sesión llegará al dispositivo móvil que tengamos registrado como se evidencia en la Figura 39 por lo que se deberá aprobar o denegar según el caso que se presente ante la autenticación del usuario.

Figura 39

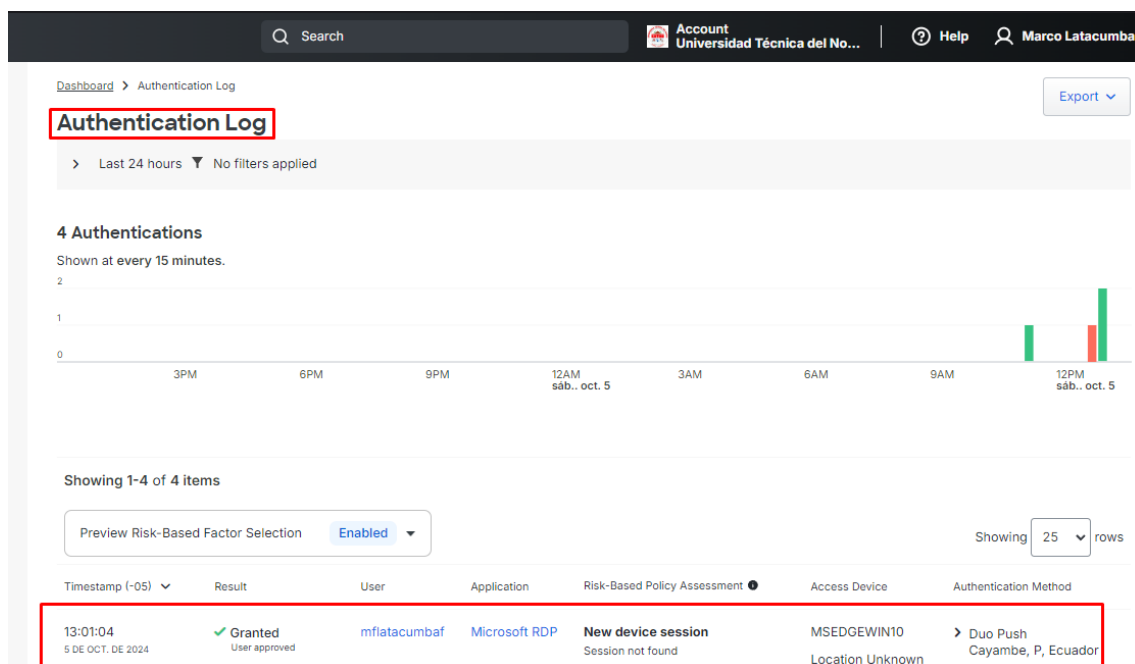
Notificación de autenticación de 2FA de Duo Mobile para el usuario mflatacumbaf



Como información adicional se puede evidenciar en la Figura 40 dentro del portal de administración de DUO la información de los logs de los usuarios que han sido autenticados por medio de 2FA en la aplicación móvil.

Figura 40

Logs de autenticación de los usuarios dentro del portal de administración de DUO



4.5.5. Certificados digitales SSL/TLS

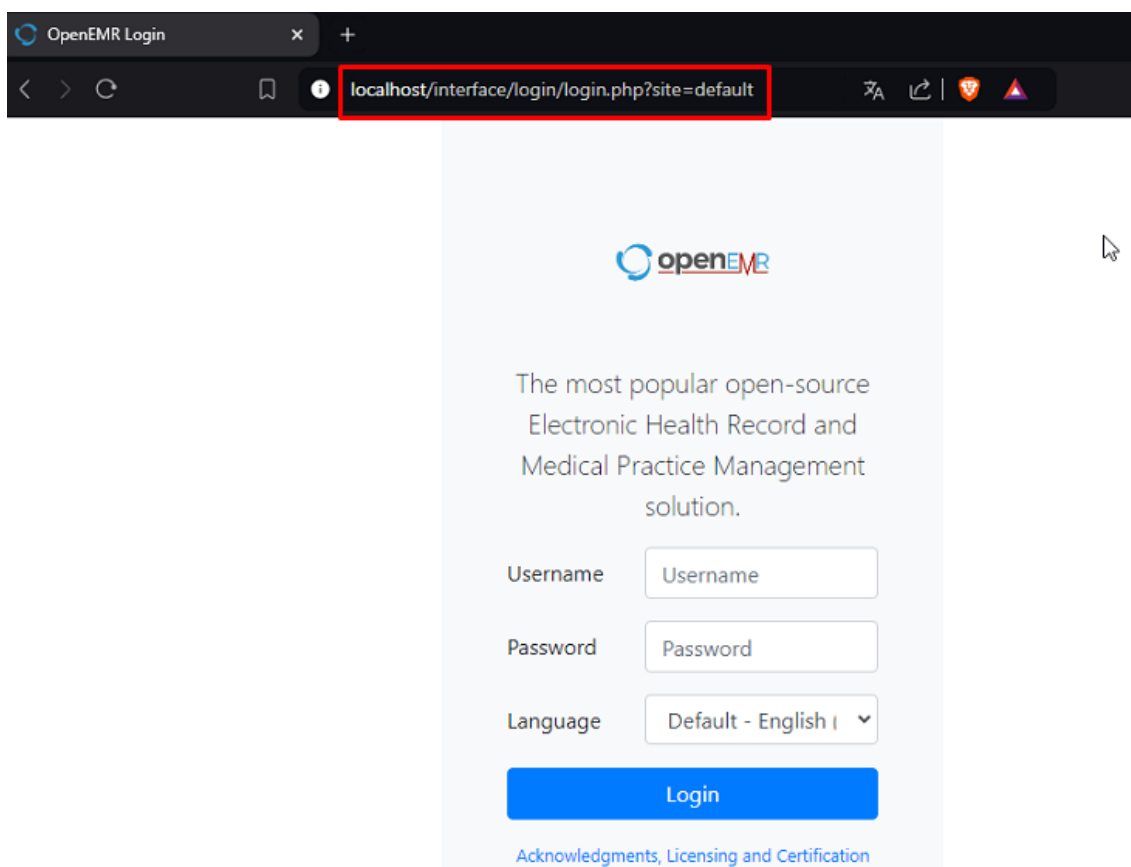
Se entiende a un certificado SSL/TL como un recurso digital que permite a sistemas autenticar la identidad de otro sistema, a su vez, establecer conexión cifrada mediante el protocolo Secure Sockets/Transport Layer Security (SSL/TLS). Estos certificados se generan utilizando sistemas criptográficos conocidos como infraestructura de clave pública (PKI), lo que permite que una parte verifique la identidad de otra a través de certificados, siempre y cuando ambas partes confíen en una entidad externa, conocida como autoridad de certificación. Así, los certificados SSL/TLS actúan como identificaciones digitales que aseguran las comunicaciones de red y establecen la identidad de los sitios web en internet, así como la de los recursos en redes privadas.

En base al estándar de la NIST Special Publication 800-52 Revision 2 y siguiendo las recomendaciones y directrices que menciona, se realiza la demostración en práctica de simulación el uso de un sistema de gestión hospitalaria Open Source (Código abierto), siendo exactamente “OpenEMR”, como se evidencia en la Figura 41, haciendo uso de

XAMPP como infraestructura que permite la ejecución de este sistema de gestión hospitalaria simulado en un entorno local. Por ende OpenEMR puede ser montada en el servidor para demostrar que este sistema permite gestionar la información de pacientes, citas, historial médico, facturación y más.

Figura 41

Portal de login del sistema de gestión hospitalaria OpenEMR.

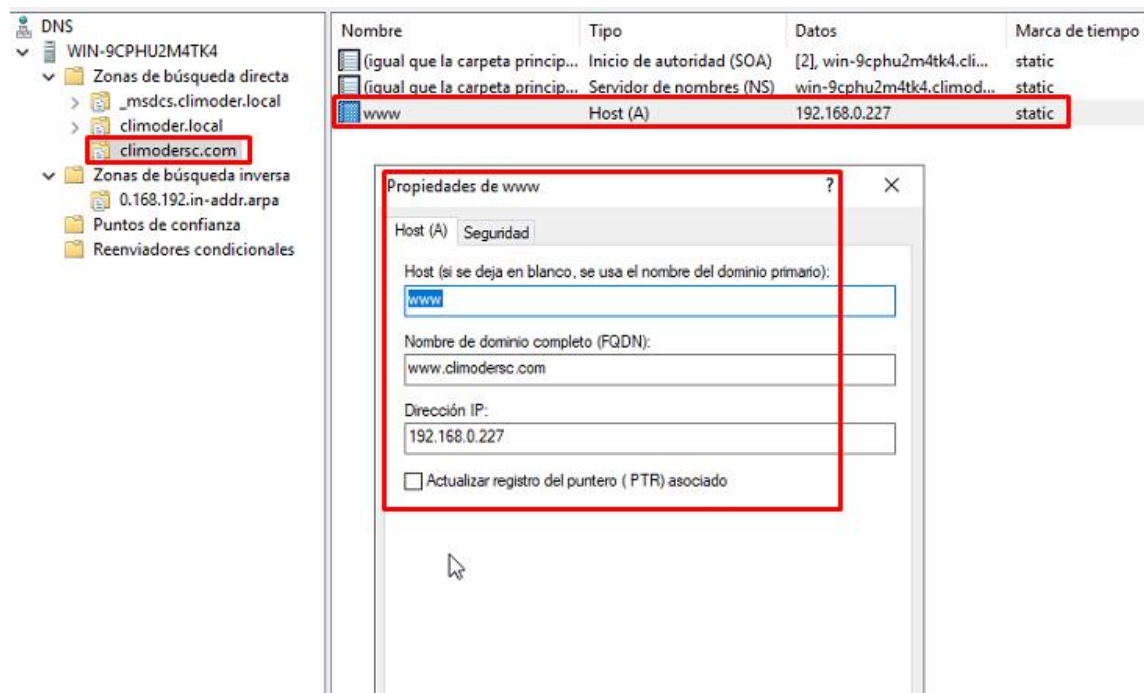


Por consiguiente, será necesario la configuración del servidor DNS de Windows server 2019 para gestionar las resoluciones de nombres de dominio y direcciones IP, almacenar información de zonas DNS, redirigir consultas DNS a servidores de nombres de raíz sugeridos. En la Figura 42 se evidencia inicialmente la creación de una zona de búsqueda directa que mapeará los nombres de host a direcciones IP, es decir, para resolver nombres de dominio en direcciones IP. Cuando un usuario quiera acceder a un recurso de

la red utilizando para este ejemplo www.climodersc.com, el servidor DNS consultará la zona de búsqueda directa para encontrar la dirección IP correspondiente del servidor.

Figura 42

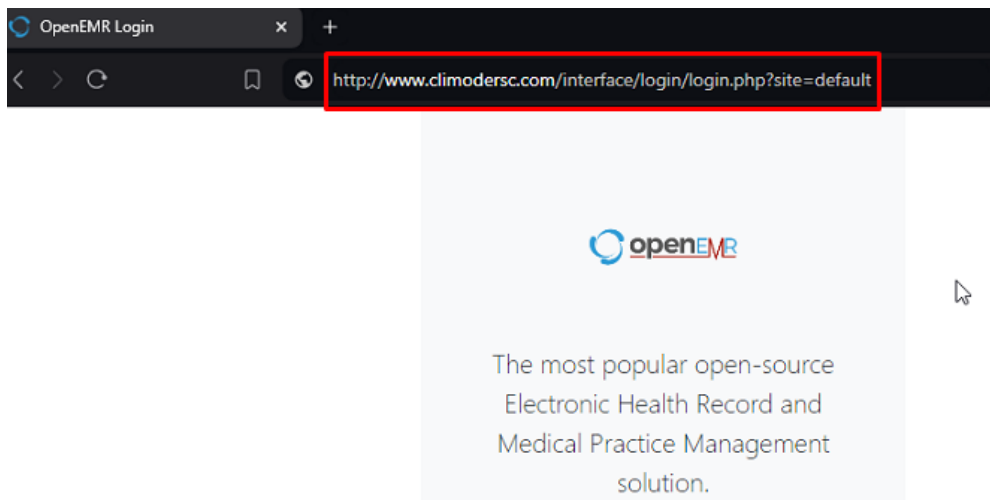
Creación de zona de búsqueda directa en el servidor DNS para www.climodersc.com



De esta manera es posible colocar un nombre de dominio a nuestro sistema de gestión hospitalaria de código abierto como se muestra en la Figura 43, en lugar de colocar localhost ahora será posible acceder por medio de www.climodersc.com de manera local a dicho sistema.

Figura 43

Acceso al sistema de gestión hospitalaria por medio del dominio www.climodersc.com

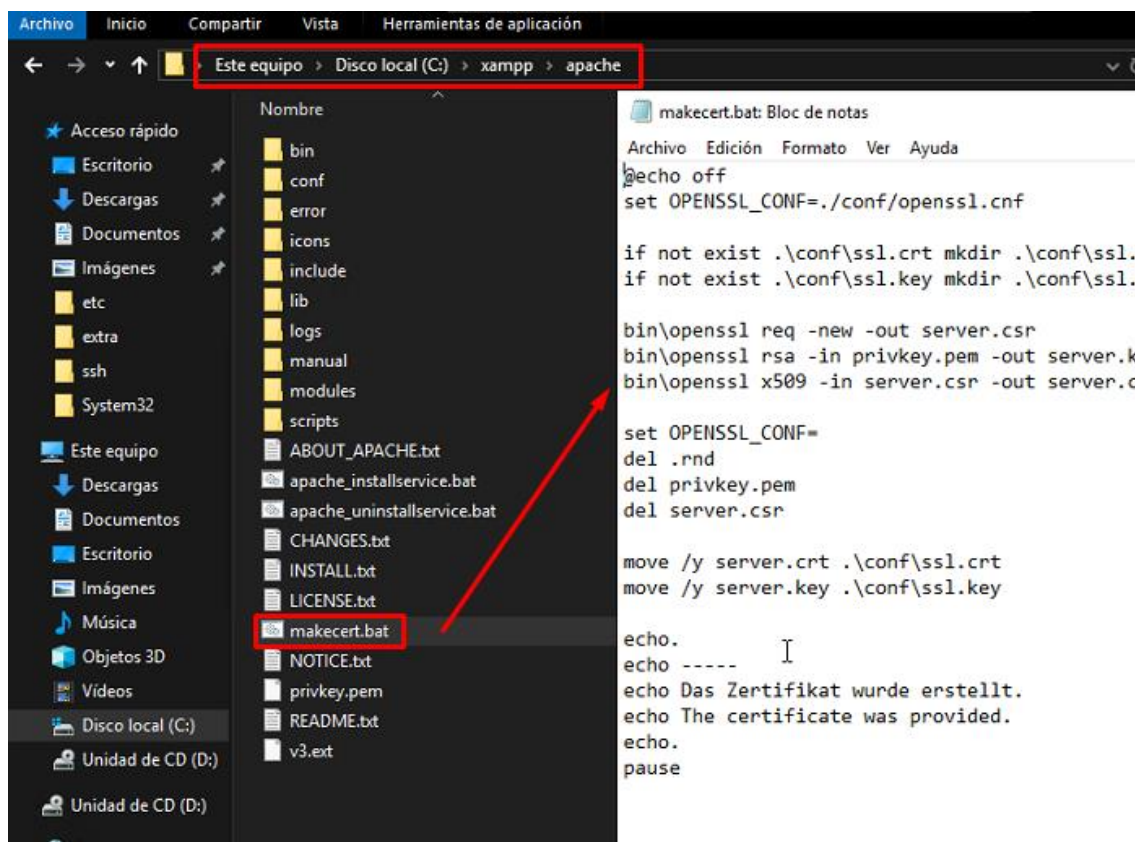


Por consiguiente se procede a la demostración de la generación de un certificado digital SSL/TLS auto firmado a modo de demostración para la práctica de simulación, por lo que para este ambiente de prueba local se hace uso de este método, pero para un ambiente de producción se debe hacer uso obligatorio de certificados firmados por autoridades de certificaciones digital de confianza.

Se inicia creando el certificado auto firmado usando OpenSSL, pero para la simplificación de este procedimiento se hace uso del archivo *makecert.bat* para facilitar la creación de certificados SSL/TLS, automatizando el uso de OpenSSL para la generación de la clave privada como el certificado sin necesidad de manipular comandos complejos como se evidencia en la Figura 44.

Figura 44

Configuración del archivo *makecert.bat* dentro de Windows Server 2019



Ahora, dentro del archivo se procede a editar la línea de la siguiente manera *bin\openssl x509 -in server.csr -out server.crt -req -signkey server.key -days 1825 -extfile v3.ext*, además de la creación del archivo *v3.ext* ingresando las líneas que se evidencian en la Figura 45, donde:

authorityKeyIdentifier: Establece al identificador de la clave de autoridad.

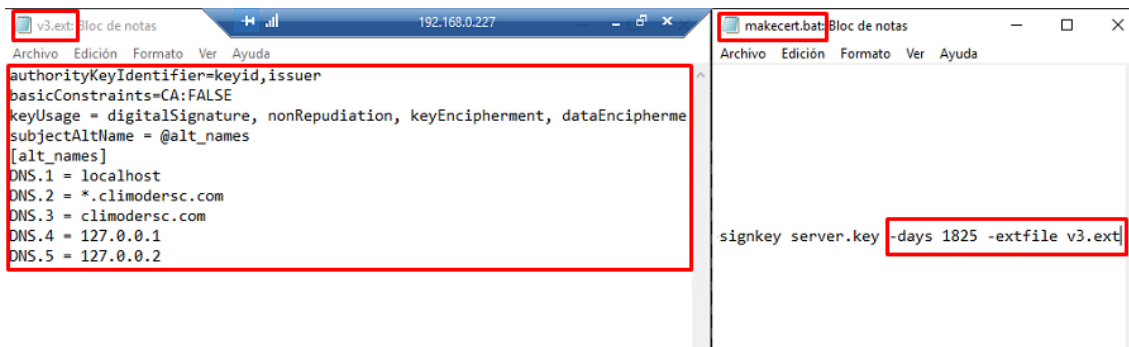
basicConstraints: Confirma que el certificado no es validad por una autoridad certificadora (CA).

keyUsage: Define los usos permitidos del certificado (firmar, cifrar, etc).

subjectAltName: Especifica nombres alternativos como; localhost, dominios específicos y direcciones IP.

Figura 45

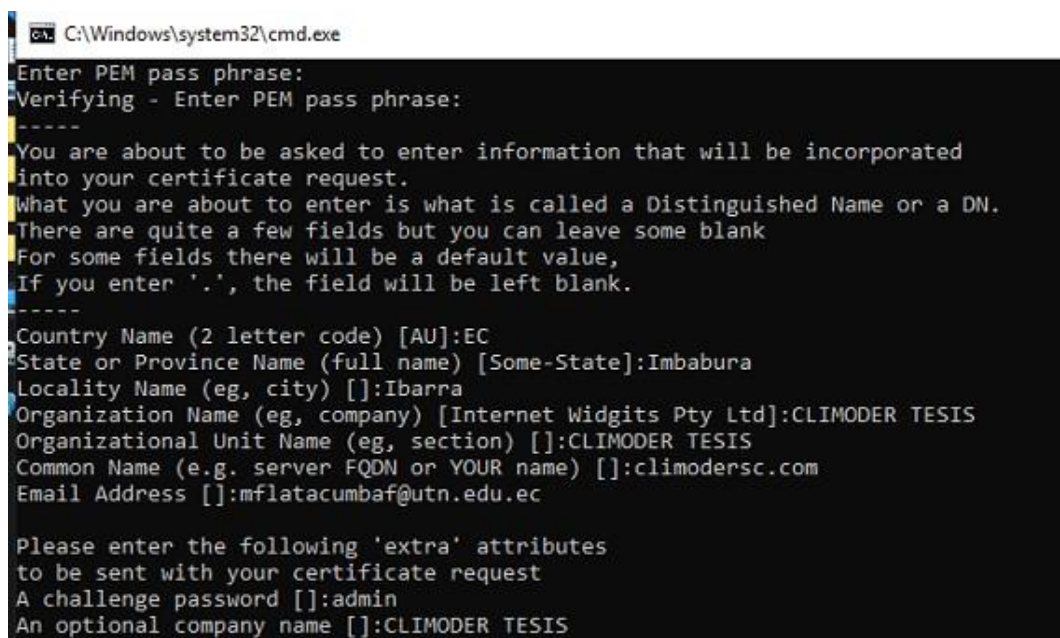
Creación y modificación de archivo v3.ext



Por consiguiente, al ejecutar el archivo *makecert.bat* se abrirá la siguiente ventana de comandos de terminal para iniciar el procedimiento de generación del certificado SSL/TLS como se muestra en la Figura 46.

Figura 46

Generación de certificado SSL/TLS auto firmado.

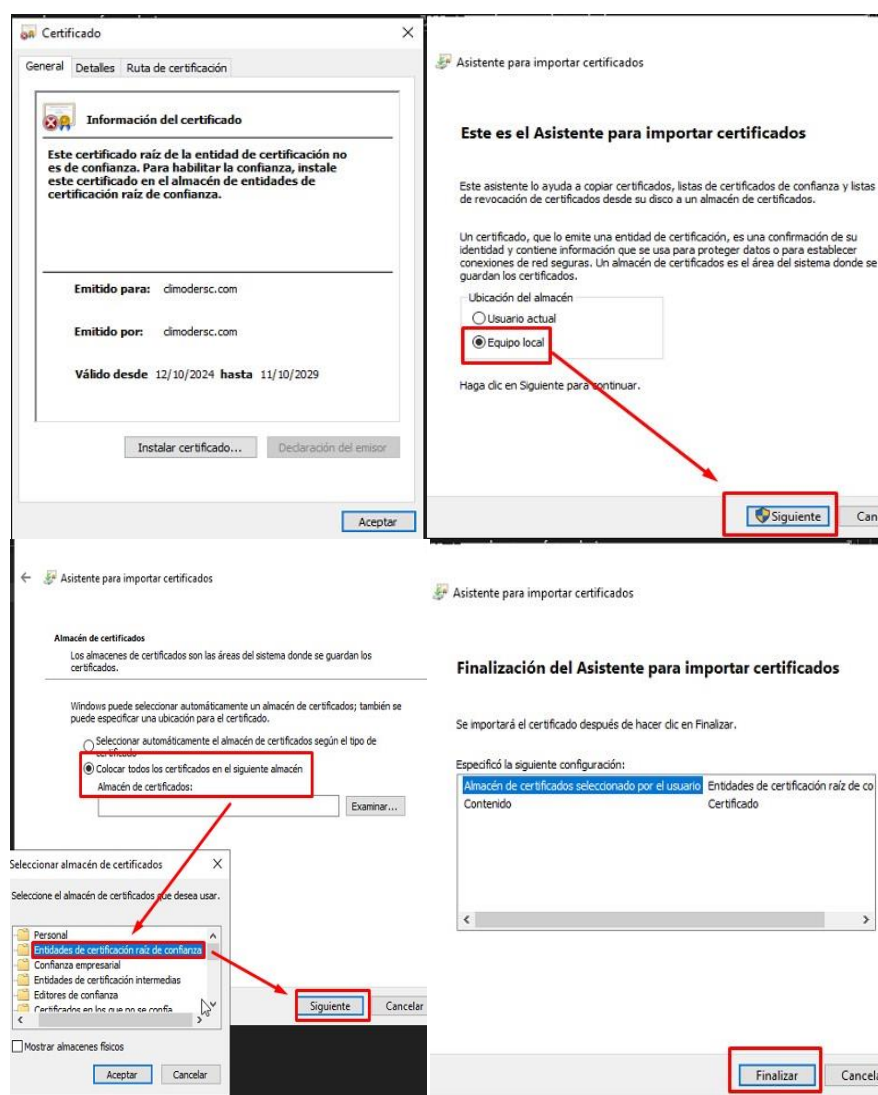


Si se ha realizado correctamente todo el proceso de creación de certificados SSL/TLS con OpenSSL al ejecutar el certificado creado, se desplegará el asistente de instalación de certificados de Windows como se muestra en la Figura 47, en donde se

realizará la importación de dicho certificado hacia el equipo local dentro del almacén de certificados “Entidades de certificación raíz de confianza”, lo que permitirá validar y confiar este certificado auto firmado para poder establecer una conexión segura y cifrada mediante el uso del certificado SSL/TLS para el ambiente de producción local de manera simulada.

Figura 47

Proceso de instalación del certificado público SSL/TLS



Finalmente, se tiene la agregación de líneas para la configuración de virtual hosts en el archivo `httpd-vhosts.conf`, que permitirá que un servidor web maneje múltiples sitios

web o dominios desde una misma dirección IP. En la Figura 48 se muestra que cada virtual host establecerá configuraciones específicas para un dominio o subdominio; VirtualHost en el puerto 80 (HTTP) redirige las solicitudes HTTP a HTTPS, haciendo uso de una regla de reescritura (RewriteRule) para garantizar que cualquier acceso a climodersc.com o www.climodersc.com sea redirigido a una conexión segura (HTTPS). Por otro lado, VirtualHost en el puerto 443 (HTTPS) define la configuración para el acceso seguro al servidor, detallando los archivos del certificado SSL/TLS (server.crt) y de clave privada (server.key) para la activación de encriptación SSL/TLS para dicho sitio.

