

NOMBRE DEL TRABAJO

IMPLEMENTACIÓN DE MEJORAS EN LA CIBERSEGURIDAD PARA MITIGAR LOS ATAQUES DIRIGIDOS A UNA EMPRESA DE L

AUTOR

ANGIE MARIELA TOMAYRO CULE

RECUENTO DE PALABRAS

18377 Words

RECUENTO DE CARACTERES

106218 Characters

RECUENTO DE PÁGINAS

132 Pages

TAMAÑO DEL ARCHIVO

7.8MB

FECHA DE ENTREGA

Apr 17, 2024 9:49 PM GMT-5

FECHA DEL INFORME

Apr 17, 2024 9:51 PM GMT-5

● 4% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 4% Base de datos de Internet
- Base de datos de Crossref
- 0% Base de datos de trabajos entregados
- 0% Base de datos de publicaciones
- Base de datos de contenido publicado de Crossref

● Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Coincidencia baja (menos de 10 palabras)

**FORMULARIO DE AUTORIZACIÓN PARA LA
PUBLICACIÓN DE TRABAJOS DE INVESTIGACIÓN EN
EL REPOSITORIO INSTITUCIONAL DE LA UNTELS
(Art. 45° de la ley N° 30220 – Ley)**

Autorización de la propiedad intelectual del autor para la publicación de tesis en el Repositorio Institucional de la Universidad Nacional Tecnológica de Lima Sur (<https://repositorio.untehs.edu.pe>), de conformidad con el Decreto Legislativo N° 822, sobre la Ley de los Derechos de Autor, Ley N° 30035 del Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto, Art. 10° del Rgto. Nacional de Trabajos de Investigación para optar grados académicos y títulos profesionales en las universidades – RENATI Res. N° 084-2022-SUNEDU/CD, publicado en El Peruano el 16 de agosto de 2022; y la RCO N° 061-2023-UNTELS del 01 marzo 2023.

TIPO DE TRABAJO DE INVESTIGACIÓN

- 1). TESIS () 2). TRABAJO DE SUFICIENCIA PROFESIONAL (x)

DATOS PERSONALES

Apellidos y Nombres: TOMAYRO CULE, ANGIE MARIELA
D.N.I.: 70988353
Otro Documento:
Nacionalidad: PERUANA
Teléfono: 931867224
e-mail: ANGIE.MARIELA127@GMAIL.COM

DATOS ACADÉMICOS

Pregrado

Facultad: FACULTAD DE INGENIERÍA Y GESTIÓN
Programa Académico: TRABAJO DE SUFICIENCIA PROFESIONAL
Título Profesional otorgado: INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

Postgrado

Universidad de Procedencia:
País:
Grado Académico otorgado:

Datos de trabajo de investigación

Título: “IMPLEMENTACIÓN DE MEJORAS EN LA CIBERSEGURIDAD PARA MITIGAR LOS ATAQUES DIRIGIDOS A UNA EMPRESA DEL SECTOR TURÍSTICO”
Fecha de Sustentación: 17 DE DICIEMBRE DEL 2023
Calificación: APROBADO CON DISTINCIÓN
Año de Publicación: 2024

AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

A través de la presente, autorizo la publicación del texto completo de la tesis, en el Repositorio Institucional de la UNTELS especificando los siguientes términos:

Marcar con una X su elección.

- 1) Usted otorga una licencia especial para publicación de obras en el REPOSITORIO INSTITUCIONAL DE LA UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR.

Si autorizo _____ No autorizo X

- 2) Usted autoriza para que la obra sea puesta a disposición del público conservando los derechos de autor y para ello se elige el siguiente tipo de acceso.

Derechos de autor		
TIPO DE ACCESO	ATRIBUCIONES DE ACCESO	ELECCIÓN
ACCESO ABIERTO 12.1(*)	info:eu-repo/semantics/openAccess (Para documentos en acceso abierto)	()

- 3) Si usted dispone de una **PATENTE** puede elegir el tipo de **ACCESO RESTRINGIDO** como derecho de autor y en el marco de confiabilidad dispuesto por los numerales 5.2 y 6.7 de la directiva N° 004-2016-CONCYTEC DEGC que regula el Repositorio Nacional Digital de CONCYTEC (Se colgará únicamente datos del autor y el resumen del trabajo de investigación).

