



SecNet : Gestión Integral de ciberseguridad para Routers Mikrotik

Alumno: Fernando Andrés Corvalan

Profesores: Silvia Victoria Poncio

Audoglio Pablo Andres

**Plan de Trabajo Final de Carrera para obtener el título de:
Licenciado en Gestión de Tecnología informática**

Año 2024

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Índice

A. Proyecto de base tecnológica en un entorno distribuido habilitado para la web.	7
Resumen Ejecutivo:	7
B. Plan de Negocios	9
1. Descripción General	9
1.1 Descripción básica del negocio	9
Idea de negocio:	9
Componentes principales:	9
Justificación:	10
Tipo de E-Business:	10
Modalidad de E-Commerce:	10
1.2 Situación actual del negocio	11
1.3 ¿Qué hace único a su negocio?	12
1.4 Describa los factores principales que usted considera harán exitoso su proyecto	13
1.5 Estrategia: Definir Misión, Visión y Propósito Estratégico	14
Misión:	14
Visión:	14
Propósito Estratégico:	14
1.6 Identificación de la oportunidad de negocio	14
1.7 Capacidades centrales	15
1.8 Propuesta de valor para el cliente	16
1.9 Valores nucleares de la organización	17
1.10 Enfoque e iniciativas estratégicas	18
1.11 Áreas claves de resultados: identificar y justificar	19
Adquisición de clientes:	20
Retención de clientes:	20
Rentabilidad:	20
Reputación y reconocimiento de marca:	20
Justificación:	20
1.12 Ingreso al sector: estrategias de inserción	21
• Rivalidad entre competidores:	21
• Poder de negociación de los compradores:	21
• Poder de negociación de los proveedores:	21
• Amenaza de nuevos competidores:	21
• Amenaza de productos sustitutos:	22
Estrategias genéricas de Porter y Kotler:	22
2. Análisis estratégico	23

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

2.1 Análisis de Contexto	23
2.1.1 Descripción del escenario local	23
2.1.2 Factores económicos	23
2.1.3 Factores Políticos	24
2.1.4 Factores Tecnológicos	26
2.1.5 Descripción del escenario: escenario-meta	26
2.1.6 Análisis sectorial	28
2.2 Análisis de la Competencia	29
2.2.1 Principales competidores directos	29
FortiWeb de Fortinet:	29
Plataforma Lumu:	30
2.2.2 Análisis de cadena de valor	30
Actividades Primarias:	31
Actividades de Soporte:	32
Ventajas competitivas de SecNet :	32
Desafíos potenciales:	32
2.2.3 Definición de Factores Críticos de Éxito (FCE)	32
Experiencia y conocimiento en ciberseguridad:	32
Enfoque proactivo en la seguridad:	33
Servicio al cliente excepcional:	33
Precios competitivos:	33
Tecnología robusta y escalable:	33
Cumplimiento de normativas:	33
2.2.4 Fortalezas y debilidades del negocio :	33
3. Análisis FODA de SecNet	35
Matriz FODA de SecNet	37
Estrategias derivadas del FODA de SecNet :	37
4 Segmentación	39
4.1 Segmentación de consumidores y/o Negocios	39
Criterios de Segmentación por sector:	39
4.2 Identificación de grupos diferenciados de consumidores	45
4.3 ¿Quiénes son los potenciales usuarios/ compradores del negocio?	46
Características:	46
Necesidades y motivaciones:	47
Comportamiento de compra:	47
4.4 Pautas de comportamiento esperado de cada segmento	47
PyMEs con necesidades básicas de ciberseguridad:	48
PyMEs con necesidades avanzadas de ciberseguridad:	48

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Consideraciones adicionales:	48
5 Plan de Acción	49
5.1 Objetivos Generales	49
5.2 Programas específicos de acción:	50
5.2.1 Programas específicos de sector Administración:	50
5.2.1.1 Administración de Compras:	50
5.2.1.2 Administración de Ventas:	50
5.2.1.3 Administración de Cobranzas:	51
5.2.1.4 Administración de Pagos:	51
5.2.1.5 Administración de Contabilidad:	51
5.2.2 Programas específicos de sector Tecnología:	51
5.2.2.1 Adquisición de Hardware:	51
5.2.2.2 Estrategias para Telecomunicaciones:	52
5.2.2.3 Estrategias para adquisición de Software:	52
5.2.3 Programas específicos de sector Producción:	53
5.2.3.1 Estrategias para Análisis de requerimientos:	53
5.2.3.2 Estrategias para Desarrollo de productos:	53
5.2.3.3 Estrategias para Pruebas de Software:	53
5.2.3.4 Estrategias para Implementación:	53
5.2.4 Programas específicos de sector Marketing:	54
5.2.4.1 Estrategias para Producto:	54
5.2.4.2 Estrategias para Precio:	54
5.2.4.3 Estrategias para Plaza:	54
5.2.4.4 Estrategias para Promoción:	54
5.2.5 Programas específicos de sector Comercialización:	55
5.2.5.1 Estrategia de Ventas:	55
5.2.5.2 Estrategia de post-venta:	55
5.2.5.3 Estrategia de logística de salida:	55
5.3 Análisis de riesgos:	56
5.4 Gantt	57
6 Plan de Marketing	58
6.1 Objetivos de Marketing	58
Objetivos SMART:	58
Justificación de los objetivos:	58
6.2 Resultados esperados en materia de cobertura y participación	58
6.3 Metas de Posicionamiento	60
6.4 Producto. Estrategia de Producto	60
6.4.1 Descripción del producto SecNet	60

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

6.4.2 ¿Es un producto/servicio durable, estacional?	61
6.4.3 ¿Cuáles son las características de su producto/ servicio que usted considera influyen sobre la decisión de compra?	62
Enfoque proactivo en la seguridad:	62
Solución integral:	62
Servicio personalizado:	62
Precios competitivos:	62
Experiencia y confianza:	63
6.4.4 ¿Existen estudios que respalden sus hipótesis?	63
Estudios de mercado:	63
Evidencia de la industria:	63
Análisis de la competencia:	64
Testimonios de clientes:	64
Conclusión:	64
6.5 Precios. Estrategia de Precios	64
6.5.1 Condicionantes del precio	64
6.5.2 Estrategia de precio	65
Precios competitivos:	66
Propuesta de valor diferenciada:	66
Enfoque en el cliente:	66
Dato adicional:	66
6.6 CIM Comunicaciones integradas de marketing	67
6.6.1 Descripción de la planificación estratégica de las acciones de comunicación	67
Público Objetivo:	67
Canales de comunicación:	67
Mensajes clave:	68
Presupuesto:	68
Seguimiento y evaluación:	68
Programa de referidos:	68
Contacto constante con el cliente:	69
Limitación en las posibilidades de expansión:	69
6.6.2 Diseño del Sitio web	69
6.7 Distribución	71
6.7.1 Factores condicionantes de la distribución - Principales canales	71
6.7.2 Estrategia de distribución	72
6.7.3 Canales (tipo y nivel)	72
6.7.4 Análisis de localización de puntos de venta propios	73
Enfoque en la presencia online:	73

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Oficina para atención de clientes corporativos:	73
Ventajas de la presencia online:	73
Ventajas de la oficina para atención de clientes:	73
6.7.5 Opciones de asociación	74
Mayoristas de equipos Mikrotik:	74
Cámaras empresariales de ISPs:	74
Empresas de consultoría en ciberseguridad:	75
7. Operaciones	76
7.1 Organización de la empresa	76
Principales departamentos:	76
7.2 Grupo fundador	76
7.3 Composición del staff gerencial y perfil de los ejecutivos claves.	76
7.4 Estructura prevista al lanzamiento y evolución	77
7.5 Filosofía y sistema de trabajo	77
7.6 Requerimientos en materia de RRHH	78
8 PLAN FINANCIERO-ECONÓMICO	79
8.1 Modelo de Ingresos:	79
8.2 Modelo de Egresos:	79
8.3 Modelo de Inversión:	79
8.4 Amortizaciones y Depreciaciones:	80
8.5 Impuestos: Impuesto a las ganancias	80
8.6 Impuestos a los Ingresos Brutos:	81
8.7 Remuneraciones y cargas sociales:	81
8.8 Presupuesto Financiero: (con Imp. ganancias del 35%):	81
8.9 Evaluación de la Inversión:	82
8.10 Escenarios de Riesgo:	83
Escenario Probable (Base): Utilizaremos los datos anteriores.	83
Escenario Optimista (Ventas +25%, Costos -15%):	83
Escenario Pesimista (Ventas -25%, Costos +15%):	83
Comparativas	84
Análisis de los escenarios:	84
8.11 Plan de Contingencia	84
Disparadores:	85
Acciones:	85
Monitoreo y Evaluación:	86
Objetivo:	86
8.12 Plan de Salida	86
Adquisición por parte de una empresa de ciberseguridad:	86

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Fusión con una empresa complementaria:	87
Venta de la licencia del software:	87
Continuar como producto independiente dentro de la consultora (Escenario de bajo crecimiento):	87
Criterios de decisión:	87
9. FACTIBILIDADES	88
9.1 Técnica	88
9.2 Comercial	90
9.3 Administrativa	91
9.4 Legal	91
C. Aspectos Descriptivos de la Solución Tecnológica	92
10. Descripción de la Solución Tecnológica	92
10.1.1 Propuesta de valor del proyecto para la empresa	92
10.1.2 Hitos importantes del proyecto	93
10.2 Visión del producto	94
10.2.1 Historias de Usuario	94
10.3 Alcance del desarrollo	95
10.4 Descripción del entorno del sistema	96
10.4.1 Requisitos de Entorno	97
10.5 Descripción del Producto	98
10.5.1 Componentes principales:	100
10.5.2 Generación de Listas en SecNet:	101
10.5.3 ¿Qué es OTX?	103
10.5.4 Otras fuentes de datos	105
10.5.5 Diagrama de secuencia	105
10.5.6 Interface de usuario	105
D. Anexos	109
11 Contenido	109
11.1 Paper CONAISI	109
Estrategias Metodológicas para la Modernización de Centros de Datos Gubernamentales	111

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

A. Proyecto de base tecnológica en un entorno distribuido habilitado para la web.

SecNet : Gestión Integral de ciberseguridad para Routers Mikrotik

Resumen Ejecutivo:

SecNet es una solución innovadora de seguridad gestionada (MSSP) desarrollada por Madrygal, consultora especializada en ciberseguridad para PyMEs. SecNet ofrece protección integral y personalizada contra amenazas cibernéticas, utilizando tecnologías de código abierto como Wazuh, filtrado DNS e IP, monitoreo y gestión remota de firewalls Mikrotik, en un entorno distribuido, habilitado para la web y accesible a través de un modelo SaaS.

SecNet se distingue por su enfoque proactivo, que va más allá de la simple reacción a incidentes. Combina la detección y respuesta a amenazas en tiempo real con la prevención mediante el análisis de inteligencia de amenazas, filtrado DNS e IP, y la experiencia del equipo Madrygal en Wazuh como solución XDR. Esta combinación proporciona una protección multicapa robusta y confiable, adaptada a las necesidades y presupuesto de cada cliente.

Ventajas Clave para el Cliente:

- **Detección y respuesta a amenazas en tiempo real:** Identificación y neutralización proactiva de amenazas.
- **Bloqueo de malware y phishing:** Filtrado DNS e IP para prevenir el acceso a sitios y direcciones maliciosas.
- **Visibilidad y control centralizado:** Monitoreo de seguridad integral desde una única consola.
- **Implementación y gestión simplificadas:** Modelo SaaS que elimina la necesidad de inversión en infraestructura y facilita la gestión.
- **Soporte técnico especializado:** Asistencia experta del equipo Madrygal para una respuesta rápida y eficiente.
- **Ahorro de costos:** Solución accesible que libera recursos internos para enfocarse en el core del negocio.

El mercado de ciberseguridad para PyMEs en Argentina está en plena expansión, impulsado por la creciente digitalización y la sofisticación de las amenazas. La baja

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 7 de 120
---	--	---------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

adopción actual de soluciones MSSP en este segmento presenta una oportunidad única para SecNet .

SecNet se ofrece como un servicio SaaS (Software as a Service) bajo un modelo B2B, brindando planes de suscripción personalizados y flexibles que se adaptan a las necesidades y presupuestos de cada empresa. El costo de licencia básica por dispositivo se estima en u\$s 25 dólares mensuales.

La proyecciones financieras a 6 semestres son las siguientes:

- Inversión inicial: \$6,000 Dol
- VAN (Valor Actual Neto): \$174.117 Dol
- TIR (Tasa Interna de Retorno): 160%
- Payback: < 13 meses

Madrygal cuenta con un equipo experimentado en ciberseguridad, con certificaciones en Wazuh y un historial comprobado en la implementación de soluciones de seguridad para PyMEs. Disponen de amplia experiencia técnica y de gestión en el ámbito privado y gubernamental, sobre infraestructura civil y militar.

SecNet está listo para revolucionar el mercado de la ciberseguridad para PyMEs usuarias de dispositivos Mikrotik. Únete a nosotros y ayudemos a las empresas argentinas a proteger sus activos digitales. Contáctanos hoy mismo

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

B. Plan de Negocios

1. Descripción General

1.1 Descripción básica del negocio

Idea de negocio:

El proyecto consiste en el desarrollo y despliegue de **SecNet**, un servicio de seguridad gestionada (**MSSP**) diseñado exclusivamente para empresas (**B2B**). SecNet brinda una solución integral contra amenazas cibernéticas, combinando la potencia del SIEM de código abierto **Wazuh** con herramientas adicionales de seguridad, ofreciendo una protección robusta y multicapa.

Componentes principales:

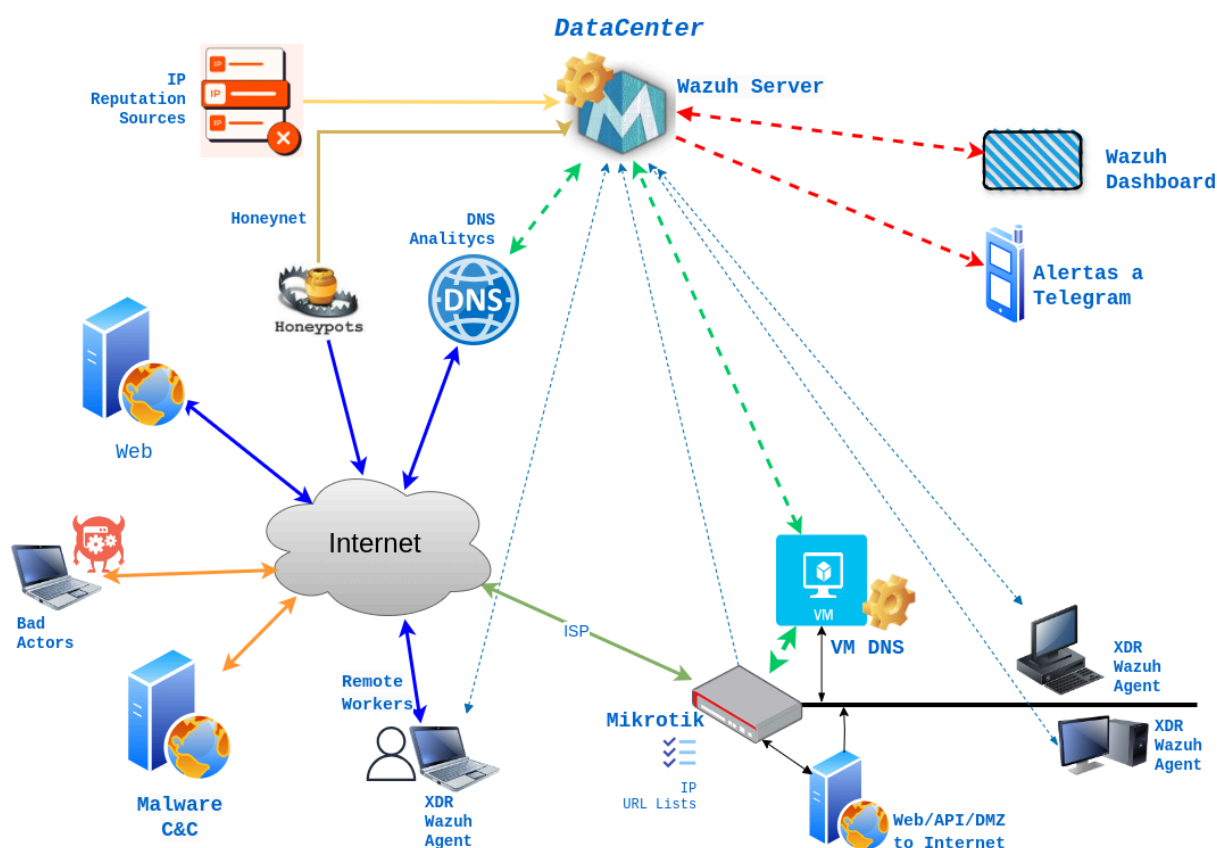
- **Wazuh SIEM:** El corazón de SecNet, recolecta y analiza eventos de seguridad de diversas fuentes, incluyendo firewalls Mikrotik, eventos e información provista por agentes Wazuh en los equipos de la red, listas de reputación IP y URL, y honeypots. Esta información centralizada permite detectar y responder a amenazas de manera proactiva.
- **Filtrado DNS con DNSMasq:** Una máquina virtual con DNSMasq, se encarga de filtrar las consultas DNS de la red corporativa utilizando listas de reputación de dominios (URLs), bloqueando el acceso a sitios web maliciosos o inapropiados y generando alertas al agente wazuh.
- **Filtrado IP en Mikrotik:** SecNet utiliza listas de reputación IP desplegadas directamente en los firewalls Mikrotik para bloquear el tráfico desde y hacia direcciones IP conocidas como maliciosas, agregando una capa adicional de seguridad perimetral.
- **Honeypots:** Desplegados estratégicamente en internet, los honeypots simulan ser objetivos atractivos para los atacantes. Al atraerlos a estos entornos controlados, SecNet puede analizar sus técnicas, dirección de origen, obtener información sobre nuevas amenazas y fortalecer las defensas de la organización de forma proactiva. Cada equipo enrolado en el sistema se convierte automáticamente mediante un grupo de reglas, en un honeypot.

 SecNet Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 9 de 120
---	--	---------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Justificación:

En la actualidad, las empresas enfrentan un panorama de amenazas cibernéticas en constante evolución. Las soluciones tradicionales de seguridad, a menudo fragmentadas, no son suficientes para hacer frente a la sofisticación y la persistencia de los ataques. SecNet surge como respuesta a esta problemática ofreciendo una solución integral, gestionada y adaptable a las necesidades específicas de cada empresa.



Tipo de E-Business:

SecNet se enfoca exclusivamente en el modelo de negocio **B2B (Business to Business)**, ofreciendo sus servicios a empresas de todos los tamaños y sectores que busquen fortalecer su seguridad informática.

Modalidad de E-Commerce:

La modalidad de comercialización es **B2B** con un modelo **SaaS (Software as a Service)**.

 SecNet Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 10 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- **B2B:** Se ofrecen planes de servicio personalizados a empresas que incluyen la consultoría, implementación, configuración, gestión y monitoreo 24/7 de SecNet .
- **SaaS:** La plataforma SecNet se aloja en la nube, permitiendo a los clientes acceder a su consola de gestión y a los reportes desde cualquier lugar con conexión a internet. Este modelo elimina la necesidad de invertir en infraestructura propia y facilita la escalabilidad del servicio.

SecNet es un servicio de seguridad gestionada (MSSP) diseñado para empresas (B2B) que integra un SIEM, filtrado DNS e IP, e inteligencia de amenazas mediante honeypots. Su enfoque proactivo y su modelo SaaS lo convierten en una solución completa y adaptable a las necesidades de seguridad del mundo empresarial actual.

1.2 Situación actual del negocio

El mercado de la ciberseguridad experimenta una expansión constante, impulsada por la creciente digitalización de las empresas y la sofisticación de las amenazas. Sin embargo, esta expansión se concentra principalmente en soluciones comerciales orientadas al mercado corporativo, que a menudo exceden el presupuesto de las PyMEs. Este contexto presenta una oportunidad para SecNet, que ofrece una solución accesible y adaptada a las necesidades de este segmento.

Un análisis del panorama actual de la ciberseguridad revela las siguientes soluciones relacionadas:

Soluciones SIEM Open Source: Wazuh¹ se destaca como una solución robusta y flexible, ofreciendo también servicios de alojamiento en la nube. Su naturaleza de código abierto permite la personalización y la adaptación a diferentes entornos, pero requiere un mayor nivel de expertise técnica para su implementación y gestión.

Lumu²: Esta plataforma comercial de Detección y Respuesta Continua (CDR) ofrece un enfoque proactivo en la identificación de amenazas, utilizando información de diversas fuentes. Si bien su implementación en la nube facilita la gestión, el costo de las licencias puede ser una barrera para las PyMEs, y su enfoque en la detección no siempre incluye servicios de prevención esenciales como el filtrado DNS e IP.

Fortinet (FortiWeb)³: Este Firewall de Aplicaciones Web (WAF) ofrece una amplia protección contra amenazas web, pero su alto costo de licencias y la complejidad de su gestión lo hacen menos accesible para las PyMEs con recursos limitados. Además, su

¹ <https://wazuh.com/>

² <https://lumu.io/>

³ <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiWeb.pdf>

 SecNeT Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 11 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

enfoque principal es reactivo, centrándose en la respuesta a incidentes más que en la prevención proactiva.

Axiom Shield⁴ para MikroTik⁵: Esta solución se centra en el filtrado basado en listas y análisis de capa 7 para dispositivos MikroTik, pero su compatibilidad limitada a la gama alta de routers (CCR Cloud Core Router) restringe su alcance en el mercado de las PyMEs.

SecNet se encuentra en fase de desarrollo como un producto que complementa el servicio principal de Madrygal Ciberseguridad. Se presenta como una solución de seguridad gestionada (MSSP) innovadora, diseñada específicamente para PyMEs que utilizan routers MikroTik. A diferencia de las soluciones existentes, SecNet combina la potencia de Wazuh con herramientas adicionales de seguridad, ofreciendo una protección integral, proactiva y accesible. Su modelo de negocio SaaS facilita la implementación y reduce la necesidad de inversión en infraestructura por parte del cliente. La experiencia de Madrygal en consultoría de seguridad para PyMEs, y su especialización en Wazuh, le otorgan una ventaja competitiva en este mercado.

1.3 ¿Qué hace único a su negocio?

A diferencia de otros servicios de seguridad gestionada, SecNet se destaca por:

Enfoque en la protección proactiva: SecNet no se limita a reaccionar ante incidentes, sino que busca anticiparse a ellos mediante el uso de honeypots y el análisis de inteligencia de amenazas.

Sistema de filtrado DNS e IP integrado: La combinación de Wazuh con DNSMasq y el filtrado IP en Mikrotik ofrece una protección multi capa que bloquea el acceso a sitios web y direcciones IP maliciosas, minimizando el riesgo de infección por malware y otras amenazas. Si la empresa tiene publicados servicios a Internet, el sistema también actúa protegiendo las comunicaciones entrantes a la infraestructura.

Monitoreo y gestión centralizada: La plataforma Wazuh SIEM permite monitorear la seguridad de toda la infraestructura desde una única consola, facilitando la detección de amenazas y la gestión de incidentes.

⁴ <https://axiomcyber.com/shield/>

⁵ <https://mikrotik.com/>

	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Adaptabilidad a las necesidades del cliente: SecNet se implementa y configura de acuerdo a las necesidades específicas de cada empresa, ofreciendo un servicio personalizado.

Experiencia en Wazuh: Madrygal cuenta con un equipo de ingenieros certificados en Wazuh, lo que garantiza un alto nivel de expertise en la implementación y gestión del SIEM.

Precios competitivos: Al basarse en software de código abierto, SecNet ofrece una solución de seguridad gestionada a un precio más accesible que las soluciones propietarias.

SecNet brinda a las empresas una protección proactiva, multicapa y personalizada contra amenazas cibernéticas, respaldada por la experiencia de Madrygal en Wazuh y a un precio competitivo para el mercado de pymes.

1.4 Describa los factores principales que usted considera harán exitoso su proyecto

Consideramos que los siguientes factores son claves para el éxito de SecNet :

Experiencia y especialización en ciberseguridad: La sólida experiencia de Madrygal en consultoría de seguridad para PyMEs, particularmente en la implementación y gestión de Wazuh, le otorga un profundo conocimiento de las necesidades del mercado y las mejores prácticas de la industria.