Figura 48

Configuración de VirtualHost en Apache para redirección de HTTP a HTTPS y habilitación de certificados SSL/TLS

```

httpd-vhosts.conf: Bloc de notas
Archivo Edición Formato Ver Ayuda
##ServerAdmin webmaster@dummy-host.example.com
##DocumentRoot "C:/xampp/htdocs/dummy-host.example.com"
##ServerName dummy-host.example.com
##ServerAlias www.dummy-host.example.com
##ErrorLog "logs/dummy-host.example.com-error.log"
##CustomLog "logs/dummy-host.example.com-access.log" common
##</VirtualHost>

##<VirtualHost *:80>
##ServerAdmin webmaster@dummy-host2.example.com
##DocumentRoot "C:/xampp/htdocs/dummy-host2.example.com"
##ServerName dummy-host2.example.com
##ErrorLog "logs/dummy-host2.example.com-error.log"
##CustomLog "logs/dummy-host2.example.com-access.log" common
##</VirtualHost>

<VirtualHost *:80>
    ServerName www.climodersc.com
    ServerAlias climodersc.com
    DocumentRoot "C:\xampp\htdocs\openemr"
    RewriteEngine on
    RewriteCond %{SERVER_NAME} =www.climodersc.com [OR]
    RewriteCond %{SERVER_NAME} =climodersc.com
    RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI} [END,NE,R=permanent]
</VirtualHost>

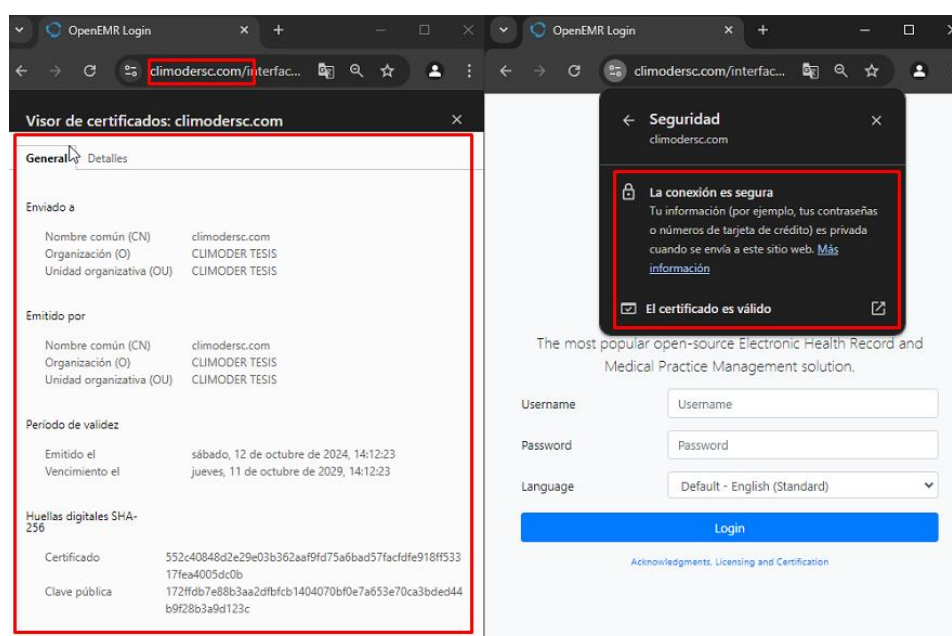
<VirtualHost *:443>
    ServerName climodersc.com
    ServerAlias climodersc.com
    DocumentRoot "C:\xampp\htdocs\openemr"
    SSLEngine on
    SSLCertificateFile "conf/ssl.crt/server.crt"
    SSLCertificateKeyFile "conf/ssl.key/server.key"
</VirtualHost>

```

En la Figura 49 es posible evidenciar la aplicación del certificado SSL/TLS instaurado para poder realizar una conexión HTTPS segura por medio del puerto 443, además de poder observar las características de dicho certificado para el servicio web del sistema de gestión hospitalaria simulado. Cabe recalcar, que, a pesar de hacer uso de estos recursos hospitalarios únicamente dentro de la red local de la empresa, no está por demás la adquisición de un certificado digital emitido por una CA y sea únicamente para un solo dominio.

Figura 49

Certificado SSL/TLS instaurado en servidor web de sistema de gestión hospitalario



4.5.6. VPN IPsec para acceso remoto

En base al estándar de la NIST Special Publication 800-46 Revision 2 y siguiendo las directrices y recomendaciones que menciona, se realiza la demostración y simulación de IPsec (Internet Protocol Security) como protocolo desarrollado para garantizar la protección de conexiones entre dispositivos sobre redes IP, brindando confidencialidad, integridad y autenticación de los datos transmitidos. IPsec opera en la capa 3 (Red) del

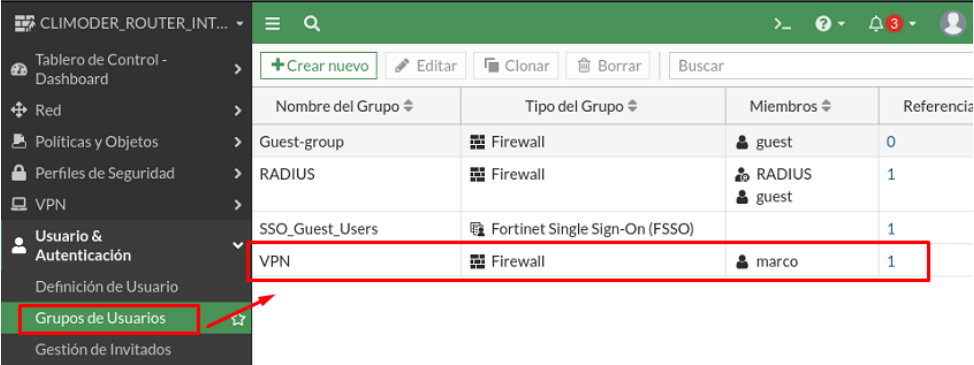
modelo OSI para proteger el tráfico de datos IP de manera unidireccional y bidireccional, utilizado mayormente en el siguiente escenario:

- **VPN remote access:** Utilizada para conectar un cliente de manera segura a los recursos de la red interna a través de internet.

Los protocolos de IPsec transmiten paquetes de datos de forma segura haciendo uso de varios protocolos y técnicas criptográficas, permitiendo una comunicación segura y cifrada. En la Figura 50 se observa la creación de un usuario local almacenado dentro de la base de datos de FortiGate para controlar el acceso a sus servicios o políticas de seguridad mediante el uso de la VPN IPsec acceso remoto, este usuario estará designado dentro de un grupo de usuarios locales al que posteriormente se aplicará permisos o configuraciones de dicho grupo, lo que facilita la administración de la red local.

Figura 50

Creación de grupo de usuarios dentro del router firewall FortiGate

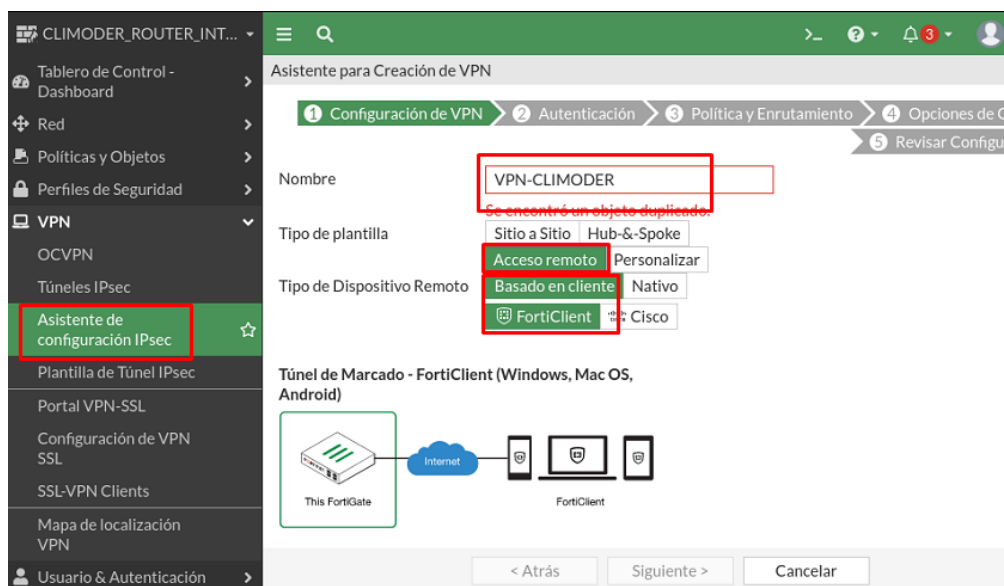


Nombre del Grupo	Tipo del Grupo	Miembros	Referencia
Guest-group	Firewall	guest	0
RADIUS	Firewall	RADIUS guest	1
SSO_Guest_Users	Fortinet Single Sign-On (FSSO)		1
VPN	Firewall	marco	1

Posteriormente se tiene la creación de la VPN IPsec modo tunneling para el acceso remoto, basado en cliente tipo FortiClient como dispositivo remoto de autenticación, como se evidencia en la Figura 51.

Figura 51

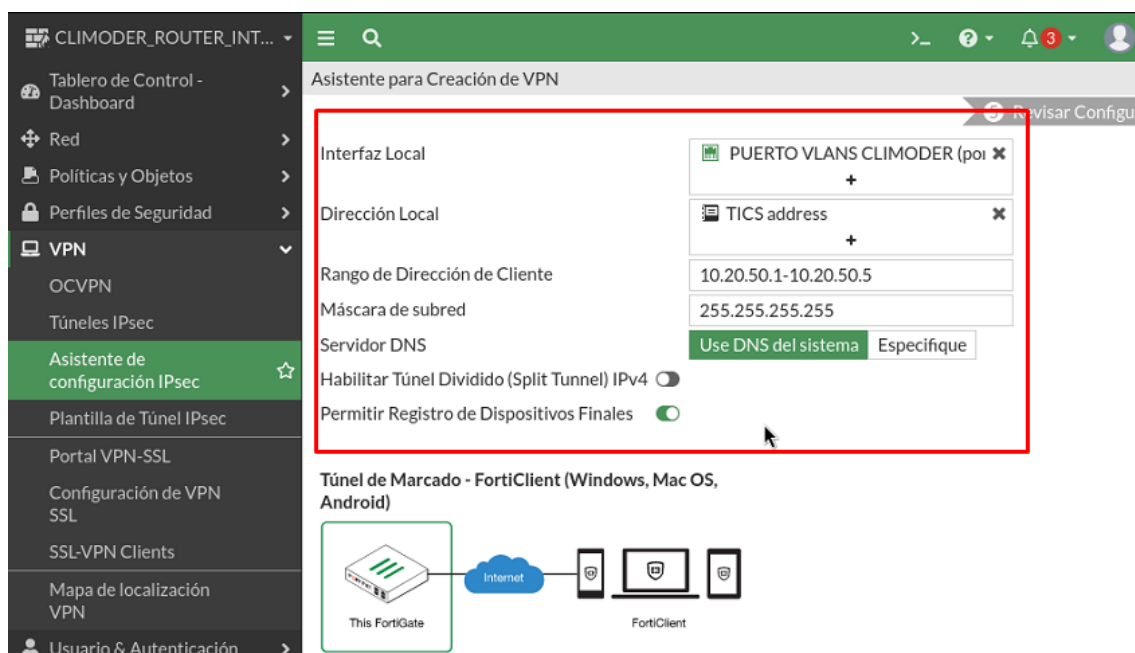
Proceso de creación de VPN IPsec dentro del router firewall FortiGate



Por consiguiente, se deberá seleccionar la interfaz local a la que se va a tener acceso mediante la conexión a la VPN IPsec de manera remota, como se evidencia en la Figura 52 se hará uso del “PUERTO VLANS CLIMODER” apuntando al grupo de direcciones designados en la VLAN de TICS donde actualmente se tiene la granja de servidores de la empresa. Además, se deberá realizar la creación de un rango de direcciones IPv4 específicas para VPN IPsec que se designará al usuario que desee conectarse de manera remota haciendo uso de la VPN, cabe recalcar además el no habilitar la opción de “Split Tunnel” debido a que se en la configuración de esta política se basa en la necesidad de garantizar un nivel óptimo de seguridad para la red corporativa.

Figura 52

Selección de interfaz local a la que se va a acceder desde el cliente remoto mediante el uso de la VPN IPsec y creación de rango de direcciones IPv4 para dicha VPN

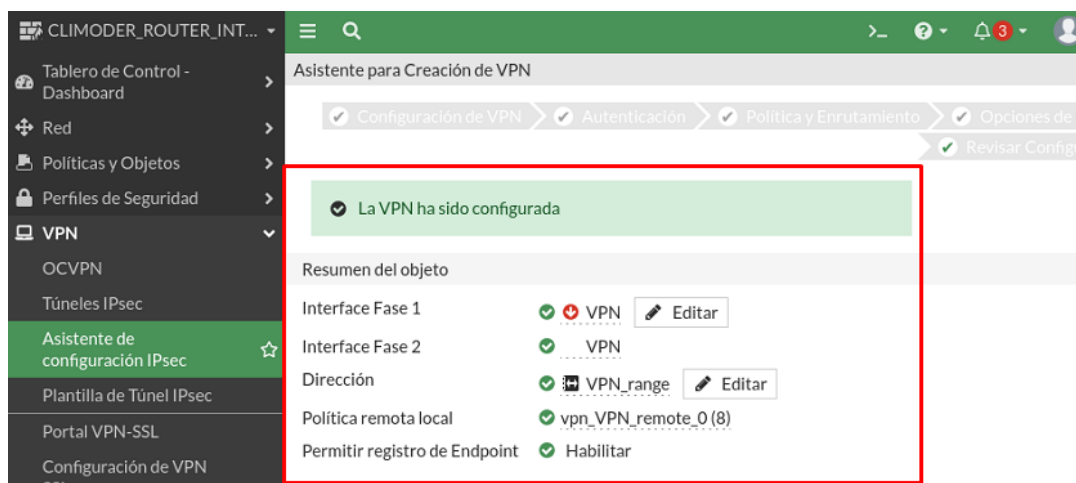


Al no permitir el túnel dividido, se asegura que todo el tráfico de los usuarios remotos pase a través de la red de la empresa, donde puede ser monitoreado, filtrado y protegido por los controles de seguridad establecidos. Esto reduce significativamente el riesgo de ataques externos y minimiza la posibilidad de que dispositivos locales comprometidos puedan acceder a recursos internos.

Finalmente, se tendrá la VPN IPsec creada dentro del router FortiGate como se evidencia en la Figura 53.

Figura 53

Creación exitosa de la VPN IPsec dentro del router firewall FortiGate

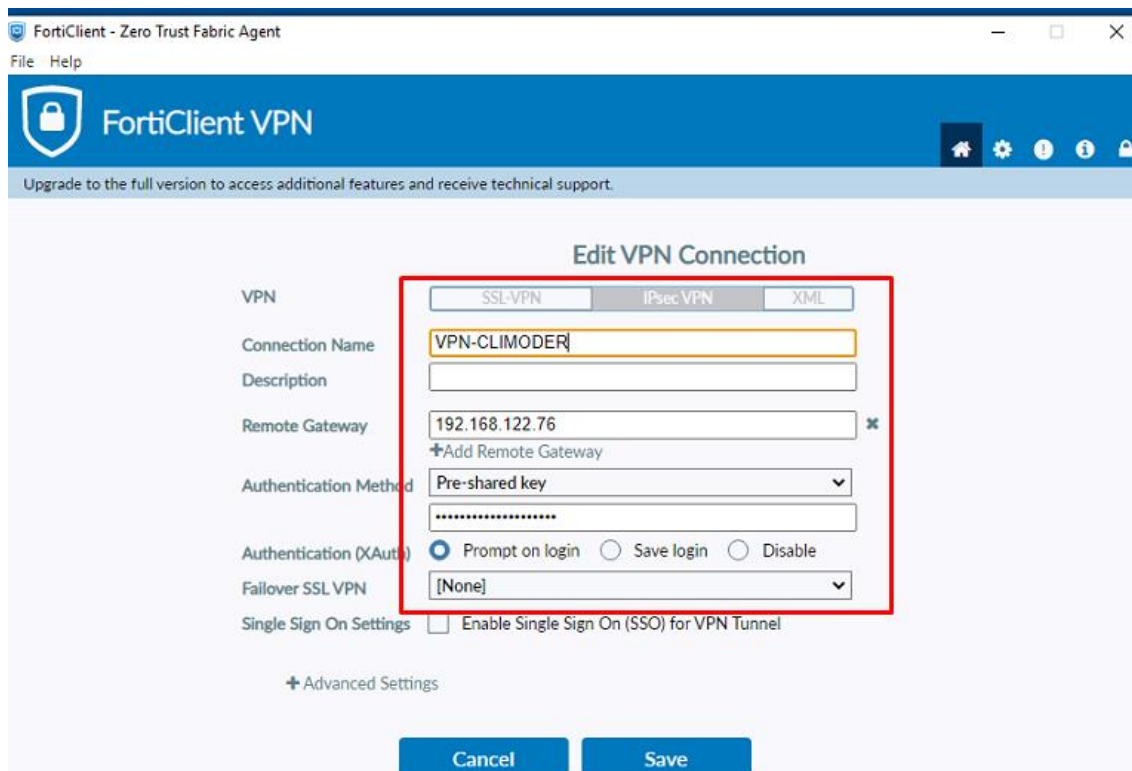


Una vez realizado todo este proceso se deberá realizar la instalación en el cliente el software FortiClient VPN conocido en versiones anteriores como FortiVPN desarrollada por Fortinet para usuarios que deseen autenticarse a sus dispositivos por medio de una VPN de manera segura y eficaz. Para la demostración se hace el uso de un cliente Windows 10 que estará fuera de la LAN y que necesitará realizar una conexión de manera remota haciendo uso de la VPN hacia el router firewall que ya hemos configurado previamente.

En la Figura 54 se evidencia la configuración de FortiVPN en el cliente Windows 10 en donde será necesario crear la conexión inicialmente colocando un nombre sencillo como referencia, seguidamente se deberá ingresar la dirección IP del router firewall FortiGate con la que se realiza la conexión y salida a internet. Además, solicitará ingresar la clave de secreto compartido que se creó previamente para la VPN IPsec en el router firewall.

Figura 54

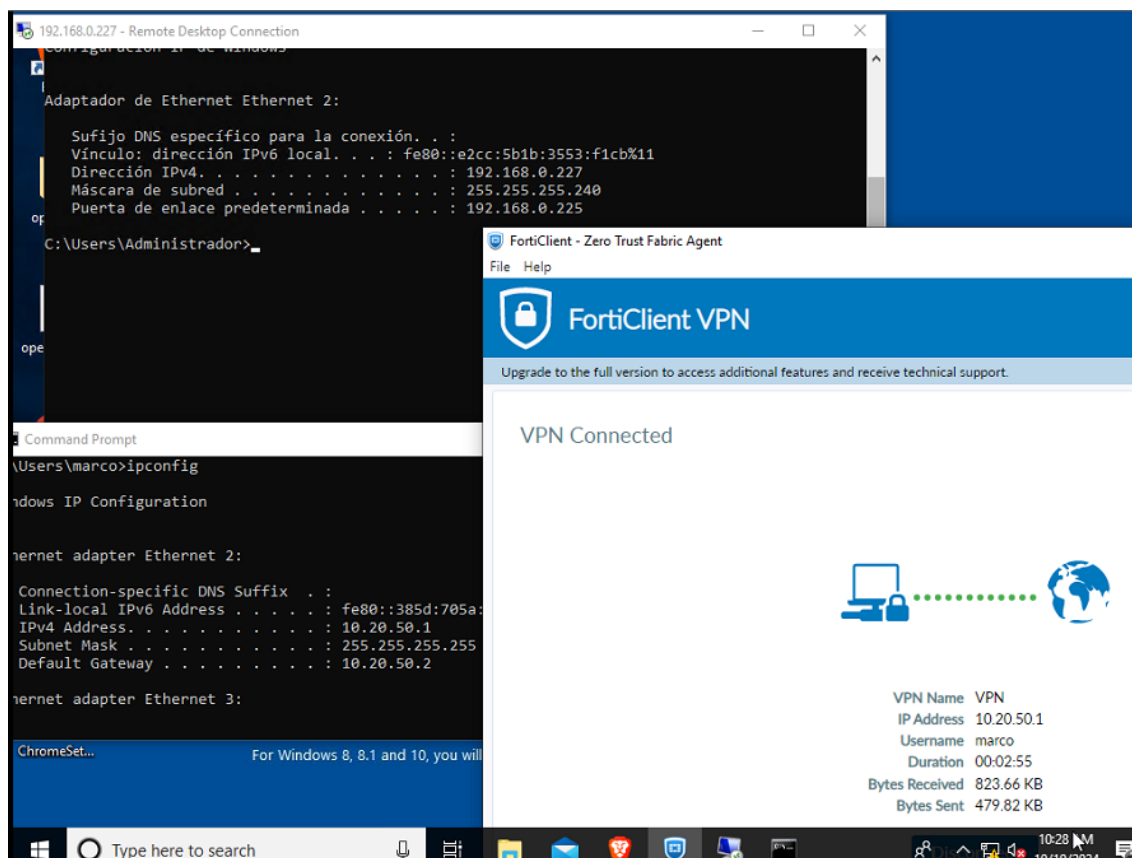
Proceso de conexión desde el portal de la aplicación FortiVPN (FortiClient VPN)



De esta manera se realiza la conexión al router firewall de manera segura y eficaz de modo que en caso de que el administrador de la red desee conectarse fuera de la empresa de manera remota a la LAN interna, podrá realizarlo por medio de la VPN IPsec y como ejemplo de acceso efectivo y seguro se demuestra en la Figura 55 el acceso al escritorio remoto RPD de Windows server 2019 desde el cliente Windows 10 por medio del uso de la VPN levantada actualmente.

Figura 55

Ejemplo de conexión exitosa de manera segura y eficaz hacia un servidor alojado dentro del rango de direcciones de la VLAN de TICS de la empresa.



4.5.7. Sistema de monitorización de redes

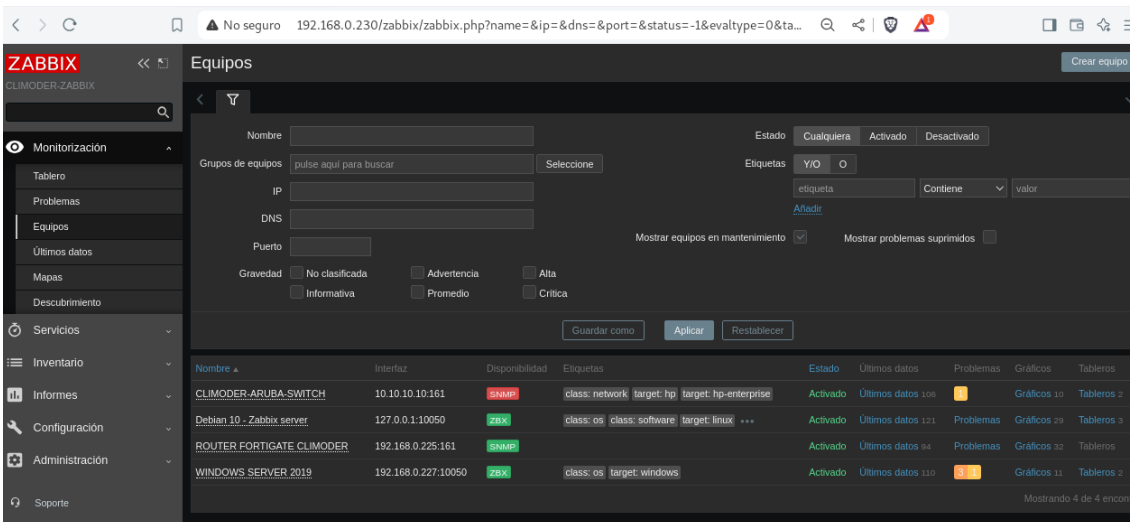
La implementación de un sistema de monitorización de redes es indispensable dentro de una red empresarial ya que permite para garantizar la disponibilidad, el rendimiento y la seguridad de los recursos tecnológicos de una red empresarial mediante monitoreo constante. Por lo que, en base al estándar de la NIST Special Publication 800-137, siguiendo las directrices y recomendaciones que menciona, se toma a modo de ejemplo el uso del sistema de monitorización Zabbix 5.0 LTS sobre una distribución Linux Debian 10 “Buster”, llegando a utilizar protocolos y arquitecturas que permiten el monitoreo en tiempo real de los dispositivos, servicios, bases de datos y aplicaciones distribuidas en la red empresarial a modo de simulación. Cabe recalcar la aclaración de

que actualmente SNMPv3 es el estándar más utilizado actualmente en comparación con las versiones anteriores (SNMPv1 y SNMPv2c) debido a varias mejoras en cuanto a la implementación de mecanismos de autenticación usando algoritmos como SHA 256, 512 y encriptación como AES 128, 256 para proteger los datos transmitidos entre los dispositivos y el servidor de monitorización Zabbix, garantizando confidencialidad y autenticación de los mensajes SNMP protegiéndolos contra accesos no autorizados y ataques.

