



**INSTITUTO DE EDUCACIÓN SUPERIOR PRIVADO
IDAT**

**PROGRAMA DE ESTUDIOS EN ADMINISTRACIÓN
DE REDES Y COMUNICACIONES DE DATOS**

**DISEÑO DE UN SISTEMA DE SEGURIDAD REDUNDANTE
PARA UNA ENTIDAD BANCARIA, 2025**

**Trabajo de aplicación profesional para obtener el título Profesional Técnico
en Redes y Comunicaciones de Datos**

JULIO CESAR SAEZ MAXIMILIANO

(0009-0009-3453-5410)

JESUS YARET VILLARROEL CERVANTES

(0009-0002-2614-9156)

Lima – Perú

2025

Dedicatoria

A mis padres, por su excelente apoyo, su guía constante y por haberme inculcado valores que han sido fundamentales en mi formación personal y profesional.

Índice General

Resumen Ejecutivo	10
Introducción	11
Capítulo I: Aspectos Generales	13
Nombre del Proyecto	13
Tipo de Proyecto.....	13
Equipo del Proyecto	13
Planteamiento del Problema	14
Objetivos.....	14
<i>Objetivo General</i>	<i>14</i>
<i>Objetivos Específicos.....</i>	<i>14</i>
Antecedentes.....	15
Descripción del Proyecto.....	15
Justificación del Proyecto	16
Interesados del Proyecto	16
Alcance del Proyecto y Productos Esperados.....	16
Capítulo II: Estudio de Mercado	18
Selección de Dispositivos de Red.....	18
Estudio Sobre el Mercado de Dispositivos de Seguridad.....	19
Comparación de Fabricantes Firewall	22
Selección de Firewall.....	23
Comparación de Fabricantes de Switch.....	24
Selección de Switch de Distribución	25
Comparación de Fabricantes de Switch.....	26
Selección de Switch de Acceso	27
Comparación de Licencias para el Firewall	28
Selección de Licencia del Firewall.....	29
Comparación de Softwares para el Switch.....	30
Selección de Software del Switch	31
Capítulo III: Estudio Técnico	32
Marco Teórico	32

Arquitectura de Red.....	33
<i>Modelo Jerárquico</i>	33
<i>Infraestructura Tecnológica</i>	34
Seguridad.....	35
<i>Principios Fundamentales</i>	35
<i>Medidas de Protección</i>	36
Redundancia y Rendimiento.....	38
<i>Propósito y Técnicas</i>	38
Protocolos y Comunicación.....	40
<i>Protocolos clave y Modelos de Referencia</i>	40
Tipos de Redes	41
Tendencias Tecnológicas.....	42
Metodologías	43
<i>Preparar</i>	43
<i>Planificar</i>	43
<i>Diseñar</i>	44
<i>Implementar</i>	44
<i>Operar</i>	44
<i>Optimizar</i>	44
Desarrollo del Trabajo	45
<i>Descripción de la Infraestructura Actual</i>	45
<i>Análisis de la Infraestructura Actual</i>	47
<i>Criterios de Diseño de la Topología de la Red Propuesta</i>	49
<i>Descripción de la Infraestructura Propuesta</i>	50
<i>Segmentación de la Red Propuesta</i>	51
Configuración de Equipamiento de la Red Propuesta.....	54
<i>Configuraciones del Router RB1(CRS309)</i>	54
<i>Configuraciones del Router RB2(CRS309)</i>	59
<i>Configuraciones del Firewall FORT1(3000F)</i>	63
<i>Configuraciones del Firewall FORT2(3000F)</i>	71
<i>Configuraciones de Gestión Unificada de Amenazas (UTM)</i>	78
<i>Configuraciones del Switch SW-DISTRI1(C9500)</i>	82
<i>Configuraciones del Switch SW-DISTRI2(C9500)</i>	84
<i>Configuraciones del Switch SW-ACCESO1(C9200L)</i>	86
<i>Configuraciones del Switch SW-ACCESO2(C9200L)</i>	87
<i>Configuraciones de Calidad de Servicio de VOIP</i>	88
Pruebas Operativas del Diseño Conceptual.....	89
<i>Prueba de Conectividad a Internet en el Router RB1</i>	89
<i>Prueba de Conectividad a Internet en el Router RB2</i>	91
<i>Prueba de Conectividad a Internet al Fallar un Router</i>	93