Propuesta de valor única: La combinación de Wazuh con filtrado DNS e IP sobre equipos Mikrotik, y el análisis de inteligencia de amenazas mediante honeypots, ofrece una solución integral y proactiva que lo diferencia de la competencia.

Enfoque en las PyMEs: Al dirigir SecNet específicamente a las PyMEs, Madrygal se centra en un mercado con un alto potencial de crecimiento y una demanda creciente de soluciones de seguridad gestionada.

Modelo de negocio SaaS: La modalidad SaaS facilita el acceso a SecNet , eliminando la necesidad de inversión en infraestructura por parte de los clientes y permitiendo una rápida implementación y escalabilidad.

Precios competitivos: Al basarse en tecnologías de código abierto, SecNet se ofrece a un precio más accesible que las soluciones propietarias, lo que lo hace atractivo para las PyMEs con presupuestos limitados.

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 13 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Servicio al cliente personalizado: Madrygal tiene la capacidad de brindar un servicio al cliente personalizado, adaptando SecNet a las necesidades específicas de cada empresa y ofreciendo soporte técnico continuo.

1.5 Estrategia: Definir Misión, Visión y Propósito Estratégico

Misión:

Proteger proactivamente los activos digitales de las Pymes a través de un servicio de seguridad gestionada (MSSP) integral y personalizado, basado en tecnologías de código abierto y un enfoque centrado en el cliente.

Visión:

Ser el proveedor líder de seguridad gestionada (MSSP) para PyMEs en Argentina, reconocido por su innovación, experiencia en Wazuh y compromiso con la excelencia en el servicio.

Propósito Estratégico:

Empoderar a las PyMEs para que puedan enfocarse en su crecimiento y éxito, teniendo la confianza de que su seguridad informática está en manos de una empresa sólida y responsable.

1.6 Identificación de la oportunidad de negocio

La oportunidad de negocio identificada para SecNet surge de la convergencia de varios factores:

Crecimiento del mercado de ciberseguridad: El mercado de ciberseguridad en Argentina se encuentra en constante expansión, impulsado por la creciente digitalización de las empresas, la sofisticación de los ataques cibernéticos y la mayor conciencia sobre la importancia de la protección de datos.

Vulnerabilidad de las PyMEs: Las Pymes, que representan el 99% de las empresas del país, son especialmente vulnerables a los ataques cibernéticos debido a sus limitados recursos y a la falta de profesionales especializados en seguridad.

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 14 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Baja adopción de soluciones de seguridad gestionada: A pesar de la creciente necesidad, la adopción de servicios de seguridad gestionada (MSSP) en Argentina es aún baja, principalmente en el segmento de las PyMEs.

Demanda de soluciones personalizadas y accesibles: Las PyMEs buscan soluciones de ciberseguridad que se adapten a sus necesidades específicas y a sus presupuestos limitados. Prefieren soluciones fáciles de implementar y gestionar, que no requieran una gran inversión inicial.

SecNet busca aprovechar esta oportunidad de negocio al ofrecer:

- Un servicio de seguridad gestionada (MSSP) integral y proactivo, que combina la detección y respuesta a amenazas con el filtrado DNS e IP, y la inteligencia de amenazas.
- Un enfoque exclusivo en las PyMEs, con planes de servicio personalizados y accesibles.
- Una modalidad SaaS que facilita la implementación y reduce los costos para el cliente.
- Un equipo de expertos en Wazuh que garantiza un alto nivel de expertise en la configuración y gestión del SIEM.

De esta manera, SecNet se posiciona como una solución atractiva para las Pymes que buscan proteger sus activos digitales de forma eficiente y a un costo accesible.

1.7 Capacidades centrales

Madrygal posee las siguientes capacidades centrales que son relevantes para el éxito de su producto SecNet :

Experiencia en seguridad informática:

- El equipo de Madrygal cuenta con una sólida experiencia en consultoría de seguridad, auditorías, implementación de soluciones de seguridad y gestión de incidentes.
- Poseen un profundo conocimiento de las mejores prácticas de la industria y de las normativas de seguridad vigentes.

Dominio de Wazuh:

- Madrygal cuenta con ingenieros certificados oficialmente en Wazuh, lo que garantiza un alto nivel de expertise en la implementación y gestión del SIEM.

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 15 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- Han desarrollado módulos personalizados para Wazuh que complementan sus funcionalidades y lo convierten en una solución más robusta y adaptable.

Experiencia con tecnologías de código abierto:

- Madrygal se especializa en la implementación de soluciones de seguridad basadas en software libre, lo que le permite ofrecer servicios más flexibles y personalizados a sus clientes.
- Poseen un amplio conocimiento de las herramientas de código abierto disponibles en el mercado y su potencial para la creación de soluciones de seguridad eficaces y accesibles.

Enfoque ágil y flexible:

- Madrygal se caracteriza por su capacidad de adaptación a las necesidades de sus clientes y a los cambios del mercado.
- Su estructura organizativa flexible le permite responder rápidamente a las demandas de sus clientes y a las nuevas amenazas cibernéticas.

Compromiso con la calidad y el servicio al cliente:

- Madrygal se compromete a brindar servicios de alta calidad, manteniendo los más altos estándares de seguridad y ética profesional.
- Su enfoque centrado en el cliente le permite construir relaciones de largo plazo y garantizar la satisfacción de sus clientes.

Estas capacidades centrales, combinadas con un profundo conocimiento del mercado de las PyMEs, constituyen una base sólida para el éxito de SecNet .

1.8 Propuesta de valor para el cliente

SecNet ofrece a las Pymes los siguientes beneficios:

Protección integral y proactiva contra amenazas cibernéticas:

- **Detección y respuesta a amenazas en tiempo real:** SecNet identifica y neutraliza amenazas antes de que puedan causar daños.
- **Bloqueo de sitios web y direcciones IP maliciosas:** SecNet impide el acceso a contenidos y fuentes de ataques conocidos.
- **Análisis de inteligencia de amenazas:** SecNet se anticipa a las amenazas mediante el uso de honeypots y el análisis de información sobre nuevas técnicas de ataque.

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 16 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Gestión de la seguridad simplificada:

- **Monitoreo centralizado:** Una única consola para visualizar el estado de seguridad de toda la infraestructura.
- **Alertas y reportes personalizados:** Información clara y concisa sobre las amenazas y la postura de seguridad.
- **Soporte técnico especializado:** Asistencia de expertos en Wazuh para resolver cualquier problema o duda.

Ahorro de costos y recursos:

- **Modalidad SaaS:** Elimina la necesidad de inversión en infraestructura y software por parte del cliente.
- **Precios competitivos:** Solución de seguridad gestionada accesible para PyMEs con presupuestos limitados.
- **Optimización de recursos internos:** Permite a las empresas enfocar sus recursos en su actividad principal, sin tener que preocuparse por la gestión de la seguridad.

Tranquilidad y confianza:

- **Seguridad robusta y confiable:** Protección de los activos digitales y la continuidad del negocio.
- **Experiencia y profesionalismo de Madrygal:** Respaldo de una consultora con amplia experiencia en ciberseguridad.

1.9 Valores nucleares de la organización

Los valores fundamentales que guían la cultura y las acciones de Madrygal son:

Compromiso con la excelencia: Buscamos constantemente la mejora continua en todos nuestros servicios y procesos, manteniendo los más altos estándares de calidad y ética profesional.

Enfoque centrado en el cliente: Ponemos al cliente en el centro de todo lo que hacemos, adaptándonos a sus necesidades y brindando un servicio personalizado y de alta calidad.

Pasión por la tecnología: Nos apasiona la tecnología y su potencial para resolver problemas y crear un mundo más seguro.

Trabajo en equipo: Creemos en el poder del trabajo en equipo y fomentamos un ambiente de colaboración, respeto y confianza.

 Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 17 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Innovación: Nos esforzamos por estar a la vanguardia en ciberseguridad, investigando y desarrollando soluciones innovadoras para nuestros clientes.

Responsabilidad social: Estamos comprometidos con el uso responsable de la tecnología y con el impacto positivo en la sociedad.

1.10 Enfoque e iniciativas estratégicas

SecNet se basa en una estrategia de **diferenciación**, buscando ofrecer a las PyMEs un servicio de seguridad gestionada (MSSP) de alta calidad, proactivo y personalizado. Este enfoque se alinea con la estrategia genérica de diferenciación de Porter, buscando una ventaja competitiva a través de: propuesta de valor única (seguridad proactiva e integral, servicio personalizado, especialización en Wazuh como solución XDR); ventaja en costos (uso de tecnologías de código abierto y modelo SaaS accesible); y enfoque en el nicho de mercado de las PyMEs que utilizan tecnología Mikrotik como router de borde.

Iniciativas clave:

Para lograr los objetivos del proyecto, se implementan las siguientes iniciativas agrupadas según las estrategias de Porter:

1. Liderazgo en costos (parcial):

- **Optimización de la eficiencia:** Procesos eficientes para la implementación y gestión minimizando los costos operativos.
- **Negociación con proveedores:** Acuerdos con proveedores de infraestructura para reducir costos.

2. Diferenciación (principal):

- **Desarrollo de producto:**
 - Finalizar la integración de todas las funcionalidades de SecNet .
 - Realizar pruebas de seguridad y pruebas de carga.
- **Marketing y ventas:**
 - Estrategia de marketing enfocada en las PyMEs, incluyendo marketing digital, redes sociales, eventos, relaciones públicas y marketing de contenidos.
- **Alianzas estratégicas:**
 - Alianzas con proveedores de servicios de internet y telecomunicaciones.
 - Colaboración con cámaras empresariales y organizaciones de PyMEs.
- **Desarrollo del equipo:**

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 18 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- Capacitar al equipo en las últimas tecnologías (incluyendo IA y ML) y en Wazuh.
- Fomentar un ambiente de trabajo colaborativo e innovador.

3. Enfoque (nicho de mercado):

- **Marketing dirigido:** Materiales de marketing y ventas específicos para usuarios de Mikrotik.
- **Alianzas con el ecosistema Mikrotik:** Proveedores y distribuidores de Mikrotik.
- **Participación en la comunidad:** Eventos y foros relacionados con Mikrotik.

Consideraciones macroambientales:

El desarrollo e implementación de estas iniciativas se realiza teniendo en cuenta los siguientes factores macroambientales:

- **Económico:** La economía argentina presenta inestabilidad, alta inflación y recesión. SecNet mitiga el riesgo ofreciendo precios competitivos, planes de pago flexibles y demostrando un claro retorno de la inversión.
- **Político-Legal:** El marco regulatorio en ciberseguridad está en desarrollo. SecNet cumple con las normativas vigentes (Ley 25.326) y adopta las mejores prácticas internacionales (por ej. ISO 27001).
- **Tecnológico:** La rápida evolución tecnológica exige constante adaptación. SecNet se mantiene actualizado e incorpora tecnologías como IA y ML para la detección de amenazas, considerando la dependencia de tecnologías de terceros y la complejidad de integración.
- **Ecológico:** SecNet minimiza el impacto ambiental mediante la virtualización y la consolidación de servidores.
- **Socio-Cultural:** La creciente digitalización y la falta de conciencia en ciberseguridad en las empresas son factores que SecNet busca abordar con su propuesta de valor y sus actividades de concientización.

De esta forma, SecNet se adapta al contexto actual y se proyecta como una solución de seguridad sólida para el mercado de las PyMEs.

1.11 Áreas claves de resultados: identificar y justificar

Para evaluar el éxito de SecNet , se han identificado las siguientes áreas claves de resultados:

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 19 de 120
---	--	----------------

	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Adquisición de clientes:

- **Número de clientes:** Se espera un crecimiento paulatino pero constante en el número de clientes que adoptan SecNet . Por el tipo de producto se espera un primer año lento, con un segundo año más explosivo y un tercero llegando al punto de saturación, lo que normalmente se conoce como crecimiento “en S”. Es un indicador clave del éxito del producto en el mercado y de la capacidad de Madrygal para captar nuevas empresas.
- **Tasa de conversión de pruebas piloto:** Un alto porcentaje de conversión de los clientes beta a clientes de pago demuestra la efectividad de SecNet y su capacidad para satisfacer las necesidades de las PyMEs.

Retención de clientes:

- **Tasa de retención de clientes:** Una alta tasa de retención de clientes indica la satisfacción con el servicio y la capacidad de Madrygal para construir relaciones de largo plazo. Es un indicador clave de la sostenibilidad del negocio.
- **Churn rate:** Un bajo churn rate, que mide el porcentaje de clientes que abandonan el servicio, es un indicador de la lealtad y la satisfacción con SecNet .

Rentabilidad:

- **Ingresos por suscripción:** Se espera un crecimiento progresivo en los ingresos generados por las suscripciones a SecNet , lo que permite demostrar la viabilidad económica del proyecto.
- **Margen de ganancia:** Un margen de ganancia saludable es fundamental para garantizar la sustentabilidad del negocio y la capacidad de Madrygal para reinvertir en el desarrollo y la mejora de SecNet .

Reputación y reconocimiento de marca:

- **Posicionamiento de marca:** Se espera que SecNet se posicione como un servicio líder de seguridad gestionada para PyMEs, lo que se refleja en el reconocimiento de marca y la reputación de Madrygal.
- **Testimonios de clientes:** Los testimonios positivos de los clientes son un indicador clave del valor percibido de SecNet y la satisfacción con el servicio.

Justificación:

Estas áreas son relevantes para el éxito de SecNet porque reflejan los aspectos clave del negocio, incluyendo el crecimiento, la retención de clientes, la rentabilidad y la reputación de

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 20 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

marca. El seguimiento de estos indicadores permite a Madrygal evaluar el desempeño de SecNet, identificar áreas de mejora y tomar decisiones estratégicas para asegurar su crecimiento y éxito a largo plazo.

1.12 Ingreso al sector: estrategias de inserción

Para ingresar al mercado de seguridad gestionada para PyMEs y competir con éxito, SecNet se implementa una combinación de estrategias, teniendo en cuenta el modelo de las 5 fuerzas de Porter y las estrategias genéricas de Porter y Kotler:

Análisis de las 5 fuerzas de Porter:

Considerando el análisis de la sección 2.1.6 del presente documento, se priorizan las siguientes estrategias para mitigar las fuerzas competitivas:

- **Rivalidad entre competidores:**
 - **Diferenciación:** SecNet se diferencia de la competencia ofreciendo un servicio más proactivo y personalizado, basado en su experiencia en Wazuh, la integración de filtrado DNS e IP, y el análisis de inteligencia de amenazas.
 - **Precios competitivos:** Se ofrecen planes de servicio a precios competitivos para atraer a las PyMEs con presupuestos limitados.
- **Poder de negociación de los compradores:**
 - **Servicio al cliente excepcional:** Se brinda un servicio al cliente personalizado y de alta calidad para fidelizar a los clientes y reducir su incentivo a cambiar de proveedor.
 - **Planes de servicio flexibles:** Se ofrecen planes de servicio flexibles que se adapten a las necesidades específicas de cada PyME.
- **Poder de negociación de los proveedores:**
 - **Diversificación de proveedores:** Se busca diversificar la base de proveedores de tecnología para reducir la dependencia de un solo proveedor, como Wazuh.
 - **Desarrollo de soluciones propias:** Invertir en I+D para desarrollar soluciones de seguridad propias que complementen a Wazuh y reduzcan la dependencia de proveedores externos.
- **Amenaza de nuevos competidores:**
 - **Construcción de una marca fuerte:** Invertir en marketing y comunicación para construir una marca fuerte y reconocida en el mercado.
 - **Creación de barreras de entrada:** Buscar crear barreras de entrada mediante la innovación, la especialización en nichos de mercado y la construcción de una base de clientes leales.

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- Amenaza de productos sustitutos:
 - **Ofrecer un servicio integral:** SecNet se posiciona como una solución completa que abarca todas las necesidades de seguridad de las PyMEs, reduciendo la atractivo de productos sustitutos.
 - **Monitoreo de tendencias:** Mantener un monitoreo constante de las tendencias del mercado para adaptar SecNet a las nuevas amenazas y a la aparición de nuevos productos sustitutos.

Estrategias genéricas de Porter y Kotler:

Madrygal aplica para SecNet la estrategia de **diferenciación**, buscando distinguirse de la competencia a través de:

- **Calidad del servicio:** Brindar un servicio al cliente personalizado y de alta calidad, con un enfoque proactivo en la prevención y la gestión de amenazas.
- **Innovación tecnológica:** SecNet incorpora tecnologías de vanguardia, como el análisis de inteligencia de amenazas y la integración con honeypots, para ofrecer un servicio de seguridad más avanzado y eficaz.
- **Especialización en Wazuh:** Aprovechar la experiencia y el expertise de Madrygal en Wazuh para ofrecer un servicio altamente especializado que satisfaga las necesidades específicas de los clientes que utilizan esta plataforma.

SecNet ingresa al mercado con una estrategia de diferenciación, enfocada en ofrecer un servicio de seguridad gestionada de alta calidad, proactivo y personalizado, para las Pymes. Se busca mitigar las fuerzas competitivas del mercado a través de la especialización, la innovación y la construcción de una marca fuerte y reconocida.

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

2. Análisis estratégico

2.1 Análisis de Contexto

2.1.1 Descripción del escenario local

El lanzamiento de SecNet se enfoca en Argentina, un país con un mercado de tecnología en crecimiento y una creciente demanda de soluciones de ciberseguridad.

Contexto geográfico:

SecNet se focaliza inicialmente en la región Centro de Argentina, que incluye las provincias de Buenos Aires, Córdoba, Santa Fe y Entre Ríos. Esta región concentra una gran parte de la actividad económica del país y alberga un número significativo de PyMEs.

Contexto socioeconómico:

- **Economía en desarrollo:** Argentina es una economía en desarrollo con un PIB per cápita de aproximadamente 13730 Dol⁶..
- **PyMEs como motor de la economía:** Las PyMEs representan el 99% de las empresas en Argentina y generan el 64% del empleo formal. Son un segmento clave de la economía y un motor de crecimiento.
- **Creciente digitalización:** Las Pymes están adoptando cada vez más tecnologías digitales para optimizar sus operaciones y alcanzar nuevos mercados. Esta tendencia aumenta la superficie de ataque y la necesidad de soluciones de ciberseguridad.
- **Conciencia sobre la ciberseguridad:** La conciencia sobre la importancia de la ciberseguridad está creciendo en Argentina, impulsada por los incidentes de seguridad de alto perfil y las regulaciones de protección de datos cada vez más estrictas.
- **Acceso a la tecnología:** Argentina cuenta con una buena infraestructura de telecomunicaciones y un creciente ecosistema de empresas de tecnología, lo que facilita la implementación de soluciones de ciberseguridad.

2.1.2 Factores económicos

El contexto económico de Argentina presenta ciertos desafíos que pueden afectar al proyecto SecNet . Las principales variables macroeconómicas a considerar son:

⁶ https://datos.bancomundial.org/indicador/NY.GDP.PCAP.CD?locations=AR&most_recent_value_desc=false

 SecNeT Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 23 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Inflación: Argentina experimenta una alta inflación, que se estima en más del 138% para el año 2024⁷.

- **Impacto en SecNet :** La inflación presiona los costos de desarrollo y operación del servicio, y puede afectar la decisión de las PyMEs de invertir en ciberseguridad.
- **Estrategia:** Se implementan mecanismos de ajuste de precios que permitan mantener la rentabilidad del servicio, buscando un equilibrio entre la necesidad de cubrir los costos y la accesibilidad para las PyMEs.

Recesión: Argentina atraviesa un período de recesión económica, con un decrecimiento del PBI estimado en al menos 3.5% según el Banco Mundial⁸.

- **Impacto en SecNet :** La recesión puede reducir la inversión en tecnología por parte de las empresas, incluyendo las soluciones de ciberseguridad.
- **Estrategia:** Enfocarse en demostrar el retorno de inversión (ROI) de SecNet , destacando los beneficios tangibles que ofrece en términos de protección de activos y prevención de pérdidas financieras.

Tipo de cambio: El peso argentino ha experimentado una fuerte devaluación frente al dólar estadounidense.

- **Impacto en SecNet:** La devaluación aumenta el costo de las tecnologías importadas, que son utilizadas en el desarrollo y la operación de SecNet .
- **Estrategia:** Se busca mitigar el impacto de la devaluación mediante la negociación de precios con los proveedores y la búsqueda de alternativas locales o de código abierto.

PBI: El Producto Bruto Interno (PBI) de Argentina es de aproximadamente 640 MM de dólares⁹.

- **Impacto en SecNet :** Si bien el PBI es un indicador general de la actividad económica, un PBI en crecimiento puede generar un ambiente más favorable para la inversión en tecnología.
- **Estrategia:** Monitorear la evolución del PBI y los indicadores de actividad económica por rubros y adaptar las estrategias de marketing y ventas en función de las perspectivas económicas del país.

2.1.3 Factores Políticos

⁷ <https://fecoi.org.ar/informe-del-bcra-proyecta-inflacion-de-1381-para-2024/>

⁸ <https://www.bancomundial.org/es/country/argentina/overview>

⁹ https://datos.bancomundial.org/indicador/NY.GDP.MKTP.CD?locations=AR&most_recent_value_desc=true

 SecNeT Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 24 de 120
---	--	----------------

	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

El contexto político y legal en Argentina presenta ciertos factores que deben ser considerados para el desarrollo del proyecto SecNet :

Marco regulatorio en ciberseguridad:

- Argentina cuenta con la Ley 25.326 de Protección de Datos Personales, que establece un marco legal para el tratamiento de datos personales.
- Sin embargo, la normativa específica en ciberseguridad aún se encuentra en desarrollo, con proyectos en discusión para regular la seguridad de la información en sectores críticos, la notificación de incidentes y la creación de una agencia nacional de ciberseguridad.
- **Impacto en SecNet** : La falta de un marco regulatorio específico en ciberseguridad genera incertidumbre y dificulta la predicción de futuros requisitos legales.
- **Estrategia:** SecNet se desarrolla cumpliendo con las normativas vigentes y adoptando las mejores prácticas internacionales, como la norma ISO 27001 para la gestión de la seguridad de la información. Se realiza un monitoreo constante de la evolución del marco regulatorio para adaptar el servicio a los nuevos requisitos que puedan surgir.

Sistema jurídico:

- Argentina tiene un sistema jurídico complejo, con procesos judiciales que pueden ser lentos y costosos.
- **Impacto en SecNet:** En caso de incidentes de seguridad, la resolución de disputas legales puede ser compleja y llevar tiempo.
- **Estrategia:** SecNet dispone cláusulas claras en sus contratos de servicio que definen y acotan las responsabilidades de Madrygal y los clientes en caso de incidentes de seguridad. Se trabaja en colaboración con abogados especializados en ciberseguridad para asegurar el cumplimiento de las normativas legales.

Estabilidad política:

- Argentina ha experimentado períodos de inestabilidad política y económica en las últimas décadas.
- **Impacto en SecNet:** La inestabilidad política puede generar incertidumbre en el mercado y afectar la decisión de las PyMEs de invertir en servicios como SecNet .
- **Estrategia:** Se monitoriza el contexto político y se adaptan las estrategias de negocio en función de la situación del país. Se busca ofrecer un servicio confiable y de alta calidad para generar confianza en los clientes a pesar de la incertidumbre política.

	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

2.1.4 Factores Tecnológicos

El panorama tecnológico actual presenta oportunidades y desafíos para SecNet . Las principales tendencias a considerar son:

Tendencias Positivas:

- **Crecimiento del Cloud Computing:** La adopción de servicios en la nube está en aumento, lo que facilita la implementación y escalabilidad de soluciones como SecNet . El modelo SaaS se beneficia de la infraestructura y los servicios ofrecidos por proveedores de nube.
- **Avances en Inteligencia Artificial (IA) y Machine Learning (ML):** Estas tecnologías permiten mejorar la detección de amenazas, automatizar tareas de seguridad y personalizar la respuesta a los incidentes. SecNet puede integrar estas tecnologías para ofrecer un servicio más sofisticado y eficaz.
- **Desarrollo de Honeypots más avanzados:** Los honeypots están evolucionando para ser más realistas y atractivos para los atacantes, lo que permite obtener información más precisa sobre las amenazas y las técnicas de ataque. SecNet se beneficia de estos avances para mejorar su capacidad de detección y análisis de amenazas.