Derechos de autor		
TIPO DE ACCESO	ATRIBUCIONES DE ACCESO	ELECCIÓN
ACCESO RESTRINGIDO	info:eu-repo/semantics/restrictedAccess (Para documentos restringidos)	(X)
	info:eu-repo/semantics/embargoedAccess (Para documentos con períodos de embargo. Se debe especificar las fechas de embargo)	()
	info:eu-repo/semantics/closedAccess (para documentos confidenciales)	()

(*) <http://renati.sunedu.gob.pe>



Rellene la siguiente información si su trabajo de investigación es de acceso restringido:

Atribuciones de acceso restringido:

info:eu-repo/semantics/restrictedAccess

Motivos de la elección del acceso restringido:

INFORMACIÓN CONFIDENCIAL QUE CONTIENE EL PRESENTE TRABAJO DE
INVESTIGACIÓN

TOMAYRO CULE, ANGIE MARIELA

APELLIDOS Y NOMBRES

70988353

DNI



Firma y huella:



Lima, 6 de MAYO del 20 24

UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

**FACULTAD DE INGENIERÍA Y GESTIÓN
ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y
TELECOMUNICACIONES**



**“IMPLEMENTACIÓN DE MEJORAS EN LA CIBERSEGURIDAD PARA
MITIGAR LOS ATAQUES DIRIGIDOS A UNA EMPRESA DEL SECTOR
TURÍSTICO”**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

TOMAYRO CULE, ANGIE MARIELA
ORCID: 0009-0003-3238-1055

ASESOR

MORÁN MONTOYA, ENRIQUE MANUEL
ORCID: 0009-0005-2964-746X

**Villa El Salvador
2023**



"Año de la unidad, la paz y el desarrollo"

VI Programa de Titulación por la Modalidad de Trabajo de Suficiencia Profesional
Decanato de la Facultad de Ingeniería y Gestión

ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL PARA OBTENER EL
TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

En Villa El Salvador, siendo las 14:17 horas del día 17 de diciembre de 2023, se reunieron en las instalaciones de la Universidad Nacional Tecnológica de Lima Sur, los miembros del Jurado Evaluador del Trabajo de Suficiencia Profesional integrado por:

Presidente	:	DR. MARK DONNY CLEMENTE ARENAS	CIP N° 181400
Secretario	:	MG. LUDWIG PASCUAL LÓPEZ HUAMAN	CIP N° 310375
Vocal	:	MG. MARTHA ROXANA QUISPE AYALA	CIP N° 124612

Designados con Resolución de Decanato de la Facultad de Ingeniería y Gestión N° 984-2023-UNTELS-R-D de fecha 13 de diciembre del 2023.

Se da inició al acto público de sustentación y evaluación del Trabajo de Suficiencia Profesional, para obtener el Título Profesional de Ingeniero Electrónico y Telecomunicaciones, bajo la modalidad de Titulación por Trabajo de Suficiencia Profesional (Resolución de Consejo Universitario N° 065-2023-UNTELS-CU de fecha 08 de agosto del 2023), en la cual se APRUEBA el "Reglamento, Directiva, Cronograma y Presupuesto del VI Programa de Titulación por la Modalidad de Trabajo de Suficiencia Profesional de la Universidad Nacional Tecnológica de Lima Sur"; siendo que el Art. 4º del precitado Reglamento establece que: "La Modalidad de Titulación prevista consiste en la presentación, aprobación y sustentación de un Trabajo de Suficiencia Profesional que dé cuenta de la experiencia profesional y además permita demostrar el logro de las competencias adquiridas en el desarrollo de los estudios de pregrado que califican para el ejercicio de la profesión correspondiente. Quienes participen en esta modalidad no podrán tramitar simultáneamente otras modalidades de titulación. Además, los participantes inscritos en esta modalidad, deberán acreditar un mínimo de dos (02) años de experiencia laboral, de acuerdo a lo establecido en la Resolución N° 174-2019- SUNEDU/CD y al anexo 1 sobre Glosario de Términos en el punto veinte (20)...", en el cual;

La Bachiller **ANGIE MARIELA TOMAYRO CULE**

Sustentó su Trabajo de Suficiencia Profesional: **IMPLEMENTACIÓN DE MEJORAS EN LA CIBERSEGURIDAD PARA MITIGAR LOS ATAQUES DIRIGIDOS A UNA EMPRESA DEL SECTOR TURÍSTICO**

Concluida la Sustentación del Trabajo de Suficiencia Profesional, se procedió a la calificación correspondiente según el siguiente detalle:

Condición APROBADO CON DISTINCIÓN Equivalencia MUY BUENO de acuerdo al Art. 65º del Reglamento General para el Otorgamiento de Grado Académico y Título Profesional de la UNTELS vigente.