<i>Prueba de Funcionamiento del Protocolo VRRP1</i>	<i>95</i>
<i>Prueba de Redundancia al Fallar un Switch.....</i>	<i>97</i>
<i>Prueba de Redundancia al Fallar el Router y el Switch</i>	<i>99</i>
<i>Prueba de Equilibrio de Carga en los Firewalls.....</i>	<i>101</i>
<i>Prueba Cambio de Rol en los Firewalls FORT1 y FORT2</i>	<i>104</i>
<i>Prueba del Protocolo LACP en el Firewall FORT1.....</i>	<i>105</i>
<i>Prueba del Protocolo LACP en el Firewall FORT1.....</i>	<i>107</i>
<i>Prueba de Llamadas VOIP</i>	<i>109</i>
<i>Prueba de Políticas de Seguridad en el Firewall FORT1</i>	<i>110</i>
<i>Prueba de Seguridad de Gestión Unificada de Amenazas</i>	<i>112</i>
<i>Prueba de Calidad de Servicio de VOIP</i>	<i>115</i>
Análisis de Resultados.....	117
Capítulo IV: Estudios de Costos	118
Costos de Equipamiento	118
Costos de Implementación	119
Costos de Contratación de Servicio de Internet.....	120
Resumen del Costo Total de Equipamiento e Implementación.....	121
Conclusiones y Recomendaciones	122
Referencias Bibliográficas	127
Anexos.....	129

Índice de Tablas

Tabla 1	<i>Integrantes del Proyecto</i>	13
Tabla 2	<i>Resumen de estudio del mercado de firewall</i>	21
Tabla 3	<i>Comparación de fabricantes Firewall</i>	22
Tabla 4	<i>Comparación de fabricantes de Switches capa 3</i>	24
Tabla 5	<i>Comparación de fabricantes de Switches capa 2</i>	26
Tabla 6	<i>Comparación de Licencias de Firewalls</i>	28
Tabla 7	<i>Características de las Licencias en el Mercado</i>	30
Tabla 8	<i>Capas del modelo jerárquico</i>	33
Tabla 9	<i>Dispositivos de red</i>	34
Tabla 10	<i>Confidencialidad, integridad y disponibilidad</i>	35
Tabla 11	<i>Medidas de protección mediante protocolos</i>	36
Tabla 12	<i>Protocolos de redundancia y rendimiento</i>	38
Tabla 13	<i>Protocolos y modelos</i>	40
Tabla 14	<i>Redes según su alcance geográfico</i>	41
Tabla 15	<i>Tendencias tecnológicas para una entidad bancaria</i>	42
Tabla 16	<i>Plan de Direccionamiento IP</i>	46
Tabla 17	<i>Resumen de Características de la Red Actual</i>	48
Tabla 18	<i>Resumen de la Infraestructura de la Red Propuesta</i>	50
Tabla 19	<i>Segmentación de Red IP</i>	51
Tabla 20	<i>Segmentación de Red IP por cada VLAN</i>	52
Tabla 21	<i>Costos de Equipamiento</i>	118
Tabla 22	<i>Costos de Implementación</i>	119
Tabla 23	<i>Costos de Servicio de Internet</i>	120
Tabla 24	<i>Resumen de Costo Total de la Implementación</i>	121