En la Figura 56 se evidencia el portal de administrador Web de Zabbix donde se evidencia al administrador “CLIMODER-ZABBIX” y posteriormente se evidencia como ejemplo a 2 servidores monitorizados como agentes Zabbix y 2 agentes SNMPv3 siendo uno de ellos el switch Core de la empresa simulado y el otro el router firewall FortiGate. Para el caso práctico se muestra a 3 de los 4 agentes activos a modo de verificación de cómo se observaría cuando unos de los agentes SNMP no está enviando MIBs hacia el servidor central Zabbix debido a alguna falla de autenticación o disponibilidad física del dispositivo.

Figura 56

Portal web de administración de software de monitorización Zabbix



The screenshot shows the Zabbix web interface for the administrator 'CLIMODER-ZABBIX'. The main view is 'Equipos' (Devices), displaying a list of monitored devices. The interface includes a search bar, filters for status and severity, and a table of device details.

Nombre	Interfaz	Disponibilidad	Etiquetas	Estado	Últimos datos	Problemas	Gráficos	Tableros
CLIMODER-ARUBA-SWITCH	10.10.10.10:161	SNMP	class: network target: hp target: hp-enterprise	Activado	Últimos datos 106	0	Gráficos 10	Tableros 2
Debian 10 - Zabbix server	127.0.0.1:10050	ZBX	class: os class: software target: linux	Activado	Últimos datos 121	Problemas	Gráficos 29	Tableros 3
ROUTER FORTIGATE CLIMODER	192.168.0.225:161	SNMP		Activado	Últimos datos 94	Problemas	Gráficos 32	Tableros 2
WINDOWS SERVER 2019	192.168.0.227:10050	ZBX	class: os target: windows	Activado	Últimos datos 110	0	Gráficos 11	Tableros 2

Configuración de alertas en Zabbix

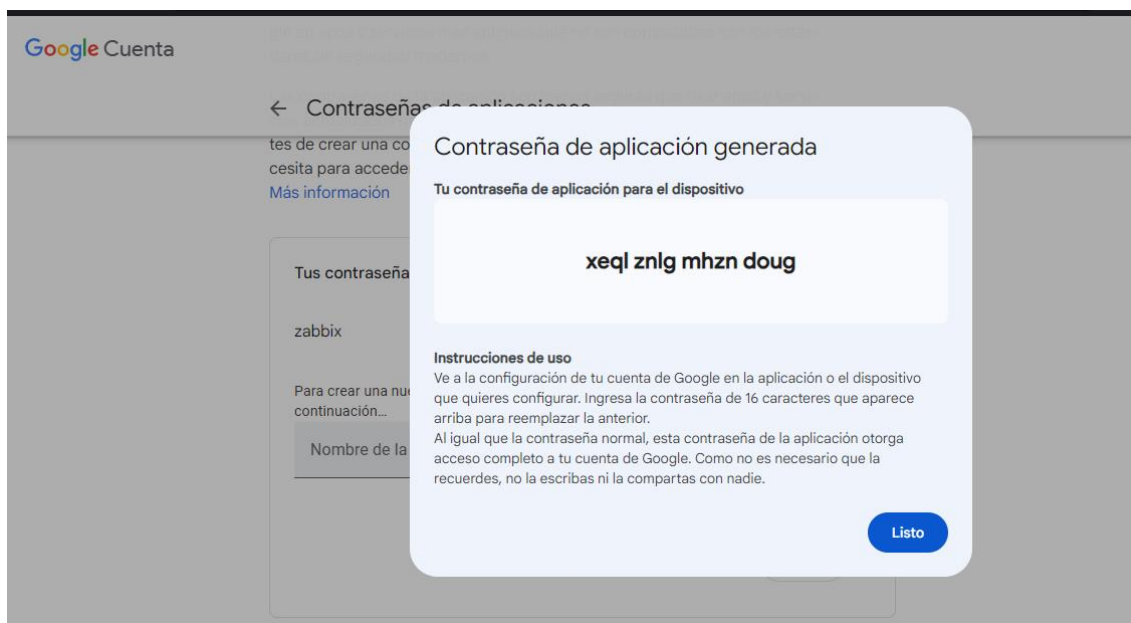
A continuación se presenta como parte de la protección, seguridad y monitoreo de equipos y servicios de la red de Telecomunicaciones de la empresa, la configuración de notificaciones de alertas de los equipos en el servidor Zabbix con un ejemplo realizado con una cuenta de Gmail a la que se enviará todas las alertas que genere Zabbix a partir de los equipos que trabajen con el protocolo SNMP o sean agentes Zabbix, mediante el uso de Triggers o condiciones lógicas utilizado para detectar problemas o situaciones anómalas en los recursos que se están monitoreando.

Para el siguiente ejemplo se toma al servidor Windows Server 2019 como equipo para recepat las notificaciones directamente a un correo electrónico personal. Se tiene como uso una dirección personal de correo electrónico de Gmail, donde, inicialmente se deberá activar el uso de la autenticación de dos pasos (2FA) para usuarios de dicho servicio como política de seguridad de Google para usuarios que deseen registrar el uso de contraseñas para aplicaciones que permitan dar acceso a la cuenta personal de Google apps y de servicios más antiguos debido a que no son compatibles con estándares de seguridad modernos y por ende Google se asegura por medio del facto de doble autenticación si en realidad la aplicación que se desee añadir al correo electrónico personal necesita una contraseña para poder acceder.

En la Figura 57 se puede evidenciar el proceso de creación de contraseña para dar permiso a la aplicación o en este caso al servidor Zabbix que se ha levantado.

Figura 57

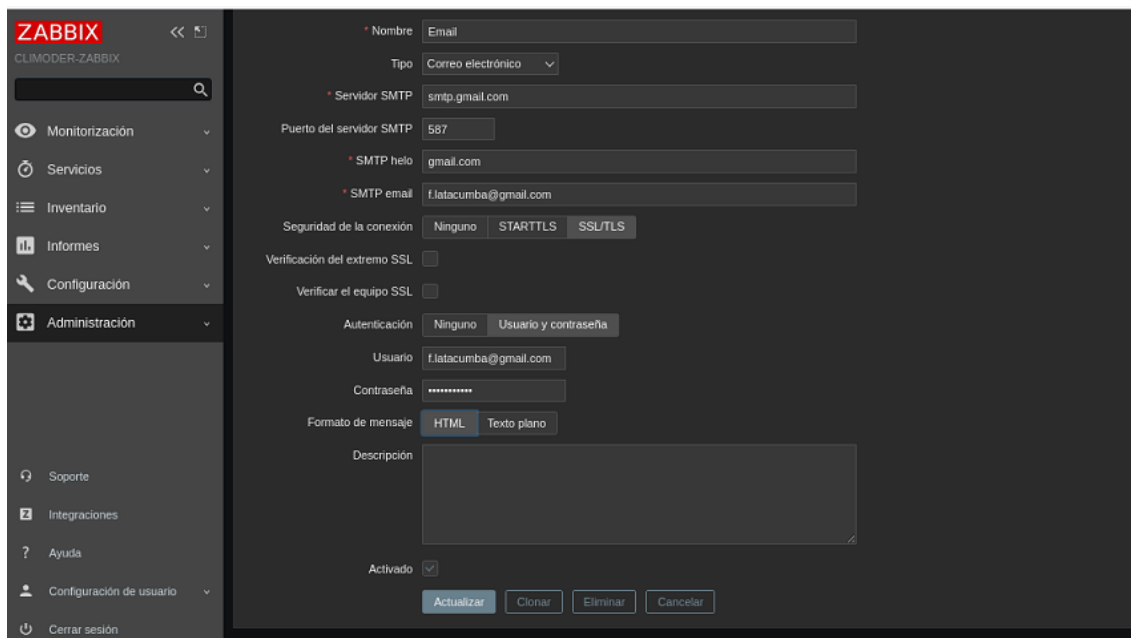
Generación de contraseña aleatorio para posterior configuración de email de alertas en el servidor Zabbix



Una vez se tenga la contraseña de la aplicación generada, será necesario ingresar con la cuenta del usuario de administración de Zabbix y en el apartado de *Administración* > *Acciones* se deberá seleccionar y activar la opción de “*Email*” en donde se desplegará lo siguientes campos para configurar el correo electrónico al que se enviará las notificaciones como se evidencia en la Figura 58. Se ha habilitado la autenticación mediante usuario y contraseña, utilizando la dirección **f.latacumba*****@gmail.com** como remitente.

Figura 58

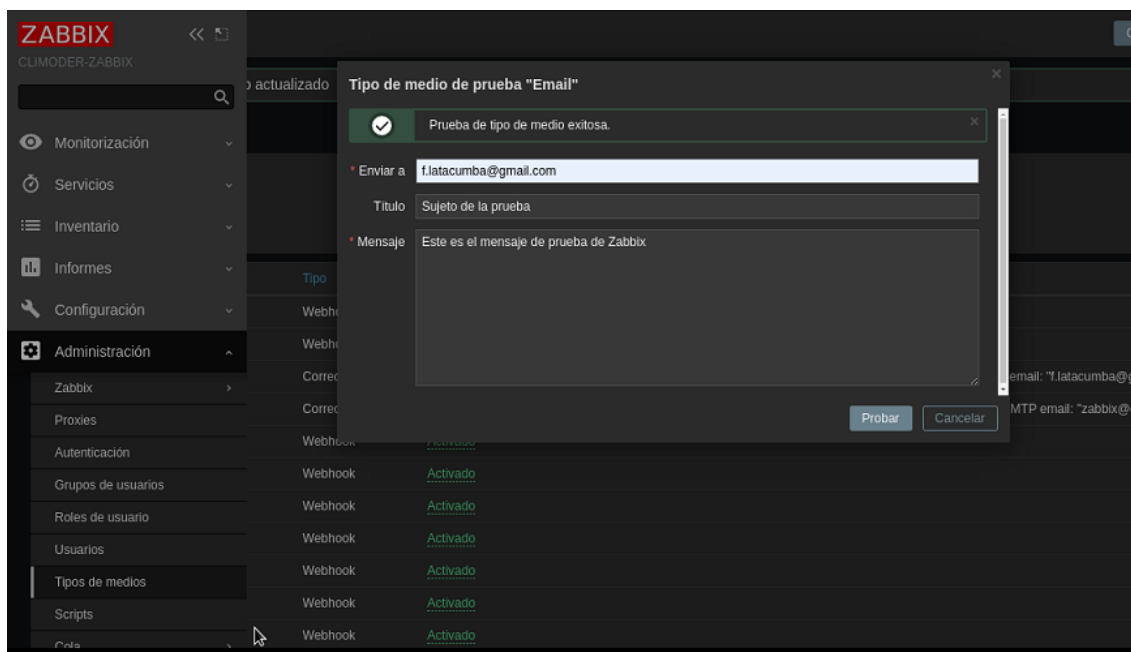
Configuración de parámetros correspondientes al correo electrónico utilizado para el envío de Triggers de los dispositivos monitoreados por Zabbix



Posteriormente se deberá realizar una prueba de envío y recepción de una alerta al correo electrónico utilizado dentro de Zabbix como se muestra en la Figura 59.

Figura 59

Prueba de envío correcto de notificaciones hacia la dirección de correo electrónico



A continuación, se evidencia la notificación de prueba que se envía al correo electrónico como se muestra en la Figura 60.

Figura 60

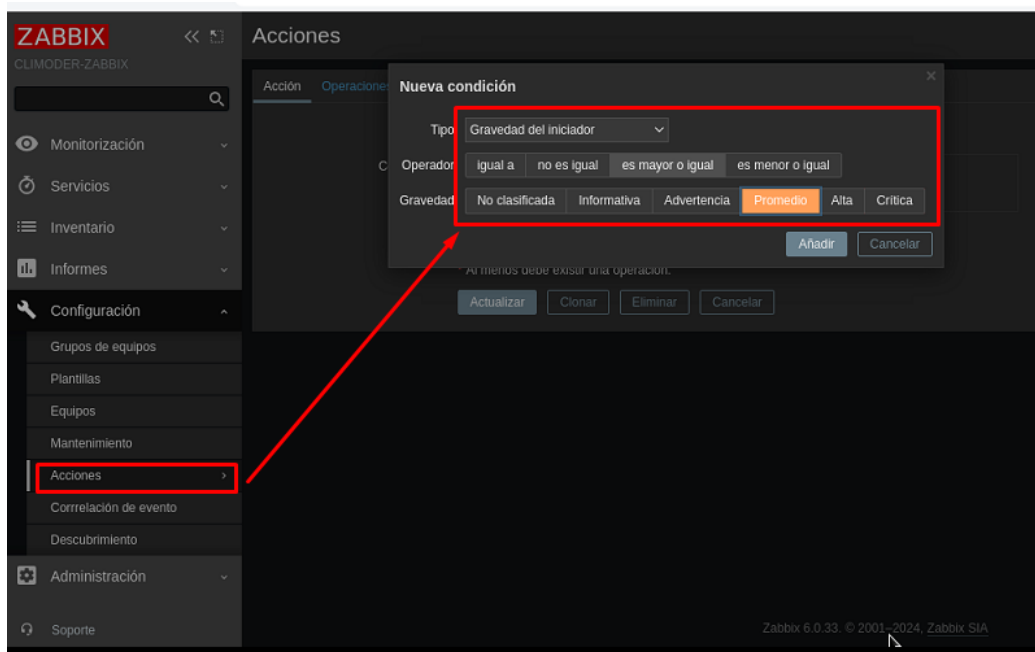
Correo de confirmación de sujeto de prueba correctamente configurado dentro de Zabbix hacia la dirección de Gmail ingresada



Ahora se procede a configurar los mensajes de notificaciones según la gravedad del equipo o servicio que se esté presentando como se evidencia en la Figura 61. Para este ejemplo y como recomendación en entorno de producción es recomendable aplicar la configuración en donde todo evento anómalo por más sencillo que parezca o resulte ser, debe ser notificado al correo electrónico.

Figura 61

Adición de nuevas condiciones según la gravedad que envíen los Triggers por medio de notificaciones de Zabbix hacia el correo electrónico



Si se ha realizado correctamente todo el proceso anterior, se podrá observar y recibir las notificaciones de los Triggers generados por Zabbix que se están enviando al correo electrónico personal como se evidencia en la Figura 62.

Figura 62

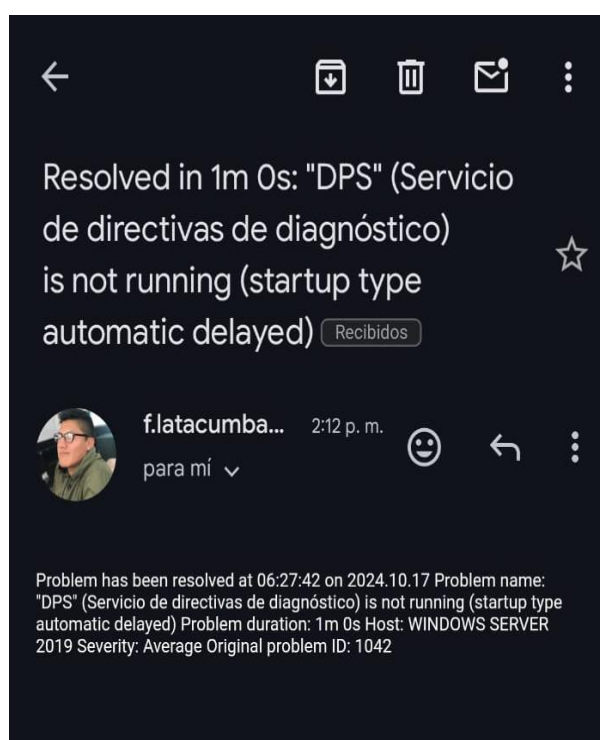
Notificación de Triggers generados por Zabbix y notificados por medio de correo



Para más detalle se evidencia en la Figura 63 el tipo de problema sobre el servicio de directivas de diagnóstico con demás características y detalles que evidencian las alertas de los Triggers que envía Zabbix sobre alguna anomalía del servidor Windows Server 2019 directamente al correo electrónico configurado.

Figura 63

Notificación detallada de Triggers generados con parámetros configurados previamente



4.5.8. Proxy Transparente

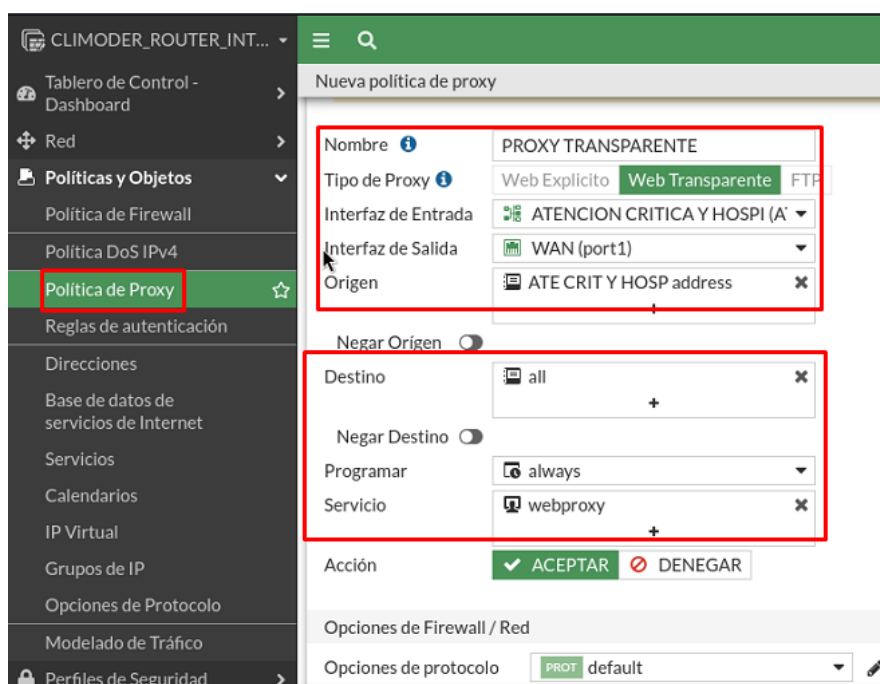
Un proxy transparente es aquel donde el usuario o dispositivo final no necesita ejecutar algún tipo de configuración para la navegación, actuando como servidor intermediario entre el dispositivo de un usuario y el sitio web al que se intenta acceder. Por lo que, basado en las recomendaciones y directrices del estándar de la NIST Special Publication 800-41 Revision 1, se configura en el router FortiGate el proxy transparente que actúa como una función integrada en lugar de un servidor proxy externo dedicado, interceptando y analizando el tráfico HTTP/HTTPS en tiempo real. Además, cuando se

habilita el proxy transparente en FortiGate, es posible aplicar políticas de seguridad, como; filtrado de contenido (bloquear sitios inapropiados), inspección de seguridad (como la detección de amenazas en tráfico web) y control de ancho de banda sin que los usuarios finales sepan que su tráfico está pasando a través de un proxy.

Para la demostración de la simulación realizada de la configuración de un proxy transparente en un router FortiGate como se evidencia en la Figura 64, se empieza creando la nueva política de proxy de tipo web transparente eligiendo la interfaz de entrada desde donde se realizará las solicitudes HTTP/HTTPS para este ejemplo se ha seleccionado la VLAN “Atención crítica y hospitalaria” y por medio de la interfaz de salida hacia el exterior por el puerto “WAN”.

Figura 64

Configuración inicial del proxy web transparente en router FortiGate

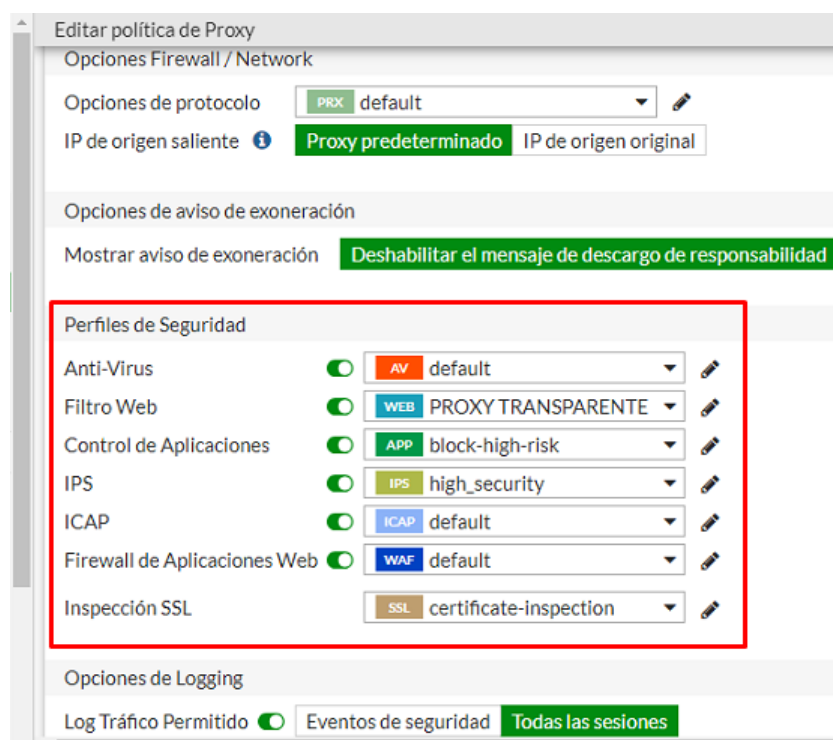


En la Figura 65 se realiza la selección de los perfiles de seguridad como; Anti – virus (AV) lo que permitirá inspeccionar el tráfico en caso de que exista malware o virus utilizando el motor antivirus que viene por defecto en FortiGate, además se hace énfasis

en la selección de filtro web (WEB) lo que significa que el proxy interceptará el tráfico y por medio de reglas de filtrado que pueden aplicarse para restringir el acceso a ciertos sitios o categorías de contenido prohibido o inapropiado. Se evidencia además la activación de IPS (Sistema de prevención de intrusiones) con un perfil de alta seguridad, permitiendo detectar y bloquear ataques o amenazas basadas en patrones de tráfico sospechoso, la selección del Firewall de aplicaciones Web (WAF) permite proteger aplicaciones web dentro de la red contra ataques como inyecciones SQL o cross – site scripting (XSS), asegurando la integridad de aplicaciones y datos web. Finalmente se evidencia la selección de inspección de tráfico cifrado SSL/TLS mediante un perfil de inspección de certificados, donde FortiGate verifica los certificados de sitios web para garantizar que el tráfico sea seguro y no esté siendo manipulado o interceptado.

Figura 65

Selección de perfiles de seguridad para política de proxy web transparente en router FortiGate.



En cuanto al bloqueo de URLs o filtro de ciertos sitios web se tiene como opción principal e intuitiva el uso de filtro basado en categorías de FortiGuard el cual es un servicio de suscripción de Fortinet que provee una base de datos constantemente actualizada de sitios web y direcciones IP que permite clasificar y restringir el acceso a contenido en internet según categorías predefinidas como “Redes sociales”, “Casinos online”, “Web oscura”, “Pornografía”, entre muchas otras. Para la demostración detallada del bloqueo de sitios web prohibidos o que no serían utilizados de manera ética, se crea manualmente el filtro URL para bloquear el sitio de apuestas “BET365” aplicando el filtro de tipo “Expresión regular” que permite definir patrones avanzados para cubrir múltiples coincidencias en lugar de especificar URLs exactas como se muestra en la Figura 66.

Figura 66

Bloqueo de URLs para el filtro web dentro de la política de proxy web transparente

Editar perfil de filtrado Web

Motores de Búsqueda

Imponer 'Búsqueda Segura' en Google, Yahoo!, Bing, Yandex

Restringir Acceso a YouTube

Registrar en log todas las palabras claves de la búsqueda

Filtro de URL Estática

Bloqueo de URLs inválidos

Filtro URL

[+ Crear nuevo](#) [Editar](#) [Borrar](#)

URL	Tipo	Acción	Estado
bet365.	Expresión Regular	<input checked="" type="checkbox"/> Bloquear	<input checked="" type="checkbox"/> Habilitar
xxx.	Expresión Regular	<input checked="" type="checkbox"/> Bloquear	<input checked="" type="checkbox"/> Habilitar

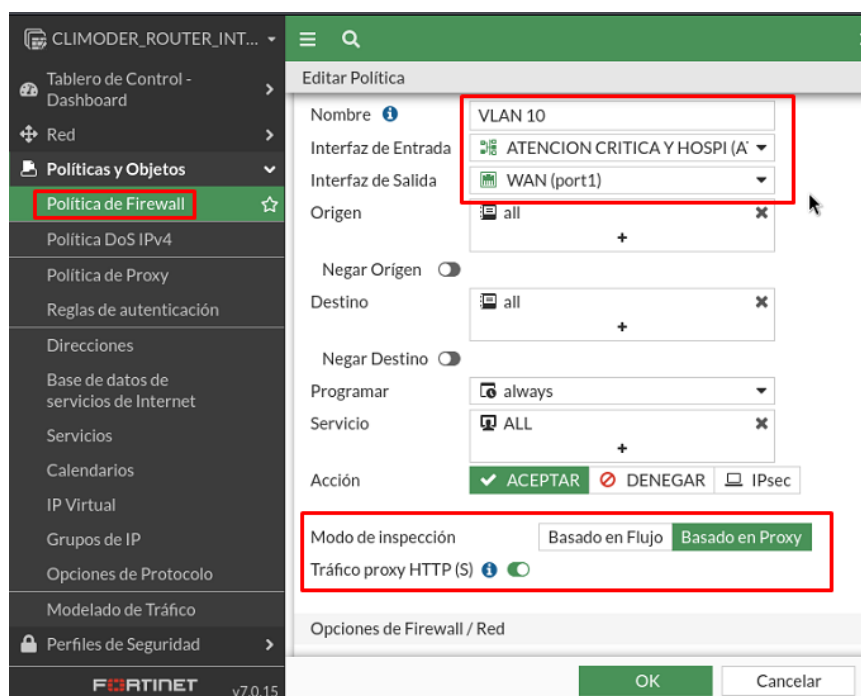
Bloquear URLs maliciosas descubiertas por FortiSandbox

Filtrado de Contenido Web

Sera necesario crear una política de firewall para el acceso a internet desde la VLAN “Atención crítica y hospitalaria” hacia la WAN como se evidencia en la Figura 67, habilitando el modo de inspección basado en proxy utilizado para una inspección más profunda del tráfico a interceptar y almacenar temporalmente los datos en el firewall, permitiendo un análisis más detallado, donde se requiere un alto nivel de seguridad y un análisis exhaustivo del contenido de tráfico detallado de aplicaciones y contenido.