Siendo las 15:05 horas del día 17 de diciembre de 2023 se dio por concluido el acto de sustentación del Trabajo de Suficiencia Profesional, firmando la presente acta los miembros del Jurado.

SECRETARIO
MG. LUDWIG PASCUAL LÓPEZ HUAMAN
CIP N° 310375

PRESIDENTE
DR. MARK DONNY CLEMENTE ARENAS
CIP N° 181400

VOCAL
MG. MARTHA ROXANA QUISPE AYALA
CIP N° 124612

Nota: Art. 14º.- La sustentación del Trabajo de Suficiencia Profesional se realizará en un acto público. De faltar algún miembro del Jurado, la sustentación procederá con los dos integrantes presentes. En caso de ausencia del presidente del Jurado, asumirá la presidencia el docente de mayor categoría y antigüedad. En caso de ausencia de dos o más miembros del Jurado, la sustentación será reprogramada durante los 05 días siguientes.

DEDICATORIA

A Dios por brindarme salud para poder lograr mis objetivos y haberme permitido llegar a esta etapa de mi vida profesional.

A mi madre Leoncia Cule Pariona, a mi padre y a mis hermanos por su apoyo y buenos consejos porque siempre estuvieron a mi lado apoyándome.

A mi mejor amigo de cuatro patas, Yako, que con su amor y compañía estuvo acompañándome y cuidándome durante estos últimos 5 años, este es un reconocimiento a su lealtad.

A mí, por nunca rendirme, por mi perseverancia y constancia.

AGRADECIMIENTO

A Dios, que me ha guiado y dado la sabiduría para alcanzar esta meta.

A mi madre Leoncia Cule Pariona, por ser una excelente madre.

ÍNDICE

DEDICATORIA.....	ii
AGRADECIMIENTO.....	iii
LISTADO DE FIGURAS	vii
LISTADO DE TABLAS	xi
RESUMEN	xii
INTRODUCCIÓN	xiii
CAPÍTULO I. ASPECTOS GENERALES	15
1.1. Contexto	15
1.2. Delimitación temporal y espacial del trabajo.....	16
1.2.1. Temporal.....	16
1.2.2. Espacial	16
1.3. Objetivos.....	16
1.3.1. Objetivo General	16
1.3.2. Objetivo Específicos	16
CAPÍTULO II. MARCO TEÓRICO.....	17
2.1. Antecedentes.....	17
2.1.1. Antecedentes Internacionales.....	17
2.1.2. Antecedentes Nacionales	19
2.2. Bases teóricas	21
2.2.1. Tipos de Redes.....	21
2.2.2. Amenazas de Seguridad.....	23
2.2.3. Soluciones de Seguridad	25
2.2.4. Capas del modelo OSI.....	26
2.2.5. Directorio Activo.....	29
2.2.6. Protocolo LDAP	32

2.2.7. Firewall Perimetral	33
2.2.8. Fortinet.....	33
2.2.9. Red Privada Virtual (VPN)	40
2.2.10. Tipos de VPN.....	41
2.2.11. Protocolos de VPN.....	42
2.2.12. Algoritmos de cifrado	44
2.2.13. Autenticación Multifactor (MFA).....	44
2.2.14. FortiToken Mobile (FTM)	45
2.2.15. Análisis de Riesgo	46
2.2.16. Matriz de riesgo	46
2.2.17. Método William T. Fine	47
2.3. Definición de términos básicos	50
CAPÍTULO III: DESARROLLO DEL TRABAJO PROFESIONAL	52
3.1. Determinación y análisis del problema	52
3.2. Modelo de solución propuesto.....	55
3.2.1. Análisis de Riesgo.....	56
3.3. Resultados.....	98
CONCLUSIONES.....	107
RECOMENDACIONES	108
REFERENCIAS BIBLIOGRÁFICAS	109
ANEXOS	116
Anexo 1. Cronograma de actividades	116
Anexo 2. Procedimiento para la atención de tickets.....	117
Anexo 3. Plantilla de categorías filtro web.....	118
Anexo 4. Plantilla de categorías control de aplicaciones.....	120
Anexo 5. Bloqueo de malware Mirai.Botnet.....	121
Anexo 6. Bloqueo de malware Gh0st.Rat.Botnet	121