Desafíos Tecnológicos:

- **Sofisticación de las amenazas:** Los atacantes utilizan técnicas cada vez más sofisticadas, como el uso de IA (Inteligencia Artificial) y ML (Machine Learning) para evadir las defensas tradicionales. SecNet debe adaptarse continuamente a estas nuevas amenazas para mantener su efectividad.
- **Dependencia de tecnologías de terceros:** SecNet se basa en Wazuh, un SIEM de código abierto, y en otras herramientas de código abierto y comerciales. La dependencia de estas tecnologías puede generar riesgos si experimentan vulnerabilidades o si sus desarrolladores dejan de darles soporte.
- **Complejidad de la integración:** La integración de diferentes tecnologías y herramientas puede ser compleja y requerir un alto nivel de expertise técnica. Madrygal debe asegurar la correcta integración de los componentes de SecNet para garantizar un servicio fluido y confiable.

2.1.5 Descripción del escenario: escenario-meta

El escenario futuro deseado para SecNet se basa en un crecimiento sostenible y una consolidación como un servicio de seguridad gestionada líder para las PyMEs en Argentina, teniendo en cuenta la evolución de los factores previamente analizados:

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 26 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Entorno Macroeconómico:

- **Inflación controlada:** Se espera que, a mediano plazo, las políticas económicas logren estabilizar la inflación en Argentina, permitiendo una mayor previsibilidad en los costos y una mejor planificación a largo plazo.
- **Recuperación económica:** Se proyecta una gradual recuperación del PBI, impulsando la inversión en tecnología por parte de las empresas, incluyendo la ciberseguridad.
- **Tipo de cambio estable:** Se espera una mayor estabilidad en el tipo de cambio, lo que reduciría la incertidumbre en los costos de las tecnologías importadas.

Marco Regulatorio:

- **Normativa en ciberseguridad:** Se espera que Argentina avance en la implementación de un marco regulatorio específico para la ciberseguridad, lo que brinda mayor claridad y seguridad jurídica a las empresas que buscan proteger sus datos.
- **Cumplimiento de estándares internacionales:** Se espera que las Pymes adopten estándares internacionales de seguridad, como la ISO 27001, para demostrar su compromiso con la protección de datos y mejorar su competitividad.

Adopción Tecnológica:

- **Mayor adopción de Cloud Computing:** Se proyecta un crecimiento significativo en la adopción de servicios en la nube por parte de las PyMEs, lo que impulsa la demanda de soluciones SaaS como SecNet.
- **Integración de IA y ML:** La Inteligencia Artificial y el Machine Learning se convierten en tecnologías clave para la seguridad, permitiendo a SecNet ofrecer un servicio más proactivo, preciso y adaptable a las necesidades del cliente.

Posicionamiento de SecNet :

En este escenario meta, SecNet se consolida como:

- **Líder en seguridad gestionada para PyMEs:** Se alcanza una posición de liderazgo en el mercado, con una amplia base de clientes satisfechos y una sólida reputación de confianza y excelencia.
- **Solución integral y adaptable:** SecNet evoluciona para ofrecer una protección aún más completa y personalizada, adaptándose a las nuevas amenazas y a las necesidades cambiantes de las PyMEs.

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 27 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- **Referente en innovación:** Madrygal se consolida como un referente en innovación en ciberseguridad, desarrollando nuevas funcionalidades y servicios para SecNet que aprovechen las últimas tecnologías.

2.1.6 Análisis sectorial

Nos concentramos en el análisis FODA del sector de ciberseguridad para PyMEs:

Fortalezas:

- Creciente demanda de servicios de ciberseguridad.
- Baja barrera de entrada para nuevas empresas y soluciones.
- Disponibilidad de tecnologías de código abierto como Wazuh, que reducen los costos y aumentan la flexibilidad.
- Apoyo gubernamental a la industria del software y los servicios informáticos.

Debilidades:

- Falta de conciencia y madurez en ciberseguridad en muchas PyMEs.
- Escasez de profesionales especializados en ciberseguridad.
- Falta de normativa específica y regulación en el sector.

Oportunidades:

- Crecimiento del mercado de e-commerce y la digitalización de las PyMEs.
- Aumento de la inversión en tecnología y ciberseguridad.
- Desarrollo de nuevas tecnologías, como la IA y el Machine Learning, aplicadas a la seguridad.

Amenazas:

- Competencia de empresas internacionales con mayor presencia de mercado.
- Inestabilidad económica que afecta la inversión de las PyMEs.
- Sofisticación de las amenazas cibernéticas.

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	



2.2 Análisis de la Competencia

2.2.1 Principales competidores directos

Los principales competidores directos de SecNet, dentro del mercado de ciberseguridad para PyMEs en Argentina, son:

FortiWeb de Fortinet:

- **Descripción:** FortiWeb es un firewall de aplicaciones web (WAF) de Fortinet, una empresa multinacional de ciberseguridad. Ofrece protección contra una amplia gama de amenazas web, como inyección SQL, cross-site scripting (XSS) y ataques de denegación de servicio (DoS).
- **Fortalezas:** Amplia cobertura de amenazas, integración con otros productos de Fortinet, reconocimiento de marca global, amplia red de distribuidores y partners.

 SecNet Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 29 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- **Debilidades:** Alto costo de licencias, solución enfocada en la protección reactiva, puede ser complejo de implementar y gestionar para PyMEs con recursos limitados.

Plataforma Lumu:

- **Descripción:** Lumu es una plataforma de detección y respuesta continua (CDR) basada en la nube. Su enfoque se centra en la identificación de amenazas que ya han comprometido la red, utilizando la información proveniente de diferentes fuentes, como los firewalls, los sistemas de detección de intrusiones (IDS) y los logs de los endpoints.
- **Fortalezas:** Enfoque proactivo en la detección de amenazas, fácil implementación y gestión a través de la nube, visualización intuitiva de las amenazas.
- **Debilidades:** Al ser un servicio en la nube, puede generar preocupaciones sobre la privacidad y la soberanía de los datos. Su enfoque en la detección de amenazas puede no ser suficiente para las PyMEs que también necesitan servicios de prevención, como el filtrado DNS e IP. El costo de licencias es importante para el presupuesto de la mayoría de las Pymes.

En general, los competidores directos de SecNet se caracterizan por:

- **Ofrecer soluciones de seguridad basadas en productos comerciales:** Esto limita su flexibilidad y puede incrementar los costos para el cliente.
- **Tener un enfoque reactivo en la seguridad:** Se centran en la detección y respuesta a incidentes, en lugar de la prevención proactiva.
- **Carecer de especialización en Wazuh:** No poseen la experiencia y el expertise de Madrygal en la implementación y gestión de esta plataforma.

SecNet se diferencia de sus competidores al ofrecer:

- Un servicio más proactivo, basado en el uso de honeypots y el análisis de inteligencia de amenazas.
- Una solución integral que combina Wazuh con filtrado DNS e IP en firewalls Mikrotik.
- Planes de servicio personalizados y accesibles para las PyMEs.
- Un alto nivel de experiencia y especialización en Wazuh como solución XDR.

2.2.2 Análisis de cadena de valor

Para comprender el posicionamiento de SecNet dentro del sector de ciberseguridad para PyMEs, se analiza la cadena de valor, identificando las actividades clave que generan valor para el cliente:

 SecNet Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 30 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Actividades Primarias:

Desarrollo de soluciones de seguridad: Esta actividad implica la investigación, el diseño y la implementación de soluciones de ciberseguridad que respondan a las necesidades del mercado.

- **Posicionamiento de SecNet :** SecNet se destaca en esta actividad al combinar un SIEM de código abierto (Wazuh) con herramientas de filtrado DNS e IP y análisis de inteligencia de amenazas.
- **Ventaja competitiva:** Ofrece una solución integral y proactiva, que va más allá de las soluciones tradicionales centradas en la detección y respuesta a incidentes.

Marketing y ventas: Esta actividad abarca la promoción y comercialización de las soluciones de seguridad, la identificación de clientes potenciales y la gestión de la relación con los clientes.

- **Posicionamiento de SecNet :** SecNet se enfoca en un marketing de precisión, dirigiéndose a nichos de mercado específicos y utilizando estrategias digitales para alcanzar a sus clientes potenciales.
- **Ventaja competitiva:** Al ser un servicio SaaS, SecNet puede llegar a un público más amplio y reducir los costos de adquisición de clientes.

Implementación y configuración: Esta actividad implica la instalación, la configuración y la puesta en marcha de las soluciones de seguridad en el entorno del cliente.

- **Posicionamiento de SecNet :** SecNet se beneficia de su modelo SaaS, que facilita la implementación y reduce el tiempo y los costos asociados a esta actividad.
- **Ventaja competitiva:** Permite a las PyMEs acceder a una solución de seguridad gestionada de forma rápida y sencilla, sin necesidad de contar con un equipo técnico especializado.

Monitoreo y gestión de seguridad: Esta actividad incluye el monitoreo continuo de la infraestructura del cliente, la detección y respuesta a incidentes, y la gestión de las actualizaciones y el mantenimiento de las soluciones de seguridad.

- **Posicionamiento de SecNet :** SecNet ofrece un monitoreo y gestión de seguridad centralizados a través de la plataforma Wazuh SIEM.
- **Ventaja competitiva:** Brinda a las PyMEs una visión integral de su postura de seguridad y les permite delegar la gestión de la seguridad a un equipo de expertos.

Soporte técnico: Esta actividad abarca la resolución de problemas técnicos, la respuesta a consultas de los clientes y la capacitación en el uso de las soluciones de seguridad.

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 31 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- **Posicionamiento de SecNet** : SecNet ofrece un servicio al cliente personalizado y de alta calidad, con soporte técnico especializado en Wazuh.
- **Ventaja competitiva**: Asegura la satisfacción del cliente y la correcta utilización de SecNet , maximizando el valor del servicio.

Actividades de Soporte:

- **Gestión de la infraestructura**: Madrygal debe contar con una infraestructura robusta y confiable para alojar y gestionar la plataforma SecNet .
- **Desarrollo de tecnología**: Madrygal debe invertir en I+D para mantener a SecNet a la vanguardia y adaptarlo a las nuevas amenazas y tecnologías.
- **Gestión de recursos humanos**: Madrygal debe disponer de un equipo técnico altamente calificado y capacitado para implementar y gestionar SecNet .

Ventajas competitivas de SecNet :

- **Enfoque proactivo en la seguridad.**
- **Servicio integral y personalizado.**
- **Modelo SaaS accesible.**
- **Experiencia y especialización en Wazuh.**

Desafíos potenciales:

- **Mantener la calidad del servicio a medida que la base de clientes crece.**
- **Gestionar la dependencia de Wazuh y otras tecnologías de terceros.**
- **Adaptarse a la rápida evolución de las amenazas y las tecnologías de ciberseguridad.**

En general, el análisis de la cadena de valor muestra que SecNet se posiciona de forma estratégica en el sector de ciberseguridad para PyMEs. Al enfocarse en las actividades clave que generan valor para el cliente y aprovechar sus ventajas competitivas, SecNet tiene el potencial de convertirse en un servicio líder en el mercado.

2.2.3 Definición de Factores Críticos de Éxito (FCE)

Para tener éxito en el mercado de seguridad gestionada para PyMEs, las empresas deben dominar los siguientes Factores Críticos de Éxito (FCE):

Experiencia y conocimiento en ciberseguridad:

- Un profundo conocimiento de las amenazas, vulnerabilidades y mejores prácticas de la industria es esencial para ofrecer soluciones de seguridad efectivas.

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 32 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- La capacidad de adaptarse a las nuevas amenazas y tecnologías es fundamental para mantener la relevancia en un entorno en constante evolución.

Enfoque proactivo en la seguridad:

- Las PyMEs necesitan soluciones de seguridad que no solo reaccionen a las amenazas, sino que también las anticipen.
- La capacidad de identificar y mitigar proactivamente los riesgos es clave para evitar incidentes de seguridad costosos.

Servicio al cliente excepcional:

- Las PyMEs valoran un servicio personalizado y de alta calidad. La capacidad de responder rápidamente a las consultas y resolver los problemas de forma eficaz es fundamental para construir relaciones de confianza y fidelizar a los clientes.

Precios competitivos:

- Las PyMEs tienen presupuestos limitados y buscan soluciones de seguridad accesibles. La capacidad de ofrecer un servicio de alta calidad a un precio competitivo es clave para atraer a este segmento de mercado.

Tecnología robusta y escalable:

- Las PyMEs necesitan soluciones de seguridad confiables y que puedan crecer junto con sus negocios.
- La capacidad de ofrecer una plataforma de seguridad robusta y escalable es fundamental para satisfacer las necesidades de las PyMEs a largo plazo.

Cumplimiento de normativas:

- Las PyMEs deben cumplir con una creciente cantidad de regulaciones de protección de datos. La capacidad de ofrecer un servicio que ayude a las PyMEs a cumplir con estas normativas es un factor clave de éxito.

2.2.4 Fortalezas y debilidades del negocio :

Ahora nos enfocamos en el análisis FODA del negocio.

Fortalezas:

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 33 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- Propuesta de valor única: Enfoque proactivo, integración con Mikrotik y especialización en Wazuh.
- Modelo SaaS accesible y escalable.
- Experiencia del equipo de Madrygal en ciberseguridad y Wazuh.
- Precios competitivos.

Debilidades:

- Reconocimiento de marca limitado.
- Dependencia de Wazuh.
- Equipo técnico reducido.

Oportunidades:

- Crecimiento del mercado de ciberseguridad para PyMEs.
- Demanda creciente de soluciones personalizadas.
- Posibilidad de integrar nuevas tecnologías como IA y ML.

Amenazas:

- Competencia de grandes empresas de seguridad.
- Inestabilidad económica que puede afectar la inversión de las PyMEs.
- Posibles vulnerabilidades en Wazuh.
- Aparición de nuevas tecnologías disruptivas.



 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

3. Análisis FODA de SecNet

Este análisis integra los factores internos y externos que influyen en el proyecto SecNet , combinando la información del análisis sectorial (2.1.6) y el FODA de SecNet (2.2.4) para formular estrategias que permitan maximizar las oportunidades, minimizar las amenazas, potenciar las fortalezas y superar las debilidades.

Fortalezas (F):

- **Propuesta de valor única:** SecNet ofrece una combinación de protección proactiva (honeypots, inteligencia de amenazas), seguridad multicapa (Wazuh, filtrado DNS e IP en firewalls Mikrotik) y servicio personalizado, que lo diferencia de la competencia.
- **Enfoque especializado en PyMEs:** SecNet se centra en las necesidades de las PyMEs, un mercado con alto potencial de crecimiento y a menudo desatendido por las grandes empresas de seguridad.
- **Modelo SaaS accesible y escalable:** El modelo SaaS facilita la implementación, reduce costos y permite la escalabilidad, haciéndolo atractivo para PyMEs con recursos limitados.
- **Experiencia y expertise en Wazuh:** El equipo de Madrygal cuenta con ingenieros certificados y experiencia comprobada en la implementación y gestión de Wazuh, lo que garantiza un servicio de alta calidad.
- **Precios competitivos:** El uso de tecnologías de código abierto permite ofrecer precios competitivos y accesibles para las PyMEs.

Debilidades (D):

- **Reconocimiento de marca limitado:** Al ser un producto nuevo, SecNet aún no cuenta con un amplio reconocimiento en el mercado.
- **Dependencia de Wazuh:** La efectividad de SecNet depende, en gran medida, de la robustez y continuidad del soporte de Wazuh.
- **Equipo técnico pequeño:** El tamaño del equipo técnico de Madrygal podría ser una limitante para la escalabilidad a corto plazo, requiriendo una adecuada planificación de crecimiento del equipo a la par del crecimiento en clientes.

Oportunidades (O):

- **Mercado en expansión:** El mercado de ciberseguridad para PyMEs está en crecimiento, impulsado por la digitalización y la creciente conciencia sobre la importancia de la seguridad.

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 35 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- **Demanda de soluciones personalizadas:** Las PyMEs buscan soluciones flexibles y adaptadas a sus necesidades y presupuestos, lo que representa una oportunidad para SecNet .
- **Aumento de la inversión en ciberseguridad:** Las PyMEs están invirtiendo cada vez más en ciberseguridad.
- **Integración con IA y Machine Learning:** Estas tecnologías ofrecen oportunidades para mejorar la detección de amenazas y la automatización de tareas, potenciando las capacidades de SecNet .

Amenazas (A):

- **Competencia de grandes empresas:** Grandes empresas del sector de ciberseguridad podrían ingresar al mercado de las PyMEs con ofertas agresivas.
- **Inestabilidad económica:** La incertidumbre económica en Argentina podría afectar las decisiones de inversión de las PyMEs, incluyendo la contratación de servicios de ciberseguridad.
- **Vulnerabilidades en Wazuh:** La dependencia de Wazuh implica un riesgo en caso de que se descubran vulnerabilidades críticas en la plataforma.
- **Aparición de nuevas tecnologías disruptivas:** La aparición de nuevas tecnologías podría volver obsoleta la arquitectura de SecNet , requiriendo adaptaciones o re-desarrollo para mantener la competitividad.

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Matriz FODA de SecNet



Estrategias derivadas del FODA de SecNet :

FO (Fortalezas-Oportunidades):

- **F1 (Valor único) + O1 (Mercado en expansión):** Aprovechar el crecimiento del mercado y la demanda de soluciones de seguridad para **impulsar la comercialización de SecNet**, destacando su propuesta de valor única e integral (prevención, detección y respuesta a amenazas). Se deben desarrollar campañas de marketing y ventas enfocadas en las PyMEs, resaltando los beneficios de una solución proactiva y multicapa.
- **F2 (Enfoque PyMEs) + O2 (Soluciones personalizadas):** **Desarrollar ofertas de SecNet personalizadas** para nichos específicos dentro del segmento de las PyMEs, como e-commerce, servicios financieros o salud. Esto permite a SecNet atender las necesidades específicas de cada nicho y ofrecer un mayor valor agregado.

 SecNet Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 37 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- **F3 (Modelo SaaS) + O3 (Aumento de inversión): Aprovechar el aumento en la inversión en ciberseguridad para promocionar la accesibilidad y escalabilidad de SecNet .** Se debe destacar el modelo SaaS como una solución costo-efectiva y fácil de implementar para las PyMEs, que les permite escalar el servicio a medida que sus necesidades crecen.
- **F4 (Experiencia en Wazuh) + O4 (IA y ML): Integrar la IA y el Machine Learning en SecNet para mejorar la detección de amenazas y la automatización de tareas.** Esto potencia las capacidades de SecNet y le permite ofrecer un servicio más sofisticado y eficaz, aprovechando la experiencia del equipo en Wazuh.

DO (Debilidades-Oportunidades):

- **D1 (Reconocimiento de marca) + O1 (Mercado en expansión): Incrementar el reconocimiento de marca de SecNet aprovechando el crecimiento del mercado.** Implementar una estrategia de marketing de contenidos y relaciones públicas para generar conciencia sobre el producto y posicionar a Madrygal como un experto en ciberseguridad para PyMEs.
- **D2 (Dependencia de Wazuh) + O4 (IA y ML): Reducir la dependencia de Wazuh explorando e integrando otras tecnologías de código abierto.** Esto permite diversificar la oferta y mitigar el riesgo asociado a las vulnerabilidades o la discontinuación del soporte de Wazuh.
- **D3 (Equipo pequeño) + O3 (Aumento de inversión): Ampliar el equipo técnico con la incorporación de nuevos profesionales especializados.** El aumento de la inversión en ciberseguridad permite a Madrygal contratar los recursos necesarios para escalar el servicio y atender la creciente demanda.

FA (Fortalezas-Amenazas):

- **F1 (Valor único) + A1 (Competencia): Enfatizar la propuesta de valor única de SecNet para diferenciarse de la competencia.** Destacar el enfoque proactivo, la integración con Mikrotik y el servicio personalizado para competir con las grandes empresas que ofrecen soluciones más estandarizadas.
- **F3 (Modelo SaaS) + A2 (Inestabilidad): Promocionar el modelo SaaS de SecNet como una solución flexible y accesible en un contexto de inestabilidad económica.** Ofrecer planes de pago flexibles y adaptados a los presupuestos reducidos de las PyMEs durante periodos de incertidumbre.
- **F4 (Experiencia Wazuh) + A3 (Vulnerabilidades): Apalancar la experiencia en Wazuh para mitigar el riesgo de vulnerabilidades.** Implementar un sistema de monitoreo y respuesta a incidentes robusto y mantenerse al tanto de las actualizaciones y parches de seguridad de Wazuh.

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 38 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

DA (Debilidades-Amenazas):

- **D1 (Reconocimiento de marca) + A1 (Competencia): Fortalecer el reconocimiento de marca de SecNet para competir con las grandes empresas.** Invertir en estrategias de marketing y comunicación para generar conciencia de marca y construir una reputación sólida.
- **D2 (Dependencia de Wazuh) + A4 (Nuevas tecnologías): Explorar e integrar nuevas tecnologías para reducir la dependencia de Wazuh a largo plazo.** Esto permite adaptarse a la aparición de nuevas tecnologías disruptivas y mantener la competitividad de SecNet.
- **D3 (Equipo pequeño) + A2 (Inestabilidad): Desarrollar un plan de crecimiento del equipo técnico que se adapte a la situación económica.** Priorizar la contratación de personal clave y buscar alternativas de financiación para el crecimiento del equipo.

4 Segmentación

4.1 Segmentación de consumidores y/o Negocios

SecNet se enfoca en el mercado **Business to Business (B2B)**, específicamente en las **Pequeñas y Medianas Empresas (PyMEs)** de Argentina.

Criterios de Segmentación por sector:

Para segmentar el mercado objetivo utilizamos los siguientes criterios:

- **Tamaño de la empresa:** Se dirige a PyMEs con un número de empleados entre 10 y 250.
- **Sector de actividad:** SecNet es aplicable a PyMEs de diversos sectores, priorizando aquellas que:
 - Manejan información sensible o crítica, como datos personales, financieros o de propiedad intelectual.
 - Requieren una alta disponibilidad de sus sistemas y servicios, como empresas de e-commerce, servicios en línea o industrias con operaciones críticas.
- **Nivel de madurez en ciberseguridad:** SecNet se adapta a PyMEs con diferentes niveles de madurez en ciberseguridad, desde aquellas que recién están comenzando a implementar medidas de seguridad hasta aquellas que buscan soluciones más avanzadas y gestionadas.

 SecNeT Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 39 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- **Ubicación geográfica:** Inicialmente, SecNet se focaliza en la región del Área Metropolitana de Buenos Aires (AMBA) y la Región Centro (Santa Fe, Córdoba, Mendoza, Entre Ríos), con planes de expansión a otras regiones de Argentina en el futuro.

SecNet se compone de varios módulos que se adaptan a la ciberseguridad de las Pymes, aunque el módulo que opera sobre el router de borde requiere que el dispositivo sea de marca Mikrotik¹⁰.

Con esta variable en la ecuación nos enfocamos en el mercado de las Pymes que utilizan un router de borde con RouterOS.

Así es que cruzamos ambos datos:

- Cantidad de pymes
- Cantidad de dispositivos Mikrotik conectados a Internet.

Bajo esa premisa identificamos en el sitio **Shodan**¹¹ los dispositivos Mikrotik vinculados a Internet.

Shodan es un motor de búsqueda que le permite al usuario encontrar iguales o diferentes tipos específicos de equipos (routers, servidores, etc.) conectados a Internet a través de una variedad de filtros. Funciona como una especie de nmap masivo de Internet. La capacidad de escaneo es impresionante, puede actualizar los dispositivos de todas las direcciones IP de Internet diariamente. Algunos también lo han descrito como un motor de búsqueda de banners de servicios, que son metadatos que el servidor envía de vuelta al cliente. Esta información puede ser sobre el software de servidor, qué opciones admite el servicio, un mensaje de bienvenida o cualquier otra cosa que el cliente pueda saber antes de interactuar con el servidor. Shodan recoge datos de todos los servicios, incluyendo HTTP (puerto 80, 8080), HTTPS (puerto 443, 8443), FTP (21), SSH (22) Telnet (23), SNMP (161) y SIP (5060), entre otros.