Figura 67

Creación de política de firewall haciendo uso de modo de inspección basado en proxy



Finalmente se tiene la comprobación mediante un cliente Windows 10 que hace una consulta al sitio web “BET365”, reflejando que la petición al sitio ha sido bloqueada debido a que esa URL ha sido baneada como se muestra en la Figura 68, comprobando la correcta aplicación y configuración del proxy transparente dentro del router FortiGate.

Figura 68

Comprobación de página bloqueada por medio del uso de proxy transparente web



Web Page Blocked!

The page you have requested has been blocked, because the URL is banned.

URL: <http://www.bet365.com/>

User name:
Group name:
URL Source: Local URLfilter Block

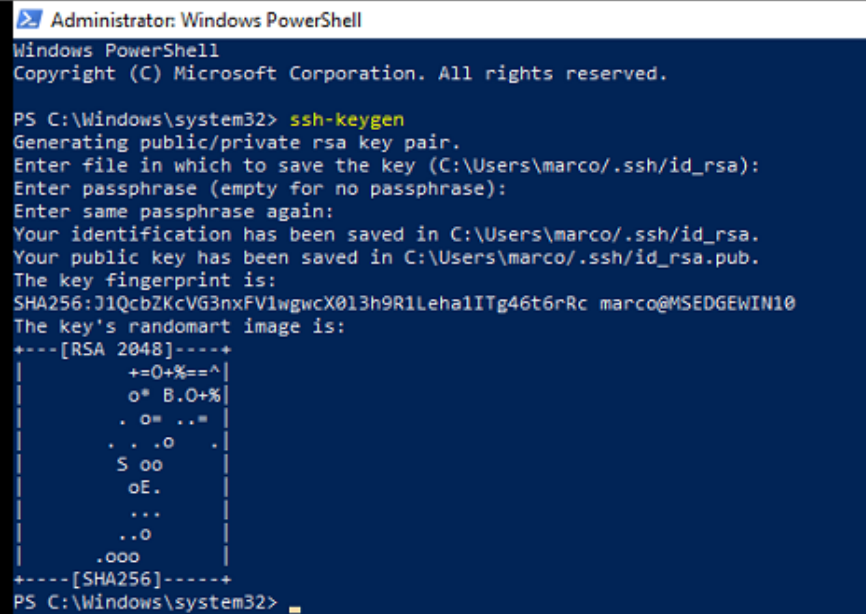
4.5.9. Acceso SSH mediante llaves criptográficas

Este método de seguridad basada en la autenticación mediante el uso de claves criptográficas, lo que permite a los usuarios conectarse a un servidor remotamente sin la necesidad de ingresar las típicas contraseñas cada vez que desee ingresar, lo que posibilita que el proceso sea más seguro y menos vulnerable a ataques de fuerza bruta o a intentos de robo de credenciales. Los pares de claves hacen referencia a los archivos de clave pública y privada que utilizan determinados protocolos de autenticación, lo que permite al servidor SSH y al cliente comparar la clave pública de un usuario proporcionado con la clave privada. Si la clave pública del servidor no se pudiera validar con la clave privada del lado del cliente, se producirá un error de autenticación.

Por lo que, en base a las directrices y recomendaciones del estándar de la NIST Special Publication 800-57 Parte 1, para la demostración se toma como ejemplo el uso del servidor Windows Server 2019 y de un cliente Windows 10 mediante el uso de OpenSSH, mismo donde se realizará la generación de claves de usuario tanto privadas y públicas con el algoritmo de encriptación RSA_2048 como se muestra en la Figura 69.

Figura 69

Generación de llave con OpenSSH en cliente Windows 10



```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

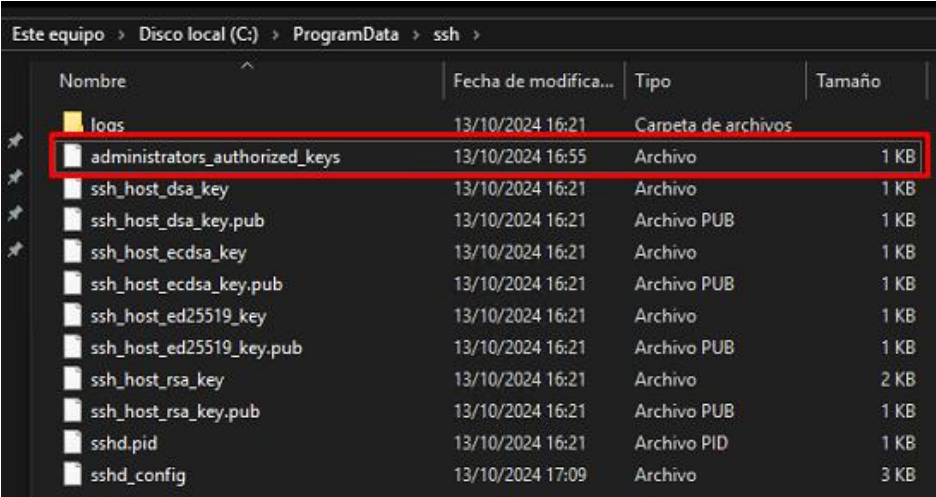
PS C:\Windows\system32> ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\marco/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\marco/.ssh/id_rsa.
Your public key has been saved in C:\Users\marco/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:J1QcbZKcVG3nxFV1wgwcX013h9R1Leha1ITg46t6rRc marco@MSEEDGEWIN10
The key's randomart image is:
+----[RSA 2048]-----+
|
|  o* B.O+%
|  . o= .."
|  . . .O .
|  S oo
|  oE.
|  ...
|  ..O
|  .ooo
+----[SHA256]-----+
PS C:\Windows\system32>

```

Para poder hacer uso de la clave del usuario que se creó previamente, se debe colocar el contenido de la clave pública (ssh_host_rsa_key.pub) en el servidor dentro de la carpeta ssh en un archivo de texto creado y nombrado manualmente como administrators_authorized_keys, dando los permisos correspondientes a dicho archivo de clave pública dentro del servidor como se evidencia en la Figura 70.

Figura 70

Administración de llave pública dentro de Windows Server 2019



Nombre	Fecha de modifica...	Tipo	Tamaño
logs	13/10/2024 16:21	Carpeta de archivos	
administrators_authorized_keys	13/10/2024 16:55	Archivo	1 KB
ssh_host_dsa_key	13/10/2024 16:21	Archivo	1 KB
ssh_host_dsa_key.pub	13/10/2024 16:21	Archivo PUB	1 KB
ssh_host_ecdsa_key	13/10/2024 16:21	Archivo	1 KB
ssh_host_ecdsa_key.pub	13/10/2024 16:21	Archivo PUB	1 KB
ssh_host_ed25519_key	13/10/2024 16:21	Archivo	1 KB
ssh_host_ed25519_key.pub	13/10/2024 16:21	Archivo PUB	1 KB
ssh_host_rsa_key	13/10/2024 16:21	Archivo	2 KB
ssh_host_rsa_key.pub	13/10/2024 16:21	Archivo PUB	1 KB
sshd.pid	13/10/2024 16:21	Archivo PID	1 KB
sshd_config	13/10/2024 17:09	Archivo	3 KB

De esta manera corta y sencilla es posible completar los pasos de configuración necesaria para usar la autenticación con OpenSSH basada en claves criptográficas, siempre y cuando el usuario desee conectarse al servidor desde cualquier cliente que tenga la clave privada, además se hace hincapié en permitir 3 intentos de inicio de sesión al momento de colocar la contraseña de la clave privada como también limitar en lo posible a 2 inicios de sesión como máximo dentro del servidor como se muestra en la Figura 71.

Figura 71

Condiciones y restricciones configuradas para el acceso de llaves criptográficas SSH

```
# Authentication:
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
MaxAuthTries 3
MaxSessions 2
PubkeyAuthentication yes
```

En la Figura 72 se evidencia como ejemplo la conexión SSH desde un cliente Windows 10 hacia Windows Server 2019 mediante el uso de claves criptográficas.

Figura 72

Comprobación de acceso a servidor Windows Server2019 mediante uso de llaves criptográficas SSH

```
Microsoft Windows [Versión 10.0.17763.6293]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

climoder\administrador@WIN-9CPHU2M4TK4 C:\Users\Administrador>
climoder\administrador@WIN-9CPHU2M4TK4 C:\Users\Administrador>exit
Connection to 192.168.0.227 closed.

C:\Windows\system32>ssh administrador@192.168.0.227
Enter passphrase for key 'C:\Users\marco/.ssh/id_ed25519':
```

4.5.10. Iptables en servidores Linux

Iptables es una aplicación de firewall basada en Linux que permite controlar el tráfico entrante y saliente, además de ser una herramienta esencial utilizada para proteger un servidor, limitar el acceso a aplicaciones o servicios específicos, mitigando en lo posible el riesgo de ataques maliciosos.

Para la demostración de esta configuración, en base a las directrices y recomendaciones que menciona el estándar de la NIST Special Publication 800-41 Revision 1, se toma como ejemplo al servidor Debian 10 simulado como parte de la verificación de las políticas de ciberseguridad para Nova Clínica Moderna, al cual se le ha aplicado mediante línea de comandos ciertas reglas que permitirán brindar mayor seguridad a los servidores Linux, como se muestran a continuación.

En ciertos entornos productivos es necesario permitir el acceso SSH para administrar el servidor de forma remota, por lo que es importante limitar este acceso solo a IPs de confianza en lo posible con el siguiente comando:

```
iptables -A INPUT -p tcp -s (Dirección IPv4) --dport (Puerto) -j ACCEPT
```

Además se agrega una limitación de intentos de conexión SSH para evitar ataques de fuerza bruta, limitando a solo 3 intentos de inicio de sesión en 60 segundos haciendo uso del siguiente comando:

```
iptables -A INPUT -p tcp --dport (Puerto) -m state --state NEW -m recent --update  
--seconds 60 --hitcount 3 -j DROP
```

También se hace énfasis en la protección contra el escaneo de puertos, bloqueando conexiones sin estado haciendo uso de los siguientes comandos:

```
iptables -A INPUT -p tcp --syn -m conntrack --ctstate NEW -j DROP
```

```
iptables -A INPUT -f -j DROP
```

Así también se implementa una regla donde se limite el tráfico ICMP que puede ayudar a evitar ciertos tipos de ataques de DoS con los siguientes comandos:

```
iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/s -j
ACCEPT
```

```
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
```

```
iptables -A INPUT -p tcp --syn -m limit --limit 1/s -j ACCEPT
```

4.5.11. Configuración de seguridad para servidor de VoIP – Elastix

Se tiene finalmente la configuración del firewall del servidor de VoIP Elastix, en base a las directrices y recomendaciones del estándar de la NIST Special Publication 800-58, donde se habilita únicamente los protocolos SIP, RTP, SRTP e IAX2, necesarios para hacer uso del servicio de VoIP dentro de la empresa únicamente en la VLAN de voz empresarial, y deshabilitando los protocolos que no intervienen dentro de dicho servicio como se evidencia en la Figura 73, mejorando así la seguridad y rendimiento al aislar el tráfico de VoIP, evitando que otros usuarios de la red puedan interceptar las llamadas y protegiendo el sistema de posibles ataques.

Figura 73

Tabla de reglas de Firewall para tráfico UDP en servidor de VoIP Elastix

<input type="checkbox"/>	24		ENTRADA: eth0	192.168.10.0/24	0.0.0.0/0	UDP	Puerto Origen: SIP Puerto Destino: SIP		
<input type="checkbox"/>	25		ENTRADA: eth0	192.168.10.0/24	0.0.0.0/0	UDP	Puerto Origen: RTP Puerto Destino: RTP		
<input type="checkbox"/>	26		ENTRADA: eth0	192.168.10.0/24	0.0.0.0/0	UDP	Puerto Origen: IAX2 Puerto Destino: IAX2		
<input type="checkbox"/>	27		SALIDA: eth0	192.168.10.0/24	0.0.0.0/0	UDP	Puerto Origen: SIP Puerto Destino: SIP		
<input type="checkbox"/>	28		SALIDA: eth0	192.168.10.0/24	0.0.0.0/0	UDP	Puerto Origen: RTP Puerto Destino: RTP		
<input type="checkbox"/>	29		SALIDA: ANY	192.168.10.0/24	0.0.0.0/0	UDP	Puerto Origen: IAX2 Puerto Destino: IAX2		

Además, se restringe el tráfico TCP específicamente HTTP y HTTPS como se evidencia en la Figura 74, para que sea accesible únicamente desde el pool de direcciones de la VLAN de voz, asegurado que la red de VoIP limite el acceso web únicamente a dispositivos autorizados. Reduciendo el riesgo de accesos no autorizado y posibles ataques desde otras partes de la red, también facilita la gestión de tráfico y la aplicación de políticas de seguridad más precisas para proteger el sistema de VoIP.

Figura 74

Tabla de reglas de Firewall para Tráfico TCP en servidor de VoIP Elastix

Orden	Tráfico	Objetivo	Interfaz	Dirección Origen	Dirección Destino	Protocolo	Detalles
22	Entrada	Permitido	eth0	192.168.10.0/24	0.0.0.0/0	TCP	Puerto Origen: HTTP Puerto Destino: HTTP
23	Salida	Permitido	eth0	192.168.10.0/24	0.0.0.0/0	TCP	Puerto Origen: HTTP Puerto Destino: HTTP
24	Entrada	Permitido	eth0	192.168.10.0/24	0.0.0.0/0	TCP	Puerto Origen: HTTPS Puerto Destino: HTTPS
25	Salida	Permitido	eth0	192.168.10.0/24	0.0.0.0/0	TCP	Puerto Origen: HTTPS Puerto Destino: HTTPS

Finalmente se tiene la deshabilitación y cambio de cierto número de puertos predeterminados para servicios de VoIP como se observa en la Figura 75, contribuyendo a la mejora de la seguridad al reducir la superficie de posibles ataques, minimizando la exposición a escaneos o posibles ataques automatizados, por lo que al usar puertos no estándar, dificultará la identificación de servicios críticos, evitando posibles intentos de explotación. Además, el cierre de puertos innecesarios limita las vías de acceso no autorizados, enfocándose en mantener el tráfico de dicha voz en los servicios esenciales para el sistema de VoIP.

Figura 75

Cambio de número de puertos configurados por protocolo en el Firewall de Servidor de VoIP Elastix.

	Nombre	Protocolo	Detalles	Opción
<input type="checkbox"/>	HTTP	TCP	Puerto 8888	Ver
<input type="checkbox"/>	HTTPS	TCP	Puerto 8443	Ver
<input type="checkbox"/>	SMTP	TCP	Puerto 2525	Ver
<input type="checkbox"/>	SIP	UDP	Puertos 5004:5082	Ver
<input type="checkbox"/>	RTP	UDP	Puertos 10000:20000	Ver
<input type="checkbox"/>	IAX2	UDP	Puerto 4569	Ver
	Nombre	Protocolo	Detalles	Opción

RESULTADOS Y ANÁLISIS

El proceso de auditoría de seguridad a la red de Telecomunicaciones de Nova Clínica Moderna tiene como propósito final el evaluar el conjunto de políticas propuestas, las cuales han sido desarrolladas a través de mesas de trabajo en colaboración con el líder del área de TIC'S de la empresa, evidenciado en el Anexo 19. Dichas políticas diseñadas como recomendaciones para su posible implementación futura, en caso de que la empresa así lo desee, no han sido aplicadas en un entorno operativo real, sin embargo, se ha realizado un análisis exhaustivo y la simulación de un conjunto selecto de políticas técnicas en entornos controlados como GNS3, tratando en lo posible englobar la mayor parte de las políticas desarrolladas. Esto ha permitido validar parcialmente su viabilidad técnica y su alineación con los objetivos de ciberseguridad que la empresa podría alcanzar en el futuro.

La verificación de los resultados se llevó conjuntamente con el líder del área de TIC'S, lo que ha contribuido en corroborar la correcta alineación con los objetivos que se plantea dentro del alcance y objetivos propuestos en el presente trabajo para mejorar la seguridad de la red a largo plazo, siempre y cuando se cuente con la aprobación de los principales directivos de la empresa. Así la organización puede considerar estas políticas como guías estratégicas que, de implementarse a futuro, contribuirían de manera significativa a la mejora de la fortaleza de protección de la infraestructura de telecomunicaciones de dicha empresa.

Riesgo residual proyectado para cableado horizontal y vertical

Inicialmente, cada riesgo potencial fue evaluado en términos de probabilidad e impacto inicial, determinando así su zona de riesgo y asignándole un valor cuantitativo en base a su nivel de criticidad. Entre los riesgos destacados para este activo crítico se mencionan; interferencia electromagnética, acceso no autorizado y fallo del cableado físico, los cuales representan amenazas significativas para la eficiencia, seguridad y continuidad de las comunicaciones. Para cada riesgo potencial identificado, se ha designado políticas específicas, con el propósito de reducir la probabilidad e impacto de estos incidentes a futuro. Estas políticas establecen controles técnicos y operativos, tales como el uso de accesos restringidos y mantenimientos periódicos, alineados con estándares de la NIST y recomendaciones de la función proteger de dicho marco de ciberseguridad.

La recomendación de estas políticas en un escenario hipotético permite visualizar en la Tabla 41 como los riesgos residuales se reducen a niveles bajos, minimizando así la probabilidad y el potencial impacto sobre el cableado estructurado de la empresa. Este análisis desarrollado mediante una mesa de trabajo junto al líder del área de TIC'S de la empresa, proporciona una base sólida para la toma de decisiones futuras en materia de seguridad y establece un marco para la mejora continua en la protección de la infraestructura crítica de la red de la empresa.

Tabla 41

Análisis de riesgos residuales para cableado horizontal y vertical dentro de la infraestructura tecnológica

Activo Crítico	Riesgo Potencial	Probabilidad Inicial	Impacto Inicial	Zona de Riesgo Inicial	Valor Cuantitativo	Política Recomendada	Probabilidad Residual	Impacto Residual	Zona de Riesgo Residual	Valor Cuantitativo
Cableado Horizontal y Vertical	Interferencia electromagnética	Baja (2)	Medio (3)	Moderado	6	Art. 9 Art. 53 Art. 54	Muy Baja (1)	Bajo (2)	Bajo	2
	Reducción significativa de la eficiencia en las comunicaciones y transferencia de datos.									
	Conexiones no autorizadas. Percepción negativa de la empresa en cuanto a la seguridad de transmisión de datos.	Baja (2)	Medio (3)	Moderado	6	Art. 9 Art. 44 Art. 53	Muy Baja (1)	Bajo (2)	Bajo	2
	Fallo del Cableado Interrupciones en los servicios de red y la operatividad de los sistemas dependientes.	Baja (2)	Alto (4)	Alto	8	Art. 9 Art. 53 Art. 54 Art. 55	Muy Baja (1)	Bajo (2)	Bajo	2

Nota: Elaborado a partir de mesa de trabajo con el líder del área de TIC'S. Adaptado de (NIST, 2012)

Riesgo residual proyectado para Routers Firewall FortiGate

Para el análisis de riesgos potenciales realizados sobre los routers de la empresa, el enfoque principal busca identificar áreas críticas donde una configuración defectuosa, políticas de firewall insuficientes o la saturación de recursos puedan comprometer la integridad y disponibilidad de los servicios críticos de la red. Por lo que, la creación y propuesta de políticas específicas para mitigar estos riesgos responde a la necesidad de establecer políticas de protección que reduzcan la probabilidad de que un evento o incidente se materialice, y pueda llegar a tener un impacto significativo dentro de los sistemas y demás recursos críticos de la empresa.

En la Tabla 42 se evidencia las políticas seleccionadas mediante un proceso de colaboración y análisis con el líder del área de TIC'S de la empresa, considerando las condiciones actuales y los recursos con los que dispone la organización para la mejora y continuidad operativa segura de la red de telecomunicaciones de la organización.

Por lo que se llega a la conclusión de la recomendación de estas políticas, que en un escenario hipotético, permitiría visualizar como los riesgos residuales se reducen a niveles moderados y bajos en caso de implementarse. Esto proporcionaría un marco de protección más robusto frente a posibles amenazas, minimizando así la probabilidad y el potencial impacto, alineando los controles de seguridad con los objetivos de continuidad y resiliencia de la red.

Tabla 42

Análisis de riesgos residuales para Routers Firewall dentro de la infraestructura tecnológica

Activo Crítico	Riesgo Potencial	Probabilidad Inicial	Impacto Inicial	Zona de Riesgo Inicial	Valor Cuantitativo	Política Recomendada	Probabilidad Residual	Impacto Residual	Zona de Riesgo Residual	Valor Cuantitativo
Routers Firewall FortiGate	Configuración defectuosa. Exposición o posible acceso no autorizado a segmentos internos críticos de la red.	Muy Baja (1)	Crítico (5)	Alto	5	Art. 9 Art. 53 Art. 54 Art. 55	Muy Baja (1)	Medio (3)	Moderado	3
	Políticas de firewall insuficientes frente a accesos a recursos y servicios no autorizados.	Baja (2)	Alto (4)	Alto	8	Art. 26 Art. 28 Art. 31 Art. 41 Art. 42	Muy Baja (1)	Medio (3)	Moderado	3
	Saturación de recursos de router firewall. Retraso de actividades operativas de la red.	Muy Baja (1)	Medio (3)	Moderado	3	Art. 23 Art. 41 Art. 43	Muy Baja (1)	Bajo (2)	Bajo	2

Nota: Elaborado a partir de mesa de trabajo con el líder del área de TIC'S. Adaptado de (NIST, 2012)

Riesgo residual proyectado para Conmutadores

Para el siguiente análisis se consideran los riesgos potenciales como; sobrecarga de tráfico, la intrusión mediante conexiones no autorizadas y el fallo de hardware o software en los conmutadores, cada uno con la probabilidad y el impacto potencial de interrumpir los servicios críticos de la empresa y afectar la percepción de seguridad. Por lo que, mediante un análisis y discusión con el líder del área de TIC'S de la empresa se determinó que las políticas seleccionadas y evidenciadas en la Tabla 43, pueden llegar a minimizar la probabilidad de interrupciones o accesos no autorizados y reducir el impacto de cualquier fallo en los conmutadores, garantizando así un entorno de red más estable y seguro para el funcionamiento operativo de la organización.

En general la posible implementación de las políticas seleccionadas en un escenario hipotético permitiría visualizar como los riesgos residuales se reducen a niveles bajos y moderables en caso de que se llegaran a aplicar, asegurando la protección frente a posibles incidentes, permitiendo a la empresa tener una infraestructura de conmutación más robusta, disminuyendo vulnerabilidades y mejorando la resiliencia de los sistemas críticos de la red.

Tabla 43

Análisis de riesgos residuales para Conmutadores dentro de la infraestructura tecnológica

Activo Crítico	Riesgo Potencial	Probabilidad Inicial	Impacto Inicial	Zona de Riesgo Inicial	Valor Cuantitativo	Política Recomendada	Probabilidad Residual	Impacto Residual	Zona de Riesgo Residual	Valor Cuantitativo
Conmutadores	Sobrecarga de Tráfico. Disminución de la velocidad de transferencia de datos.	Baja (2)	Medio (3)	Moderado	6	Art. 23 Art. 24 Art. 33	Muy Baja (1)	Bajo (2)	Bajo	2
	Intrusión en la Red mediante conexiones ethernet no autorizadas. Percepción de inseguridad en los servicios de la empresa.	Baja (2)	Medio (3)	Moderado	6	Art. 25 Art. 27 Art. 20 Art. 21	Muy Baja (1)	Bajo (2)	Bajo	2
	Fallo de los Conmutadores. Retraso de ejecución de servicios y operaciones de la red.	Baja (2)	Alto (4)	Alto	8	Art. 44 Art. 46 Art. 47 Art. 51 Art. 53	Muy Baja (1)	Alto (4)	Moderado	4

Nota: Elaborado a partir de mesa de trabajo con el líder del área de TIC'S. Adaptado de (NIST, 2012)

Riesgo residual proyectado para Equipos Servidores

Para el análisis de riesgos en los equipos servidores de la empresa se llegó a identificar riesgos potenciales como; configuración defectuosa, brechas de seguridad física y posibles interrupciones de servicio. Por lo que, mediante una mesa de trabajo con el líder del área de TIC'S se discutió y llegó a la conclusión de que las políticas seleccionadas y evidenciadas en la Tabla 44, están diseñados para reducir dichos riesgos potenciales, enfocándose en la configuración segura, la protección física del acceso a los servidores, así como también, los planes de contingencia ante fallos o interrupciones. Aunque dichas políticas se proponen como recomendaciones para un escenario hipotético, su implementación futura podría contribuir con la protección de la infraestructura de la red, garantizando la continuidad operativa de los servicios críticos y alineándose con los objetivos de seguridad y protección de datos de la empresa.