Anexo 7. Bloqueo de malware SystemBC.Botnet	123
Anexo 8. Bloqueo de malware Bladabindi.Botnet.....	124
Anexo 9. Bloqueo de acceso a la aplicación WireGuard	125
Anexo 10. Bloqueo de acceso a la aplicación Pure.VPN	125
Anexo 11. Bloqueo de acceso a la aplicación Hotspot.Shield	126
Anexo 12. Bloqueo de acceso a la aplicación Psiphon	126
Anexo 13. Bloqueo de acceso a la aplicación AnyDesk.....	127
Anexo 14. Bloqueo de acceso a la aplicación TeamViewer	127
Anexo 15. Bloqueo de acceso a la aplicación Xbox	128
Anexo 16. Bloqueo de acceso a la aplicación Steam	128
Anexo 17. Bloqueo de acceso a la aplicación Epic.Games.....	129
Anexo 18. Bloqueo de acceso a la aplicación Apple.Game.Center.....	129
Anexo 19. Bloqueo de acceso a la aplicación BitTorrent	130
Anexo 20. Vulnerabilidad CVE-2023-25610	131
Anexo 21. Estimación de costo de la implementación	132

LISTADO DE FIGURAS

Figura 1. Panorama Global de Amenazas (Fortinet, 2022)	xiii
Figura 2. LAN separadas y conectadas por la red WAN (Cisco Networking Academy, 2013)	22
Figura 3. LAN y WAN conectadas a internet (Cisco Networking Academy, 2013)	22
Figura 4. Actividad de una botnet sobre un servidor web (Aguilera López, 2010)	24
Figura 5. Capas del modelo OSI (Cisco Networking Academy, 2013)	26
Figura 6. Capa de aplicación (Cisco Networking Academy, 2013).....	27
Figura 7. Capa de presentación (Cisco Networking Academy, 2013)	27
Figura 8. Capa de sesión (Cisco Networking Academy, 2013)	27
Figura 9. Capa de transporte (Cisco Networking Academy, 2013).....	28
Figura 10. Capa de red (Cisco Networking Academy, 2013)	28
Figura 11. Capa de enlace de datos (Cisco Networking Academy, 2013)	29
Figura 12. Capa física (Cisco Networking Academy, 2013)	29
Figura 13. Esquema de un bosque en Directorio Activo (Maciá et al., 2008).....	31
Figura 14. Unidades organizativas de un dominio (Maciá et al., 2008)	32
Figura 15. Esquema de LDAP (Maciá et al., 2008)	32
Figura 16. Cuadrante Mágico de Firewalls de Red (Fortinet, 2022)	34
Figura 17. Administrador de Dispositivos	36
Figura 18. Vista de registros.....	37
Figura 19. Plantillas de reportes del FortiAnalyzer	37
Figura 20. Monitor de eventos del FortiAnalyzer	38
Figura 21. Firmas de ataques detectados	38
Figura 22. Mapa de amenazas detectadas	39
Figura 23. Principales amenazas detectadas	39
Figura 24. Topología VPN Site to Site (Fortinet, 2017)	42
Figura 25. VPN SSL modo web y túnel (Fortinet, 2017).....	43
Figura 26. VPN SSL con autenticación FortiToken (Fortinet, 2022).....	45
Figura 27. Matriz de riesgos (López Ruíz, 2008).....	47
Figura 28. Acceso a software AnyDesk y TeamViewer en el 2023	53
Figura 29. Archivos de la Entidad Turística encriptados	53
Figura 30. Nota de rescate de ciberdelincuentes dirigida a la Entidad Turística ..	54