Fue lanzado en 2009 por el informático John Matherly, en 2003 concibió la idea de buscar dispositivos vinculados a Internet. El nombre Shodan es una referencia a SHODAN, un personaje de la serie de videojuegos System Shock

Si realizamos una búsqueda por la etiqueta “Mikrotik” en el buscador Shodan (<https://www.shodan.io/search?query=MikroTik>) nos devuelve una cantidad de 3.268.818 dispositivos. Estos los encuentra en base al banner que devuelven los servicios (winbox, web admin, vpn, servidor de ancho de banda, ftp, etc)

¹⁰ <https://www.mikrotik.com>

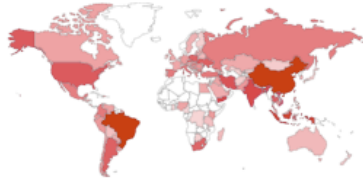
¹¹ [https:// www.shodan.io](https://www.shodan.io)

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 40 de 120
---	--	----------------

TOTAL RESULTS

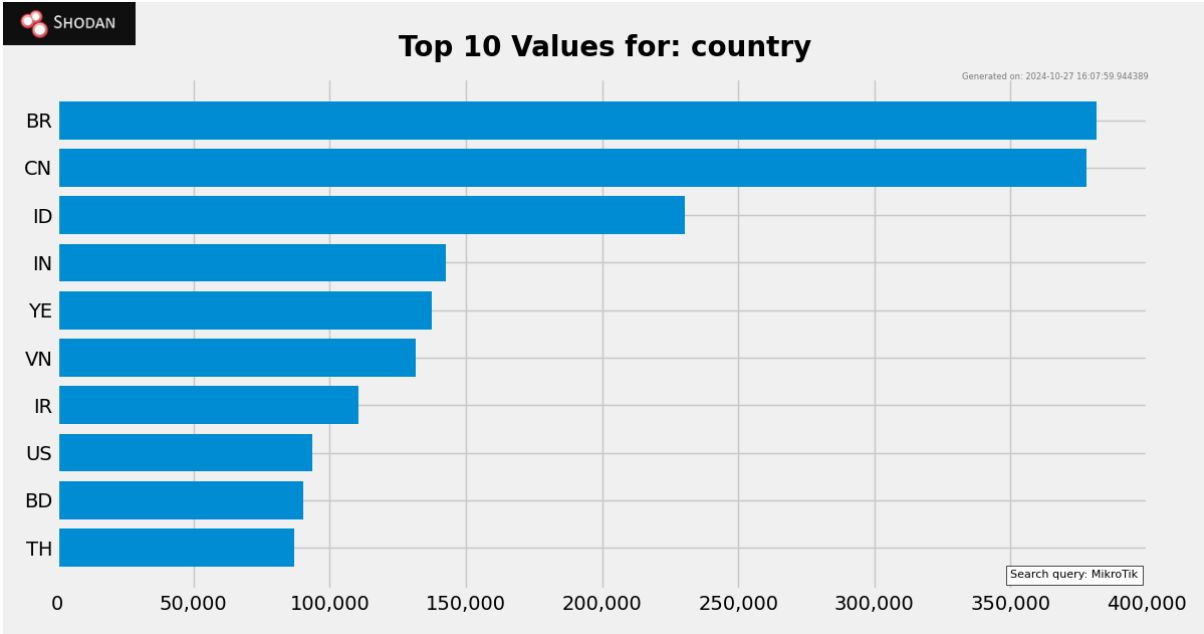
3,268,818

TOP COUNTRIES



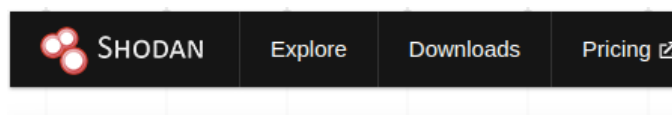
Brazil	381,360
China	377,819
Indonesia	230,183
India	142,752
Yemen	137,486

Esta herramienta permite también buscar por país. (<https://www.shodan.io/search?query=MikroTik+country%3A%22AR%22>). Nos interesan las cifras de Argentina y el resto de los países de la región.



 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Pais	Código	Cantidad	Porcentaje
Total de dispositivos		3.268.818	100%
Brasil	BR	381.420	11,66%
Argentina	AR	83.119	2,55%
Colombia	CO	46.703	1,45%
España	ES	45.818	1,40%
Mexico	MX	40.885	1,25%
Ecuador	EC	21.062	0,65%
Perú	PE	19.856	0,61%
Uruguay	UY	16.744	0,51%
Chile	CL	14.566	0,45%
Paraguay	PY	7.957	0,24%
Bolivia	BO	5.412	0,17%
Mercado hispanoamericano		683.542	20.9%



TOTAL RESULTS

83,119

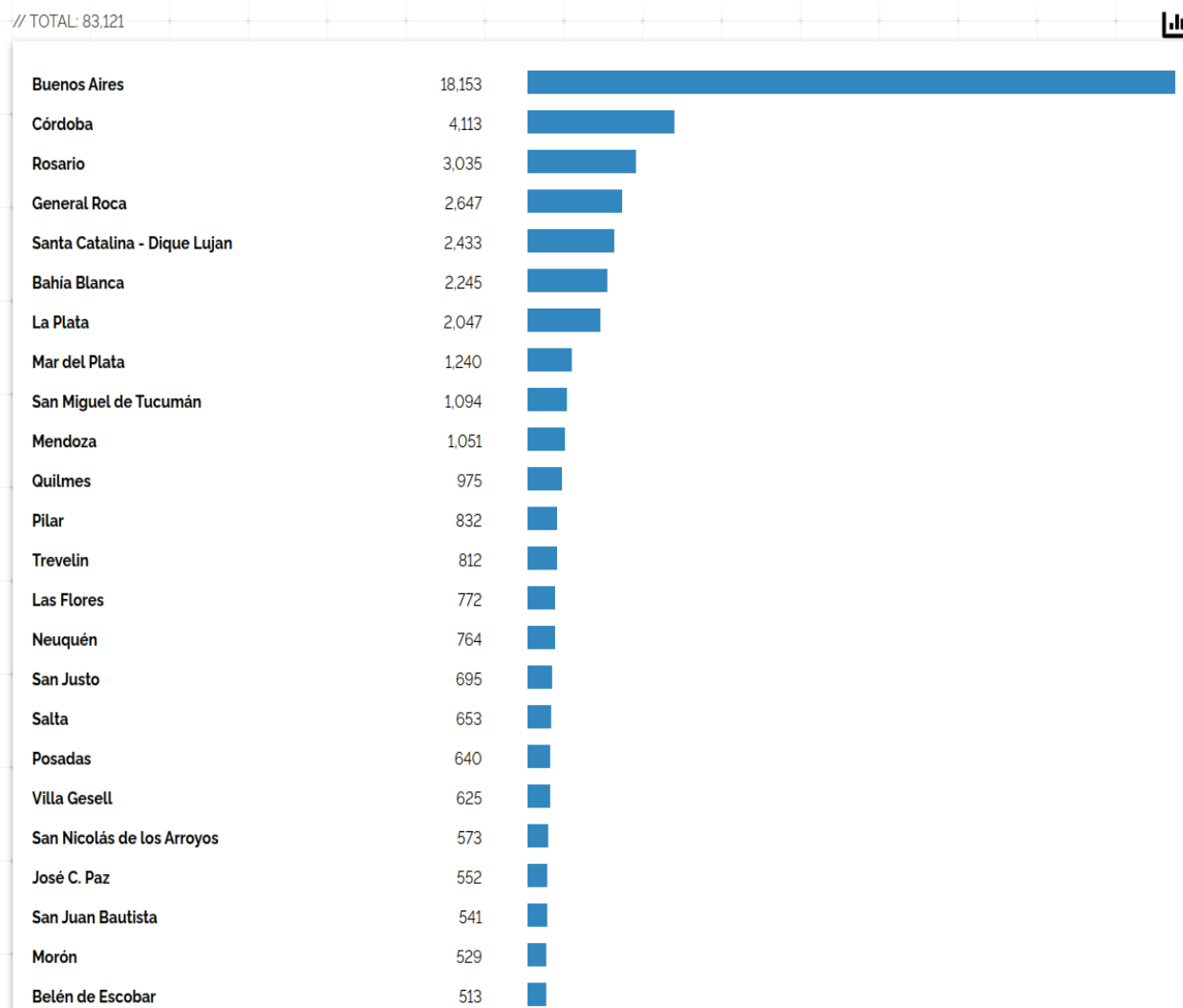
TOP CITIES

Buenos Aires	18,151
Córdoba	4,113
Rosario	3,035
General Roca	2,647
Santa Catalina - Dique Lujan	2,433

 SecNeT Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 42 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

El mercado argentino es el segundo en hispanoamérica detrás de Brasil, por lo que la estrategia de consolidarse primero como marca en Argentina para después desplegar en Latam parece la indicada. También tenemos una búsqueda por ciudades que nos puede facilitar la selección de objetivos y publicaciones.



Con estos datos podemos definir la segmentación de mercado,

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	



Metricas a 3 años	Dispositivos (clientes)	Porcentaje
Total de equipos	3.268.818	100%
Atendible (100% Latam)	683.542	20,9%
Factible (100% Argentina)	83.119	2,55%
Objetivo 3 años (2% de AR)	1660	0,05%

- Estrategias de marketing:** Se implementan estrategias de marketing enfocadas en la generación de conciencia de marca, la atracción de clientes potenciales y la fidelización de los clientes existentes, como:
 - Marketing de contenidos:** Creación de un blog con contenido educativo sobre ciberseguridad y SecNet . Lanzamiento de una campaña de marketing de contenidos en redes sociales.
 - Eventos y conferencias:** Participación en eventos y conferencias de ciberseguridad para posicionar a SecNet como un servicio líder.
 - Relaciones públicas:** Generación de relaciones con medios de comunicación y expertos en ciberseguridad para promocionar SecNet y construir una reputación positiva de marca.
 - Programa de referidos:** Creación un programa de comisiones para aquellos colegas que sumen un cliente que utilice los servicios o productos de Madrygal por suscripción.

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- **Responsabilidad Social Empresaria (RSE):** Como parte de las acciones de RSE, Madrygal brinda charlas en instituciones educativas sobre ciberseguridad y prevención de ciberdelitos.

4.2 Identificación de grupos diferenciados de consumidores

Dentro del segmento objetivo de PyMEs, SecNet se dirige a dos grupos de clientes con características y necesidades distintas:

1. PyMEs con necesidades básicas de ciberseguridad:

- **Características:**
 - Número de empleados: 10-50
 - Sector: Comercio minorista, servicios profesionales, pequeñas industrias.
 - Nivel de digitalización: Básico, con escasa presencia en línea y uso de correo electrónico.
 - Madurez en ciberseguridad: Baja, con medidas de seguridad limitadas o inexistentes.
- **Necesidades:**
 - Protección básica contra amenazas comunes, como virus, malware y ataques de phishing.
 - Control de acceso a la red y los dispositivos.
 - Respaldo de datos.
- **Comportamiento de compra:**
 - Buscan soluciones de seguridad accesibles y fáciles de implementar.
 - Priorizan el precio y la simplicidad sobre las funcionalidades avanzadas.
- **Motivaciones:**
 - Cumplir con los requisitos mínimos de seguridad.
 - Evitar interrupciones en el negocio debido a incidentes de seguridad.
 - Proteger su reputación.

2. PyMEs con necesidades avanzadas de ciberseguridad:

- **Características:**
 - Número de empleados: 50-250
 - Sector: E-commerce, servicios financieros, salud, tecnología.
 - Nivel de digitalización: Alto, con sistemas y aplicaciones críticas para el negocio.

 SecNeT Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 45 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- Madurez en ciberseguridad: Intermedia o alta, con políticas y procedimientos de seguridad implementados o en proceso de implementación.
- **Necesidades:**
 - Protección avanzada contra amenazas sofisticadas, como ataques dirigidos y ransomware.
 - Monitoreo y gestión de seguridad centralizados.
 - Respuesta a incidentes y recuperación de desastres.
- **Comportamiento de compra:**
 - Buscan soluciones de seguridad integrales y gestionadas.
 - Están dispuestos a invertir en soluciones de alta calidad que ofrezcan un alto nivel de protección.
- **Motivaciones:**
 - Proteger su información y sus sistemas críticos.
 - Cumplir con las regulaciones de protección de datos y los requisitos de sus clientes.
 - Mantener la continuidad del negocio y proteger su reputación.

SecNet ofrece planes de servicio adaptados a las necesidades de ambos grupos de clientes:

- Para las PyMEs con necesidades básicas, se ofrece un plan de servicio que incluye las funcionalidades esenciales de protección, a un precio accesible.
- Para las PyMEs con necesidades avanzadas, ya se dispone un plan de servicio más completo, que incluye monitoreo, gestión de incidentes y otras funcionalidades avanzadas, a un precio superior y con una instancia de Wazuh exclusiva. Este producto ya es parte del portfolio de la consultora y queda fuera del análisis económico del presente documento.

De esta forma, Madrygal busca satisfacer la demanda de un amplio espectro de PyMEs, ofreciendo un servicio flexible y escalable que se adapta a sus necesidades y presupuestos.

4.3 ¿Quiénes son los potenciales usuarios/compradores del negocio?

El cliente ideal para SecNet es una PyME con las siguientes características:

Características:

- **Tamaño:** Entre 25 y 150 empleados.

 SecNeT Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 46 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- **Sector:** Pertenece a sectores como e-commerce, servicios financieros, salud o tecnología, donde el manejo de información sensible y la disponibilidad de los sistemas son críticos para el negocio.
- **Nivel de digitalización:** Tiene una fuerte dependencia de las tecnologías de la información y la comunicación en sus operaciones.
- **Madurez en ciberseguridad:** Posee un nivel de madurez en ciberseguridad básico o intermedio. Reconoce la importancia de la seguridad, pero carece de los recursos internos o el expertise para gestionarla de forma eficaz.

Necesidades y motivaciones:

- Busca una solución de seguridad gestionada (MSSP) que le permita delegar la gestión de la seguridad a un equipo de expertos, ya que carece de recursos humanos propios especializados en ciberseguridad.
- Necesita proteger su información y sus sistemas críticos contra una amplia gama de amenazas, incluyendo ataques dirigidos, ransomware y filtrado de DNS malicioso.
- Busca un servicio que sea fácil de implementar y gestionar, y que no requiera una gran inversión inicial.
- Valora un servicio personalizado que se adapte a sus necesidades específicas y que le brinde soporte técnico continuo.

Comportamiento de compra:

- El cliente ideal de SecNet es proactivo en la búsqueda de soluciones de seguridad y está dispuesto a invertir en un servicio de alta calidad que le brinde tranquilidad y confianza.
- Se informa a través de canales digitales, como sitios web especializados, blogs y redes sociales.
- Valora las recomendaciones de otros profesionales de TI y las opiniones de otros clientes.

El cliente ideal de SecNet es una PyME con una alta dependencia de la tecnología, consciente de la importancia de la ciberseguridad, pero con limitaciones para gestionarla internamente. Busca una solución gestionada, completa, personalizada y accesible, que le permita proteger su negocio y enfocarse en su crecimiento y éxito.

4.4 Pautas de comportamiento esperado de cada segmento

 SecNet Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 47 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

PyMEs con necesidades básicas de ciberseguridad:

- **Hábitos de compra:**
 - Suelen buscar soluciones de seguridad a través de referencias de otros empresarios o profesionales de TI de confianza.
 - Priorizan el precio y la facilidad de uso en su decisión de compra.
 - Es probable que opten por soluciones básicas y estandarizadas.
- **Uso de productos similares:**
 - Es posible que utilicen antivirus gratuitos o de bajo costo, y que no tengan un firewall o un sistema de detección de intrusiones.
 - Pueden no tener políticas de seguridad formalizadas o un plan de respuesta a incidentes.
- **Preferencias de comunicación:**
 - Prefieren la comunicación directa y personalizada, ya sea por teléfono o correo electrónico.
 - Valoran la rapidez de respuesta y la claridad en la información.

PyMEs con necesidades avanzadas de ciberseguridad:

- **Hábitos de compra:**
 - Suelen realizar una investigación más exhaustiva antes de tomar una decisión de compra, consultando sitios web especializados, analistas de la industria y casos de éxito.
 - Están dispuestos a invertir en soluciones de alta calidad que ofrezcan una protección completa y confiable.
- **Uso de productos similares:**
 - Es probable que ya utilicen soluciones de seguridad como firewalls, sistemas de detección de intrusiones y software antivirus.
 - Pueden tener políticas de seguridad implementadas, pero buscan externalizar la gestión y el monitoreo de la seguridad.
- **Preferencias de comunicación:**
 - Están abiertos a diferentes canales de comunicación, como correo electrónico, teléfono, videoconferencias y plataformas de mensajería instantánea.
 - Valoran la información técnica detallada y los reportes personalizados.

Consideraciones adicionales:

- Ambos segmentos de clientes son susceptibles a las estrategias de marketing de contenido, como blogs, white papers y webinars. El contenido de alta calidad sobre

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 48 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

ciberseguridad puede ser una herramienta eficaz para educar a los clientes potenciales y generar confianza en la marca SecNet .

- La participación en eventos y conferencias de ciberseguridad es una buena forma de llegar a ambos segmentos de clientes, generar contactos y posicionar a Madrygal como un experto en el sector.

5 Plan de Acción

5.1 Objetivos Generales

El Plan de Acción de SecNet se articula en torno a los siguientes objetivos generales, que guían las estrategias y acciones específicas detalladas en la sección 5.2:

1. **Lanzamiento exitoso de SecNet:** Asegurar un lanzamiento fluido y efectivo de SecNet al mercado, cumpliendo con los plazos establecidos y los objetivos iniciales de adquisición de clientes. Esto implica:
 - Finalización del desarrollo del producto, incluyendo pruebas de seguridad y rendimiento.
 - Implementación de la infraestructura necesaria y escalable.
 - Ejecución de una estrategia de marketing inicial efectiva.
2. **Penetración en el mercado de las PyMEs:** Alcanzar una participación significativa en el mercado objetivo de PyMEs que utilizan tecnología Mikrotik en Argentina, estableciendo a SecNet como una solución líder en seguridad gestionada. Se busca lograr esto a través de:
 - Una propuesta de valor diferenciada.
 - Precios competitivos.
 - Un enfoque centrado en las necesidades de las PyMEs.
3. **Escalabilidad y crecimiento sostenible:** Desarrollar una estructura escalable y un modelo de negocio sostenible que permita a SecNet crecer junto con la demanda del mercado, manteniendo la rentabilidad. Esto incluye:
 - Optimización de procesos y automatización de tareas.
 - Gestión eficiente de los recursos.
 - Búsqueda de financiación para el crecimiento.
 - Desarrollo de un plan de escalabilidad de la infraestructura.
4. **Construcción de una marca fuerte y reconocida:** Posicionar a SecNet como una marca líder en ciberseguridad para PyMEs en Argentina, generando confianza y credibilidad. Las acciones se centran en:
 - Marketing de contenidos, relaciones públicas, y participación en eventos.
 - Desarrollo de un programa de referidos.
 - Generación de casos de éxito y testimonios de clientes satisfechos.

 SecNet Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 49 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- Medición del reconocimiento de marca (ej. número de menciones, seguidores en redes sociales).
- 5. **Generación de valor para Madrygal:** Asegurar que SecNet contribuya significativamente a los ingresos y la rentabilidad de Madrygal, convirtiéndose en un producto clave en su portfolio de servicios. Esto implica:
 - Maximización de las ventas y optimización de los costos.
 - Generación de un margen de ganancia saludable.
 - Desarrollo de nuevas líneas de productos y servicios complementarios.

5.2 Programas específicos de acción:

5.2.1 Programas específicos de sector Administración:

5.2.1.1 Administración de Compras:

- **Acciones:**
 - Implementar un sistema de gestión de compras basado en una herramienta de código abierto, como Odoo, para optimizar el proceso de compra de hardware y software.
 - Definir un proceso de selección de proveedores que incluya la evaluación de la calidad de los productos y la capacidad de respuesta del proveedor.
 - Establecer un sistema de control de gastos para asegurar que las compras se realicen dentro del presupuesto establecido.
 - Implementar un sistema de seguimiento de los pedidos de compra para monitorear el estado de cada pedido y asegurar la entrega a tiempo.

5.2.1.2 Administración de Ventas:

- **Acciones:**
 - Implementar un sistema de gestión (CRM) para registrar los datos de los clientes y sus necesidades, y realizar un seguimiento de las oportunidades de venta.
 - Capacitar al equipo de ventas en el uso de SecNet y en las mejores prácticas de ventas de software.
 - Desarrollar materiales de marketing y ventas específicos para SecNet , incluyendo folletos, presentaciones y videos que destaquen los beneficios del servicio.
 - Establecer un sistema de seguimiento de las ventas para analizar el desempeño del equipo de ventas y realizar ajustes en las estrategias de marketing (CRM)

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

5.2.1.3 Administración de Cobranzas:

- **Acciones:**
 - Implementar un sistema de gestión de cobranzas que permita llevar un seguimiento de las facturas pendientes, los recibos emitidos y los deudores morosos.
 - Establecer un proceso de recuperación de cuentas por cobrar para minimizar las pérdidas por morosidad.
 - Capacitar al equipo de cobranzas en el uso de las herramientas de gestión de cobranzas y en las mejores prácticas de gestión de deudores.

5.2.1.4 Administración de Pagos:

- **Acciones:**
 - Implementar un sistema de gestión de pagos que permita llevar un seguimiento de las órdenes de pago a proveedores, los cheques emitidos y los pagos realizados.
 - Establecer un proceso de control de pagos para asegurar que las transacciones se realicen de forma eficiente y segura.
 - Capacitar al equipo de pagos en el uso de las herramientas de gestión de pagos y en las mejores prácticas de gestión financiera.

5.2.1.5 Administración de Contabilidad:

- **Acciones:**
 - Implementar un sistema de gestión de la contabilidad basado en software libre, como Odoo o OpenERP, para llevar un control eficiente de las operaciones contables de SecNet .
 - Establecer un proceso de reconciliación de las cuentas bancarias y de las facturas para asegurar la exactitud de la información contable.
 - Capacitar al equipo de contabilidad en el uso de las herramientas de gestión contable y en las mejores prácticas de gestión financiera.

5.2.2 Programas específicos de sector Tecnología:

5.2.2.1 Adquisición de Hardware:

- **Acciones:**
 - Definir las especificaciones técnicas del hardware que se necesita para la infraestructura de SecNet .

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 51 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- Solicitar cotizaciones a diferentes proveedores de hardware y evaluar la relación calidad-precio.
- Seleccionar el hardware más adecuado para el proyecto y realizar la compra.
- Instalar el hardware y configurarlo de acuerdo con las necesidades del proyecto.
- Implementar un sistema de inventario de hardware para el control de los equipos y la planificación de futuras actualizaciones.

5.2.2.2 Estrategias para Telecomunicaciones:

- **Acciones:**
 - Investigar y seleccionar un proveedor de servicios de internet y telefonía que ofrezca un servicio fiable y con una buena relación calidad-precio.
 - Negociar un contrato de servicios de internet y telefonía que cumpla con las necesidades del proyecto y que ofrezca una buena disponibilidad de banda ancha.
 - Instalar y configurar el equipo de red para asegurar una conectividad eficiente y segura.
 - Realizar pruebas de la conectividad de la red para garantizar la disponibilidad del servicio.
 - Implementar un sistema de monitoreo de la conectividad de la red para identificar y resolver los problemas de forma rápida y eficiente.

5.2.2.3 Estrategias para adquisición de Software:

- **Acciones:**
 - Definir las especificaciones técnicas del software que se necesita para el desarrollo de SecNet .
 - Investigar y seleccionar los programas de software más adecuados para el proyecto, considerando la licencia, el costo y las funcionalidades.
 - Negociar con los proveedores de software las condiciones de licencia y de pago.
 - Adquirir las licencias del software necesario para el proyecto.
 - Instalar y configurar el software de acuerdo con las necesidades del proyecto.
 - Implementar un sistema de control de versiones de software para asegurar que las actualizaciones se realicen de forma eficiente y segura.

	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

5.2.3 Programas específicos de sector Producción:

5.2.3.1 Estrategias para Análisis de requerimientos:

- **Acciones:**
 - Establecer un proceso de recopilación de requisitos de los clientes que incluya entrevistas, encuestas y reuniones.
 - Documentar los requisitos de forma clara y concisa.
 - Realizar un análisis de los requisitos para identificar las necesidades específicas de cada cliente.
 - Definir las funcionalidades de SecNet que se necesitan para satisfacer los requisitos del cliente.

5.2.3.2 Estrategias para Desarrollo de productos:

- **Acciones:**
 - Definir la arquitectura del producto.
 - Seleccionar el lenguaje de programación y las herramientas de desarrollo más adecuadas.
 - Implementar un proceso de desarrollo ágil para asegurar que las actualizaciones se realicen de forma rápida y eficiente.
 - Realizar pruebas unitarias e integradas para garantizar la calidad del código.
 - Documentar el código de forma adecuada.

5.2.3.3 Estrategias para Pruebas de Software:

- **Acciones:**
 - Definir un plan de pruebas de software que incluya pruebas funcionales, pruebas de rendimiento y pruebas de seguridad.
 - Seleccionar las herramientas de prueba más adecuadas para el proyecto.
 - Realizar las pruebas de acuerdo con el plan de pruebas.
 - Documentar los resultados de las pruebas.
 - Corregir los errores detectados en las pruebas.