En conclusión, la posible implementación de las políticas seleccionadas en un escenario hipotético permitiría visualizar como los riesgos residuales se reducen a niveles bajos y moderables en caso de que se llegaran a aplicar, garantizando el fortalecimiento de la resiliencia y seguridad de los servidores críticos, así también, la disponibilidad y eficiencia de los sistemas dentro de la red de la empresa.

Tabla 44

Análisis de riesgos residuales para Equipos Servidores dentro de la infraestructura tecnológica

Activo Crítico	Riesgo Potencial	Probabilidad Inicial	Impacto Inicial	Zona de Riesgo Inicial	Valor Cuantitativo	Política Recomendada	Probabilidad Residual	Impacto Residual	Zona de Riesgo Residual	Valor Cuantitativo
Equipos Servidores	Configuración defectuosa. Interrupciones y disminución de eficiencia de servicios.	Baja (2)	Medio (3)	Moderado	6	Art. 49 Art. 50 Art. 51 Art. 52	Baja (2)	Bajo (2)	Bajo	4
	Brechas de Seguridad expuestas, debido a la exposición de acceso físico no autorizado al área de servidores.	Baja (2)	Medio (3)	Moderado	6	Art. 13 Art. 16 Art. 55	Muy Baja (1)	Bajo (2)	Bajo	2
	Interrupciones de Servicio. Paralización de operaciones dependientes de los servidores.	Baja (2)	Crítico (5)	Extremo	10	Art. 29 Art. 30 Art. 38 Art. 40 Art. 47 Art. 51 Art. 52 Art. 55	Muy Baja (1)	Alto (4)	Moderado	4

Nota: Elaborado a partir de mesa de trabajo con el líder del área de TIC'S. Adaptado de (NIST, 2012)

Riesgo residual proyectado para Troncal SIP

Para los riesgos de la Troncal SIP, activo crítico para las comunicaciones de voz en la organización, se llevó a cabo un análisis y discusión con el líder del área de TIC'S y se llegó a la conclusión de la moderada dependencia de los servicios de voz en los procesos operativos y administrativos de la empresa. Por lo que, a través de la auditoría, se han evaluado riesgos potenciales como; congestión de red, interceptación de llamadas y posibles interrupciones en el servicio, los cuales afectan tanto la calidad como la seguridad de las comunicaciones. Así también, se llegó a seleccionar un grupo selecto de políticas evidenciados en la Tabla 45, los cuales buscan disminuir estos riesgos mediante controles específicos que garantizan la continuidad y seguridad de los servicios de voz alineándose con las normativas de seguridad y protección de la infraestructura de red de la organización.

En general la posible implementación de las políticas seleccionadas en un escenario hipotético permitiría visualizar como los riesgos residuales se reducen a niveles muy bajos en caso de que se llegaran a aplicar, garantizando la continuidad operativa y la protección de los datos en las comunicaciones de voz, promoviendo un entorno seguro y eficiente para el desarrollo de las funciones que dependan de este servicio.

Tabla 45

Análisis de riesgos residuales para Troncal SIP dentro de la infraestructura tecnológica

Activo Crítico	Riesgo Potencial	Probabilidad Inicial	Impacto Inicial	Zona de Riesgo Inicial	Valor Cuantitativo	Política Recomendada	Probabilidad Residual	Impacto Residual	Zona de Riesgo Residual	Valor Cuantitativo
Troncal SIP	Congestión de Red. Reducción en la calidad y velocidad de las comunicaciones de voz.	Baja (2)	Medio (3)	Moderado	6	Art. 33 Art. 46	Muy Baja (1)	Muy Bajo (1)	Bajo	1
	Interceptación de Llamadas Percepción negativa de la seguridad de las comunicaciones.	Baja (2)	Medio (3)	Moderado	6	Art. 32 Art. 34 Art. 49 Art. 50	Muy Baja (1)	Muy Bajo (1)	Bajo	1
	Interrupción del Servicio de Voz. Afectación de las operaciones que dependen de las comunicaciones de voz.	Baja (2)	Alto (4)	Alto	8	Art. 32 Art. 51	Muy Baja (1)	Muy Bajo (1)	Bajo	1

Nota: Elaborado a partir de mesa de trabajo con el líder del área de TIC'S. Adaptado de (NIST, 2012)

Riesgo residual proyectado para Troncal analógica (FXO SIP Gateway)

Aunque actualmente muy poco utilizada dentro de la empresa debido al constante avance tecnológico en cuanto a los servicios de comunicaciones de voz se refiere, durante el análisis inicial de dicho activo junto al líder del área de TIC'S, se llega a la conclusión del declive de dependencia de dicho servicio dentro de la empresa en la actualidad, sin embargo, se han identificado riesgos potenciales como; posibles interferencias en las comunicaciones, riesgos de manipulación no autorizada y posibles fallos (hardware o software) en el sistema de comunicaciones, cada uno con su impacto en la calidad del servicio y seguridad de la red. Por lo que, para reducir estos riesgos, se han seleccionado políticas de seguridad específicas para dicho activo evidenciado en la Tabla 46, con el fin de reducir la posible probabilidad de ocurrencia y el posible impacto de posibles amenazas.

En conclusión, la recomendación e implementación de estas políticas en un escenario hipotético, permitiría visualizar como los riesgos residuales se reducen a niveles muy bajos en caso de que llegaran a aplicar. Esto proporcionaría un marco de protección más robusto para la integridad de las comunicaciones de voz analógicas, garantizando la continuidad operativa y prevenir, aunque muy mínimo, algún tipo de interrupción que pueda afectar el servicio tanto para clientes como para la empresa, promoviendo un entornos seguro y estable en la infraestructura de telecomunicaciones.

Tabla 46

Análisis de riesgos residuales para Troncal analógica (FXO SIP Gateway) dentro de la infraestructura tecnológica

Activo Crítico	Riesgo Potencial	Probabilidad Inicial	Impacto Inicial	Zona de Riesgo Inicial	Valor Cuantitativo	Política Recomendada	Probabilidad Residual	Impacto Residual	Zona de Riesgo Residual	Valor Cuantitativo
Troncal analógica (FXO SIP Gateway)	Interferencias en la Comunicación. Reducción en la calidad de las llamadas.	Media (3)	Bajo (2)	Moderado	6	Art. 33 Art. 46	Muy Baja (1)	Muy Bajo (1)	Bajo	1
	Manipulación no Autorizada. Riesgo de daños, pérdida de conectividad y fallos en las comunicaciones	Muy Baja (1)	Bajo (2)	Baja	2	Art. 9 Art. 13 Art. 16	Muy Baja (1)	Muy Bajo (1)	Bajo	1
	Fallo del Sistema de Comunicaciones. Paralización de servicios que dependen de las comunicaciones telefónicas.	Baja (2)	Medio (3)	Moderado	6	Art. 32 Art. 51	Muy Baja (1)	Muy Bajo (1)	Bajo	1

Nota: Elaborado a partir de mesa de trabajo con el líder del área de TIC'S. Adaptado de (NIST, 2012)

Riesgo residual proyectado para Infraestructura Wireless

En lo que respecta a la infraestructura inalámbrica, mediante una mesa de trabajo con el líder del área de TIC'S se llegó a identificar y cuantificar posibles riesgos potencialmente significativos que pueden comprometer la calidad del servicio y la seguridad de la red. Entre los principales riesgos evaluados se encuentra; interferencias de señal, la interrupción de la conectividad inalámbrica y la falta de autenticación en la red empresarial, lo que podría derivar en accesos no autorizados y comprometer los datos sensibles que se manipulen dentro de la organización. Además, se ha identificado un posible riesgo debido a la falta de mantenimiento del hardware y software de los puntos de acceso inalámbricos, lo cual podría afectar la disponibilidad y continuidad de las operaciones que dependen de esta conectividad.

Por lo que, para reducir la posible probabilidad de ocurrencia y posible impacto de la amenaza de estos riesgos potenciales, se han seleccionado políticas específicas de todo el conjunto, evidenciadas en la Tabla 47, como recomendación e implementación en un escenario hipotético, lo que permitiría visualizar como los riesgos residuales se reducen a niveles moderados y bajos en caso de que llegaran a aplicar. Estas políticas incluyen la implementación de controles de autenticación robustos, mantenimientos periódicos y la aplicación de mejores prácticas en la gestión de redes inalámbricas, con el objetivo de garantizar la seguridad y estabilidad de la infraestructura inalámbrica, brindando una conectividad confiable que soporte las operaciones y proteja la información crítica, al tiempo que se minimicen las interrupciones que podrían afectar la operaciones dependientes de este activo crítico.

Tabla 47

Análisis de riesgos residuales para Infraestructura Wireless dentro de la infraestructura tecnológica

Activo Crítico	Riesgo Potencial	Probabilidad Inicial	Impacto Inicial	Zona de Riesgo Inicial	Valor Cuantitativo	Política Recomendada	Probabilidad Residual	Impacto Residual	Zona de Riesgo Residual	Valor Cuantitativo
Infraestructura Wireless	Interferencias de Señal inalámbrica. Interrupción de la red inalámbrica	Baja (2)	Medio (3)	Moderado	6	Art. 48 Art. 52	Muy Baja (1)	Bajo (2)	Bajo	2
	Falta de autenticación de usuarios en la red con posible pérdida de datos sensibles	Baja (2)	Alto (4)	Alto	8	Art. 18 Art. 19 Art. 20 Art. 25	Muy Baja (1)	Medio (3)	Moderado	3
	Falta de mantenimiento de hardware y software de equipos. Afectación de operaciones que dependen de la conectividad inalámbrica.	Baja (2)	Medio (3)	Moderado	6	Art. 44 Art. 46 Art. 52 Art. 53	Muy Baja (1)	Bajo (2)	Bajo	2

Nota: Elaborado a partir de mesa de trabajo con el líder del área de TIC'S. Adaptado de (NIST, 2012)

Riesgo residual proyectado para las Estaciones de Trabajo

Para las estaciones de trabajo de la empresa, se ha evaluado y discutido de igual manera mediante una mesa de trabajo en conjunto con el líder del área d TIC'S, la selección de políticas de seguridad específicas a partir del conjunto desarrollado, con el objetivo de que tengan enfoque principal para reducir posibles riesgos potenciales como; pérdida de conectividad, accesos no autorizados, fallos de hardware, entre otros. Así mismo, estos riesgos han sido clasificados según los niveles de posible probabilidad e impacto potencial, por lo que, basado en la discusión y análisis realizado se logró seleccionas políticas que abarcan desde la implementación de autenticación robusta, la protección activa de la estaciones de trabajo y la adopción de medidas para evitar daños físicos de los equipos.

Por ende, en análisis de riesgos inicial y residual proporciona una visión cuantitativa y cualitativa del efecto de esta políticas de llegarse a aplicar en un escenario hipotético, reflejando como disminuye dichos riesgos a niveles moderados y bajos respectivamente, como se evidencia en la Tabla 48. El objetivo final es lograr un entorno seguro, donde se minimicen interrupciones operativas y se asegure la protección de datos sensibles que manipule el personal de la empresa, con un enfoque preventivo correctivo ajustado a los posibles riesgos potenciales en las estaciones de trabajo de la empresa.

Tabla 48

Análisis de riesgos residuales para Estaciones de Trabajo dentro de la infraestructura tecnológica

Activo Crítico	Riesgo Potencial	Probabilidad Inicial	Impacto Inicial	Zona de Riesgo Inicial	Valor Cuantitativo	Política Recomendada	Probabilidad Residual	Impacto Residual	Zona de Riesgo Residual	Valor Cuantitativo
Estaciones de Trabajo	Pérdida de conectividad debido a interrupciones en la red o por instalación de software malicioso que comprometa el rendimiento de los computadores.	Baja (2)	Medio (3)	Moderado	6	Art. 67 Art. 45 Art. 46 Art. 52	Muy Baja (1)	Medio (3)	Moderado	3
	Acceso no autorizado a las estaciones de trabajo, fuga de datos sensibles debido falta de seguridad como contraseñas débiles o falta de autenticación en los computadores.	Baja (2)	Alto (4)	Alto	8	Art. 18 Art. 25 Art. 26 Art. 27 Art. 62 Art. 63	Muy Baja (1)	Medio (3)	Moderado	3
	Fallos de hardware debido a picos de voltaje o fallo de software que afecte la operatividad de las estaciones de trabajo	Baja (2)	Medio (3)	Moderado	6	Art. 54 Art. 56 Art. 57	Muy Baja (1)	Bajo (2)	Bajo	2

Nota: Elaborado a partir de mesa de trabajo con el líder del área de TIC'S. Adaptado de (NIST, 2012)

DISCUSIÓN

Los resultados obtenidos durante el desarrollo del presente proyecto demuestran la disminución de riesgos residuales proyectada a futuro para una infraestructura de telecomunicaciones desde una perspectiva técnica; la auditoría logró presentar una posible reducción promedio del 67% en base a los posibles riesgos mencionados de dicha infraestructura tecnológica, destacando a los servicios de telefonía, donde el riesgo podría disminuir en un 83%. Este enfoque cuantitativo no solo evalúa la efectividad de las políticas desarrolladas en el caso de que se llegaran a implementar, sino que además respalda las decisiones estratégicas de la organización al priorizar la protección y seguridad de los activos críticos. Una de las principales diferencias radica en la orientación y alcance de los trabajos como el de (Bracho Ortega, 2017); estudio realizado a una empresa pública que se centra en evaluar y mejorar las medidas de seguridad de la organización mediante una auditoría de seguridad informática basándose en el estándar COBITv5 y siguiendo las directrices de la metodología OSSTMMv3, identificando puntos vulnerables dentro de la infraestructura tecnológica, lo que permitió recomendar medidas correctivas necesarias para mejorar la eficiencia y seguridad, implementando un conjunto de políticas de seguridad para mejorar la protección de la información y la continuidad operativa de dicha empresa pública.

Así también, se menciona el trabajo desarrollado por (León Gudiño, 2017); auditoría de seguridad de la información a la red interna de la Universidad Técnica del Norte mediante el uso de la metodología Offensive Security Professional Training and Tools For Security Specialists, lo que permitió identificar múltiples vulnerabilidades en la red interna y a partir de esos hallazgos, desarrollar políticas de seguridad alineadas con la norma ISO/IEC 27001, enfocadas en prevenir ataques cibernético como accesos no

autorizados, manipulación de servicios por terceros, denegación de servicios, ayudando fortalecer la protección de equipos, para los servicios WEB y DNS.

A diferencia de los anteriores trabajos desarrollados en instituciones públicas y académicas, donde las limitaciones presupuestarias y la ausencia de políticas de ciberseguridad son factores recurrentes, mientras que este trabajo aborda el estudio de una infraestructura de telecomunicaciones crítica de una empresa de salud privada, donde la confidencialidad e integridad de los datos tienen una prioridad superior, por lo que desde un inicio se corroboró que dicha empresa privada ya contaba con sólidas bases de seguridad en su infraestructura tecnológica para poder realizar el presente trabajo con el fin de fortalecer aun más la resiliencia operativa y la protección de los activos críticos de la red.

Finalmente se destaca la integración del marco de ciberseguridad de la NIST y la metodología OCTAVE, lo que permitió vincular la gestión de riesgos con la planificación estratégica de la organización, un aspecto que se destaca frente a los trabajos previamente revisados. Esto aseguró un enfoque más proactivo y adaptable para infraestructuras críticas, logrando resultados medibles que fortalecen la seguridad tecnológica, además de realizar pruebas de simulación de políticas específicas en entornos controlados como GNS3 para comprobar que la propuesta realizada se alinea con los estándares y metodologías usados durante el desarrollo del presente trabajo.

CONCLUSIONES

- El proceso de auditoría de seguridad a la red de Telecomunicaciones de Nova Clínica Moderna tuvo como finalidad, no solo identificar posibles falencias dentro de la red empresarial, sino además, brindar un conjunto de pautas y propuestas mediante un conjunto de políticas de seguridad para brindar protección y disminuir la posibilidad de que un riesgo pueda materializarse y afectar las operaciones críticas que dependan de los activos críticos que compone dicha infraestructura tecnológica.
- Al englobar al marco de ciberseguridad de la NIST, con enfoque en la función “Proteger”, y la metodología OCTAVE, utilizadas durante el proceso de auditoría y desarrollo de políticas, se llegó a investigar y acoplar dentro del presente trabajo temas como; identificación, valoración y perfilamiento de activos, gestión de seguridad, análisis de riesgos, entre otros. Así también, la revisión de publicaciones especiales de la NIST y estándares de ciberseguridad con respaldo de fuentes bibliográficas que sustenten el estudio realizado durante el desarrollo del proyecto, aportando mayor validez y eficacia al cumplimiento de los objetivos planteados.
- Tanto el análisis y evaluación de la situación actual de la infraestructura tecnológica, el desarrollo de las políticas de seguridad, y la verificación de los resultados obtenidos se llevaron a cabo de la mano y guía del líder del área de TIC'S de la empresa, cuya amplia experiencia y conocimiento especializado fueron fundamentales para asegurar una comprensión integral de la red y la adecuada creación de las políticas propuestas. Por lo que, su colaboración fue de suma importancia para orientar el proceso y garantizar que dichas políticas

estuvieran alineadas con las necesidades específicas y los objetivos estratégicos de la organización.

- Aunque Nova Clínica Moderna no tiene actualmente como objetivo principal el fortalecimiento de la seguridad en la red de telecomunicaciones, la empresa cuenta con sólidas bases de ciberseguridad, respaldada por su categorización y su destacada reputación tanto a nivel local como nacional. Si bien sus estándares actuales cumplen con las expectativas de una empresa de salud privada de alto prestigio, realizar este tipo de estudios y auditorías en esta área representa una oportunidad estratégica para robustecer aún más su infraestructura tecnológica, garantizando la operatividad segura de la empresa, además de preservar y fortalecer la imagen de confianza y excelencia que la empresa ha construido a lo largo de los años.
- La creación e implementación de políticas de seguridad permitirá a la empresa establecer un marco claro de protección de sus activos y datos dentro de la red de telecomunicaciones. Dichas políticas fomentarán prácticas que ayuden a reducir los riesgos y mejorar la resiliencia ante posibles amenazas, mediante una planificación estratégica que asegure la efectividad de cada medida de seguridad, mediante una previa evaluación que permita priorizar las necesidades principales y los recursos disponibles, adecuando las políticas al contexto organizacional.
- Los análisis de riesgos iniciales en comparación de los riesgos residuales de la infraestructura tecnológica muestran una posible reducción promedio del 67%, en caso de que exista la posibilidad de implementación de las políticas desarrolladas. Los riesgos iniciales en promedio alcanzaban valores cuantitativos de 7 puntos sobre 10, reduciéndose a un promedio de 2.3 puntos sobre 10, destacando activos como los servicios de telefonía que logran una reducción del riesgo del 83%.

RECOMENDACIONES

- Se recomienda realizar auditorías periódicas de seguridad dentro de la red empresarial siguiendo directrices de metodologías enfocadas en el análisis de riesgos que se pueden tomar como referencia para poder identificar vulnerabilidades, evaluar configuraciones, analizar el tráfico, entre otros. Esto debe complementarse con planes de mejora, actualizaciones regulares de software y capacitación del personal, asegurando así un entorno de red más seguro y protegido contra amenazas emergentes.
- Los altos directivos de la organización deberían prestar especial atención a las políticas y recomendaciones desarrolladas dentro del proyecto, con el fin de garantizar una futura implementación adecuada de medidas que fortalezcan la seguridad de la infraestructura tecnológica. Este compromiso sería clave para mantener un nivel óptimo de protección frente a posibles amenazas emergentes, asegurando la continuidad operativa de los activos críticos.
- Es recomendable que el área de TIC'S habilite un espacio de virtualización dentro de la empresa que este orientado a realizar pruebas de penetración y demás proyectos relacionados con la ciberseguridad. Esto permitirá simular configuraciones, escenarios de prueba y posibles amenazas que se puedan materializar de manera controlada, facilitando la identificación de vulnerabilidades y la evaluación de soluciones con mayor precisión y datos más reales.
- Se recomienda a la empresa incentivar y priorizar la capacitación continua del personal del área de TIC'S, mediante cursos especializados y la obtención de certificaciones reconocidas en ciberseguridad, como; ISO/IEC 27001, Cyber Essentials y SOC 2. Lo que permitirá asegurar el cumplimiento de estándares

internacionales, mediante la inversión de este tipo de formación, por ende la empresa podrá asegurar un marco de protección estructurado para su infraestructura de telecomunicaciones, alineando con las mejores prácticas del sector, reforzando su compromiso con la excelencia operativa y la preservación de su alta reputación.

REFERENCIAS BIBLIOGRÁFICAS

- Alberts, C., Dorofee, A., & Stevens, J. (2003). Introduction to the OCTAVE ® Approach. *Carnegie Mellon Software Engineering Institute*.
- Al-Matari, O. M., Helal, I. M. A., Mazen, S. A., & Elhennawy, S. (2018). Cybersecurity tools for IS auditing. *Proceedings - 2018 6th International Conference on Enterprise Systems, ES 2018*, 217–223. <https://doi.org/10.1109/ES.2018.00040>
- Asamblea Nacional de la República del Ecuador. (2002). *Ley de Comercio Electrónico, Firmas y Mensajes de Datos*. www.lexis.com.ec
- Asamblea Nacional de la República del Ecuador. (2008). CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR. *Registro Oficial*, 449(20), 25–2021. www.lexis.com.ec
- Asamblea Nacional de la República del Ecuador. (2014). *Ley de Propiedad Intelectual*. www.lexis.com.ec
- Asamblea Nacional de la República del Ecuador. (2015). *Ley Orgánica de Telecomunicaciones*.
- Asamblea Nacional de la República del Ecuador. (2019). *Ley Orgánica de Comunicación*. www.lexis.com.ec
- Asamblea Nacional de la República del Ecuador. (2020). *Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional*. www.lexis.com.ec
- Asamblea Nacional de la República del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*.
- Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., & Scarfone, K. (2016). *Guide for cybersecurity event recovery*. <https://doi.org/10.6028/NIST.SP.800-184>
- Barzilay, M. (2019). *IT Security Audit*. <https://www.researchgate.net/publication/333682624>
- Bracho Ortega, C. L. (2017). *Auditoría de seguridad informática dirigida al gobierno autónomo descentralizado del cantón Mira basado en el estándar cobitv5, siguiendo la metodología osstmmv3* [Universidad Técnica del Norte]. <https://repositorio.utn.edu.ec/handle/123456789/6878>
- Cauja Altamirano, M. J. (2024). *Metodología de un sistema DLP (Data Loss Prevention) para la entidad financiera “Cooperativa de Ahorro y Crédito Santa Anita Ltda.” basada en la norma ISO/IEC 27002:2022, sección 5.12 y 8.12*. <https://repositorio.utn.edu.ec/handle/123456789/15625>
- CSF NIST. (2018). Marco para la mejora de la seguridad cibernética en infraestructuras críticas. *Instituto Nacional de Estándares y Tecnología, Versión 1.1*. <https://doi.org/10.6028/NIST.CSWP.04162018es>
- Dac-Nhuong Le, Raghvendra Kumar, Brojo Kishore Mishra, Manju Khari, & Jyotir Moy Chetterjee. (2018). Introduction on Cybersecurity. In *Cyber Security in Parallel and Distributed Computing* (John Wiley & Sons, pp. 1–37). Wiley. <https://doi.org/10.1002/9781119488330.ch1>
- Daimi, K., & Peoples, C. (2021). Advances in cybersecurity management. In *Advances in Cybersecurity Management*. Springer International Publishing. <https://doi.org/10.1007/978-3-030-71381-2>