Índice de Figuras

Figura 1 <i>Crecimiento de nivel de ciberseguridad en los bancos a nivel mundial</i>	18
Figura 2 <i>Bancos con mayor nivel de ciberseguridad y redundancia</i>	19
Figura 3 <i>Crecimiento del mercado de ciberseguridad por región</i>	20
Figura 4 <i>FortiGate 3000F</i>	23
Figura 5 <i>Cisco C9500-24Y4C</i>	25
Figura 6 <i>Switch Cisco C9200L-48PB</i>	27
Figura 7 <i>Licencia UTM Completa</i>	29
Figura 8 <i>DNA Advantage</i>	31
Figura 9 <i>Mapa conceptual del trabajo de aplicación</i>	32
Figura 10 <i>Núcleo, distribución y acceso</i>	33
Figura 11 <i>Dispositivos para la red propuesta</i>	34
Figura 12 <i>Cifrado, protección y redundancia</i>	35
Figura 13 <i>VPN de sitio a sitio</i>	37
Figura 14 <i>VLANs</i>	37
Figura 15 <i>HSRP, VRRP, LACP, STP y QoS</i>	39
Figura 16 <i>Protocolos y modelos</i>	40
Figura 17 <i>Redes LAN, MAN y WAN</i>	41
Figura 18 <i>Tendencias Tecnológicas</i>	42
Figura 19 <i>Metodología PPDIOO Cisco</i>	43
Figura 20 <i>Infraestructura actual de la red</i>	47
Figura 21 <i>Topología de la Red propuesta</i>	53
Figura 22 <i>Configuración del Cliente DHCP en el Router RB1</i>	54
Figura 23 <i>Regla NAT para Salida a Internet por WAN1 y WAN2</i>	55
Figura 24 <i>Conmutación por Falla entre WAN1 y WAN2</i>	55
Figura 25 <i>Asignación de IP para el Protocolo VRRP</i>	56
Figura 26 <i>Configuración de Interfaces VRRP en el Router RB1</i>	57
Figura 27 <i>Configuración del Servidor DHCP para VRRP1 y VRRP2</i>	57
Figura 28 <i>Configuración del Script para Monitoreo en el Router Maestro RB1</i>	58
Figura 29 <i>Configuración del Cliente DHCP en el Router RB2</i>	59
Figura 30 <i>Regla NAT para Salida a Internet por WAN1 y WAN2</i>	60
Figura 31 <i>Conmutación por Falla entre WAN1 y WAN2</i>	60
Figura 32 <i>Asignación de IP para el Protocolo VRRP</i>	61
Figura 33 <i>Configuración de Interfaces VRRP en el Router RB2</i>	62
Figura 34 <i>Configuración del Servidor DHCP para VRRP1 y VRRP2</i>	62
Figura 35 <i>Configuración de Monitor de Enlace en el Firewall FORTI</i>	63
Figura 36 <i>Configuración de la Interfaz WAN1 en el Firewall FORTI</i>	64
Figura 37 <i>Configuración de la Interfaz WAN2 del Firewall FORTI</i>	65
Figura 38 <i>Configuración de Rutas Estáticas en el Firewall FORTI</i>	66
Figura 39 <i>Configuración de la Interfaz Agregada (LACP) en el Firewall FORTI</i>	67
Figura 40 <i>Creación de VLANs en el Firewall FORTI</i>	67