Figura 31. Servicios habilitados en las políticas del firewall FortiGate	54
Figura 32. Estado actual de políticas en el firewall FortiGate.....	55
Figura 33. Estructura del trabajo	56
Figura 34. Información del sistema	61
Figura 35. Ruta de actualización	62
Figura 36. Descarga de firmware	62
Figura 37. Imagen del firmware 7.0.12.....	63
Figura 38. Imagen del firmware 7.2.25.....	63
Figura 39. Actualización del FortiGate	64
Figura 40. Reinicio del firewall FortiGate.....	64
Figura 41. Firmware v7.0.12.....	65
Figura 42. Firmware v7.2.5.....	65
Figura 43. Administradores del firewall FortiGate.....	66
Figura 44. Configuración del Trusted Hosts	66
Figura 45. Acceso administrativo del firewall por Hosts Confiables	67
Figura 46. Topología VPN SSL	68
Figura 47. Configuración de la conexión VPN SSL	69
Figura 48. Configuración VPN SSL en modo túnel	69
Figura 49. Configuración del Portal de acceso VPN SSL.....	70
Figura 50. Autenticación/Asignación de portal	71
Figura 51. Configuración del protocolo LDAP en el firewall	71
Figura 52. Integración del protocolo LDAP en el Firewall.....	72
Figura 53. Test de conectividad con el directorio activo	72
Figura 54. Registro del LDAP server en el firewall	72
Figura 55. Creación de usuario LDAP remoto.....	73
Figura 56. Búsqueda de usuarios LDAP	73
Figura 57. Lista de usuarios VPN.....	74
Figura 58. Asignación de FortiToken a usuario VPN.....	74
Figura 59. Código de activación FortiToken	75
Figura 60. Configuración del FortiToken	76
Figura 61. Activación del FortiToken Mobile.....	76
Figura 62. Usuarios VPN con doble factor de autenticación	77
Figura 63. Política para el acceso VPN SSL en el firewall FortiGate	78
Figura 64. Configuración en el FortiClient VPN.....	79

Figura 65. Reportes creados en el FortiAnalyzer	80
Figura 66. Perfiles de seguridad Antivirus	81
Figura 67. Configuración del perfil antivirus	81
Figura 68. Perfiles de filtro web	82
Figura 69. Configuración del perfil filtrado web	83
Figura 70. Perfiles de control de aplicaciones	84
Figura 71. Configuración del perfil control de aplicaciones	84
Figura 72. Perfiles del Sistema de prevención de intrusos (IPS).....	85
Figura 73. Configuración del perfil IPS.....	86
Figura 74. Perfiles del Inspección SSL/SSH	87
Figura 75. Configuración del perfil certificate-inspection	87
Figura 76. Políticas de navegación a internet.....	88
Figura 77. Comando debug.....	89
Figura 78. Estado de la CPU.....	89
Figura 79. Estado de la memoria	90
Figura 80. Intentos de inicio de sesión fallidas.....	90
Figura 81. Solicitud de Token para nueva conexión VPN	91
Figura 82. Conexión del usuario en el FortiClient.....	92
Figura 83. Tráfico de la política	92
Figura 84. Monitoreo de conexiones VPN SSL	93
Figura 85. Conexión por ping hacia la red interna.....	93
Figura 86. Registro del tráfico de la política “Acceso a internet_Piso1”	94
Figura 87. Registro de aplicaciones en la política	94
Figura 88. Aplicación bloqueada por el perfil control de aplicaciones	95
Figura 89. Registro de sitios web en la política	95
Figura 90. Mensaje de bloqueo hacia la página web	96
Figura 91. Mensaje de bloqueo a página web ilegal o poco ético	97
Figura 92. Registro de bloqueos del perfil Antivirus	97
Figura 93. Intentos de inicio de sesión fallidas del mes de julio	99
Figura 94. Conexiones VPN SSL del mes de julio	99
Figura 95. Asignación de FortiToken a usuarios VPN	100
Figura 96. Detección y bloqueo de Malware durante el mes de julio	101
Figura 97. Archivos analizados durante el mes de julio	102
Figura 98. Tipos de archivos analizados durante el mes de julio	102

Figura 99. Intentos de acceso - Categoría Proxy	103
Figura 100. Intentos de acceso - Categoría Acceso Remoto	104
Figura 101. Intentos de acceso - Categoría Juegos	104
Figura 102. Intentos de acceso - Categoría P2P	105
Figura 103. Intentos de acceso - categorías del filtro web	109

LISTADO DE TABLAS

Tabla 1. Ranking de las consecuencias del riesgo (C) en el método William T. Fine (Semchenko et al. 2022)	48
Tabla 2. Ranking de la probabilidad de ocurrencia del riesgo (P) en el método William T. Fine (Semchenko et al. 2022).....	49
Tabla 3. Frecuencia de exposición en el método William T. Fine (Rubio, 2004) ..	49
Tabla 4. Identificación de los riesgos	57
Tabla 5. Escala de probabilidad del riesgo.....	57
Tabla 6. Grado de severidad de las consecuencias.....	58
Tabla 7. Cálculo del grado de riesgo.....	58
Tabla 8. Tipo grado de riesgo.....	59
Tabla 9. Asignación del grado de riesgo	59
Tabla 10. Matriz de riesgo	60
Tabla 11. Vulnerabilidades FortiGuard.....	98