- Dempsey, K. L., Chawla, N. S., Johnson, L. A., Johnston, R., Jones, A. C., Orebaugh, A. D., Scholl, M. A., & Stine, K. M. (2011). *Information Security Continuous Monitoring (ISCM) for federal information systems and organizations*.
<https://doi.org/10.6028/NIST.SP.800-137>
- Drägerwerk AG & Co. KGaA. (2017). Ciberataques: riesgo para los centros sanitarios. *Static.Draeger.Com*. <https://youtu.be/yLQ-BZ6dnHc>,
- Dykstra, J., Mathur, R., & Spoor, A. (2020). Cybersecurity in Medical Private Practice: Results of a Survey in Audiology. *Proceedings - 2020 IEEE 6th International Conference on Collaboration and Internet Computing, CIC 2020*, 169–176.
<https://doi.org/10.1109/CIC50333.2020.00029>
- Enrique, J., Chang, A., Juan, T., & Aguirre, B. (2020). ANÁLISIS DE ATAQUES CIBERNÉTICOS HACIA EL ECUADOR. *Revista Científica Aristas*, 2(1).
- Ervural, B. C., & Ervural, B. (2018). Overview of Cyber Security in the Industry 4.0 Era. In *Springer Series in Advanced Manufacturing* (pp. 267–284). Springer Nature.
https://doi.org/10.1007/978-3-319-57870-5_16
- Fernandez, E. B., Yoshioka, N., Washizaki, H., & Yoder, J. (2022). Abstract security patterns and the design of secure systems. *Cybersecurity*, 5(1), 1–17.
<https://doi.org/10.1186/S42400-022-00109-W/TABLES/1>
- Fernando Maymi, & Shon Harris. (2021). *Security Models and Architecture* (McGraw-Hill/Osborne Media, Ed.; #9a). McGraw Hill.
- Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, 58, 102726. <https://doi.org/10.1016/J.JISA.2020.102726>
- Hewlett Packard Enterprise Development LP. (2022). HOJA TÉCNICA SWITCHES CON ADMINISTRACIÓN INTELIGENTE CARACTERÍSTICAS CLAVE. *Hewlett Packard Enterprise*.
- Inc, F. (2021). FortiGate 80E Series Data Sheet. *Fortinet, Inc*.
- Jadhav, K. D. (2023). *THE ROLE OF CYBER SECURITY AUDITS THE ROLE OF CYBER SECURITY AUDITS IN MANAGING COMPANY SYSTEMS AND APPLICATIONS* View project *THE ROLE OF CYBER SECURITY AUDITS IN MANAGING COMPANY SYSTEMS AND APPLICATIONS*. <https://www.researchgate.net/publication/367559332>
- Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973–993. <https://doi.org/10.1016/j.jcss.2014.02.005>
- Kosutic, D. (2021). *The Impact of Cybersecurity on Competitive Advantage*. GRENOBLE ECOLE DE MANAGEMENT.
- León Gudiño, M. W. (2017). *Auditoría de seguridad informática en la red interna de la Universidad Técnica del Norte según la metodología Offensive Security Professional Training and Tools For Security Specialists y planteamiento de políticas de seguridad basadas en la norma ISO/IEC 27001* [Universidad Técnica del Norte].
<https://repositorio.utn.edu.ec/handle/123456789/6975>
- Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A., & Vrontis, D. (2021). Internal auditing and cyber security: Audit role and procedural contribution. *International Journal of*

- Managerial and Financial Accounting*, 13(1), 25–47.
<https://doi.org/10.1504/IJMFA.2021.116207>
- Mario, F., Tjiptabudi, H., Bernardino, R., & Tjiptabudi, F. M. H. (2019). Information System Security of Indonesia Terrestrial Border Control Internet of Thing View project software enterprise development for the organization View project Information System Security of Indonesia Terrestrial Border Control. In *Communication & Information Technology Journal* (Vol. 13, Issue 2). <https://www.researchgate.net/publication/337006427>
- MINTEL, & DINARDAP. (2021). LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES. *Asamblea Nacional de La República Del Ecuador*.
<https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf>
- Moore, W., & Frye, S. (2019). Review of HIPAA, Part 1: History, protected health information, and privacy and security rules. *Journal of Nuclear Medicine Technology*, 47(4), 269–272.
<https://doi.org/10.2967/JNMT.119.227819>
- Nabila, M. A., Mas'udia, P. E., & Saptono, R. (2023). Analysis and Implementation of the ISSAF Framework on OSSTMM on Website Security Vulnerabilities Testing in Polinema. *Journal of Telecommunication Network*, 13(1).
- NIST. (2011). *Managing information security risk*. <https://doi.org/10.6028/NIST.SP.800-39>
- NIST. (2012). *Guide for conducting risk assessments*. <https://doi.org/10.6028/NIST.SP.800-30r1>
- NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*.
<https://doi.org/10.6028/NIST.CSWP.04162018>
- NIST Cybersecurity Framework. (2021, May 4). *Protect | NIST*. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. <https://www.nist.gov/cyberframework/protect>
- Office of Civil Rights, H. (2013). *HIPAA Administrative Simplification Regulation Text*.
- ONU. (2023). *Objetivos y metas de desarrollo sostenible - Desarrollo Sostenible*. Organización de Las Naciones Unidas. <https://www.un.org/sustainabledevelopment/es/sustainable-development-goals/>
- Organización Mundial de la Salud. (2012). *Protección y seguridad en internet: Retos y avances en los Estados Miembros*.
https://apps.who.int/iris/bitstream/handle/10665/77348/9789243564395_spa.pdf?sequence=1&isAllowed=y
- Ortega Sáenz, A. A. (2020, October 27). *EL GRAN RETO DE LA CIBERSEGURIDAD EN LOS HOSPITALES*. LinkedIn. <https://www.linkedin.com/pulse/el-gran-reto-de-la-ciberseguridad-en-los-hospitales-ortega-s%C3%A1enz/?originalSubdomain=es>
- POLÍTICA DE CIBERSEGURIDAD (2021). <https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf>
- Pyka, M., & Sobieski, Ś. (2012). Implementation of the OCTAVE methodology in security risk management process for business resources. *Advances in Intelligent and Soft Computing*, 118, 235–252. https://doi.org/10.1007/978-3-642-25355-3_21

- Qadir, S., & Quadri, S. M. K. (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. *Journal of Information Security*, 07(03), 185–194. <https://doi.org/10.4236/jis.2016.73014>
- Rajamaki, J., Nevmerzhitskaya, J., & Virag, C. (2018). Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF). *IEEE Global Engineering Education Conference, EDUCON, 2018-April*, 2042–2046. <https://doi.org/10.1109/EDUCON.2018.8363488>
- Ross, R., McEvilley, M., & Oren, J. C. (2018). *Systems security engineering: considerations for a multidisciplinary approach in the engineering of trustworthy secure systems, volume 1*. <https://doi.org/10.6028/NIST.SP.800-160v1>
- Scarfone, K. A., Souppaya, M. P., Cody, A., & Orebaugh, A. D. (2008). *Technical guide to information security testing and assessment*. <https://doi.org/10.6028/NIST.SP.800-115>
- Shetty, S., & Shetty, K. (2019). Ethical Hacking: The Art of Manipulation. *International Journal of Advanced Scientific Research and Management*, 4(12). <https://doi.org/10.36282/ijasrm/4.12.2019.1672>
- Stine, K., Kissel, R., Barker, W. C., Fahlsing, J., & Gulick, J. (2008). *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*. <https://doi.org/10.6028/NIST.SP.800-60v1r1>
- Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security*. <https://doi.org/10.6028/NIST.SP.800-82r2>
- Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). *Contingency planning guide for federal information systems*. <https://doi.org/10.6028/NIST.SP.800-34r1>
- Tomar, S. K., & Singh, P. (2021). Cyber Security Methodologies and Attack Management. *Journal of Management and Service Science (JMSS)*, 1(1), 1–8. <https://doi.org/10.54060/JMSS/001.01.002>
- TP-Link Ecuador. (n.d.). Retrieved May 12, 2024, from <https://www.tp-link.com/ec/>
- UniFi AC Mesh Datasheet. (n.d.).
- U.S. Department of Health & Human Services. (2018, December 28). 2020-12-31 08:51 / *Archivo de HHS.gov*. HHS. <https://public3.pagefreezer.com/browse/HHS.gov/31-12-2020T08:51/https://www.hhs.gov/about/news/2018/12/28/hhs-in-partnership-with-industry-releases-voluntary-cybersecurity-practices-for-the-health-industry.html>
- Van Den Hout, N. J. (2019). *Standardised Penetration Testing? Examining the Usefulness of Current Penetration Testing Methodologies*. <https://www.researchgate.net/publication/335652869>
- Vega, R. G., Arroyo, R., Yoo, S. G., & Sangolquí, E. (2017). Experience in Applying the Analysis and Risk Management Methodology called MAGERIT to Identify Threats and Vulnerabilities in an Agro-industrial Experience in Applying the Analysis and Risk Management Methodology called MAGERIT to Identify Threats and Vulnerabilities in an Agro-industrial Company. In *International Journal of Applied Engineering Research* (Vol. 12). <http://www.ripublication.com>

ANEXOS

Anexo 1. Recolección de información de stakeholders



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE TELECOMUNICACIONES

Tema: Auditoria de la seguridad a la red de Telecomunicaciones de Nova Clínica Moderna en base al marco de ciberseguridad de la NIST

Fecha: 16/04/02024

Entrevistado: Líder de área de TIC'S

Entrevistador: Marco Latacumba

Objetivo: Recopilar información detallada sobre el conocimiento de los stakeholders involucrados en la seguridad de la red de Telecomunicaciones de Nova Clínica Moderna con el fin de tener una meta objetiva durante la auditoría. Se adaptarán los controles de dominio de la ISO 27001 como marco de referencia para garantizar la adecuada identificación y evaluación de los stakeholders, de esta manera establecer medidas de seguridad efectivas y cumplir con los requisitos del proceso de aplicación de la Metodología durante el desarrollo del proyecto de titulación.

Instructivo: En base a la adaptación de los dominios de la norma ISO 27001 que se detallan a continuación, responder las siguientes preguntas.

1. Liderazgo y compromiso de la dirección

¿Cómo lidera la alta dirección la implementación y mantenimiento de medidas de seguridad en la red de telecomunicaciones de Nova Clínica Moderna?

¿Cuál es el compromiso de la dirección con la protección de la red de telecomunicaciones y la gestión de riesgos de ciberseguridad?

2. Política de seguridad de la información

¿Actualmente, existe una política de seguridad específica para la red de telecomunicaciones de la clínica?

3. Roles y responsabilidades en seguridad de la red

¿Cuáles son los roles y responsabilidades específicos del personal encargado de la seguridad de la red de Telecomunicaciones?

En caso de existir controles de seguridad a la red de Telecomunicaciones de la clínica.

¿Cómo se asignan y comunican las responsabilidades para la implementación y mantenimiento de estos controles?

4. Gestión de activos de la red

¿Qué activos de información críticos se manejan a través de la red de telecomunicaciones de la empresa?

¿Cómo se identifican, clasifican y protegen estos activos en cuanto a tema de ciberseguridad?

5. Control de acceso

¿Cómo se controla y gestiona el acceso a los sistemas y de los datos de la red?

¿Existen medidas adecuadas implementadas para garantizar la autenticación y autorización en los dispositivos de la red?

6. Seguridad física y del entorno

¿Existen medidas para proteger la infraestructura física de la red, como; servidores, conmutadores, enrutadores, cableado estructurado?

7. Seguridad de las operaciones

¿Cómo se garantiza la operatividad de la red de telecomunicaciones en caso de algún incidente o interrupción?

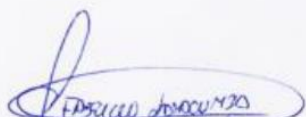
¿Existen procedimientos y controles para asegurar la integridad y disponibilidad de la red?

8. Seguridad en el desarrollo de sistemas y gestión de proyectos

¿Existe alguna consideración o control de seguridad en el diseño o implementación de nuevos sistemas y proyectos de telecomunicaciones en la empresa?

9. Relaciones con proveedores

¿Se evalúa y gestionan los requisitos de seguridad asociados con proveedores de servicios y equipos tecnológicos en la empresa?


Firma Estudiante


Ing. Marcelo Rea
LIDÉR DE TIC'S
Revisado por jefe de área de TIC'S

Anexo 2. Recolección de información del área tecnológica de la empresa



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE TELECOMUNICACIONES

Tema: Auditoria de la seguridad a la red de Telecomunicaciones de Nova Clínica Moderna en base al marco de ciberseguridad de la NIST

Fecha: 11/04/2024

Entrevistado: Líder de área de TIC'S

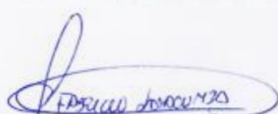
Entrevistador: Marco Latacumba

Objetivo: Recopilar información sobre la situación actual del área tecnológica y de los recursos de telecomunicaciones organizacionales de manera general para identificar posibles áreas de mejora y optimización durante el desarrollo del proyecto de titulación.

Instructivo: En base a la siguiente tabla proporcionada, responda a las siguientes preguntas de la sección "Situación Actual".

Departamento	Situación Actual
1. Área Tecnológica	- ¿Los integrantes cumplen con los requisitos del área, es decir, son personas capacitadas y preparadas en el ámbito tecnológico empresarial?
2. Talento Humano del área	- ¿El personal se rigen bajo las reglas o disposiciones internas de la empresa?

3. Hardware disponible	<ul style="list-style-type: none"> - ¿El hardware con el que dispone la empresa es suficiente para cumplir las tareas que requiere y compone la red? - ¿La empresa dispone de UPS de backups de energía, etc? - ¿Quién es el encargado de su mantenimiento y revisión constante o ante una posible catástrofe? - ¿Algunos de los dispositivos cuentan con garantía y mantenimiento de terceros?
4. Software disponible	<ul style="list-style-type: none"> - ¿El software de los equipos que componen la red satisface los requisitos para cumplir las actividades diarias de la clínica? - ¿Los equipos, en su mayoría, cuentan con licencias pagadas y autorizadas por sus distribuidores en todos los equipos?
5. Cableado y conexión inalámbrica de la empresa	<ul style="list-style-type: none"> - La fibra óptica, cables de cobre, etc. ¿Están certificada por estándares internacionales? - ¿Qué tiempo de vida tiene de uso el cableado, los tipos de cables que usados para conexión entre los equipos? - ¿Hacen uso de conexiones inalámbricas(antenas) hacia otros edificios?
6. Sistemas de información disponible	<ul style="list-style-type: none"> - ¿La empresa cuenta con algún sistema integrado donde se realice la mayoría de las actividades? - ¿Dispone de alguna página web que sirva de información y consulta para los clientes y personas interesadas acerca de la clínica?


Firma Estudiante


Ing. Marcelo Rea
LÍDER DE TIC'S
Revisado por jefe de área de TIC'S

ANEXO 3. Cuestionario para la obtención de información de la topología de red

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE TELECOMUNICACIONES

Tema: Auditoria de la seguridad a la red de Telecomunicaciones de Nova Clínica Moderna en base al marco de ciberseguridad de la NIST

Fecha: 02/05/2024

Entrevistado: Líder de área de TIC'S

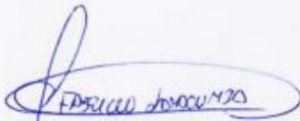
Entrevistador: Marco Latacumba

Objetivo: Recopilar información referente a la topología física y lógica de la red de telecomunicaciones de Nova Clínica Moderna, dando enfoque a los aspectos técnicos y estructurales de la red. Posteriormente graficar en Draw.io las topologías para tener un panorama más amplio de cómo está compuesta la red de la empresa.

Instructivo: Responder a las siguientes preguntas y realizar el diseño de la topología física y lógica de la red de Nova Clínica Moderna.

1. ¿Cuál es la configuración actual de la topología lógica y física de la red de telecomunicaciones de Nova Clínica Moderna?
2. Describa los componentes principales que integran la infraestructura física de la red (Router, conmutadores, servidores, etc).
3. ¿Cómo están conectados físicamente estos dispositivos entre sí y como se conectan a los periféricos en las estaciones de trabajo?
4. ¿Qué tipo de tecnologías de conexión inalámbrica se empleando dentro de la infraestructura y como se integran con la red cableada?

5. Describa la topología lógica de la red, incluyendo: subredes, VLANS, protocolos de enrutamiento, etc.
6. ¿Cómo se gestiona la seguridad y el acceso en las diferentes capas de la red?
7. ¿Se planea expandir o actualizar la red a corto o largo plazo, ¿Cuáles serían estas mejoras específicas?
8. ¿Cómo se monitorea y se maneja el tráfico de la red para asegurar la eficiencia y seguridad?
9. ¿Qué desafíos actualmente enfrenta la empresa con respecto a la infraestructura de la red y como se abordarían estos retos a futuro?


Firma Estudiante


Ing. Marcelo Rea
LÍDER DE TIC'S
Revisado por jefe de área de TIC'S

ANEXO 4. Cuestionario de recolección de información de activos críticos

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE TELECOMUNICACIONES

Tema: Auditoria de la seguridad a la red de Telecomunicaciones de Nova Clínica Moderna en base al marco de ciberseguridad de la NIST

Fecha: 25/04/02024

Entrevistado: Líder de área de TIC'S

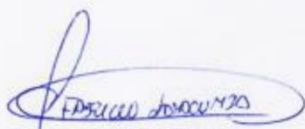
Entrevistador: Marco Latacumba

Objetivo: Recopilar información acerca de los activos críticos tecnológicos que componen la red de la empresa y son de vital funcionamiento para las actividades diarias, de esta manera iniciar con el perfilamiento de los activos críticos.

Instructivo: Responder las siguientes preguntas.

1. ¿Cuáles de los activos de la red de telecomunicaciones son de mayor valor para su organización?
2. ¿Qué activos de la red de telecomunicaciones son lo más críticos y se utilizan en los procesos de labor diaria en Nova clínica moderna?
3. En caso de pérdida o daño de un activo que compone la red. ¿Cuál o cuáles interrumpirían significativamente la capacidad de la empresa para lograr sus objetivos?
4. ¿Qué otros activos están estrechamente relacionados con estos activos críticos?
5. ¿Cuál es el nombre común para estos activos?

6. ¿Cuáles activos de la red de la empresa son lógicos y cuáles son físicos?
7. ¿Quién es la persona responsable del mantenimiento y gestión de estos activos de la red?
8. ¿Cuáles son los procesos de negocios que más dependen de estos activos?
9. ¿Quién sería responsable de establecer el valor cuantitativo de estos activos?
10. ¿Quiénes se verían más afectados en caso de que estos activos se comprometieran?


Firma Estudiante


Ing. Marcelo Rea
LIDÉR DE TIC'S
Revisado por jefe de área de TIC'S

ANEXO 5. Recolección de información de hardware y software de la empresa

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE TELECOMUNICACIONES

Tema: Auditoria de la seguridad a la red de Telecomunicaciones de Nova Clínica Moderna en base al marco de ciberseguridad de la NIST

Fecha: 30/04/2024

Entrevistado: Líder de área de TIC'S

Entrevistador: Marco Latacumba

Objetivo: Por medio de una reunión con el jefe de área de TIC'S, obtener información acerca del hardware y software que actualmente hace uso Nova Clínica Moderna en todas sus áreas.

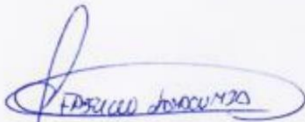
Instructivo: En base a las siguientes tablas proporcionadas, describa el software y sistemas de información de la empresa y enumere los dispositivos disponibles por áreas.

- **Hardware disponible en Nova Clínica Moderna**

Área	Área de atención crítica y hospitalaria	Diagnóstico y apoyo	Comercial	Talento y bienestar humano	TIC' S	SSO A	Mantenimiento Hospitalario	Contabilidad	Cobranza y facturación
Hardware									
Router									
Conmutadores									
Servidores									
Central de VoIP									
UPS									
Computadores de Escritorio									
Computadores Portátiles									
Puntos de acceso inalámbrico									
Faceplates									
Impresoras									
Discos Externos									
Teléfonos									
Cámaras análogas									

- **Software y sistemas de información disponible en nova clínica moderna**

Software	Tipo	Ubicación / Equipo



Federico Jarama

Firma Estudiante



Ing. Marcelo Rea
LÍDER DE TIC'S
Revisado por jefe de área de TIC'S

ANEXO 6. Matriz de evaluación de marco de ciberseguridad de la NIST

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE TELECOMUNICACIONES

Tema: Auditoria de la seguridad a la red de Telecomunicaciones de Nova Clínica Moderna en base al marco de ciberseguridad de la NIST

Fecha: 02/05/2024

Entrevistado: Líder de área de TIC'S

Entrevistador: Marco Latacumba

Objetivo: Realizar una entrevista con el jefe de áreas de TIC'S de Nova Clínica Moderna en el que se aplicará la matriz de evaluación de seguridad del CSF de la NIST en la que se perfilará el estado actual, el perfil objetivo deseado y la brecha que posiblemente exista para alcanzar los niveles de seguridad deseados.

Instructivo: En base a la siguiente matriz proporcionada del CSF de la NIST, elegir el nivel del estado actual, el nivel de objetivo deseado y la prioridad para alcanzar posibles metas a futuro. A continuación, se explicará más a detalle el significado de cada nivel que proporciona esta matriz para la evaluación.

Nivel 1. Parcial: Las prácticas de gestión de riesgos cibernéticos en la organización son informales y reactivas, además no se tiene una estructura sistemática para estas prácticas. Se tiene limitada conciencia por parte de la organización sobre los riesgos de seguridad cibernética, lo que resulta en respuestas inconsistentes y poco eficaces ante una amenaza de seguridad.

Nivel 2. Riesgo Informado: La gestión de riesgos de ciberseguridad cuenta con el respaldo de la alta dirección, pero no se ha formalizado completamente a través de políticas dentro de la organización. Además, existe una conciencia sobre los riesgos cibernéticos, sin documentación o método organizacional para su gestión y aunque reconoce su papel en un contexto más amplio, la comprensión no es totalmente integral.

Nivel 3. Repetible: En este nivel las prácticas de gestión de riesgos de la organización están formalmente establecidas en políticas y formalizadas en la empresa. Se entiende de manera clara las responsabilidades de manera más amplia, contribuyendo al conocimiento general sobre los riesgos de ciberseguridad en el entorno empresarial.

Nivel 4. Adaptable: En este nivel la organización mejora continuamente sus estrategias de ciberseguridad en base a previas y actuales experiencias. Este nivel permite la implementación de políticas de seguridad y procedimiento informados sobre los riesgos para la prevención y respuesta antes posibles incidentes de ciberseguridad. Además, la organización tiene un entendimiento mucho más amplio sobre los riesgos cibernéticos en el entorno.