5.2.3.4 Estrategias para Implementación:

- **Acciones:**
 - Desarrollar un plan de implementación que incluya la instalación del producto en el entorno del cliente, la configuración del producto y la capacitación de los usuarios.

	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- Definir un proceso de gestión de incidentes para resolver los problemas que puedan surgir durante la implementación.
- Establecer un sistema de seguimiento de la implementación para monitorear el progreso del proyecto y asegurar que las acciones se realicen de acuerdo con el plan.

5.2.4 Programas específicos de sector Marketing:

5.2.4.1 Estrategias para Producto:

- **Acciones:**
 - Definir las características y los beneficios clave del producto SecNet , enfocándose en las necesidades de las PyMEs.
 - Desarrollar un mensaje de marketing claro y conciso que comunique el valor de SecNet y que atraiga a los clientes potenciales.
 - Crear un sistema de gestión de contenidos para el sitio web de SecNet y las redes sociales, con información relevante sobre ciberseguridad y SecNet .

5.2.4.2 Estrategias para Precio:

- **Acciones:**
 - Analizar los precios de la competencia y determinar un precio competitivo para SecNet .
 - Ofrecer diferentes planes de suscripción para adaptarse a las necesidades y presupuestos de las PyMEs.
 - Desarrollar una estrategia de descuentos y promociones para atraer nuevos clientes.

5.2.4.3 Estrategias para Plaza:

- **Acciones:**
 - Definir los canales de distribución de SecNet , enfocándose en las PyMEs y en el mercado argentino.
 - Seleccionar los canales de distribución más eficaces y rentables para SecNet , como el sitio web, las redes sociales y los eventos de ciberseguridad.
 - Establecer un sistema de gestión de la logística para asegurar que los productos se entregan a tiempo y de forma segura.

5.2.4.4 Estrategias para Promoción:

- **Acciones:**

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 54 de 120
---	--	----------------

	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- Desarrollar una estrategia de promoción que incluya la publicidad en línea y offline, la participación en eventos, las relaciones públicas y las promociones de ventas.
- Crear una campaña de publicidad en línea para promocionar SecNet en los motores de búsqueda y en las redes sociales.
- Participar en eventos y conferencias de ciberseguridad para generar conciencia de marca y atraer clientes potenciales.
- Desarrollar un programa de relaciones públicas para fortalecer la reputación de la marca SecNet .
- Ofrecer descuentos y promociones especiales para atraer nuevos clientes y fidelizar a los clientes existentes.

5.2.5 Programas específicos de sector Comercialización:

5.2.5.1 Estrategia de Ventas:

- **Acciones:**
 - Capacitar al equipo de ventas en el uso de SecNet y en las mejores prácticas de ventas de software.
 - Desarrollar materiales de marketing y ventas específicos para SecNet , incluyendo folletos, presentaciones y videos que destaquen los beneficios del servicio.
 - Establecer un sistema de seguimiento de las ventas para analizar el desempeño del equipo de ventas y realizar ajustes en las estrategias de marketing.
 - Implementar un sistema de gestión de relaciones con los clientes (CRM) para registrar los datos de los clientes y sus necesidades, y para llevar un seguimiento de las oportunidades de venta.

5.2.5.2 Estrategia de post-venta:

- **Acciones:**
 - Establecer un proceso de atención al cliente para resolver dudas y problemas de forma rápida y eficiente.
 - Implementar un sistema de seguimiento de satisfacción del cliente para identificar las áreas de mejora y mantener la confianza de los clientes.
 - Ofrecer servicios de capacitación y actualización a los clientes.

5.2.5.3 Estrategia de logística de salida:

- **Acciones:**

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 55 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

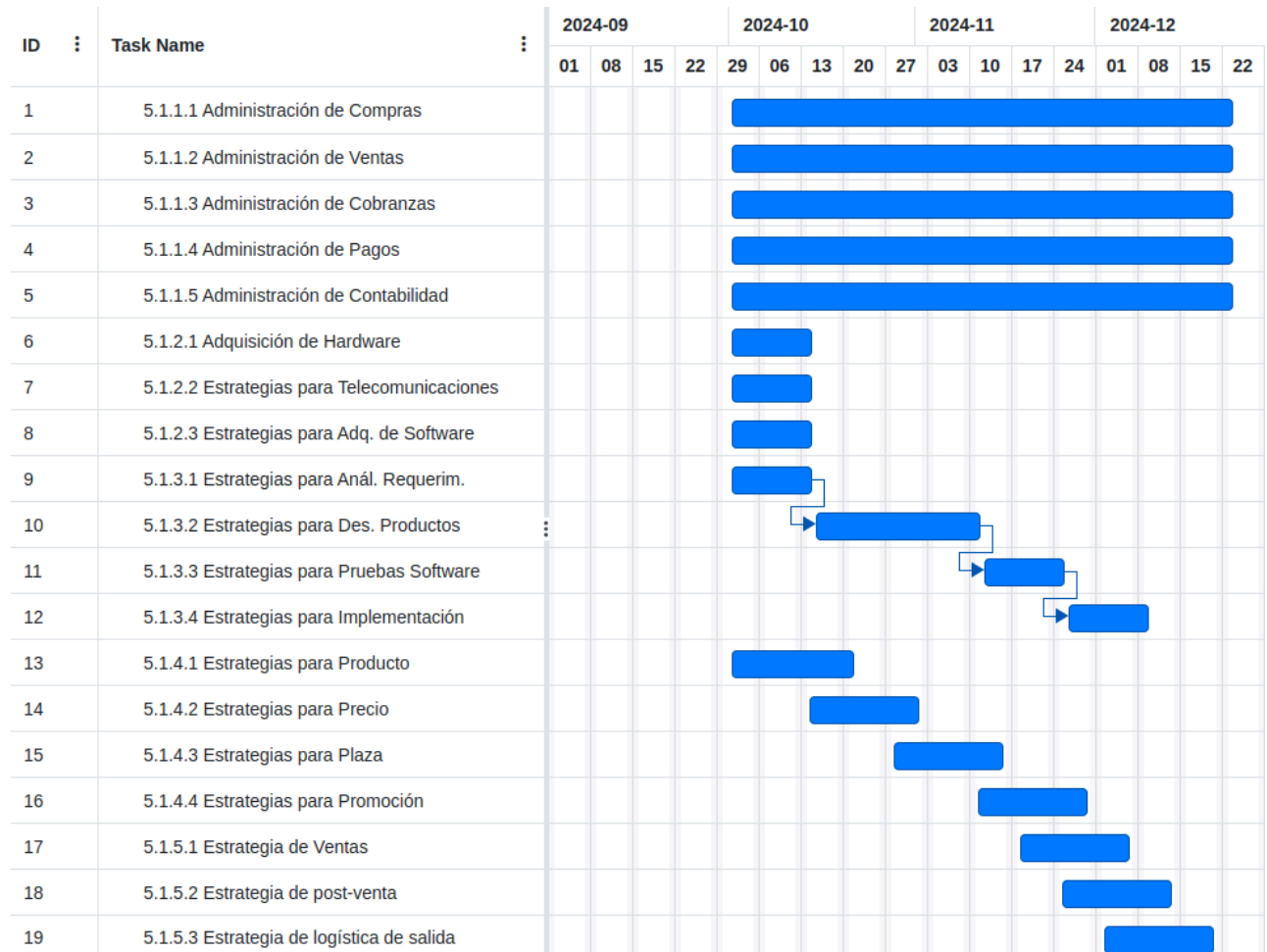
- Definir el proceso de entrega del servicio SecNet a los clientes.
- Establecer un sistema de gestión de la logística para asegurar que las entregas se realicen de forma eficiente y a tiempo.
- Implementar un sistema de seguimiento de las entregas para monitorear el estado de cada entrega.

5.3 Análisis de riesgos:

- **Riesgo 1: Falta de reconocimiento de marca.**
 - **Probabilidad:** Media
 - **Impacto:** Alto
 - **Plan de contingencia:** Implementar una estrategia de marketing y comunicación más agresiva, enfocada en la generación de conciencia de marca y la captación de clientes potenciales.
- **Riesgo 2: Cambios en la regulación de ciberseguridad.**
 - **Probabilidad:** Media
 - **Impacto:** Alto
 - **Plan de contingencia:** Monitorear la evolución del marco regulatorio y adaptar las estrategias de SecNet a los nuevos requisitos.
- **Riesgo 3: Dependencia de Wazuh.**
 - **Probabilidad:** Baja
 - **Impacto:** Alto
 - **Plan de contingencia:** Diversificar la base tecnológica de SecNet , invirtiendo en el desarrollo de soluciones propias.
- **Riesgo 4: Aparición de nuevas tecnologías de seguridad disruptivas.**
 - **Probabilidad:** Alta
 - **Impacto:** Medio
 - **Plan de contingencia:** Mantener un seguimiento constante de las tendencias tecnológicas en ciberseguridad y adaptar SecNet a las nuevas tecnologías que puedan surgir.
- **Riesgo 5: Inestabilidad económica en Argentina.**
 - **Probabilidad:** Alta
 - **Impacto:** Medio
 - **Plan de contingencia:** Ofrecer planes de pago flexibles y adaptar las estrategias de marketing y ventas en función de la situación económica del país.

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

5.4 Gantt



 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

6 Plan de Marketing

6.1 Objetivos de Marketing

Los objetivos de marketing para SecNet se enfocan en generar conciencia de marca, atraer clientes potenciales y fidelizar a los clientes existentes, con el fin de impulsar el crecimiento y el éxito del servicio.

Objetivos SMART:

- **Aumentar el conocimiento de marca de SecNet en un 20% en el mercado de las Pymes durante el año 2024.** Esto se evalúa a través de la cantidad de menciones de SecNet en medios de comunicación digitales y el número de usuarios que visitan el sitio web de Madrygal.
- **Captar al menos 20 nuevos clientes para SecNet durante Q1-2025.** Esto se mide mediante el número de contratos de servicio firmados.
- **Lograr una calificación promedio de satisfacción del cliente igual o superior a 4 de 5 estrellas en las encuestas de satisfacción realizadas durante el año 2024.**

Justificación de los objetivos:

- **Aumento del conocimiento de marca:** Es esencial para posicionar a SecNet como un servicio líder en el mercado. Un mayor conocimiento de marca permite a SecNet atraer a un público más amplio y generar más oportunidades de venta.
- **Captación de nuevos clientes:** Es fundamental para el crecimiento del negocio. Un aumento en el número de clientes permite a SecNet generar más ingresos y expandirse a nuevos mercados.
- **Satisfacción del cliente:** Es clave para fidelizar a los clientes existentes y para atraer nuevos clientes. Un alto nivel de satisfacción del cliente aumenta la retención y reduce la Tasa de abandono.

6.2 Resultados esperados en materia de cobertura y participación

SecNet busca alcanzar los siguientes resultados en materia de cobertura de mercado y participación:

Cobertura de mercado:

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 58 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- Argentina tiene unas 520.000 pymes en todo el país ¹². En CABA se concentran 25.3%, en Provincia de Buenos Aires 31.9%, sigue Santa Fe con 8.8%, Córdoba con 8.7%, Mendoza con 3.6% y Entre Ríos con 2.6%¹³
- En el país existen vinculados a Internet 83119 dispositivos de la marca. No disponemos de la identificación de las empresas, pero mediante el buscador Shodan si tenemos información de su IP, lo que facilita en parte su localización regional.
- **Alcanzar una cobertura del 2% del mercado de PyMEs que utilizan dispositivos Mikrotik a los tres años del lanzamiento de SecNet** . Esto significa que SecNet está presente en aproximadamente 1660 PyMEs de Argentina.

2. Participación en el mercado:

- **Obtener una participación del 2% del mercado de seguridad gestionada para PyMEs con equipos Mikrotik a los tres años de lanzamiento (1660 clientes)**. Se espera que SecNet genere aproximadamente 33.200 dólares en ingresos mensuales al final del sexto semestre.

Justificación:

Estos resultados se basaron en un análisis detallado del mercado de ciberseguridad para PyMEs, teniendo en cuenta la tasa de crecimiento del mercado, la cantidad de PyMEs potenciales y la demanda de soluciones de seguridad gestionada. También se consideró la capacidad de SecNet para ofrecer un valor diferencial y su potencial para captar nuevos clientes.

Estrategias para alcanzar los resultados:

- **Fortalecer la marca de SecNet** : Implementar una estrategia de marketing de contenidos, relaciones públicas y eventos para generar conciencia de marca y atraer clientes potenciales.
- **Ofrecer planes de servicio personalizados y competitivos**: Adaptar las soluciones de SecNet a las necesidades específicas de cada PyME y ofrecer precios competitivos.
- **Construir relaciones de largo plazo con los clientes**: Brindar un excelente servicio al cliente e implementar programas de fidelización para mantener la confianza de los clientes existentes.
- **Expandir la presencia de SecNet a nuevas regiones**: Implementar una estrategia de expansión estratégica que permita alcanzar una cobertura nacional.

¹² <https://www.somospymes.com.ar/informes/cuantas-pymes-existen-argentina-n5391016>

¹³ <https://www.comunidadbice.com.ar/mapa/>

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

6.3 Metas de Posicionamiento

SecNet se posiciona en la mente del consumidor objetivo como la **solución de seguridad gestionada más completa, proactiva y accesible para las PyMEs**, basada en tecnologías de código abierto y un enfoque centrado en el cliente.

Imagen que se quiere proyectar:

- **Confiable:** SecNet se percibe como un servicio seguro, fiable y estable, con un equipo de expertos en ciberseguridad que garantiza la protección de los activos digitales de los clientes.
- **Proactivo:** SecNet no se limita a reaccionar ante las amenazas, sino que busca anticiparlas mediante el uso de honeypots y el análisis de inteligencia de amenazas, brindando una protección más completa.
- **Personalizado:** SecNet se adapta a las necesidades específicas de cada PyME, ofreciendo un servicio flexible y personalizado, con soporte técnico continuo.
- **Accesible:** SecNet se ofrece a un precio competitivo, haciendo que la ciberseguridad sea accesible para las PyMEs con presupuestos limitados.
- **Innovador:** SecNet se encuentra a la vanguardia en la implementación de las últimas tecnologías de ciberseguridad, como Wazuh, DNSMasq y honeypots, brindando una solución más eficaz y moderna.

Comunicación de la imagen:

- La comunicación de SecNet se basa en un lenguaje claro, conciso y fácil de entender para el público objetivo.
- Se utilizan imágenes y vídeos atractivos para transmitir la confianza y la seguridad que ofrece SecNet.
- Se enfatiza el valor del servicio personalizado y la capacidad de SecNet para adaptarse a las necesidades específicas de cada cliente.

6.4 Producto. Estrategia de Producto

6.4.1 Descripción del producto SecNet

SecNet es un servicio de seguridad gestionada (MSSP) basado en la nube y en la integración de soluciones de software libre, diseñado para proteger a las PyMEs que utilizan routers de borde marca Mikrotik contra las amenazas cibernéticas.

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 60 de 120
---	--	----------------

	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

SecNet combina las siguientes tecnologías y servicios para ofrecer una solución integral y proactiva:

- **Wazuh:** Un SIEM de código abierto que recolecta y analiza eventos de seguridad provenientes de firewalls Mikrotik, agentes Wazuh en los equipos de la red y otras fuentes, como listas de reputación IP y URL.
- **Filtrado DNS:** Una máquina virtual con DNSMasq que filtra las consultas DNS mediante listas de reputación de dominios (URLs) para bloquear el acceso a sitios web maliciosos.
- **Filtrado de IP:** Las listas de reputación IP se despliegan en los firewalls Mikrotik para bloquear el tráfico desde y hacia direcciones IP conocidas como maliciosas.
- **Honeypots:** SecNet despliega honeypots en internet para atraer a los atacantes, analizar su comportamiento y obtener información sobre las nuevas amenazas.
- **Dashboard personalizado:** Brinda a los clientes una visión centralizada de la información de seguridad a través de una interfaz web intuitiva.
- **Servicio al cliente especializado:** El equipo de Madrygal, con experiencia y certificación en Wazuh, ofrece un servicio al cliente proactivo y personalizado.

SecNet NO es:

- **Un producto comercial enlatado.** SecNet se adapta a las necesidades específicas de cada cliente.
- **Un simple firewall o antivirus.** SecNet ofrece una protección integral y proactiva contra una amplia gama de amenazas.
- **Un sistema de seguridad que se gestiona localmente.** SecNet es un servicio en la nube que se gestiona de forma centralizada por Madrygal.

SecNet es un servicio de seguridad gestionada que integra diferentes tecnologías y servicios para ofrecer una protección completa y personalizada a las PyMEs, basada en tecnologías de código abierto y un enfoque centrado en el cliente.

6.4.2 ¿Es un producto/servicio durable, estacional?

SecNet es un **servicio durable**, no perecedero, y su demanda es constante, sin estacionalidad.

Justificación:

- **Servicio durable:** La ciberseguridad es un servicio esencial para las empresas en la actualidad. Las amenazas cibernéticas son constantes y la necesidad de proteger los activos digitales es permanente.
- **Demanda constante:** La demanda por servicios de ciberseguridad no tiene estacionalidad pronunciada. Las empresas necesitan protegerse de las amenazas cibernéticas a lo largo de todo el año.

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 61 de 120
---	--	----------------

	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Sin embargo, el consumo de servicios de ciberseguridad puede variar levemente en función de eventos específicos o tendencias del mercado, como la aparición de una nueva amenaza o un incremento de los ataques cibernéticos en ciertos periodos.

Madrygal debe monitorear las tendencias del mercado para adaptar su estrategia de marketing y ventas en función de la demanda de SecNet en diferentes épocas del año.

6.4.3 ¿Cuáles son las características de su producto/ servicio que usted considera influyen sobre la decisión de compra?

Las características de SecNet que consideramos más influyentes en la decisión de compra de las Pymes son:

Enfoque proactivo en la seguridad:

- **Prevención:** SecNet no se limita a reaccionar ante las amenazas cibernéticas, sino que busca anticiparse mediante el uso de honeypots y el análisis de inteligencia de amenazas.
- **Detección temprana:** Esto permite a las PyMEs identificar y mitigar las amenazas antes de que puedan causar daños significativos.

Solución integral:

- **Multicapa:** SecNet combina diferentes tecnologías y servicios para brindar una protección completa contra una amplia gama de amenazas.
- **Integración:** La integración de Wazuh, filtrado DNS e IP, y honeypots ofrece una visión centralizada del panorama de seguridad y permite una gestión más eficaz de los riesgos.

Servicio personalizado:

- **Adaptación a las necesidades del cliente:** SecNet se adapta a los requerimientos específicos de cada empresa.
- **Soporte técnico continuo:** Madrygal brinda un servicio al cliente proactivo y personalizado, con soporte técnico especializado en Wazuh.

Precios competitivos:

- **Modelo SaaS accesible:** SecNet es más accesible que las soluciones comerciales tradicionales de ciberseguridad, lo que lo hace atractivo para las PyMEs con presupuestos limitados.

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 62 de 120
---	--	----------------

	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Experiencia y confianza:

- **Equipo de expertos en ciberseguridad:** Madrygal cuenta con un equipo con amplia experiencia en ciberseguridad, lo que genera confianza en los clientes.
- **Uso de tecnologías de código abierto:** SecNet se basa en Wazuh, un SIEM de código abierto, lo que brinda a los clientes una mayor transparencia y confianza en la tecnología utilizada.

Los clientes valoran las siguientes características de SecNet :

- **Protección proactiva y completa**
- **Adaptabilidad y personalización**
- **Precio accesible**
- **Servicio al cliente excepcional**
- **Confianza en la experiencia de Madrygal**

6.4.4 ¿Existen estudios que respalden sus hipótesis?

Se han realizado estudios de mercado y se dispone de evidencia que respalda las hipótesis sobre las características de SecNet y su influencia en la decisión de compra:

Estudios de mercado:

- Se analizaron informes de la Cámara de Empresas de Software & Servicios Informáticos de la República Argentina (CESSI) y del Ministerio de Economía de Argentina, que indican un crecimiento sostenido en el mercado de ciberseguridad para PyMEs.
- Se realizaron encuestas a PyMEs para identificar sus necesidades de seguridad y sus preferencias de compra de servicios de seguridad gestionada.
- Se analizaron las tendencias de consumo en el mercado de software de ciberseguridad a través de plataformas de e-commerce, como Mercado Libre y Amazon.

Evidencia de la industria:

- La creciente cantidad de incidentes de seguridad informática en Argentina demuestra la necesidad de soluciones de seguridad gestionada.
- La alta demanda por servicios de seguridad gestionada en el mercado global, y en particular en países con contextos similares al argentino, respalda la hipótesis de que SecNet tiene una buena aceptación.

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 63 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Análisis de la competencia:

- Se analizaron las características y las debilidades de los principales competidores de SecNet, como FortiWeb, Lumu y otras soluciones comerciales. Este análisis permitió identificar los elementos diferenciadores de SecNet y su potencial para competir en el mercado.

Testimonios de clientes:

- Aunque SecNet aún no se ha lanzado al mercado, Madrygal cuenta con testimonios de clientes que han utilizado sus servicios de consultoría en ciberseguridad con Wazuh, lo que respalda la experiencia y la capacidad del equipo de Madrygal.

Conclusión:

La evidencia recopilada respalda las hipótesis sobre las características de SecNet y su influencia en la decisión de compra. El crecimiento del mercado de ciberseguridad para PyMEs en Argentina, la demanda de soluciones personalizadas y la creciente conciencia sobre la importancia de la seguridad informática son factores clave que favorecen la adopción de SecNet.

6.5 Precios. Estrategia de Precios

6.5.1 Condicionantes del precio

La determinación del precio de SecNet se basa en un análisis de los siguientes factores internos y externos:

Factores internos:

- Costos de desarrollo y operación:** SecNet requiere una inversión significativa en tecnología, infraestructura y personal cualificado. El costo de desarrollo y operación del servicio es un factor clave en la determinación del precio.
- Estructura de costos:** Madrygal tiene una estructura de costos flexible, con un enfoque en la optimización de los recursos. Esto le permite ofrecer precios competitivos sin comprometer la calidad del servicio.
- Margen de rentabilidad:** Madrygal busca obtener un margen de rentabilidad que le permita reinvertir en el desarrollo y la mejora de SecNet, y garantizar la sostenibilidad del negocio.
- Propuesta de valor diferencial:** SecNet se diferencia de la competencia por su enfoque proactivo en la seguridad, su integración de tecnologías de código abierto y

 SecNeT Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 64 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

su servicio personalizado. Esta propuesta de valor le permite a Madrygal justificar un precio superior al de sus competidores.

Factores externos:

- **Precios de la competencia:** El mercado de seguridad gestionada es bastante competitivo y los precios de las soluciones comerciales pueden variar considerablemente. SecNet se posiciona con un precio competitivo, teniendo en cuenta las necesidades de las PyMEs y el valor que ofrece su propuesta de valor.
- **Poder de negociación de los clientes:** Las PyMEs tienen un cierto poder de negociación en el mercado. SecNet debe ofrecer planes de servicio flexibles y precios competitivos para mantener la fidelización de sus clientes.
- **Condiciones del mercado:** El contexto económico y político de Argentina puede influir en la decisión de compra de las PyMEs. La inflación, la recesión y la devaluación del peso argentino pueden afectar la capacidad de las PyMEs para invertir en tecnología y ciberseguridad.
- **Tendencias tecnológicas:** La rápida evolución de las tecnologías de seguridad impacta en los costos de desarrollo y en la demanda de soluciones de seguridad. SecNet debe mantenerse al tanto de estas tendencias para ofrecer soluciones actualizadas y competitivas.

Dato adicional:

Se ofrece de manera adicional un VPS con Wazuh exclusivo para clientes a un tercio del valor que lo ofrece en la nube directamente Wazuh.com. A eso hay que agregarle como diferencial el soporte (el producto de Wazuh en nube no dispone de soporte).

Este dato adicional es un factor clave para la determinación del precio de SecNet . Madrygal puede utilizar este punto como una ventaja competitiva para atraer a los clientes que buscan una solución de seguridad más accesible y con un mejor soporte.

En conclusión, la determinación del precio de SecNet requiere un análisis cuidadoso de los factores internos y externos. El objetivo es establecer un precio competitivo que permita obtener una rentabilidad adecuada para Madrygal y que sea atractivo para los clientes potenciales.