Figura 41 Configuración de Políticas en el Firewall FORT1	68
Figura 42 Configuración de Interfaces Heartbeat en el Firewall FORT1	69
Figura 43 Configuración del Clúster de Alta Disponibilidad en el Firewall FORT1	69
Figura 44 Configuración del Clúster de Alta Disponibilidad en el Firewall FORT2	71
Figura 45 Estado del Clúster de Alta disponibilidad en los Firewalls FORT1-FORT2	72
Figura 46 Configuración para Acceso Individual en el Firewall FORT1	73
Figura 47 Configuración de IP para el Acceso Individual al Firewall FORT1	74
Figura 48 Asignación de la Zona DMZ para Servidores	75
Figura 49 Configuración de Conectividad a la Zona DMZ por Internet	76
Figura 50 Configuración de Conectividad a Internet por medio de DMZ	77
Figura 51 Configuración de Antivirus y Antimalware	78
Figura 52 Configuración de Filtro de Web	79
Figura 53 Configuración de Sistema de Prevención de Intrusos	80
Figura 54 Configuración de IP para Acceso Individual al Firewall FORT2	81
Figura 55 Configuración de LACP en el Switch SW-DISTR1I	82
Figura 56 Creación de VLANs en el Switch SW-DISTR1I	83
Figura 57 Configuración de Interfaces Troncales en el Switch SW-DISTR1I	83
Figura 58 Configuración de LACP en el Switch SW-DISTR12	84
Figura 59 Creación de VLANs en el Switch SW-DISTR12	85
Figura 60 Configuración de Interfaces Troncales en el Switch SW-DISTR12	85
Figura 61 Configuraciones de Interfaces Troncales en el Switch SW-ACCESO1	86
Figura 62 Configuraciones de Interfaces en el Switch SW-ACCESO2	87
Figura 63 Calidad de Servicio VOIP	88
Figura 64 Conectividad a Internet al Apagar la Interfaz ether2 del Router RB1	89
Figura 65 Redirección de Tráfico al Encender la Interfaz ether2 del Router RB1	90
Figura 66 Conectividad a Internet al Apagar la Interfaz ether3 del Router RB2	91
Figura 67 Redirección de Tráfico al Reactivar la Interfaz ether3 del Router RB2	92
Figura 68 Apagado del Router RB1	93
Figura 69 Conectividad a Internet al Apagar el Router RB1	94
Figura 70 Cambio de Rol en el Router RB2	95
Figura 71 Retoma de Rol en el Router RB1	96
Figura 72 Conectividad al Apagar el Switch SW-VRRP-IZQUIERDA	97
Figura 73 Conectividad por medio del protocolo VRRP2	98
Figura 74 Apagado del Router RB1 y el Switch SW-VRRP-IZQUIERDA	99
Figura 75 Continuidad de Servicio al Apagar la Red Principal	100
Figura 76 Alta Disponibilidad y Balanceo de Carga	101
Figura 77 Apagado del Firewall FORT1	102
Figura 78 Alta Disponibilidad al Fallar el Firewall FORT1	103
Figura 79 Cambio de Rol en los Firewalls	104
Figura 80 Apagado de la Interfaz Física del Switch SW-DISTR1I	105
Figura 81 Salida a Internet al Apagar la Interface LACP	106
Figura 82 Apagado del Interface Port-Channel 1 en el Switch SW-DISTR1I	107
Figura 83 Redundancia del Port-Channel en el Firewall FORT2	108

Figura 84 <i>Llamada entre VLANs</i>	109
Figura 85 <i>Acceso Controlado de VLAN 5 a VLAN 15</i>	110
Figura 86 <i>Acceso Controlado de VLAN 15 a VLAN 5</i>	111
Figura 87 <i>Prueba de Filtrado Web</i>	112
Figura 88 <i>Prueba de Operación del Antivirus</i>	113
Figura 89 <i>Prueba de Prevención de Intrusos (IPS)</i>	114
Figura 90 <i>Prueba Calidad de Servicio VOIP</i>	115
Figura 91 <i>Prueba de Captura de Etiqueta DSCP con Wireshark</i>	116

Resumen Ejecutivo

El presente proyecto tuvo como objetivo fortalecer la infraestructura de ciberseguridad de una entidad bancaria mediante la implementación de soluciones tecnológicas avanzadas. La creciente sofisticación de las amenazas cibernéticas y el incremento en la exposición digital exigieron una estrategia robusta que garantizara la confidencialidad, integridad y disponibilidad de los datos sensibles, así como la continuidad de los servicios bancarios.

La propuesta contempló la incorporación de un firewall de próxima generación para proteger la red perimetral del banco contra accesos no autorizados y ataques cibernéticos. Además, se integraron herramientas para el análisis, monitoreo de tráfico, eventos de seguridad, sistemas de gestión centralizada de dispositivos y soluciones para la protección de puntos finales. Estas tecnologías se combinaron para ofrecer una visibilidad integral y una respuesta automatizada ante incidentes de seguridad.

Entre los principales beneficios obtenidos se destacaron la protección contra amenazas cibernéticas, la reducción significativa de riesgos, la mejora en los tiempos de respuesta ante incidentes, el cumplimiento de normativas de seguridad y la optimización operativa. Asimismo, se incluyó la capacitación del personal técnico, lo cual permitió garantizar la sostenibilidad del sistema implementado.

Este proyecto representó una inversión estratégica en la protección de los activos digitales del banco, asegurando un entorno confiable para la operación actual y su escalabilidad futura. También se logró fortalecer la confianza de los clientes en los servicios ofrecidos por la entidad.

Palabras clave: Firewall de próxima generación; red perimetral; visibilidad integral; escalabilidad; confidencialidad; integridad y disponibilidad.