Función	Categoría	Subcategoría	Estado actual		Objetivo deseado		Prioridad		
			Logro	Nivel	Logro	Nivel	Brecha	Prioridad	
IDENTIFICAR (ID)	Gestión de activos (ID.AM): Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.	ID.AM-1: Los dispositivos y sistemas físicos dentro de la organización están inventariados.	Adaptable	4	Adaptable	4	0	Objetivo alcanzado	
		ID.AM-2: Las plataformas de software y las aplicaciones dentro de la organización están inventariadas.	Adaptable	4	Adaptable	4	0	Objetivo alcanzado	
		ID.AM-3: La comunicación organizacional y los flujos de datos están mapeados.	Riesgo Informado	2	Repetible	3	1	Baja	
		ID.AM-4: Los sistemas de información externos están catalogados.	Adaptable	4	Adaptable	4	0	Objetivo alcanzado	
		ID.AM-5: Los recursos (por ejemplo, hardware, dispositivos, datos, tiempo, personal y software) se priorizan en función de su clasificación, criticidad y valor comercial.	Repetible	3	Adaptable	4	1	Baja	
		ID.AM-6: Los roles y las responsabilidades de la seguridad cibernética para toda la fuerza de trabajo y terceros interesados (por ejemplo, proveedores, clientes, socios) están establecidas.	Riesgo Informado	2	Repetible	3	1	Baja	
	Resumen de la categoría "ID-AM: Gestión de activos"			%Logro	79,17%	%Objetivo	91,67%	12,50%	%Prioridad
	Entorno empresarial (ID.BE): Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética.	ID.BE-1: Se identifica y se comunica la función de la organización en la cadena de suministro.	Riesgo Informado	2	Repetible	3	1	Baja	
		ID.BE-2: Se identifica y se comunica el lugar de la organización en la infraestructura crítica y su sector industrial.	Riesgo Informado	2	Repetible	3	1	Baja	
		ID.BE-3: Se establecen y se comunican las prioridades para la misión, los objetivos y las actividades de la organización.	Repetible	3	Adaptable	4	1	Baja	
		ID.BE-4: Se establecen las dependencias y funciones fundamentales para la entrega de servicios críticos.	Riesgo Informado	2	Repetible	3	1	Baja	
		ID.BE-5: Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).	Riesgo Informado	2	Repetible	3	1	Baja	
	Resumen de la categoría "ID-BE: Entorno empresarial"			%Logro	55,00%	%Objetivo	80,00%	25,00%	%Prioridad
	Gobernanza (ID.GV): Las políticas, los procedimientos y los procesos para administrar y monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos de la organización se comprenden y se informan a la gestión del riesgo de seguridad cibernética.	ID.GV-1: Se establece y se comunica la política de seguridad cibernética organizacional.	Parcial	1	Repetible	3	2	Media	
		ID.GV-2: Los roles y las responsabilidades de seguridad cibernética están coordinados y alineados con roles internos y socios externos.	Riesgo Informado	2	Repetible	3	1	Baja	
		ID.GV-3: Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles.	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo alcanzado	
		ID.GV-4: Los procesos de gobernanza y gestión de riesgos abordan los riesgos de seguridad cibernética.	Riesgo Informado	2	Repetible	3	1	Baja	
	Resumen de la categoría "ID-GV: Gobernanza"			%Logro	43,75%	%Objetivo	68,75%	25,00%	%Prioridad
	Evaluación de riesgos (ID.RA): La organización comprende el riesgo de seguridad cibernética para	ID.RA-1: Se identifican y se documentan las vulnerabilidades de los activos.	Riesgo Informado	2	Repetible	3	1	Baja	

	las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.	ID.RA-2: La inteligencia de amenazas cibernéticas se recibe de foros y fuentes de intercambio de información.	Repetible	3	Adaptable	4	1	Baja
		ID.RA-3: Se identifican y se documentan las amenazas, tanto internas como externas.	Riesgo Informado	2	Repetible	3	1	Baja
		ID.RA-4: Se identifican los impactos y las probabilidades de riesgo del negocio.	Parcial	1	Riesgo Informado	2	1	Baja
		ID.RA-5: Se utilizan las amenazas, las vulnerabilidades, las probabilidades y los impactos para determinar el riesgo.	Parcial	1	Repetible	3	2	Media
		ID.RA-6: Se identifican y priorizan las respuestas al riesgo.	Parcial	1	Riesgo Informado	2	1	Baja
		Resumen de la categoría "ID-RA: Evaluación de riesgos"		%Logro	41,67%	%Objetivo	70,83%	29,17%
	Estrategia de gestión de riesgos (ID.RM): Se establecen las prioridades, restricciones, tolerancias de riesgo y suposiciones de la organización y se usan para respaldar las decisiones de riesgos operacionales.	ID.RM-1: Los actores de la organización establecen, gestionan y acuerdan los procesos de gestión de riesgos.	Parcial	1	Riesgo Informado	2	1	Baja
		ID.RM-2: La tolerancia al riesgo organizacional se determina y se expresa claramente.	Parcial	1	Riesgo Informado	2	1	Baja
		ID.RM-3: La determinación de la tolerancia del riesgo de la organización se basa en parte en su rol en la infraestructura crítica y el análisis del riesgo específico del sector.	Parcial	1	Riesgo Informado	2	1	Baja
	Resumen de la categoría "ID-RM: Estrategia de gestión de riesgos"		%Logro	25,00%	%Objetivo	50,00%	25,00%	%Prioridad
Gestión del riesgo de la cadena de suministro (ID.SC): Las prioridades, limitaciones, tolerancias de riesgo y suposiciones de la organización se establecen y se utilizan para respaldar las decisiones de riesgo asociadas con la gestión del riesgo de la cadena de suministro. La organización ha establecido e implementado los procesos para identificar, evaluar y gestionar los riesgos de la cadena de suministro.	ID.SC-1: Los actores de la organización identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión del riesgo de la cadena de suministro cibernética.	Parcial	1	Riesgo Informado	2	1	Baja	
	ID.SC-2: Los proveedores y socios externos de los sistemas de información, componentes y servicios se identifican, se priorizan y se evalúan mediante un proceso de evaluación de riesgos de la cadena de suministro cibernético.	Parcial	1	Riesgo Informado	2	1	Baja	
	ID.SC-3: Los contratos con proveedores y socios externos se utilizan para implementar medidas apropiadas diseñadas para cumplir con los objetivos del programa de seguridad cibernética de una organización y el plan de gestión de riesgos de la cadena de suministro cibernético.	Parcial	1	Riesgo Informado	2	1	Baja	
	ID.SC-4: Los proveedores y los socios externos se evalúan de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluación para confirmar que cumplen con sus obligaciones contractuales.	Parcial	1	Riesgo Informado	2	1	Baja	
	ID.SC-5: Las pruebas y la planificación de respuesta y recuperación se llevan a cabo con proveedores.	Parcial	1	Riesgo Informado	2	1	Baja	
	Resumen de la categoría "ID-SC: Gestión del riesgo de la cadena de suministro"		%Logro	25,00%	%Objetivo	50,00%	25,00%	%Prioridad
PROTEGER (PR)	Gestión de identidad, autenticación y control de acceso (PR.AC): El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	PR.AC-1: Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.	Riesgo Informado	2	Repetible	3	1	Baja
		PR.AC-2: Se gestiona y se protege el acceso físico a los activos.	Repetible	3	Adaptable	4	1	Baja
		PR.AC-3: Se gestiona el acceso remoto.	Repetible	3	Adaptable	4	1	Baja
		PR.AC-4: Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.	Riesgo Informado	2	Repetible	3	1	Baja
		PR.AC-5: Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red).	Repetible	3	Adaptable	4	1	Baja
		PR.AC-6: Las identidades son verificadas y vinculadas a credenciales y afirmadas en las interacciones.	Riesgo Informado	2	Repetible	3	1	Baja

	PR.AC-7: Se autentican los usuarios, dispositivos y otros activos (por ejemplo, autenticación de un solo factor o múltiples factores) acorde al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las organizaciones).	Riesgo Informado	2	Repetible	3	1	Baja
Resumen de la categoría "PR-AC: Gestión de identidad, autenticación y control de acceso"		%Logro	60,71%	%Objetivo	85,71%	25,00%	%Prioridad
Concienciación y capacitación (PR.AT): El personal y los socios de la organización reciben educación de concienciación sobre la seguridad cibernética y son capacitados para cumplir con sus deberes y responsabilidades relacionados con la seguridad cibernética, en conformidad con las políticas, los procedimientos y los acuerdos relacionados al campo.	PR.AT-1: Todos los usuarios están informados y capacitados.	Riesgo Informado	2	Adaptable	4	2	Media
	PR.AT-2: Los usuarios privilegiados comprenden sus roles y responsabilidades.	Riesgo Informado	2	Repetible	3	1	Baja
	PR.AT-3: Los terceros interesados (por ejemplo, proveedores, clientes, socios) comprenden sus roles y responsabilidades.	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo alcanzado
	PR.AT-4: Los ejecutivos superiores comprenden sus roles y responsabilidades.	Riesgo Informado	2	Repetible	3	1	Baja
	PR.AT-5: El personal de seguridad física y cibernética comprende sus roles y responsabilidades.	Riesgo Informado	2	Repetible	3	1	Baja
Resumen de la categoría "PR-AT: Concienciación y capacitación"		%Logro	50,00%	%Objetivo	75,00%	25,00%	%Prioridad
Seguridad de los datos (PR.DS): La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	PR.DS-1: Los datos en reposo están protegidos.	Repetible	3	Repetible	3	0	Objetivo alcanzado
	PR.DS-2: Los datos en tránsito están protegidos.	Repetible	3	Repetible	3	0	Objetivo alcanzado
	PR.DS-3: Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.	Riesgo Informado	2	Repetible	3	1	Baja
	PR.DS-4: Se mantiene una capacidad adecuada para asegurar la disponibilidad.	Parcial	1	Riesgo Informado	2	1	Baja
	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.	Parcial	1	Repetible	3	2	Media
	PR.DS-6: Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.	Parcial	1	Riesgo Informado	2	1	Baja
	PR.DS-7: Los entornos de desarrollo y prueba(s) están separados del entorno de producción.	Riesgo Informado	2	Repetible	3	1	Baja
	PR.DS-8: Se utilizan mecanismos de comprobación de la integridad para verificar la integridad del hardware.	Repetible	3	Repetible	3	0	Objetivo alcanzado
Resumen de la categoría "PR-DS: Seguridad de los datos"		%Logro	50,00%	%Objetivo	68,75%	18,75%	%Prioridad
Procesos y procedimientos de protección de la información (PR.IP): Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	PR.IP-1: Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).	Parcial	1	Riesgo Informado	2	1	Baja
	PR.IP-2: Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas.	Repetible	3	Repetible	3	0	Objetivo alcanzado
	PR.IP-3: Se encuentran establecidos procesos de control de cambio de la configuración.	Riesgo Informado	2	Repetible	3	1	Baja
	PR.IP-4: Se realizan, se mantienen y se prueban copias de seguridad de la información.	Repetible	3	Adaptable	4	1	Baja
	PR.IP-5: Se cumplen las regulaciones y la política con respecto al entorno operativo físico para los activos organizativos.	Riesgo Informado	2	Repetible	3	1	Baja
	PR.IP-6: Los datos son eliminados de acuerdo con las políticas.	Riesgo Informado	2	Repetible	3	1	Baja

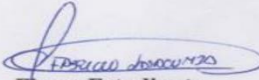
		PR.IP-7: Se mejoran los procesos de protección.	Riesgo Informado	2	Repetible	3	1	Baja	
		PR.IP-8: Se comparte la efectividad de las tecnologías de protección.	Riesgo Informado	2	Repetible	3	1	Baja	
		PR.IP-9: Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de Incidentes y Recuperación de Desastres).	Parcial	1	Riesgo Informado	2	1	Baja	
		PR.IP-10: Se prueban los planes de respuesta y recuperación.	Parcial	1	Riesgo Informado	2	1	Baja	
		PR.IP-11: La seguridad cibernética se encuentra incluida en las prácticas de recursos humanos (por ejemplo, desaprovisionamiento, selección del personal).	Parcial	1	Parcial	1	0	Objetivo alcanzado	
		PR.IP-12: Se desarrolla y se implementa un plan de gestión de las vulnerabilidades.	Riesgo Informado	2	Repetible	3	1	Baja	
	Resumen de la categoría "PR-IP: Procesos y procedimientos de protección de la información"			%Logro	45,83%	%Objetivo	66,67%	20,83%	%Prioridad
	Mantenimiento (PR.MA): El mantenimiento y la reparación de los componentes del sistema de información y del control industrial se realizan de acuerdo con las políticas y los procedimientos.	PR.MA-1: El mantenimiento y la reparación de los activos de la organización se realizan y están registrados con herramientas aprobadas y controladas.	Repetible	3	Repetible	3	0	Objetivo alcanzado	
		PR.MA-2: El mantenimiento remoto de los activos de la organización se aprueba, se registra y se realiza de manera que evite el acceso no autorizado.	Parcial	1	Repetible	3	2	Media	
	Resumen de la categoría "PR-MA: Procesos y procedimientos de protección de la información"			%Logro	50,00%	%Objetivo	75,00%	25,00%	%Prioridad
	Tecnología de protección (PR.PT): Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y la capacidad de recuperación de los sistemas y activos, en consonancia con las políticas, procedimientos y acuerdos relacionados.	PR.PT-1: Los registros de auditoría o archivos se determinan, se documentan, se implementan y se revisan en conformidad con la política.	Parcial	1	Riesgo Informado	2	1	Baja	
		PR.PT-2: Los medios extraíbles están protegidos y su uso se encuentra restringido de acuerdo con la política.	Riesgo Informado	2	Repetible	3	1	Baja	
PR.PT-3: Se incorpora el principio de menor funcionalidad mediante la configuración de los sistemas para proporcionar solo las capacidades esenciales.		Riesgo Informado	2	Repetible	3	1	Baja		
PR.PT-4: Las redes de comunicaciones y control están protegidas.		Riesgo Informado	2	Repetible	3	1	Baja		
PR.PT-5: Se implementan mecanismos (por ejemplo, a prueba de fallas, equilibrio de carga, cambio en caliente o "hot swap") para lograr los requisitos de resiliencia en situaciones normales y adversas.		Parcial	1	Riesgo Informado	2	1	Baja		
Resumen de la categoría "PR-PT: Tecnología de protección"			%Logro	40,00%	%Objetivo	65,00%	25,00%	%Prioridad	
DETECTAR (DE)	Anomalías y Eventos (DE.AE): se detecta actividad anómala y se comprende el impacto potencial de los eventos.	DE.AE-1: Se establece y se gestiona una base de referencia para operaciones de red y flujos de datos esperados para los usuarios y sistemas.	Riesgo Informado	2	Repetible	3	1	Baja	

		DE.AE-2: Se analizan los eventos detectados para comprender los objetivos y métodos de ataque.	Repetible	3	Repetible	3	0	Objetivo alcanzado
		DE.AE-3: Los datos de los eventos se recopilan y se correlacionan de múltiples fuentes y sensores.	Riesgo Informado	2	Repetible	3	1	Baja
		DE.AE-4: Se determina el impacto de los eventos.	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo alcanzado
		DE.AE-5: Se establecen umbrales de alerta de incidentes.	Riesgo Informado	2	Repetible	3	1	Baja
		Resumen de la categoría "DE-AE: Anomalías y Eventos"	%Logro	55,00%	%Objetivo	70,00%	15,00%	%Prioridad
	Monitoreo Continuo de la Seguridad (DE.CM): El sistema de información y los activos son monitoreados a fin de identificar eventos de seguridad cibernética y verificar la eficacia de las medidas de protección.	DE.CM-1: Se monitorea la red para detectar posibles eventos de seguridad cibernética.	Riesgo Informado	2	Repetible	3	1	Baja
		DE.CM-2: Se monitorea el entorno físico para detectar posibles eventos de seguridad cibernética.	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo alcanzado
		DE.CM-3: Se monitorea la actividad del personal para detectar posibles eventos de seguridad cibernética.	Riesgo Informado	2	Repetible	3	1	Baja
		DE.CM-4: Se detecta el código malicioso.	Repetible	3	Repetible	3	0	Objetivo alcanzado
		DE.CM-5: Se detecta el código móvil no autorizado.	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo alcanzado
DE.CM-6: Se monitorea la actividad de los proveedores de servicios externos para detectar posibles eventos de seguridad cibernética.		Riesgo Informado	2	Riesgo Informado	2	0	Objetivo alcanzado	
DE.CM-7: Se realiza el monitoreo del personal, conexiones, dispositivos y software no autorizados.		Riesgo Informado	2	Repetible	3	1	Baja	
DE.CM-8: Se realizan escaneos de vulnerabilidades.		Parcial	1	Repetible	3	2	Media	
	Resumen de la categoría "DE-CM: Monitoreo Continuo de la Seguridad"	%Logro	50,00%	%Objetivo	65,63%	15,63%	%Prioridad	
Procesos de Detección (DE.DP): Se mantienen y se aprueban los procesos y procedimientos de detección para garantizar el conocimiento de los eventos anómalos.	DE.DP-1: Los roles y los deberes de detección están bien definidos para asegurar la responsabilidad.	Parcial	1	Riesgo Informado	2	1	Baja	
	DE.DP-2: Las actividades de detección cumplen con todos los requisitos aplicables.	Riesgo Informado	2	Repetible	3	1	Baja	
	DE.DP-3: Se prueban los procesos de detección.	Parcial	1	Riesgo Informado	2	1	Baja	
	DE.DP-4: Se comunica la información de la detección de eventos.	Parcial	1	Riesgo Informado	2	1	Baja	
	DE.DP-5: los procesos de detección se mejoran continuamente.	Repetible	3	Repetible	3	0	Objetivo alcanzado	
	Resumen de la categoría "DE-DP: Procesos de Detección"	%Logro	40,00%	%Objetivo	60,00%	20,00%	%Prioridad	
RESPONDER (RS)	Planificación de la Respuesta (RS.RP): Los procesos y procedimientos de respuesta se ejecutan y se mantienen a fin de garantizar la respuesta a los incidentes de seguridad cibernética detectados.	RS.RP-1: El plan de respuesta se ejecuta durante o después de un incidente.	Riesgo Informado	2	Repetible	3	1	Baja
		Resumen de la categoría "RS-RP: Planificación de la Respuesta"	%Logro	50,00%	%Objetivo	75,00%	25,00%	%Prioridad
	Comunicaciones (RS.CO): Las actividades de respuesta se coordinan con las partes interesadas internas y externas (por ejemplo, el apoyo externo de organismos encargados de hacer cumplir la ley).	RS.CO-1: El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta.	Parcial	1	Riesgo Informado	2	1	Baja
RS.CO-2: Los incidentes se informan de acuerdo con los criterios establecidos.		Parcial	1	Riesgo Informado	2	1	Baja	

		RS.CO-3: La información se comparte de acuerdo con los planes de respuesta.	Parcial	1	Riesgo Informado	2	1	Baja		
		RS.CO-4: La coordinación con las partes interesadas se realiza en consonancia con los planes de respuesta.	Parcial	1	Riesgo Informado	2	1	Baja		
		RS.CO-5: El intercambio voluntario de información se produce con las partes interesadas externas para lograr una mayor conciencia situacional de seguridad cibernética.	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo alcanzado		
		Resumen de la categoría "RS-CO: Comunicaciones"		%Logro	30,00%	%Objetivo	50,00%	20,00%	%Prioridad	
		Análisis (RS.AN): Se lleva a cabo el análisis para garantizar una respuesta eficaz y apoyar las actividades de recuperación.	RS.AN-1: Se investigan las notificaciones de los sistemas de detección.	Repetible	3	Repetible	3	0	Objetivo alcanzado	
			RS.AN-2: Se comprende el impacto del incidente.	Repetible	3	Repetible	3	0	Objetivo alcanzado	
			RS.AN-3: Se realizan análisis forenses.	Riesgo Informado	2	Repetible	3	1	Baja	
			RS.AN-4: Los incidentes se clasifican de acuerdo con los planes de respuesta.	Parcial	1	Riesgo Informado	2	1	Baja	
			RS.AN-5: Se establecen procesos para recibir, analizar y responder a las vulnerabilidades divulgadas a la organización desde fuentes internas y externas (por ejemplo, pruebas internas, boletines de seguridad o investigadores de seguridad).	Riesgo Informado	2	Repetible	3	1	Baja	
			Resumen de la categoría "RS-AN: Análisis"		%Logro	55,00%	%Objetivo	70,00%	15,00%	%Prioridad
		Mitigación (RS.MI): Se realizan actividades para evitar la expansión de un evento, mitigar sus efectos y resolver el incidente.	RS.MI-1: Los incidentes son contenidos.	Repetible	3	Repetible	3	0	Objetivo alcanzado	
			RS.MI-2: Los incidentes son mitigados.	Repetible	3	Repetible	3	0	Objetivo alcanzado	
			RS.MI-3: Las vulnerabilidades recientemente identificadas son mitigadas o se documentan como riesgos aceptados.	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo alcanzado	
			Resumen de la categoría "RS-MI: Mitigación"		%Logro	66,67%	%Objetivo	66,67%	0,00%	%Prioridad
		Mejoras (RS.IM): Las actividades de respuesta de la organización se mejoran al incorporar las lecciones aprendidas de las actividades de detección y respuesta actuales y previas.	RS.IM-1: Los planes de respuesta incorporan las lecciones aprendidas.	Parcial	1	Repetible	3	2	Media	
	RS.IM-2: Se actualizan las estrategias de respuesta.		Parcial	1	Riesgo Informado	2	1	Baja		
		Resumen de la categoría "RS-IM: Mejoras"		%Logro	25,00%	%Objetivo	62,50%	37,50%	%Prioridad	
RECUPERAR (RC)	Planificación de la recuperación (RC.RP): Los procesos y procedimientos de recuperación se ejecutan y se mantienen para asegurar la restauración de los sistemas o activos afectados por incidentes de seguridad cibernética.	RC.RP-1: El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.	Parcial	1	Riesgo Informado	2	1	Baja		
		Resumen de la categoría "RC-RP: Planificación de la recuperación"		%Logro	25,00%	%Objetivo	50,00%	25,00%	%Prioridad	
	Mejoras (RC.IM): La planificación y los procesos de recuperación se mejoran al incorporar en las actividades futuras las lecciones aprendidas.	RC.IM-1: Los planes de recuperación incorporan las lecciones aprendidas.	Parcial	1	Riesgo Informado	2	1	Baja		
		RC.IM-2: Se actualizan las estrategias de recuperación.	Parcial	1	Riesgo Informado	2	1	Baja		
		Resumen de la categoría "RC-IM: Mejoras"		%Logro	25,00%	%Objetivo	50,00%	25,00%	%Prioridad	

CNSD - Pag. 7

Comunicaciones (RC.CO): Las actividades de restauración se coordinan con partes internas y externas (por ejemplo, centros de coordinación, proveedores de servicios de Internet, propietarios de sistemas de ataque, víctimas, otros CSIRT y vendedores).	RC.CO-1: Se gestionan las relaciones públicas.	Riesgo Informado	2	Riesgo Informado	2	0	Objetivo alcanzado
	RC.CO-2: La reputación se repara después de un incidente.	Parcial	1	Riesgo Informado	2	1	Baja
	RC.CO-3: Las actividades de recuperación se comunican a las partes interesadas internas y externas, así como también a los equipos ejecutivos y de administración.	Parcial	1	Riesgo Informado	2	1	Baja
	Resumen de la categoría "RC-CO: Comunicaciones"		%Logro	33,33%	%Objetivo	50,00%	16,67%


Firma Estudiante


Ing. Marcelo Rea
 LÍDER DE TIC'S
 Revisado por jefe de área de TIC'S

ANEXO 7. Matriz de valoración de activos críticos de infraestructura tecnológica

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE TELECOMUNICACIONES

Tema: Auditoria de la seguridad a la red de Telecomunicaciones de Nova Clínica Moderna en base al marco de ciberseguridad de la NIST

Fecha: 09/05/02024

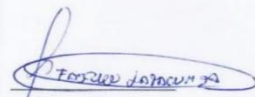
Entrevistado: Líder de área de TIC'S

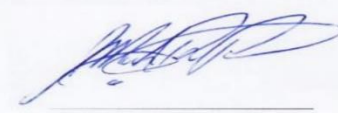
Entrevistador: Marco Latacumba

Objetivo: Realizar una entrevista con el líder de áreas de TIC'S de Nova Clínica Moderna en el que se aplicará la matriz de valoración de activos críticos de la red de telecomunicaciones en base a los parámetros que brinda el marco de ciberseguridad de la NIST.

Instructivo: En base a la siguiente matriz proporcionada del CSF de la NIST, valorar los activos críticos en base a confidencialidad, integridad y disponibilidad.

Activo Crítico	Disponibilidad	Confidencialidad	Integridad	Nivel de criticidad	Categorías de la función "Proteger" del NIST CSF
Routers Firewall					
Conmutadores					
Servidores Internos					
Cableado horizontal y Vertical					
Troncal SIP					
Troncal analógica					
Infraestructura Wireless					
Estaciones de trabajo					


Estudiante


Líder del área de TIC'S

ANEXO 8. Matriz de identificación de vulnerabilidades, amenazas y riesgos de los activos críticos de la infraestructura tecnológica



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE TELECOMUNICACIONES

Tema: Auditoria de la seguridad a la red de Telecomunicaciones de Nova Clínica Moderna en base al marco de ciberseguridad de la NIST

Fecha: 16/05/2024

Entrevistado: Líder de área de TIC'S

Entrevistador: Marco Latacumba

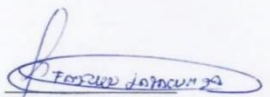
Objetivo: Realizar una entrevista con el Líder del área de TIC'S de Nova Clínica Moderna en el que se aplicará la matriz de identificación de riesgos de activos críticos en base a directrices proporcionadas por el marco de ciberseguridad de la NIST

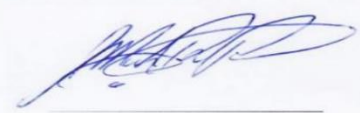
Instructivo: En base a la siguiente matriz proporcionada del CSF de la NIST, identificar las posibles vulnerabilidades, amenazas y riesgos de los activos críticos de la red de telecomunicaciones de la empresa.

Activo Crítico (Ac)	ID	Vulnerabilidad (V)	ID	Amenaza (A)	ID	Riesgo (R)
Cableado Horizontal y Vertical	V1 - Ac1		A1 - Ac1		R1-Ac1	
	V2 - Ac1		A2 - Ac1		R2-Ac1	
	V3 - Ac1		A3 - Ac1		R3-Ac1	
Activo Crítico (Ac)	ID	Vulnerabilidad (V)	ID	Amenaza (A)	ID	Riesgo (R)
Fortinet Routers Firewall	V1 - Ac2		A1 - Ac2		R1-Ac2	
	V2 - Ac2		A2 - Ac2		R2-Ac2	
	V3 - Ac2		A3 - Ac2		R3-Ac2	
Activo Crítico (Ac)	ID	Vulnerabilidad (V)	ID	Amenaza (A)	ID	Riesgo (R)
Conmutadores	V1 - Ac3		A1 - Ac3		R1-Ac3	
	V2 - Ac3		A2 - Ac3		R2-Ac3	

	V3 – Ac3		A3 – Ac3		R3-Ac3	
Activo Crítico (Ac)	ID	Vulnerabilidad (V)	ID	Amenaza (A)	ID	Riesgo (R)
Equipos Servidores	V1 – Ac4		A1 – Ac4		R1-Ac4	
	V2 – Ac4		A2 – Ac4		R2-Ac4	
	V3 – Ac4		A3 – Ac4		R3-Ac4	
Activo Crítico (Ac)	ID	Vulnerabilidad (V)	ID	Amenaza (A)	ID	Riesgo (R)
Troncal SIP	V1 – Ac5		A1 – Ac5		R1-Ac5	
	V2 – Ac5		A2 – Ac5		R2-Ac5	
	V3 – Ac5		A3 – Ac5		R3-Ac5	
Activo Crítico (Ac)	ID	Vulnerabilidad (V)	ID	Amenaza (A)	ID	Riesgo (R)
	V1 – Ac5		A1 – Ac5		R1-Ac5	

Troncal Analógica	V2 – Ac5		A2 – Ac5		R2-Ac5	
	V3 – Ac5		A3 – Ac5		R3-Ac5	
Activo Crítico (Ac)	ID	Vulnerabilidad (V)	ID	Amenaza (A)	ID	Riesgo (R)
	V1 – Ac6		A1 – Ac6		R1-Ac6	
Infraestructura Wireless	V2 – Ac6		A2 – Ac6		R2-Ac6	
	V3 – Ac6		A3 – Ac6		R3-Ac6	
Activo Crítico (Ac)	ID	Vulnerabilidad (V)	ID	Amenaza (A)	ID	Riesgo (R)
	V1 – Ac7		A1 – Ac7		R1-Ac7	
Estaciones de trabajo	V2 – Ac7		A2 – Ac7		R2-Ac7	
	V3 – Ac7		A3 – Ac7		R3-Ac7	


Estudiante


Líder del área de TIC'S

ANEXO 9. Matriz de evaluación de zona de riesgo potencial a partir de análisis de probabilidad e impacto en los activos críticos



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE TELECOMUNICACIONES

Tema: Auditoria de la seguridad a la red de Telecomunicaciones de Nova Clínica Moderna en base al marco de ciberseguridad de la NIST

Fecha: 26/09/2024

Entrevistado: Líder de área de TIC'S

Entrevistador: Marco Latacumba

Objetivo: Realizar una mesa de trabajo con el líder del área de TIC'S de Nova Clínica Moderna analizar y seleccionar en base a los activos críticos y los riesgos potenciales iniciales según la valoración de probabilidad e impacto.