6.5.2 Estrategia de precio

SecNet utiliza una **estrategia de precios competitivos por valor**, combinando precios atractivos con una propuesta de valor diferenciada para las PyMEs:

 SecNeT Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 65 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Precios competitivos:

- SecNet se posiciona con un precio más accesible que las soluciones tradicionales de seguridad comerciales, como FortiWeb y Lumu, principales competidores.
- El costo de licencias de SecNet es inferior al de los productos de la competencia, lo que lo hace más atractivo para las PyMEs con presupuestos limitados y en pesos.
- Se ofrecen diferentes planes de suscripción con precios escalonados en función de las necesidades del cliente, permitiendo que las PyMEs seleccionen el plan que mejor se adapte a sus requerimientos.

Propuesta de valor diferenciada:

- SecNet se diferencia de la competencia por su enfoque proactivo en la seguridad, su integración de Wazuh, DNSMasq y honeypots, y su servicio al cliente personalizado.
- El valor que SecNet brinda a los clientes es superior al de las soluciones tradicionales, lo que justifica un precio más elevado, pero competitivo en el mercado.

Enfoque en el cliente:

- Se consideran las necesidades específicas de cada cliente al momento de definir el precio del servicio.
- Se ofrecen descuentos y promociones especiales para atraer nuevos clientes y fidelizar a los clientes existentes.

Dato adicional:

Como dato adicional, el valor por usuario de SecNet es muy inferior al de las licencias de FortiWeb o Lumu. Este punto es un diferencial competitivo clave para SecNet y permite atraer a los clientes que buscan una solución de seguridad más accesible.

La estrategia de precios competitivos por valor de SecNet busca atraer a las PyMEs que buscan una solución de seguridad gestionada eficiente y accesible, sin comprometer la calidad del servicio. Se combinan precios competitivos con una propuesta de valor diferenciada para generar valor para el cliente y asegurar la rentabilidad del negocio.

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

6.6 CIM Comunicaciones integradas de marketing

6.6.1 Descripción de la planificación estratégica de las acciones de comunicación

La estrategia de comunicación de SecNet se basa en un enfoque integrado, que combina diferentes canales y mensajes para alcanzar a su público objetivo y generar un impacto positivo en la percepción de la marca.

Público Objetivo:

- **PyMEs:** SecNet se enfoca en las Pymes que buscan soluciones de seguridad gestionada para proteger sus activos digitales y garantizar la continuidad de sus negocios.
- **Decisores de compra:** El público objetivo son los gerentes de TI, los directores de seguridad y los dueños de las empresas que tienen la autoridad para tomar decisiones de compra de software y servicios de ciberseguridad.
- **Influenciadores:** Se busca la influencia de expertos en ciberseguridad y líderes de opinión en el sector para generar confianza en la marca.

Canales de comunicación:

- **Sitio web:** Se implementa un sitio web profesional y atractivo con información relevante sobre SecNet, los servicios que ofrece, la tecnología utilizada, casos de éxito y testimonios de clientes.
- **Redes sociales:** Se crean perfiles en las redes sociales más relevantes para el público objetivo, como LinkedIn, Twitter y Facebook, para generar contenido de valor, interactuar con los usuarios y difundir información sobre SecNet.
- **Eventos y conferencias:** Se participa en eventos y conferencias de ciberseguridad para posicionar a SecNet como un servicio líder y generar clientes potenciales.
- **Marketing de contenidos:** Se genera contenido educativo de alta calidad sobre ciberseguridad, como blogs, white papers y webinars, para educar al público objetivo y generar confianza en la marca.
- **Publicidad online:** Se utilizan plataformas de publicidad online para llegar a un público objetivo más amplio y generar clientes potenciales.
- **Relaciones públicas:** Se busca generar relaciones con medios de comunicación y expertos en ciberseguridad para promocionar SecNet y construir una reputación positiva de marca.
- **Relaciones institucionales:** Se realizan contactos con Federaciones y Cámaras empresarias para que promuevan los servicios a sus afiliados mediante convenios.

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

de beneficios, especialmente mediante charlas, jornadas o webinars sobre temas de actualidad en tecnología, ciberseguridad o ciberdelitos

Mensajes clave:

- **Seguridad proactiva y completa:** SecNet ofrece un enfoque proactivo en la seguridad, anticipándose a las amenazas y brindando una protección más completa.
- **Soluciones personalizadas:** SecNet se adapta a las necesidades específicas de cada cliente.
- **Precios competitivos:** SecNet es más accesible que las soluciones tradicionales de ciberseguridad.
- **Experiencia y expertise:** Madrygal cuenta con un equipo de expertos certificados en Wazuh que garantiza un servicio altamente especializado.

Presupuesto:

- Se destina un presupuesto acotado, incluido en la sección de gastos por periodo para las acciones de marketing y comunicación de SecNet durante el plan trianual.
- El uso de redes sociales y eventos permite la ejecución de la estrategia con mínima inversión.

Seguimiento y evaluación:

- Se monitorea el impacto de las acciones de marketing y comunicación a través de indicadores clave, como el número de menciones de marca, el número de usuarios que visitan el sitio web, el número de clientes captados y el nivel de satisfacción del cliente.
- Se realizan ajustes y mejoras en las acciones de marketing y comunicación en función de los resultados obtenidos.

Con esta estrategia de comunicación integrada, SecNet busca posicionarse como un servicio de seguridad gestionada líder en el mercado de las Pymes , atraer nuevos clientes y fidelizar a los clientes existentes.

Programa de referidos:

- Se implementa un programa de comisiones para aquellos colegas que traigan un cliente que utilice los servicios o productos de Madrygal por suscripción como SecNet o Wazuh..
- El programa de referidos ayuda a expandir la base de clientes de Madrygal y SecNet y a fortalecer las relaciones con los profesionales de la industria.

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 68 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Contacto constante con el cliente:

- El equipo técnico comercial de Madrygal mantiene contacto constante con los clientes para poder fidelizarlos y ofrecerles más productos del portfolio.
- Este enfoque ayuda a construir relaciones de largo plazo con los clientes y a generar más oportunidades de venta cruzada.

Limitación en las posibilidades de expansión:

- La estrategia de Madrygal no apunta a un crecimiento explosivo, se enfoca en la fidelización de los clientes existentes y en el desarrollo de un crecimiento paulatino, permitiendo también el paulatino y firme crecimiento de su plantilla profesional.

6.6.2 Diseño del Sitio web

El diseño del sitio web de SecNet se integra en el sitio web actual de Madrygal, <https://www.madrygal.com.ar>, adaptándolo a las necesidades específicas del producto y al enfoque estratégico de marketing de SecNet . Se utiliza software libre para su implementación, basado en la plataforma Odoo (ERP, CRM, E-commerce, E-learning, Marketing digital). De igual manera se reserva el dominio <https://www.SecNet.com.ar> para posicionar la marca en los buscadores.

Diseño general:

- **Imagen profesional y confiable:** El sitio web se diseña con una estética limpia, moderna y profesional, que transmita confianza y seguridad. Se utilizan colores y tipografías que reflejen la imagen de seriedad y experiencia de Madrygal y SecNet .
- **Enfoque en el usuario:** El sitio web es fácil e intuitivo de navegar, con un menú claro y conciso que permita a los usuarios encontrar rápidamente la información que buscan.
- **Diseño responsive:** El sitio web se adapta a diferentes dispositivos, como computadoras de escritorio, tabletas y teléfonos móviles, para asegurar una experiencia óptima para todos los usuarios.

Secciones principales:

- **Inicio:** Presenta una breve descripción de SecNet , su propuesta de valor y los beneficios para las PyMEs. Incluye un llamado a la acción para contactar con Madrygal y solicitar una demostración del servicio.
- **Servicios:** Detalla los diferentes servicios que ofrece SecNet , incluyendo Wazuh SIEM, filtrado DNS e IP para plataformas Mikrotik y servicios de gestión de

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 69 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

incidentes. Cada sección incluye una descripción detallada del servicio, los beneficios para el cliente y un llamado a la acción para obtener más información.

- **Casos de éxito:** Presenta ejemplos de cómo SecNet ha ayudado a las PyMEs a mejorar su seguridad informática. Cada caso de éxito incluye una descripción de la problemática y cómo SecNet les ayudó a resolverla. Los datos de clientes se manejan por convenios de confidencialidad.
- **Clientes:** Muestra un listado de las actividades de los clientes de Madrygal, destacando la diversidad de sectores y tamaños de las empresas. No pondremos un listado de los mismos salvo que se disponga la expresa autorización del cliente. Al ser una consultora de ciberseguridad, la mayoría de las actividades se rigen por convenios de confidencialidad. Por otro lado, exponer sus nombres o datos podría “invitar” a actores maliciosos a realizar ataques a su infraestructura.
- **Equipo:** Presenta al equipo de expertos de Madrygal, destacando su experiencia y su conocimiento en ciberseguridad. Incluye fotos y biografías de los miembros del equipo de Madrygal.
- **Blog:** Publica artículos informativos y de actualidad sobre ciberseguridad, las últimas amenazas y las mejores prácticas de seguridad.
- **Contacto:** Proporciona información de contacto con Madrygal para que los usuarios puedan solicitar una demostración del servicio, hacer consultas o recibir más información.

Funcionalidad:

- **Formulario de contacto:** Permite a los usuarios enviar consultas o solicitar una demostración del servicio.
- **Descarga de contenidos:** Permite a los usuarios descargar información relevante, como folletos, white papers y casos de éxito.
- **Registro de usuarios:** Permite a los usuarios registrarse para recibir información sobre SecNet y los servicios de Madrygal. Mensualmente se envía un newsletter.
- **Integración con redes sociales:** Permite a los usuarios compartir contenido de SecNet en las redes sociales o ver las publicaciones en las redes de Madrygal.

Usabilidad:

- **Navegación intuitiva:** El sitio web se diseña para que sea fácil de navegar y que los usuarios puedan encontrar rápidamente la información que buscan.
- **Diseño responsive:** El sitio web se adapta a diferentes dispositivos, como computadoras de escritorio, tabletas y teléfonos móviles, para asegurar una experiencia óptima para todos los usuarios.

Alineación con la imagen y los objetivos:

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 70 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

El diseño del sitio web de SecNet esta alineado con la imagen que se quiere proyectar y con los objetivos del proyecto:

- **Imagen profesional y confiable:** El sitio web transmite confianza y seguridad a los clientes potenciales, lo que es fundamental para un servicio de ciberseguridad.
- **Enfoque en el cliente:** El sitio web está diseñado para facilitar la experiencia del usuario y brindar un servicio de alta calidad.
- **Atraer nuevos clientes:** El sitio web está optimizado para la generación de clientes potenciales y para promocionar los beneficios de SecNet .
- **Fidelizar a los clientes existentes:** El sitio web incluye contenido de valor y herramientas para mejorar la relación con los clientes y mantener su satisfacción.

El sitio web de SecNet es una herramienta esencial para el éxito del producto y core de la estrategia de marketing electrónico. Ayuda a generar conciencia de marca, atraer nuevos clientes y fidelizar a los clientes existentes.

Con esta estrategia de comunicación integrada, SecNet busca posicionarse como un servicio de seguridad gestionada líder en el mercado de las Pymes , atraer nuevos clientes y fidelizar a los clientes existentes.

6.7 Distribución

6.7.1 Factores condicionantes de la distribución - Principales canales

Los factores que influyen en la elección de los canales de distribución de SecNet son:

- **Naturaleza del servicio:** SecNet es un servicio digital que se ofrece a través de la nube. Esto limita las opciones de distribución tradicionales, como la venta a través de tiendas físicas.
- **Enfoque en las PyMEs:** SecNet se enfoca en las Pymes , que suelen tener un presupuesto limitado y que no siempre tienen la capacidad de gestionar complejas operaciones de compra.
- **Servicio personalizado:** SecNet se caracteriza por ofrecer un servicio personalizado y de alta calidad, lo que requiere un canal de distribución que permita un contacto directo con el cliente.

Principales canales de distribución:

- **Sitio web:** El sitio web de SecNet es la principal herramienta de distribución. Permite a los clientes potenciales obtener información sobre el servicio, solicitar una demostración y contactar con el equipo de Madrygal.

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 71 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- **Redes sociales:** Las redes sociales se utilizan para promocionar SecNet y para interactuar con los usuarios y generar clientes potenciales.
- **Eventos y conferencias:** Se participa en eventos y conferencias de ciberseguridad para promocionar SecNet y para establecer contactos con clientes potenciales.
- **Marketing de contenidos:** Se genera contenido educativo sobre ciberseguridad y las ventajas de SecNet para generar conciencia de marca y atraer clientes potenciales.
- **Programa de referidos:** Se ofrece un programa de comisiones para aquellos colegas que traigan un cliente que utilice los servicios o productos de Madrygal por suscripción.

6.7.2 Estrategia de distribución

SecNet aplica una estrategia de distribución **directa**, enfocada en la relación directa con el cliente y el objetivo de la fidelización.

Canales de distribución:

- **Sitio web:** El sitio web de SecNet es el principal canal de distribución. Permite a los clientes potenciales obtener información sobre el servicio, solicitar una demostración y contactar con el equipo de Madrygal.
- **Redes sociales:** Las redes sociales se utilizan para promocionar SecNet y para interactuar con los usuarios y generar clientes potenciales.
- **Eventos y conferencias:** Se participa en eventos y conferencias de ciberseguridad para promocionar SecNet y para establecer contactos con clientes potenciales.

6.7.3 Canales (tipo y nivel)

Los canales de distribución de SecNet se clasifican como **directos** y se ubican en el **nivel de cliente final**.

- **Sitio web:** Es un canal directo de distribución que permite a los clientes potenciales acceder a la información sobre el servicio, solicitar una demostración y contactar con el equipo de Madrygal.
- **Redes sociales:** Las redes sociales son un canal directo de distribución que permite a Madrygal interactuar con los usuarios y generar clientes potenciales.
- **Eventos y conferencias:** Los eventos y conferencias son un canal directo de distribución que permiten a Madrygal establecer contactos con clientes potenciales y promocionar SecNet .

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 72 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

La estrategia de distribución directa permite a la consultora mantener un control directo sobre la relación con el cliente, personalizar el servicio y construir relaciones de largo plazo.

6.7.4 Análisis de localización de puntos de venta propios

Dado el tipo de servicios que ofrece SecNet , no se contempla la apertura de puntos de venta físicos propios.

Enfoque en la presencia online:

- La estrategia de distribución de SecNet se basa en la **presencia online**, utilizando el sitio web como principal canal de distribución y las redes sociales para generar conciencia de marca y atraer clientes potenciales.
- Se prioriza la optimización del sitio web para que sea fácil de navegar, intuitivo y atractivo para los usuarios y para que cumpla con las necesidades de marketing y ventas.

Oficina para atención de clientes corporativos:

- SecNet dispone a mediano plazo una oficina para atender a los clientes corporativos de forma presencial de ser necesario.
- La ubicación de esta oficina se determina en función de la concentración de las PyMEs objetivo, y se privilegia una ubicación estratégica y accesible.

Ventajas de la presencia online:

- **Mayor alcance:** El sitio web y las redes sociales permiten alcanzar a un público más amplio que un punto de venta físico.
- **Menor costo:** La presencia online es más económica que la apertura de puntos de venta físicos.
- **Flexibilidad:** El sitio web y las redes sociales se pueden actualizar de forma fácil y rápida, lo que permite adaptar la estrategia de marketing a las necesidades del mercado.

Ventajas de la oficina para atención de clientes:

- **Relación personalizada:** Permite establecer una relación más estrecha y personalizada con los clientes corporativos.
- **Servicio más completo:** Permite ofrecer servicios de consultoría más complejos y personalizados que no se pueden ofrecer a través del sitio web.

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 73 de 120
---	--	----------------

	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

La estrategia de distribución de SecNet se enfoca en la presencia online para alcanzar un público más amplio y para optimizar los costos de marketing. La oficina para atención de clientes corporativos se utiliza como un complemento de la estrategia online.

6.7.5 Opciones de asociación

SecNet es un producto cuyo mercado objetivo actual son los dispositivos de marca Mikrotik, por eso se considera establecer asociaciones estratégicas para ampliar su alcance y mejorar la distribución del servicio:

Mayoristas de equipos Mikrotik:

- **Descripción:** Son empresas que comercializan equipos Mikrotik a gran escala y que tienen una amplia red de distribución.
- **Beneficios:**
 - Acceso a una audiencia más amplia de PyMEs que ya utilizan tecnología Mikrotik.
 - Mayor visibilidad de SecNet en el mercado de las PyMEs que utilizan equipos Mikrotik.
 - Posibilidad de generar una relación de confianza y colaboración con los mayoristas para el desarrollo de acciones de marketing conjuntas.
- **Modalidad:** Se podrían establecer acuerdos de colaboración en los que los mayoristas promocionen SecNet a sus clientes, con comisiones por suscripciones pero también potenciando sus ventas de equipamiento al contar con nuevos servicios para esos equipos.

Cámaras empresariales de ISPs:

- **Descripción:** Son organizaciones que agrupan a pequeños y medianos ISPs (Proveedores de Servicios de Internet) que utilizan mayormente tecnología Mikrotik.
- **Beneficios:**
 - Acceso a un segmento específico de PyMEs con una alta demanda de soluciones de ciberseguridad.
 - Posibilidad de generar alianzas estratégicas para ofrecer servicios de ciberseguridad completos y personalizados a los ISPs.
 - Mayor conocimiento de las necesidades y los desafíos de los ISPs en materia de ciberseguridad.
- **Modalidad:** Se podrían establecer acuerdos de colaboración en los que las cámaras empresariales promocionen SecNet a sus miembros y un paquete de beneficios por cada venta que se concrete.

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Empresas de consultoría en ciberseguridad:

- **Descripción:** Son empresas que brindan servicios de consultoría en ciberseguridad a las PyMEs.
- **Beneficios:**
 - Acceso a una red de clientes potenciales que ya conocen la importancia de la ciberseguridad.
 - Posibilidad de colaborar con empresas de consultoría para ofrecer servicios complementarios y crear soluciones integradas de ciberseguridad.
 - Mayor reconocimiento de marca en el sector de la ciberseguridad.
- **Modalidad:** Se podrían establecer acuerdos de colaboración en los que las empresas de consultoría recomienden SecNet a sus clientes y reciban comisiones por cada venta que se concrete.

Consideraciones:

- Es importante seleccionar socios estratégicos que compartan los mismos valores y objetivos que Madrygal y SecNet .
- Se establecen acuerdos de colaboración claros y beneficiosos para todas las partes involucradas (Win-Win).

Estas asociaciones no limitan las actuales acciones de vinculación con Federaciones y Cámaras empresarias de diversos rubros y actividades con los que se realizan convenios, sino que son más específicas y requieren una estrategia de atención diferenciada.

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

7. Operaciones

7.1 Organización de la empresa

La estructura organizativa de Madrygal se basa en un modelo **matricial**, que combina elementos de la estructura funcional con la estructura divisional. Esta estructura le permite a Madrygal ser más flexible y adaptarse a las necesidades de las PyMEs y a las tendencias del mercado.

Principales departamentos:

- **Junta directiva:** Está formada por los 4 socios fundadores, que toman las decisiones estratégicas y supervisan el funcionamiento general de la empresa.
- **Tecnología:** Se encarga del desarrollo y la implementación de las soluciones de ciberseguridad, incluyendo la gestión de la infraestructura tecnológica.
- **Comercial:** Se encarga de la gestión de clientes, relaciones institucionales y ventas. El marketing y la administración están tercerizadas y gestionadas desde esta área.

7.2 Grupo fundador

- **Grupo fundador:** Madrygal fue fundada por cuatro profesionales, quienes poseen una amplia experiencia en el sector de las tecnologías de la información y la ciberseguridad.
- **Composición del directorio:** El directorio de Madrygal está formado por los 4 socios fundadores, quienes toman las decisiones en conjunto.

7.3 Composición del staff gerencial y perfil de los ejecutivos claves.

- **Staff gerencial:** El equipo directivo de Madrygal está formado por los 4 socios fundadores, que desempeñan los siguientes roles:
 - **Gerente de Tecnología:** Se encarga del desarrollo y la implementación de las soluciones de ciberseguridad.
 - **Gerente de Comercialización:** Se encarga de la gestión de clientes, las relaciones y las ventas. Marketing y administración están tercerizadas.
- **Perfil de los ejecutivos claves:** Los socios fundadores poseen una amplia experiencia en el sector de las tecnologías de la información y la ciberseguridad. Han desarrollado exitosas carreras en otras empresas tecnológicas de las que también son socios y tienen un profundo conocimiento del mercado. Madrygal nace específicamente para brindar servicios de ciberseguridad. Sus habilidades y experiencia son relevantes para el éxito de Madrygal y del producto SecNet .

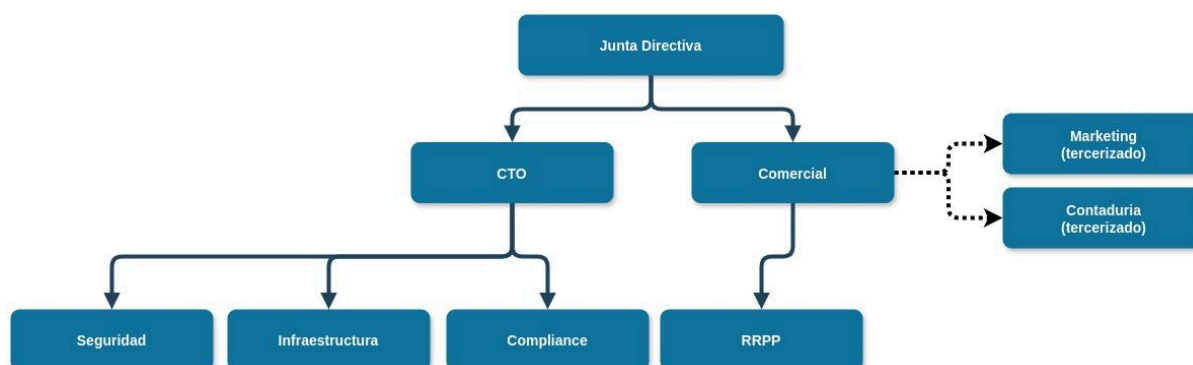
	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 76 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

7.4 Estructura prevista al lanzamiento y evolución

- **Estructura prevista al lanzamiento:** En la fase de lanzamiento, Madrygal cuenta con un equipo pequeño, formado por los 4 socios fundadores y un pequeño equipo de profesionales adicionales bajo la modalidad de contratación por demanda.
- **Evolución:** A medida que el negocio crece, Madrygal amplía su equipo, con nuevos departamentos y contratando más personal.
 - **Departamento de Marketing:** Se crea un departamento de marketing para implementar las estrategias de marketing y generar clientes potenciales.
 - **Departamento de Producción:** Se crea un departamento de producción para desarrollar y mantener las soluciones de ciberseguridad, que dependería del CTO

Organigrama:



7.5 Filosofía y sistema de trabajo

La filosofía de trabajo de Madrygal se basa en los siguientes valores:

- **Compromiso con la excelencia:** Madrygal se compromete a brindar soluciones de ciberseguridad de alta calidad, manteniendo los más altos estándares de seguridad y ética profesional.
- **Orientación al cliente:** Madrygal se centra en entender las necesidades de sus clientes y en ofrecer soluciones personalizadas que satisfagan sus expectativas.
- **Trabajo en equipo:** Madrygal fomenta un ambiente de colaboración y trabajo en equipo, donde cada miembro aporta sus habilidades y experiencia para alcanzar los objetivos comunes.
- **Innovación:** Madrygal busca constantemente nuevas soluciones y tecnologías para mejorar sus servicios y ofrecer a sus clientes las mejores herramientas de seguridad.

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- **Profesionalismo:** Madrygal se esfuerza por mantener los más altos estándares de profesionalismo en todos sus servicios y relaciones.

Sistema de trabajo:

- **Trabajo colaborativo:** Madrygal fomenta el trabajo en equipo y la comunicación abierta entre los miembros del equipo.
- **Metodologías ágiles:** Madrygal utiliza metodologías ágiles de desarrollo de software para adaptarse a los cambios del mercado y para responder rápidamente a las necesidades de los clientes.
- **Orientación al cliente:** Madrygal prioriza la satisfacción del cliente y se esfuerza por brindar un servicio personalizado y de alta calidad.