Instructivo: En base a la siguiente matriz proporcionada del CSF de la NIST completar la siguiente tabla según los parámetros que se muestran para la identificación de posibles riesgos potenciales de los activos críticos de la red de telecomunicaciones de la empresa.

Activo Crítico	Riesgo Potencial	Criterio De impacto	Probabilidad	Valor de Impacto	Puntuación	Zona de Riesgo
Cableado Horizontal y Vertical	Interferencia electromagnética Reducción significativa de la eficiencia en las comunicaciones y transferencia de datos.	Rendimiento				
	Conexiones no autorizadas. Percepción negativa de la empresa en cuanto a la seguridad de transmisión de datos.	Reputación				
	Fallo del Cableado Interrupciones en los servicios de red y la operatividad de los sistemas dependientes.	Operatividad				
	Configuración defectuosa. Exposición o posible acceso no autorizado a	Rendimiento				

Fortinet Routers Firewall	segmentos internos críticos de la red.	Reputación
	Políticas de firewall insuficientes frente a accesos a recursos y servicios no autorizados.	
	Saturación de recursos de router firewall. Retraso de actividades operativas de la red.	Operatividad
Conmutadores	Sobrecarga de Tráfico. Disminución de la velocidad de transferencia de datos.	Rendimiento
	Intrusión en la Red mediante conexiones ethernet no autorizadas.	Reputación
	Percepción de inseguridad en los servicios de la empresa.	
	Fallo de los Conmutadores. Retraso de ejecución	Operatividad

	de servicios y operaciones de la red.	
Equipos Servidores	Configuración defectuosa. Interrupciones y disminución de eficiencia de servicios.	Rendimiento
	Brechas de Seguridad expuestas, debido a la exposición de acceso físico no autorizado al área de servidores.	Reputación
	Interrupciones de Servicio. Paralización de operaciones dependientes de los servidores.	Operatividad
Troncal SIP	Congestión de Red. Reducción en la calidad y velocidad de las comunicaciones de voz.	Rendimiento
	Interceptación de Llamadas Percepción negativa de la	Reputación

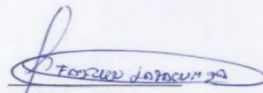
	seguridad de las comunicaciones.	
	Interrupción del Servicio de Voz. Afectación de las operaciones que dependen de las comunicaciones de voz.	Operatividad
Troncal Analógica (FXO SIP Gateway)	Interferencias en la Comunicación.	Rendimiento
	Reducción en la calidad de las llamadas.	
	Manipulación no Autorizada. Riesgo de daños, pérdida de conectividad y fallos en las comunicaciones	Reputación
	Fallo del Sistema de Comunicaciones. Paralización de servicios que dependen de las comunicaciones telefónicas.	Operatividad

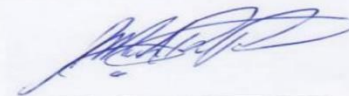
Infraestructura Wireless	Interferencias de Señal inalámbrica. Interrupción de la red inalámbrica	Rendimiento
	Falta de autenticación de usuarios en la red con posible pérdida de datos sensibles	Reputación
	Falta de mantenimiento de hardware y software de equipos. Afectación de operaciones que dependen de la conectividad inalámbrica.	Operatividad
Estaciones de trabajo	Pérdida de conectividad debido a interrupciones en la red o por instalación de software malicioso que comprometa el rendimiento de los computadores.	Rendimiento
	Acceso no autorizado a las estaciones de	Reputación

trabajo, fuga de datos sensibles debido falta de seguridad como contraseñas débiles o falta de autenticación en los computadores.

Fallos de hardware debido a picos de voltaje o fallo de software que afecte la operatividad de las estaciones de trabajo.

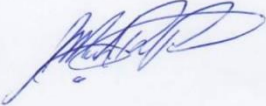
Operatividad


Estudiante


Líder del área de TIC'S

ANEXO 10. Tabla de validación de políticas desarrolladas

Elaborado por:	Marco Latacumba		Fecha de revisión:		24/10/2024
Políticas desarrolladas por evaluar	¿Política valida para implementación a futuro?		¿Podría ser eludible?		Observaciones
	SI	NO	SI	NO	
Art.1	✓			✓	
Art.2	✓			✓	
Art.3	✓			✓	
Art.4	✓			✓	
Art.5	✓			✓	
Art.6	✓			✓	
Art.7	✓			✓	
Art.8	✓			✓	
Art.9	✓			✓	
Art.10		✓	✓		
Art.11	✓			✓	
Art.12	✓			✓	
Art.13	✓			✓	
Art.14	✓			✓	
Art.15	✓			✓	
Art.16	✓			✓	
Art.17	✓			✓	
Art.18	✓		✓		
Art.19	✓			✓	
Art.20	✓		✓		
Art.21	✓			✓	
Art.22	✓			✓	
Art.23	✓			✓	
Art.24	✓		✓		
Art.25	✓		✓		
Art.26	✓		✓		
Art.27	✓		✓		
Art.28	✓		✓		
Art.29	✓		✓		
Art.30	✓		✓		
Art.31	✓		✓		
Art.32	✓			✓	
Art.33	✓		✓		
Art.34	✓			✓	
Art.35	✓			✓	

Art.36	✓		✓		
Art.37	✓		✓		
Art.38	✓		✓		
Art.39	✓		✓		
Art.40	✓			✓	
Art.41	✓			✓	
Art.42	✓			✓	
Art.43	✓		✓		
Art.44	✓			✓	
Art.45	✓			✓	
Art.46	✓		✓		
Art.47	✓		✓		
Art.48	✓			✓	
Art.49	✓		✓		
Art.50	✓		✓		
Art.51	✓			✓	
Art.52	✓			✓	
Art.53	✓			✓	
Art.54	✓			✓	
Art.55	✓			✓	
Art.56	✓			✓	
Art.57	✓			✓	
Art.58	✓			✓	
Art.59	✓			✓	
Art.60	✓			✓	
Art.61	✓			✓	
Art.62	✓			✓	
Art.63	✓			✓	
Art.64	✓			✓	
Art.65	✓			✓	
Art.66	✓			✓	
Art.67	✓			✓	
Art.68	✓			✓	
Art.69	✓			✓	
Art.70	✓			✓	
Art.71	✓			✓	
Art.72	✓			✓	
Art.73	✓			✓	
Art.74	✓			✓	
Revisado por Lider de área de TIC'S					

ANEXO 12. Formato de solicitud de acceso del personal a los servicios críticos**Formato solicitud de acceso a servicio crítico de la red empresarial de Nova Clínica Moderna**

Ibarra, _____ de _____ del _____

Área de TICS

Ing, _____ líder del área

Asunto: Solicitud de acceso a _____

Yo _____ con cedula de ciudadanía N° _____, me permito solicitar acceso de conexión a la red empresarial de Nova Clínica Moderna, específicamente al área de _____, para realizar funciones y/o actividades correspondientes a _____ con fines éticos y profesionales dentro de la empresa durante el tiempo de _____.

Atentamente

Ente encargado

ANEXO 15. Formato para atención y respuesta ante incidentes en la red**Plazo máximo de atención y respuesta del área de TICS**

Incidencia o falla	Tiempo de respuesta
Fallas en la red LAN	3 horas hábiles
Fallas en Herramientas Ofimáticas	4 horas hábiles
Fallas en Periféricos	3 horas hábiles
Asesoría en Manejo de herramientas ofimáticas	3 días hábiles
Asesoría en manejo de herramientas web	3 días hábiles
Fallas de impresión	3 horas hábiles
Infección por virus informáticos	3 horas hábiles
Daño o Perdida de Archivos	3 horas hábiles
Cambio de Usuarios, privilegios y contraseñas	3 días hábiles
Fallas en Sistemas Operativos	3 horas hábiles
Falla en rack de comunicaciones	1 día hábil
Falla en Servidores	1 día hábil
Fallas en sistemas de información	1 día hábil
Fallas en sistemas de respaldo	1 día hábil
Reinicio de Usuario y Contraseña para control de Acceso	3-5 días hábiles
Se deberán hacer efectivas las garantías con los proveedores	7 días Hábiles

ANEXO 16. Formato para gestión de incidentes en la infraestructura tecnológica

Formato de gestión de vulnerabilidades e incidentes en la red de Telecomunicaciones de Nova Clínica Moderna

1. Datos de quien informa

Nombre:	
Cargo dentro de la empresa:	
Correo electrónico:	
Teléfono:	
Área a la que ha reportado el incidente dentro de la empresa:	

2. Información del incidente

Fecha y hora:	
Área afectada:	
Descripción breve del incidente:	
Elementos de la infraestructura tecnológica que se vieron afectados por el incidente de ciberseguridad:	
Medios de atención para clientes impactados por el incidente:	
Grado aproximado de daño o efecto generado por el incidente de ciberseguridad:	
Especificar las medidas inmediatas que se han tomado para reducir el impacto del incidente de ciberseguridad:	

3. Categorizar el incidente de ciberseguridad descrito en este anexo según las siguientes definiciones.

Tipo de incidente	Aplica Si / No	Detalle del tipo de incidente en específico
Ataques físicos (intencionados o deliberados) que incluyen: sabotajes, actos de vandalismo, robo de equipos, filtraciones de información en soportes físicos, accesos no autorizados, coerción, extorsión, actos terroristas, entre otros.		
Daños no intencionales o accidentes, como la pérdida de información o activos, que abarcan: divulgación inapropiada de información, errores o fallos en sistemas o dispositivos, fallas en procedimientos o controles, modificaciones no autorizadas de datos, y pérdida de información o dispositivos, entre otros.		
Incidentes provocados por desastres naturales o ambientales, tales como: terremotos, inundaciones, huracanes, incendios, radiación, corrosión, explosiones, entre otros.		
Incidentes relacionados con fallas o mal funcionamiento, incluyendo: fallos en dispositivos o sistemas, problemas de comunicación, interrupciones en servicios de terceros o en la cadena de suministro, entre otros.		
Incidentes derivados de interrupciones o falta de suministros, tales como: ausencia de personal, huelgas, cortes en el suministro de energía, agua o telecomunicaciones, entre otros.		
Incidentes relacionados con la interceptación de datos, como: espionaje, interceptación de mensajes, wardriving, ataques de hombre en medio, secuestro de sesiones, programas sniffer, robo de mensajes, entre otros.		
Incidentes originados por actividades maliciosas (ciberataques) destinadas a tomar control, desestabilizar o dañar sistemas informáticos, tales como: robo de identidad, phishing, ataques de		

<p>denegación de servicio (DOS, DDOS), software malicioso (malware, troyanos, gusanos, inyección de código, virus, ransomware), ingeniería social, violación de certificados (suplantación de sitios, certificados falsos), manipulación de hardware (proxies anónimos, skimmers, sniffers), alteración de información (suplantación de direccionamiento y tablas de enrutamiento, envenenamiento de DNS, modificación de configuraciones), abuso de aplicaciones de auditoría, ataques de fuerza bruta, y abuso de autorizaciones, entre otros.</p>		
<p>Incidentes provocados por cuestiones legales, como: incumplimiento de cláusulas y acuerdos, violación de confidencialidad, y decisiones adversas (resoluciones judiciales en la misma jurisdicción o en otras), entre otros.</p>		

ANEXO 17. Formato de acuerdo de confidencialidad para funcionarios de la empresa

Acuerdo de confidencialidad sobre el manejo y divulgación de información por parte de los empleados/as

Yo _____, con cédula de identidad _____, en mi calidad de empleado y en reconocimiento de la relación laboral que mantengo con Nova Clínica Moderna, así como del acceso que se me concede a sus bases de datos, servicios críticos e información, declaro lo siguiente:

- 1) Estoy plenamente consciente de la relevancia de mis responsabilidades respecto a la protección de la integridad, disponibilidad y confidencialidad de la información manejada por la Nova Clínica Moderna.

- 2) Me comprometo a cumplir rigurosamente con todas las disposiciones establecidas en las políticas de seguridad de la red de Telecomunicaciones de Nova Clínica Moderna sobre el uso y la divulgación de información, y a no divulgar ningún dato al que tenga acceso durante mi relación laboral. Este deber de confidencialidad permanecerá vigente incluso después de finalizar la relación laboral, ya sea que la información pertenezca a Nova Clínica Moderna, a sus clientes o a cualquier otra entidad que nos otorgue acceso a dicha información. Además, queda estrictamente prohibido realizar copias de esta información sin la debida autorización.

- 3) Comprendo que el incumplimiento de cualquiera de las obligaciones descritas en el presente documento ya sea de forma intencional o por negligencia, podría resultar en sanciones disciplinarias por parte de Nova Clínica Moderna, así como en posibles

reclamaciones por los daños económicos ocasionados.

Con esta declaración, asumo la responsabilidad de adherirme a las normas y políticas de confidencialidad de Nova Clínica Moderna.

C.I

Líder del área de TIC'S

ANEXO 19. Matriz de riesgos residuales obtenidos mediante el análisis y evaluación de políticas desarrolladas

Activo Crítico	Riesgo Potencial	Probabilidad Inicial	Impacto Inicial	Zona de Riesgo Inicial	Valor Cuantitativo	Política Recomendada	Probabilidad Residual	Impacto Residual	Zona de Riesgo Residual	Valor Cuantitativo
Cableado Horizontal y Vertical	Interferencia electromagnética	Baja (2)	Medio (3)	Moderado	6	Art. 9 Art. 53 Art. 54	Muy Baja (1)	Bajo (2)	Bajo	2
	Reducción significativa de la eficiencia en las comunicaciones y transferencia de datos.									
	Conexiones no autorizadas. Percepción negativa de la empresa en cuanto a la seguridad de transmisión de datos.	Baja (2)	Medio (3)	Moderado	6	Art. 9 Art. 44 Art. 53	Muy Baja (1)	Bajo (2)	Bajo	2
	Fallo del Cableado Interrupciones en los servicios de red y la operatividad de los sistemas dependientes.	Baja (2)	Alto (4)	Alto	8	Art. 9 Art. 53 Art. 54 Art. 55	Muy Baja (1)	Bajo (2)	Bajo	2

Activo Crítico	Riesgo Potencial	Probabilidad Inicial	Impacto Inicial	Zona de Riesgo Inicial	Valor Cuantitativo	Política Recomendada	Probabilidad Residual	Impacto Residual	Zona de Riesgo Residual	Valor Cuantitativo
Routers Firewall FortiGate	Configuración defectuosa. Exposición o posible acceso no autorizado a segmentos internos críticos de la red.	Muy Baja (1)	Crítico (5)	Alto	5	Art. 23 Art. 24 Art. 42	Muy Baja (1)	Medio (3)	Moderado	3
	Políticas de firewall insuficientes frente a accesos a recursos y servicios no autorizados.	Baja (2)	Alto (4)	Alto	8	Art. 26 Art. 28 Art. 31 Art. 41 Art. 42	Muy Baja (1)	Medio (3)	Moderado	3
	Saturación de recursos de router firewall. Retraso de actividades operativas de la red.	Muy Baja (1)	Medio (3)	Moderado	3	Art. 23 Art. 41 Art. 43	Muy Baja (1)	Bajo (2)	Bajo	2

Activo Crítico	Riesgo Potencial	Probabilidad Inicial	Impacto Inicial	Zona de Riesgo Inicial	Valor Cuantitativo	Política Recomendada	Probabilidad Residual	Impacto Residual	Zona de Riesgo Residual	Valor Cuantitativo
Conmutadores	Sobrecarga de Tráfico. Disminución de la velocidad de transferencia de datos.	Baja (2)	Medio (3)	Moderado	6	Art. 23 Art. 24 Art. 33	Muy Baja (1)	Bajo (2)	Bajo	2
	Intrusión en la Red mediante conexiones ethernet no autorizadas. Percepción de inseguridad en los servicios de la empresa.	Baja (2)	Medio (3)	Moderado	6	Art. 25 Art. 27 Art. 20 Art. 21	Muy Baja (1)	Bajo (2)	Bajo	2
	Fallo de los Conmutadores. Retraso de ejecución de servicios y operaciones de la red.	Baja (2)	Alto (4)	Alto	8	Art. 44 Art. 46 Art. 47 Art. 51 Art. 53	Muy Baja (1)	Alto (4)	Moderado	4

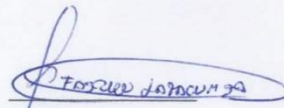
Activo Crítico	Riesgo Potencial	Probabilidad Inicial	Impacto Inicial	Zona de Riesgo Inicial	Valor Cuantitativo	Política Recomendada	Probabilidad Residual	Impacto Residual	Zona de Riesgo Residual	Valor Cuantitativo
Equipos Servidores	Configuración defectuosa. Interrupciones y disminución de eficiencia de servicios.	Baja (2)	Medio (3)	Moderado	6	Art. 49 Art. 50 Art. 51 Art. 52	Baja (2)	Bajo (2)	Bajo	4
	Brechas de Seguridad expuestas, debido a la exposición de acceso físico no autorizado al área de servidores.	Baja (2)	Medio (3)	Moderado	6	Art. 13 Art. 16 Art. 55	Muy Baja (1)	Bajo (2)	Bajo	2
	Interrupciones de Servicio. Paralización de operaciones dependientes de los servidores.	Baja (2)	Crítico (5)	Extremo	10	Art. 29 Art. 30 Art. 38 Art. 40 Art. 47 Art. 51 Art. 52 Art. 55	Muy Baja (1)	Alto (4)	Moderado	4

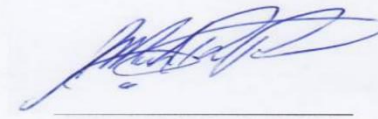
Activo Crítico	Riesgo Potencial	Probabilidad Inicial	Impacto Inicial	Zona de Riesgo Inicial	Valor Cuantitativo	Política Recomendada	Probabilidad Residual	Impacto Residual	Zona de Riesgo Residual	Valor Cuantitativo
Troncal SIP	Congestión de Red. Reducción en la calidad y velocidad de las comunicaciones de voz.	Baja (2)	Medio (3)	Moderado	6	Art. 33 Art. 46	Muy Baja (1)	Muy Bajo (1)	Bajo	1
	Interceptación de Llamadas Percepción negativa de la seguridad de las comunicaciones.	Baja (2)	Medio (3)	Moderado	6	Art. 32 Art. 34 Art. 49 Art. 50	Muy Baja (1)	Muy Bajo (1)	Bajo	1
	Interrupción del Servicio de Voz. Afectación de las operaciones que dependen de las comunicaciones de voz.	Baja (2)	Alto (4)	Alto	8	Art. 32 Art. 51	Muy Baja (1)	Muy Bajo (1)	Bajo	1

Activo Crítico	Riesgo Potencial	Probabilidad Inicial	Impacto Inicial	Zona de Riesgo Inicial	Valor Cuantitativo	Política Recomendada	Probabilidad Residual	Impacto Residual	Zona de Riesgo Residual	Valor Cuantitativo
Troncal analógica (FXO SIP Gateway)	Interferencias en la Comunicación. Reducción en la calidad de las llamadas.	Media (3)	Bajo (2)	Moderado	6	Art. 33 Art. 46	Muy Baja (1)	Muy Bajo (1)	Bajo	1
	Manipulación no Autorizada. Riesgo de daños, pérdida de conectividad y fallos en las comunicaciones	Muy Baja (1)	Bajo (2)	Baja	2	Art. 9 Art. 13 Art. 16	Muy Baja (1)	Muy Bajo (1)	Bajo	1
	Fallo del Sistema de Comunicaciones. Paralización de servicios que dependen de las comunicaciones telefónicas.	Baja (2)	Medio (3)	Moderado	6	Art. 32 Art. 51	Muy Baja (1)	Muy Bajo (1)	Bajo	1

Activo Crítico	Riesgo Potencial	Probabilidad Inicial	Impacto Inicial	Zona de Riesgo Inicial	Valor Cuantitativo	Política Recomendada	Probabilidad Residual	Impacto Residual	Zona de Riesgo Residual	Valor Cuantitativo
Infraestructura Wireless	Interferencias de Señal inalámbrica. Interrupción de la red inalámbrica	Baja (2)	Medio (3)	Moderado	6	Art. 48 Art. 52	Muy Baja (1)	Bajo (2)	Bajo	2
	Falta de autenticación de usuarios en la red con posible pérdida de datos sensibles	Baja (2)	Alto (4)	Alto	8	Art. 18 Art. 19 Art. 20 Art. 25	Muy Baja (1)	Medio (3)	Moderado	3
	Falta de mantenimiento de hardware y software de equipos. Afectación de operaciones que dependen de la conectividad inalámbrica.	Baja (2)	Medio (3)	Moderado	6	Art. 44 Art. 46 Art. 52 Art. 53	Muy Baja (1)	Bajo (2)	Bajo	2

Activo Crítico	Riesgo Potencial	Probabilidad Inicial	Impacto Inicial	Zona de Riesgo Inicial	Valor Cuantitativo	Política Recomendada	Probabilidad Residual	Impacto Residual	Zona de Riesgo Residual	Valor Cuantitativo
Estaciones de Trabajo	Pérdida de conectividad debido a interrupciones en la red o por instalación de software malicioso que comprometa el rendimiento de los computadores.	Baja (2)	Medio (3)	Moderado	6	Art. 67 Art. 45 Art. 46 Art. 52	Muy Baja (1)	Medio (3)	Moderado	3
	Acceso no autorizado a las estaciones de trabajo, fuga de datos sensibles debido falta de seguridad como contraseñas débiles o falta de autenticación en los computadores.	Baja (2)	Alto (4)	Alto	8	Art. 18 Art. 25 Art. 26 Art. 27 Art. 62 Art. 63	Muy Baja (1)	Medio (3)	Moderado	3
	Fallos de hardware debido a picos de voltaje o fallo de software que afecte la operatividad de las estaciones de trabajo	Baja (2)	Medio (3)	Moderado	6	Art. 54 Art. 56 Art. 57	Muy Baja (1)	Bajo (2)	Bajo	2


Estudiante


Líder del área de TIC'S



ACTA DE ENTREGA RECEPCIÓN

PROCESO: TICs

DESCRIPCION: PROYECTO DE TESIS

COMPARECIENTES

En la ciudad de Ibarra al 2 de diciembre del 2024, comparecen para la firma de la presente Acta de Entrega Recepción, Ing. Marcelo Rea **Líder de TIC's**, Marco Fabricio Latacumba Farinango, como **Estudiante Telecomunicaciones - UTN** y por otra la Ing. Ximena Andrade como Gerente, al tenor de las siguientes cláusulas:

Primera Antecedentes. – El señor Marco Fabricio Latacumba Farinango, estudiante de la carrera de Telecomunicaciones de la Universidad Técnica del Norte, realizó el proyecto de Tesis titulado "Auditoria de la seguridad a la red de Telecomunicaciones de Nova Clínica Moderna en base al marco de ciberseguridad de la NIST".

Que Nova Clínica Moderna, proporcionó al estudiante la apertura y todas las facilidades para que pueda realizar su proyecto dirigido a la empresa.

Segunda Condiciones Generales de Ejecución. –

El señor Marco Fabricio Latacumba Farinango, estudiante de la carrera de Telecomunicaciones de la Universidad Técnica del Norte, entregó el "Manual de políticas de seguridad para la red de Telecomunicaciones de Nova Clínica Moderna en base al marco de ciberseguridad de la NIST con enfoque en la función Proteger", como producto de su proyecto de tesis.

El Ingeniero Marcelo Rea, líder de TIC's recibe el "Manual de políticas de seguridad para la red de Telecomunicaciones de Nova Clínica Moderna en base al marco de ciberseguridad de la NIST con enfoque en la función Proteger"

Para constancia y conformidad de lo expresado en la presente acta entrega de recepción se procede a suscribir la misma, en un original y una copia de igual contenido.

Marco Fabricio Latacumba Farinango
Estudiante Telecomunicaciones - UTN

Ing. Marcelo Rea
Líder de TIC's

CLÍNICA MODERNA

Ing. Marcelo Rea
LIDER DE TIC's

Ing. Ximena Andrade
Gerente

más de 50 años...

Victor Gómez Jurado 5-132 y Av. Mariano Acosta (junto al Supermaxi)

info@climoder.com  www.climoder.com

PBX: (06) 500 40 40 / Emergencias 24 Horas: 099 821 9470

IBARRA