7.6 Requerimientos en materia de RRHH

- **Cantidad de personas:** En la fase de lanzamiento, Madrygal cuenta con un equipo de aproximadamente 6 personas, incluyendo los 4 socios fundadores.
- **Perfil de los candidatos:** Se busca personal con experiencia en el sector de las tecnologías de la información y la ciberseguridad, con conocimiento de Wazuh, redes, internet, software libre y otras herramientas de seguridad. Se valora la capacidad de trabajo en equipo, la comunicación eficaz y la orientación al cliente.
- **Estrategias de reclutamiento y selección:** Madrygal utiliza una combinación de estrategias de reclutamiento, incluyendo la publicación de ofertas de trabajo en portales especializados y en redes sociales, el contacto con universidades y centros de investigación, y la recomendación de profesionales de confianza.
- **Capacitación:** Madrygal invierte en la capacitación de su equipo para asegurar que todos los miembros cuentan con las habilidades y los conocimientos necesarios para brindar un servicio de alta calidad.

Contar con un equipo competente y capacitado, permite brindar un servicio de seguridad gestionada de alta calidad y con un alto nivel de satisfacción para el cliente.

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

8 PLAN FINANCIERO-ECONÓMICO

8.1 Modelo de Ingresos:

- **Fuente de ingresos:** Licencias de software SecNet (una por dispositivo suscripto). Al ser un producto adicional de una consultora, se asume que no existen otros ingresos directamente relacionados con SecNet en esta etapa.
- **Precio de venta:** \$25 por licencia mensual.
- **Proyecciones de ventas:** Basado en el crecimiento proyectado de clientes:
 - Año 1: 100 clientes promedio * \$25/cliente * 12 meses = \$30,000
 - Año 2: 500 clientes promedio * \$25/cliente * 12 meses = \$150,000
 - Año 3: 1380 clientes promedio * \$25/cliente * 12 meses = \$414,000

8.2 Modelo de Egresos:

- **Costos Operativos:** Estos costos incluyen energía, internet, y horas de soporte de personal junior. A partir del segundo año, se incluye la suscripción mensual de \$300 a servicios de inteligencia de amenazas para mejorar el servicio.
 - Año 1: \$1,500 mensuales * 12 meses = \$18,000
 - Año 2: (\$3,000 + \$300) mensuales * 12 meses = \$39,600
 - Año 3: (\$4,500 + \$300) mensuales * 12 meses = \$57,600
- **Remuneraciones y cargas sociales:** NO APLICA. Al ser un producto adicional sin personal dedicado, no hay costos de remuneraciones ni cargas sociales directamente atribuibles a SecNet. Las horas de soporte al cliente están cuantificadas en el ítem “costos operativos”

Hay previsto un margen de comisión de \$5 por cada licencia vendida si se hace por canales externos o el recurso comercial interno, esto debe incluirse en los egresos. Como el precio de la licencia es de \$25, y suponemos que la comisión se paga sobre este precio sobre el total de licencias vendidas, el impacto en los costos es proporcional al número de clientes.

- **Cálculo del costo de comisión:**
 - Año 1: 100 clientes * 12 meses * \$5/cliente = \$6,000
 - Año 2: 500 clientes * 12 meses * \$5/cliente = \$30,000
 - Año 3: 1380 clientes * 12 meses * \$5/cliente = \$82,800

8.3 Modelo de Inversión:

La inversión total de \$6,000 se desglosa de la siguiente manera:

 SecNeT Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 79 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- **Activos Fijos:**
 - 2 Servidores: \$1,500/servidor * 2 servidores = \$3,000
- **Activos Intangibles:**
 - Desarrollo de Software: \$2,000
- **Capital de Trabajo (Marketing Inicial):**
 - \$1,000
- **Total Inversión:** \$3,000 + \$2,000 + \$1,000 = \$6,000

8.4 Amortizaciones y Depreciaciones:

- **Depreciación de Servidores:**
 - Valor: \$3,000
 - Vida útil (asumida): 5 años
 - Método de depreciación: Línea recta
 - Depreciación anual: \$3,000 / 5 años = \$600/año
- **Amortización de Software:**
 - Valor: \$2,000
 - Vida útil (asumida): 5 años
 - Método de amortización: Línea recta
 - Amortización anual: \$2,000 / 5 años = \$400/año
- **Marketing Inicial:** Se considera un gasto en el momento en que se incurre, por lo que no se amortiza ni deprecia.

8.5 Impuestos: Impuesto a las ganancias

Si SecNet se considera parte integral de las operaciones de la consultora y no una entidad separada, entonces, desde una perspectiva contable, no se calcularía un impuesto a las ganancias *aislado* para SecNet. Los ingresos y egresos de SecNet se consolidan con los de la consultora, y el impuesto a las ganancias se calcula sobre el resultado global de la consultora.

Sin embargo, para evaluar la rentabilidad de SecNet como proyecto o producto dentro de la consultora, es útil considerar el impacto impositivo *potencial* que tendría si fuera una entidad independiente. Esto permite entender mejor la contribución de SecNet a la rentabilidad global de la consultora.

Dos enfoques:

1. **Sin cálculo de impuesto a las ganancias para SecNet:** En este caso, simplemente se omite el cálculo del impuesto a las ganancias en la sección 8.5, y el flujo de caja libre calculado anteriormente se considera el flujo de caja después de

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

impuestos. Se debe aclarar en la sección que SecNet se integra a la contabilidad general de la consultora y que no se calcula un impuesto a las ganancias separado para el producto.

2. **Cálculo del impuesto a las ganancias *potencial*:** Se calcula el impuesto a las ganancias *como si* SecNet fuera una entidad independiente, aplicando la tasa impositiva corporativa correspondiente a la jurisdicción. Esto brinda una idea de la rentabilidad de SecNet después de impuestos. Sin embargo, es importante aclarar que este cálculo es sólo para fines de análisis y que el impuesto real se calcula a nivel de la consultora integrando otras actividades, gastos e ingresos..

Con una tasa de impuesto a las ganancias del 35%, el flujo de caja libre y las métricas de rentabilidad utilizaremos la opción 2 a fines de cálculo aislado

8.6 Impuestos a los Ingresos Brutos:

La consultora Madrygal dispone de la exención de pago de IIBB en la jurisdicción de Santa Fe, ya que se adhiere a los beneficios de la economía del conocimiento. Las empresas desarrolladoras de software están exceptuadas del pago de IIBB previa inspección y acreditación de las actividades.

8.7 Remuneraciones y cargas sociales:

Tal como fue aclarado en los párrafos anteriores, no se calculan remuneraciones ni cargas sociales ya que el producto es parte del portfolio de una consultora. Se utilizan algunas horas de soporte que están contempladas en el costo operativo.

8.8 Presupuesto Financiero: (con Imp. ganancias del 35%):

Descripción	Año 0	Año 1	Año 2	Año 3
Ingresos Totales		\$30,000	\$150,000	\$414,000
Costos Operativos		\$18,000	\$39,600	\$57,600
Comisión de Ventas		\$6,000	\$30,000	\$82,800
Depreciación		\$600	\$600	\$600
Amortización		\$400	\$400	\$400
Ganancia antes de Impuestos		\$5,400	\$80,000	\$273,200

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Impuesto a las Ganancias (35%)		\$1,890	\$28,000	\$95,620
Flujo de Caja Libre (después de impuestos)	-\$6,000	\$3,510	\$51,400	\$176,980

8.9 Evaluación de la Inversión:

Datos:

- Inversión inicial: \$6,000
- Flujo de caja libre (después de impuestos):
 - Año 1: \$3,510
 - Año 2: \$51,400
 - Año 3: \$176,980
- Tasa de descuento (para el VAN): 10%

Cálculos:

- **VAN (10%):**

$$VAN = (3510 / 1.1) + (51400 / 1.1^2) + (176980 / 1.1^3) - 6000$$

$$VAN = 3190.91 + 42479.34 + 134447.34 - 6000$$

$$VAN \approx 174117.59$$
- **TIR:** Utilizando una calculadora financiera o software (como Excel o una calculadora online de TIR), la TIR para estos flujos de caja es aproximadamente **160%**.
- **Payback:**
 - Año 1: \$3.510
 - Restante: \$6.000 - \$3.510 = \$2.490
 - Año 2 (fracción): \$2.490 / \$51.400 $\approx$ 0,048
 - Payback: 1 + 0,048 $\approx$ < 13 meses
- **VAN (10%):** \$174.118
- **TIR:** 160%
- **Payback:** (< 13 meses)

Aunque el impuesto a las ganancias reduce la rentabilidad, el proyecto sigue siendo financieramente viable con un VAN positivo y una TIR significativamente mayor que la tasa de descuento. El payback de poco más de un año también es un indicador positivo.

El análisis incluye valores extremos en un escenario ampliamente pesimista en erogaciones impositivas y operativas:

- Se tributa el total de ganancias por los ingresos netos (35%)
- Se abona comisión de ventas por el total de las licencias.

 SecNeT Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 82 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

8.10 Escenarios de Riesgo:

Escenario Probable (Base): Utilizaremos los datos anteriores.

Descripción	Año 1	Año 2	Año 3
Ingresos	\$30,000	\$150,000	\$414,000
Costos	\$25,000	\$69,600	\$140,400
FCL (Después de Impuestos)	\$3,510	\$51,400	\$176,980

Escenario Optimista (Ventas +25%, Costos -15%):

Descripción	Año 1	Año 2	Año 3
Ingresos	\$37,500	\$187,500	\$517,500
Costos	\$21,250	\$59,160	\$120,000
FCL (Después de Impuestos)	\$10,368.75	\$89,670	\$263,853.75

Cálculos optimistas:

- Ingresos: Valor base * 1,25
- Costos: Valor base * 0,85
- FCL: (Ingresos - Costos) * (1 - 0,35) Aplicando el 35% de impuesto a las ganancias

Escenario Pesimista (Ventas -25%, Costos +15%):

Descripción	Año 1	Año 2	Año 3
Ingresos	\$22,500	\$112,500	\$310,500
Costos	\$28,750	\$79,960	\$160,400
FCL (Después de Impuestos)	-\$4,261.25	\$21,060	\$97,476.25

Cálculos pesimistas:

- Ingresos: Valor base * 0.75
- Costos: Valor base * 1.15
- FCL: (Ingresos - Costos) * (1 - 0.35) Aplicando el 35% de impuesto a las ganancias

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Comparativas

Descripción	Escenario Probable	Escenario Optimista	Escenario Pesimista
Año 1			
Ingresos	\$30,000	\$37,500	\$22,500
Costos	\$25,000	\$21,250	\$28,750
FCL (Después de Impuestos)	\$3,510	\$10,368.75	-\$4,261.25
Año 2			
Ingresos	\$150,000	\$187,500	\$112,500
Costos	\$69,600	\$59,160	\$79,960
FCL (Después de Impuestos)	\$51,400	\$89,670	\$21,060
Año 3			
Ingresos	\$414,000	\$517,500	\$310,500
Costos	\$140,400	\$120,000	\$160,400
FCL (Después de Impuestos)	\$176,980	\$263,853.75	\$97,476.25

Análisis de los escenarios:

El escenario optimista muestra un aumento significativo en la rentabilidad, mientras que el escenario pesimista resulta en pérdidas en el primer año y una rentabilidad mucho menor en los años siguientes. Esto resalta la importancia de monitorear de cerca las ventas y los costos, y de tener un plan de contingencia para mitigar los riesgos en caso de que el escenario pesimista se materialice.

8.11 Plan de Contingencia

El análisis de escenarios (8.10) ha identificado un posible escenario pesimista donde las ventas son menores y los costos mayores a lo proyectado. Este plan de contingencia describe las acciones a tomar si el proyecto comienza a acercarse a ese escenario. El

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

objetivo es minimizar las pérdidas y volver al escenario probable o, idealmente, al escenario optimista.

Disparadores:

- **Ventas:** Si las ventas al final del primer semestre son un 20% menores a lo proyectado (menos de 40 clientes), activar el plan de contingencia.
- **Costos:** Si los costos operativos superan el presupuesto en un 10% durante dos meses consecutivos, activar el plan de contingencia.

Acciones:

1. Aumentar las Ventas:

- **Marketing Intensificado:** Incrementar la inversión en marketing digital, enfocándose en campañas de pago por clic (PPC) y optimización para motores de búsqueda (SEO) para atraer más clientes potenciales.
- **Programas de Referidos:** Implementar un programa de referidos para incentivar a los clientes existentes a recomendar SecNet.
- **Alianzas Estratégicas:** Realizar alianzas con otras empresas del sector para llegar a un público más amplio.
- **Ajustes de precios (con cautela):** Explorar la posibilidad de ofrecer descuentos o promociones temporales para impulsar las ventas, o se ajustan los precios si el mercado lo permite.
- **Mejora del producto:** Si la baja en ventas se debe a la falta de alguna característica o funcionalidad, priorizar el desarrollo de mejoras en el producto para hacerlo más atractivo.

2. Reducir Costos:

- **Renegociación de contratos:** Revisar los contratos con proveedores para buscar mejores condiciones y reducir costos.
- **Optimización de recursos:** Analizar los gastos operativos para identificar áreas donde se puedan reducir costos sin afectar la calidad del servicio. Esto puede incluir la reducción de gastos en energía, internet, o herramientas de software.
- **Postergar inversiones:** Postergar inversiones no esenciales hasta que la situación financiera mejore.
- **Reducción de horas de soporte:** Optimizar los procesos de soporte para reducir las horas de personal junior dedicadas a SecNet, priorizando la automatización y la documentación.

3. Financiación Adicional (último recurso):

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 85 de 120
---	--	----------------

	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- **Búsqueda de inversión:** Se explora la posibilidad de buscar financiación adicional a través de inversores ángeles, capital semilla, o préstamos para cubrir las necesidades de capital de trabajo en caso de un escenario pesimista prolongado.

Monitoreo y Evaluación:

- **Seguimiento mensual:** Se realiza un seguimiento mensual de las ventas, los costos y la rentabilidad para evaluar la efectividad del plan de contingencia.
- **Revisión trimestral:** Se revisa el plan de contingencia cada tres meses para ajustarlo a las condiciones del mercado y los resultados obtenidos.

Objetivo:

El objetivo principal del plan de contingencia es volver al escenario probable dentro de los seis meses posteriores a su activación. Si después de seis meses la situación no mejora, se evalúa la viabilidad del proyecto y se consideran otras opciones, incluyendo la posibilidad de suspender el proyecto o buscar una estrategia de salida alternativa. Este plan de contingencia proporciona un marco para la toma de decisiones en caso de que el proyecto enfrente dificultades. Es importante que sea flexible y se adapte a las circunstancias específicas que se presenten. La comunicación constante y el monitoreo continuo son claves para su éxito.

8.12 Plan de Salida

El plan de salida para SecNet se basa en maximizar el retorno de la inversión considerando diferentes escenarios y plazos. Se contemplan las siguientes estrategias:

Adquisición por parte de una empresa de ciberseguridad:

- **Plazo:** 3-5 años.
- **Descripción:** Esta es la estrategia de salida más probable. Se busca la adquisición por parte de una empresa de ciberseguridad más grande que busque expandir su portafolio de productos o acceder a la base de clientes de SecNet.
- **Ventajas:** Potencialmente la opción más lucrativa, ofreciendo una salida completa y un retorno significativo de la inversión.
- **Desventajas:** Requiere un crecimiento sostenido y una sólida posición en el mercado para atraer a posibles compradores.
- **Acciones:** Construir una base de clientes sólida, desarrollar un producto escalable y diferenciador, y establecer relaciones con potenciales compradores en la industria.

	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Fusión con una empresa complementaria:

- **Plazo:** 3-5 años.
- **Descripción:** Fusionarse con una empresa que ofrezca servicios complementarios en ciberseguridad o tecnología para crear sinergias y aumentar el valor de ambas empresas.
- **Ventajas:** Generar un crecimiento más rápido y una mayor rentabilidad a largo plazo.
- **Desventajas:** Requiere encontrar una empresa compatible y gestionar la integración de ambas organizaciones.
- **Acciones:** Identificar posibles empresas complementarias y explorar oportunidades de colaboración.

Venta de la licencia del software:

- **Plazo:** A partir del cuarto año.
- **Descripción:** Vender la licencia del software a otras empresas que deseen integrar SecNet en sus propias soluciones y ofrecerlo a sus clientes.
- **Ventajas:** Genera ingresos recurrentes a través de regalías o tarifas de licencia.
- **Desventajas:** Puede limitar el potencial de crecimiento a largo plazo si se cede el control del producto.
- **Acciones:** Desarrollar un programa de licencias atractivo y buscar activamente socios comerciales.

Continuar como producto independiente dentro de la consultora

(Escenario de bajo crecimiento):

- **Plazo:** Indefinido.
- **Descripción:** Si el crecimiento no alcanza las proyecciones, SecNet puede continuar como un producto independiente dentro de la consultora, generando ingresos recurrentes y complementando los servicios existentes.
- **Ventajas:** Menor riesgo y requiere menos inversión adicional.
- **Desventajas:** Menor potencial de retorno de la inversión en comparación con las otras estrategias.
- **Acciones:** Optimizar la operación de SecNet para maximizar la rentabilidad y minimizar los costos.

Criterios de decisión:

La elección de la estrategia de salida depende de varios factores, incluyendo:

- **Crecimiento del mercado de ciberseguridad.**

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 87 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- Rendimiento financiero de SecNet.
- Interés de potenciales compradores o socios.
- Condiciones del mercado en el momento de la salida.

El plan de salida proporciona una hoja de ruta para maximizar el valor de SecNet y asegurar un retorno de la inversión con revisión anual para adaptarse a las condiciones cambiantes del mercado y los resultados del proyecto. La flexibilidad y la adaptabilidad son claves para elegir la mejor estrategia en el momento oportuno.

9. FACTIBILIDADES

9.1 Técnica

SecNet es técnicamente viable. Se basa en tecnologías de código abierto y en la nube, lo que facilita su implementación y gestión a un costo accesible.

Se basa en la administración remota de routers mikrotik en complemento con una máquina virtual en la LAN que concentra el tráfico DNS y se vincula con el backend de SecNet para reportar y recibir la información, para luego gestionar el router.

Requisitos técnicos:

Client side

- **Infraestructura tecnológica:**
Un router mikrotik (Router OS version 6.4.x o superior) y una VM linux ubuntu, el software basado en DNSMasq, el agente de wazuh y el agente SecNet:
 - Sistema operativo: Ubuntu 22.04 Server.
 - Hardware: 2 vCore, 2Gb de Ram, 100 Gb de almacenamiento.
 - Es recomendable su instalación en 2 equipos por redundancia y distribución de la carga.
- **Software:** Se necesitan las siguientes licencias de software:
 - Agente Wazuh
 - DNSMASQ: Software de código abierto gratuito.
 - Cliente SecNet (desarrollo propio en Python).
- **Conectividad:** Se requiere una conexión a internet (a proteger) para asegurar el funcionamiento óptimo de SecNet . Funciona también en esquemas multi wan.

Server side

- **Infraestructura tecnológica:**

 SecNeT Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 88 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- Servidor físico Intel i7, con 128 Gb de Ram, 2 discos de 2TB SSD, 2 HDD de 4TB y 2 placas de red. Hipervisor basado en HyperV - Dos equipos.
- Router Mikrotik RB 3011 para gestionar Internet
- UPS Online 3KVA
- Server Wazuh
 - Sistema operativo: Ubuntu 22.04 Server.
 - Hardware: 2 vCore, 3 Gb de Ram, 200Gb de almacenamiento (depende del tiempo de retención de logs).
- Server SecNet (3 para toda la plataforma)
 - Sistema operativo: Ubuntu 22.04 Server.
 - Hardware: 4 vCore, 3 Gb de Ram, 200Gb de almacenamiento
- Server Odoo (exclusivo de Madrygal)
 - Sistema operativo: Ubuntu 22.04 Server.
 - Hardware: 2 vCore, 2 Gb de Ram, 100Gb de almacenamiento
 - Odoo server versión community
- Server Nginx (Frontend web para el sitio. Gestiona certificados SSL del sitio y de API's)
 - Sistema operativo: Ubuntu 22.04 Server.
 - Hardware: 2 vCore, 2 Gb de Ram, 100Gb de almacenamiento
- **Software:** Se necesitan las siguientes licencias de software:
 - Server Wazuh (Software libre)
 - Servidor SecNet (desarrollo propio en Python).
- **Conectividad:** Se requiere una conexión a internet de calidad para asegurar el funcionamiento óptimo de SecNet Server. En la práctica es un esquema multi wan con conexiones redundantes de diferentes proveedores

Ventajas técnicas:

- **Escalabilidad:** SecNet es una solución escalable que se adapta a las necesidades de las PyMEs en crecimiento.
- **Flexibilidad:** SecNet es una solución flexible que se adapta a las necesidades específicas de cada cliente.
- **Seguridad:** SecNet se basa en tecnologías de código abierto y en la nube, lo que la hace más segura y fiable que las soluciones tradicionales de seguridad.
- **Costo efectivo:** SecNet es una solución más accesible que las soluciones comerciales tradicionales de ciberseguridad.

Limitaciones técnicas:

- **Dispositivos de línea baja:** SecNet es una solución híbrida. Parte es SaaS y otra reside en el dispositivo Mikrotik. Para una cobertura completa, la lista de bloqueo

 SecNeT Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 89 de 120
---	--	----------------

	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

debe tener una cantidad de registros que exceda los recursos de memoria y almacenamiento de algunos de los productos de línea baja.

- **Solución:** Para mitigar esa limitación de recursos se generan dos tipos de listas, una completa y otra con menos registros, clasificados por severidad y tiempo (los más actuales) que permiten dotar de una protección mínima a dispositivos de línea baja.

9.2 Comercial

La factibilidad comercial de SecNet se basa en la creciente demanda de servicios de ciberseguridad en el mercado de las Pymes y la capacidad del producto para satisfacer estas necesidades de forma efectiva y a un costo accesible.

Demanda:

- El mercado de ciberseguridad para PyMEs en Argentina está en expansión, impulsado por la creciente digitalización de las empresas y la mayor concientización sobre la importancia de la seguridad.
- Existe una demanda insatisfecha de soluciones de seguridad gestionada personalizadas y accesibles para las PyMEs.

Oferta:

- SecNet ofrece una propuesta de valor única que combina protección proactiva, seguridad multicapa, servicio personalizado y un precio competitivo.
- Madrygal cuenta con la experiencia y el *expertise* necesarios para implementar y gestionar SecNet de forma eficaz.

Estrategia Comercial:

- **Marketing y ventas:** Implementar una estrategia de marketing digital, relaciones públicas y participación en eventos para generar conciencia sobre SecNet y captar clientes potenciales.
- **Canales de distribución:** Utilizar un modelo de distribución directa a través del sitio web de Madrygal, redes sociales y contacto directo con clientes potenciales.
- **Precios:** Ofrecer planes de suscripción competitivos y adaptados a las necesidades de las PyMEs.

Proyecciones de ventas:

- Se espera alcanzar una penetración del 100% en el mercado objetivo en los primeros seis semestres.

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 90 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- Se proyectan 150 clientes para el primer año con un crecimiento acelerado para llegar a los 1660 cliente al final del sexto semestre

Análisis de la competencia:

- SecNet se diferencia de la competencia por su expertise, su enfoque proactivo, la integración con Mikrotik, el modelo SaaS y la especialización en Wazuh.
- SecNet se posiciona como una alternativa más completa, personalizada y accesible que las soluciones de la competencia.

La creciente demanda del mercado, la propuesta de valor de SecNet y la experiencia de Madrygal en ciberseguridad hacen que el proyecto sea comercialmente viable y con un alto potencial de éxito.

9.3 Administrativa

- **Gestión administrativa:** SecNet se administra a través de un equipo tercerizado, responsable de la gestión de facturación, cobranza, pago a proveedores, presentaciones fiscales, etc. Al menos hasta disponer de un volumen de clientes que justifique la incorporación de personal administrativo contable.
- **Software:** Se utilizan herramientas de software libre para la gestión administrativa, en este caso Odoo server versión community, que permiten llevar un control eficiente de las compras, ventas, cobranzas, pagos y la contabilidad.
- **Costos de administración:** Se estima que el costo mensual de gestión administrativa en aproximadamente 350 dólares.

9.4 Legal

- **Normativa legal:** SecNet cumple con la legislación argentina en materia de protección de datos personales (Ley 25.326) y la vinculación con sus clientes se basa en convenios de confidencialidad para el tratamiento de datos y procesos.
- Las responsabilidades ante un incidente en un cliente quedan desvinculadas mediante cláusulas específicas del contrato inicial que abarcan:
 - **Limitación de responsabilidad** a un máximo equivalente al monto de los últimos 12 meses contratados, y en ningún caso es responsable de daños indirectos.
 - **Exclusión de garantías:** Madrygal no garantiza que los servicios de SecNet están 100% libres de errores, interrupciones o que se previenen todos los ataques o pérdidas de datos. El Cliente reconoce que la seguridad informática es un proceso continuo y que ningún sistema puede garantizar una protección absoluta

 SecNeT Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 91 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- **Limitaciones por Fuerza mayor:** No se responsabiliza por incumplimiento del acuerdo por eventos fuera de su control razonable (desastres naturales, actos terroristas o de guerra, actos de gobierno, fallas de proveedores de servicios e Interrupciones masivas de Internet.
- **Responsabilidad del Cliente:** El Cliente es responsable de mantener la confidencialidad de sus credenciales de acceso a SecNet y de implementar las mejores prácticas de seguridad en su propia red, con otros servicios de Madrygal o terceros. El Cliente reconoce que el uso de SecNet no reemplaza la necesidad de otras medidas de seguridad, como la capacitación de los empleados y la implementación de políticas de seguridad.
- **Limitaciones del Producto:** SecNet está diseñado para funcionar con routers Mikrotik y su efectividad depende de la correcta configuración del router y la disponibilidad de una conexión a internet. SecNet no es responsable por las vulnerabilidades o las limitaciones de los routers Mikrotik y su sistema operativo Router OS, ni por las interrupciones del servicio de internet ajenas a Madrygal.
- **Marcas y patentes:** SecNet no ha registrado marcas ni patentes hasta el momento, pero se evalúa la posibilidad de registrar la marca y el software bajo protección de las leyes de propiedad intelectual.

C. Aspectos Descriptivos de la Solución Tecnológica

10. Descripción de la Solución Tecnológica

SecNet surge de la necesidad crucial de las PyMEs de proteger sus activos digitales y garantizar la continuidad de sus operaciones en un entorno digital cada vez más complejo y amenazante, pero con limitaciones de presupuesto y personal capacitado. A diferencia de las soluciones de seguridad tradicionales, que suelen ser costosas, complejas de implementar y gestionar, y enfocadas en grandes empresas, SecNet ofrece una solución accesible, personalizada y proactiva, específicamente diseñada para las PyMEs que utilizan routers Mikrotik.

10.1.1 Propuesta de valor del proyecto para la empresa

SecNet aporta a Madrygal los siguientes beneficios:

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 92 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- **Ampliación de la oferta de servicios:** SecNet permite a Madrygal ofrecer un nuevo servicio de seguridad gestionada (MSSP), expandiendo su portfolio de soluciones y abriendo nuevas oportunidades de negocio.
- **Posicionamiento como líder en el mercado:** SecNet permite a Madrygal posicionarse como un proveedor líder de ciberseguridad para PyMEs, captando un público objetivo con una alta demanda de servicios de seguridad gestionada.
- **Mayor rentabilidad:** SecNet tiene un alto potencial de rentabilidad, con un modelo SaaS que le permite a Madrygal escalar el servicio sin una gran inversión inicial.
- **Fortalecimiento de la marca:** SecNet ayuda a Madrygal a fortalecer su reconocimiento de marca y su reputación en el mercado de la ciberseguridad.
- **Innovación tecnológica:** SecNet integra modernas tecnologías de ciberseguridad, lo que le permitiera Madrygal mantenerse a la vanguardia en el sector. En el roadmap de producto se analiza la integración con modelos de IA o LLM mediante las API 's de Wazuh.

Se espera que SecNet genere un incremento del 450% en los ingresos de Madrygal durante los próximos 3 años en el segmento servicios por suscripción.

10.1.2 Hitos importantes del proyecto

Hito	Fecha de inicio	Fecha de fin	Responsable
Finalizar el desarrollo de SecNet	01/10/2024	31/12/2024	CTO
Lanzamiento de la versión beta de SecNet	01/01/2025	30/01/2025	CTO
Lanzamiento comercial de SecNet	01/02/2025	31/12/2025	Gerente de Comercialización
Captación de 50 nuevos clientes	01/01/2025	30/06/2025	Gerente de Comercialización
Lograr una calificación promedio de satisfacción del cliente superior a 4 estrellas	01/01/2025	30/06/2025	Gerente de Comercialización

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

10.2 Visión del producto

10.2.1 Historias de Usuario

Las "Historias de Usuario", se enfocan en los requerimientos funcionales del producto desde la perspectiva del usuario, Normalmente podemos describirlas con el formato "Como (rol), necesito (funcionalidad) para (beneficio)".

Autenticación y Autorización:

- Como **usuario**, necesito **poder iniciar sesión de forma segura en la plataforma web para acceder a las funcionalidades de SecNet.**
- Como **administrador**, necesito **poder gestionar los usuarios y sus permisos para controlar el acceso a las diferentes funciones de la plataforma.**

Monitoreo:

- Como **usuario**, necesito **visualizar el estado de seguridad de mi red en tiempo real para identificar posibles amenazas y vulnerabilidades.**
- Como **usuario**, necesito **recibir alertas de seguridad en tiempo real para poder responder rápidamente a incidentes críticos.**
- Como **usuario**, necesito **acceder a reportes de seguridad personalizados para analizar la información de seguridad y tomar decisiones informadas.**

Filtrado de tráfico:

- Como **usuario**, necesito **que SecNet bloquee automáticamente el acceso a sitios web y direcciones IP maliciosas para proteger mi red de infecciones y ataques.**
- Como **administrador**, necesito **personalizar las listas de dominios e IPs bloqueados para adaptar el filtrado a las necesidades específicas de mi empresa.**

Honeypots:

- Como **usuario**, necesito **que SecNet implemente honeypots en mi red para detectar actividades maliciosas y obtener información sobre las amenazas.**

Gestión de incidentes:

- Como **usuario**, necesito **herramientas para analizar los incidentes de seguridad para poder comprender las causas y tomar medidas correctivas.**

Otras funcionalidades:

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 94 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- Como **usuario**, necesito **poder configurar las notificaciones de alertas** para recibir información relevante y evitar la saturación de alertas.
- Como **usuario**, necesito **acceder a la documentación y guías de usuario** para poder utilizar SecNet de forma efectiva.

10.3 Alcance del desarrollo

El desarrollo de SecNet abarca la creación de las siguientes funcionalidades:

- **Sistema generador de listas:** Con insumos provenientes de diversas fuentes, **se procesan** indicadores de compromiso e incidentes reportados por investigadores. Utilizando diversos scripts en Python, consultas Whois, DNSBL, GeolIP y listas blancas de direcciones IP y dominios, **se generan** listas de direcciones IP y dominios (URLs) maliciosas. Estas listas **se despliegan** en un servidor web y tanto los equipos MikroTik suscritos como las máquinas virtuales de gestión y control DNS **se actualizan** periódicamente desde allí.
- **Wazuh SIEM:** **Se integra** con firewalls MikroTik y agentes Wazuh para la recopilación y el análisis de eventos de seguridad. Los eventos son enviados desde el log del dispositivo Mikrotik mediante la funcionalidad de Syslog a un servidor Wazuh central que procesa cada evento. En caso de eventos de gravedad crítica superior, el servidor de Wazuh genera alertas a través de Telegram al responsable del dispositivo.
- **Filtrado DNS:** **Se implementa** una máquina virtual con DNSMasq para el filtrado de consultas DNS mediante listas de reputación de dominios (URLs).
- **Filtrado de IP:** **Se configura** el filtrado de IP en los firewalls MikroTik utilizando reglas de forward y listas de reputación de IPs para bloquear el tráfico desde y hacia direcciones IP conocidas como maliciosas.
- **Honeypots :** **Se integra** honeypots en la infraestructura de SecNet para atraer a los atacantes, analizar su comportamiento y obtener información sobre las nuevas amenazas. Cada router enrolado al sistema se comporta, mediante reglas, como un Honeypot que reporta actividad no autorizada al sistema central.
- **Servicio al cliente especializado:** **Se brinda** un servicio al cliente proactivo y personalizado, con soporte técnico especializado en Wazuh.

El desarrollo de SecNet NO incluye:

- Integración con otras herramientas de seguridad: El enfoque es brindar una solución integral para dispositivos MikroTik mediante DNSMasq y Wazuh.
- Desarrollo de nuevos módulos de seguridad: SecNet se basa en la integración de herramientas existentes.

 SecNet Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 95 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- No se incluye soporte de insumos de inteligencia de amenazas de fuentes comerciales, solo la basada en OTX y el feedback de los honeypots propios.

10.4 Descripción del entorno del sistema

SecNet se despliega en un entorno distribuido, con componentes tanto del lado del cliente como del lado de Madrygal (proveedor del servicio).

Entorno del cliente:

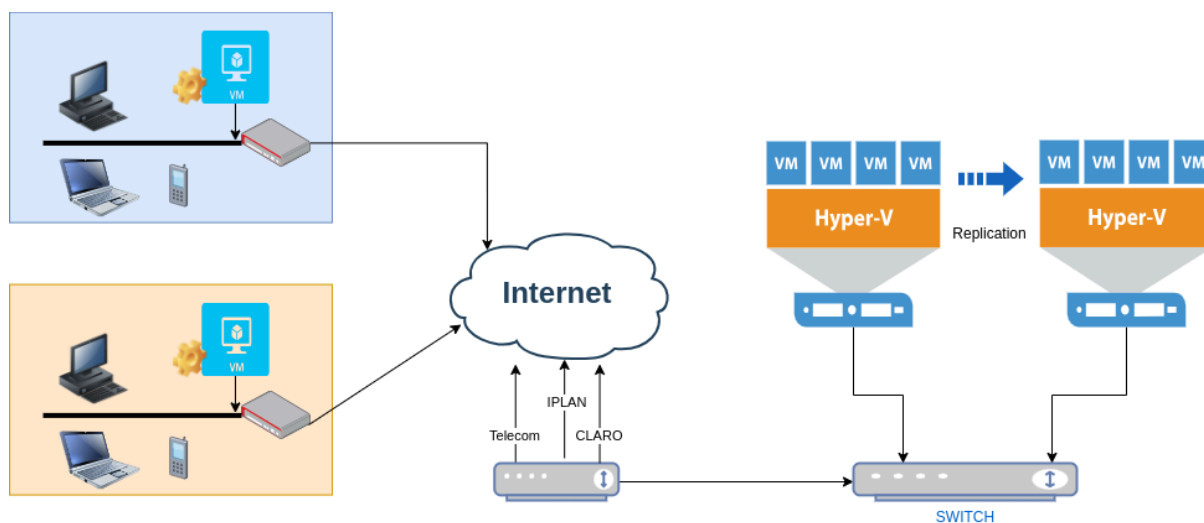
- **Router Mikrotik:** El router Mikrotik del cliente es el punto de entrada de SecNet en la red de la empresa. Se configura para enviar logs vía syslog al servidor Wazuh de Madrygal y para descargar y aplicar las listas de control de acceso (ACLs) que contienen las direcciones IP y los dominios maliciosos. Además, se configura el firewall para implementar honeypots.
- **Máquinas virtuales (VMs) con DNSMASQ:** Dos VMs funcionan como servidores DNS locales, ejecutando DNSMASQ para el filtrado de DNS. Estas VMs se actualizan automáticamente con las listas de dominios maliciosos desde el servidor web de SecNet. También incluyen un agente Wazuh que reporta los bloqueos de DNS.
- **Agente Wazuh (opcional - Plan VPS):** En el plan VPS, se instala un agente Wazuh en los equipos de la red del cliente para recolectar eventos de seguridad a nivel de endpoint.

Entorno de Madrygal:

- **Servidor Web SecNet:** Almacena y distribuye las listas de control de acceso (ACLs) para el filtrado de IP y DNS. Gestiona la autenticación de usuarios y las licencias.
- **Servidor Wazuh:** Recibe logs vía syslog, los correlaciona, los analiza, los almacena, genera alertas y las envía a la plataforma de visualización.
- **Base de datos:** Almacena la configuración del sistema, los logs, las listas de IPs y dominios y otros datos relevantes.
- **Servidor Nginx:** Actúa como *reverse proxy* y terminador SSL para el servidor web, brindando seguridad y optimización.
- **Servidores de Backup:** Dos servidores que realizan backups de las VMs de Wazuh y las listas dos veces al día, y replicación con Hyper V para alta disponibilidad.
- **Servidores Honeypot:** En corto plazo se utilizan reglas en cada dispositivo Mikrotik que detectan actividad anormal y la reportan a Wazuh via Syslog. A mediano plazo se estima instalar servidores TPOT en entornos productivos a fin de detectar actores maliciosos de manera más detallada.

 SecNeT Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 96 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

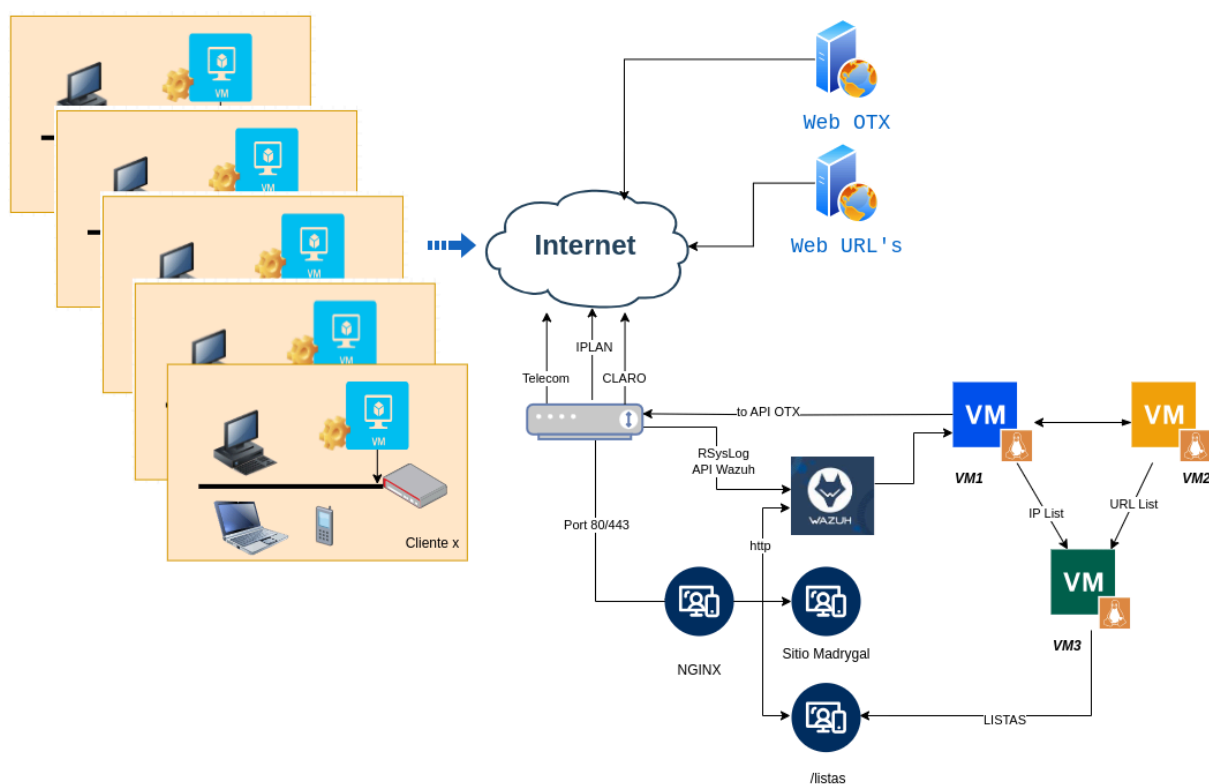


10.4.1 Requisitos de Entorno

- **Cliente:**
 - **Conexión a Internet:** Requerida para la comunicación con los servidores de Madrygal, la descarga de listas y la actualización de la plataforma.
 - **Router Mikrotik:** RouterOS versión 6.4.o superior, con suficientes recursos para procesar las reglas de firewall y las listas de control de acceso.
 - **VM (DNSMASQ/Wazuh Agent):** Sistema operativo Ubuntu 22.04 Server, 2 vCores, 2GB RAM, 100GB de almacenamiento. Se recomiendan dos VMs para alta disponibilidad.
 - **Recursos de hardware para el cliente:** Para la lista completa: Hardware capaz de manejar 80.000 registros en las listas de control de acceso. Para la lista reducida: Hardware con menos recursos, capaz de manejar 25.000 registros.
- **Madrygal (Backend):**
 - **Servidores físicos (2):** Intel i7, 128GB RAM, 2x2TB SSD, 2x4TB HDD, 2 placas de red. Hipervisor basado en Hyper V. UPS de 3KVA.
 - **Servidor Web SecNet:** Ubuntu 22.04 Server, 4 Cores, 3GB RAM, 200GB almacenamiento (3 instancias).
 - **Servidor Wazuh:** Ubuntu 22.04 Server, 2 Cores, 3GB RAM, 200GB almacenamiento (escalable según la retención de logs).
 - **Servidor Nginx:** Ubuntu 22.04 Server, 2 Cores, 2GB RAM, 100 GB almacenamiento.
 - **Servidor Odoo:** Ubuntu 22.04 Server, 2 Cores, 2GB RAM, 100 GB almacenamiento.

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

- **Router Mikrotik RB3011 v7** o superior
 - Switch 24 ports Gigabit administrable con soporte de VLAN
- **Seguridad:**
 - **Firewall:** Reglas de firewall para proteger los servidores y la infraestructura, incluyendo filtrado por GeoIP y restricciones de acceso por IP.
 - **Autenticación:** Autenticación segura para el acceso a la plataforma web y la API.
- **Backup:** Backups diarios de las VMs de Wazuh y de las listas, además de la replicación con Hyper V.



10.5 Descripción del Producto

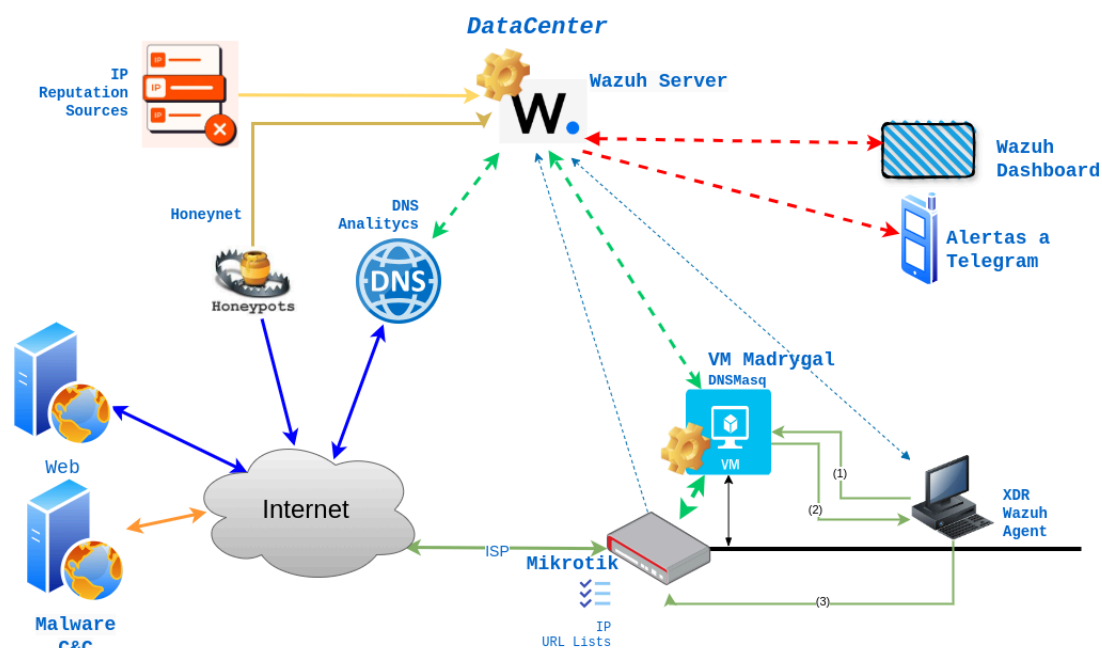
SecNet es un sistema de seguridad gestionada, diseñado específicamente para pequeñas y medianas empresas (PyMEs) que utilizan routers Mikrotik. Funciona como un servicio en la nube (SaaS) y se encarga de monitorear y proteger la red de la empresa contra diversas amenazas cibernéticas.

Funcionamiento:

 SecNet Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 98 de 120
---	--	----------------

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Cada vez que una computadora cliente quiere conectarse a un sitio en Internet, realiza la consulta DNS a la VM-DNS1 (proceso 1), DNSMasq revisa que no este entre los más de 3 millones de sitios indexados como maliciosos y si esta ok le responde con la IP del host de destino (proceso 2) o bien una IP nula si se encuentra bloqueado. Luego, en caso de no ser un sitio bloqueado, con la IP intenta salir por el router (proceso 3), Allí un nuevo control verifica que esa IP no esté en ninguna lista de bloqueo, si el proceso es correcto, la petición continua al host de destino.



Bloqueo: Si la IP consultada está en una lista o coincide con una subnet bloqueada, la petición es denegada, se genera un log que se envía a Wazuh informando el incidente y tanto la IP destino como la del cliente se almacenan en listas de direcciones para posterior auditoría. Si el bloqueo se produce en el DNSMasq, además de bloquearlo y devolver un null en la IP, se genera un log que se envía a Wazuh. En ambos casos de bloqueo se le notifica al administrador vía Telegram de la posibilidad de un equipo comprometido en la red lan.

```

38 chain=forward action=drop dst-address-list=Madrygal_block1 out-interface-list=WAN log=yes log-prefix="BLOCK"
39 chain=forward action=add-dst-to-address-list dst-address-list=Madrygal_block1 address-list=bloqueados out-interface-list=WAN log=yes log-prefix="BLOCK"

```

Detalle de las reglas de bloqueo en el router Mikrotik

 SecNeT Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 99 de 120
---	--	----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Procesos:

1. Configuración inicial: Se configura el router Mikrotik para enviar logs al servidor Wazuh y descargar las listas de IPs y dominios maliciosos. Se configuran las VMs con DNSMASQ y se apunta el DNS local del cliente a ellas. Se crean reglas de filtrado basado en las listas, con reporte activo al LOG.
2. Monitoreo continuo: El servidor Wazuh recibe y analiza los logs del router Mikrotik y de los agentes Wazuh (si corresponde).
3. Detección de amenazas: Si Wazuh detecta una amenaza, genera una alerta y la envía al dashboard de SecNet y, en algunos casos, directamente al celular del responsable vía Telegram.
4. Filtrado de tráfico: El router Mikrotik y DNSMASQ bloquean el tráfico malicioso utilizando las listas de IPs y dominios. El router Mikrotik también usa reglas de firewall para simular honeypots y detectar ataques.
5. Actualización de listas: Las listas de IPs y dominios maliciosos se actualizan automáticamente cada 8 horas y cada 24 horas (lista reducida) en el servidor web de SecNet y se descargan en los routers Mikrotik y los servidores DNS del cliente mediante scripts programados.
6. Generación de reportes: SecNet genera reportes de seguridad que se visualizan en el dashboard, brindando al cliente información sobre las amenazas detectadas y la postura de seguridad de su red.

SecNet funciona de forma proactiva y automatizada, combinando la potencia de un SIEM con el filtrado de tráfico y la inteligencia de amenazas, para brindar una solución de seguridad integral y personalizada para las PyMEs.

10.5.1 Componentes principales:

1. **Router Mikrotik:** Es el router principal de la red de la empresa cliente. SecNet interactúa con él para implementar las reglas de seguridad y recolectar información sobre el tráfico de red.
2. **VM Cliente (Máquina Virtual):** Se instalan dos máquinas virtuales en la red del cliente, funcionando como servidores DNS locales. Estas VMs ejecutan DNSMASQ para el filtrado de DNS, bloqueando el acceso a sitios web maliciosos, y un agente Wazuh que reporta los bloqueos al servidor central.
3. **Servidor Web SecNet:** Alojado en el Data Center de Madrygal, este servidor almacena y distribuye las listas de direcciones IP y dominios maliciosos que se utilizan para el filtrado. También gestiona la autenticación de usuarios y las licencias. Está compuesto por 3 VMs que trabajan de forma conjunta.
4. **Servidor Wazuh:** También en el Data Center de Madrygal, este servidor es el corazón del sistema SIEM (Security Information and Event Management). Recibe los

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

logs de seguridad del router Mikrotik y de los agentes Wazuh (en el caso de los planes VPS), los analiza y genera alertas en tiempo real.

5. **Firewall Madrygal:** Protege el Data Center de Madrygal y sus servidores.
6. **Servidor Nginx:** Actúa como *reverse proxy* y terminador SSL para el servidor web de SecNet, proporcionando seguridad y optimización del rendimiento.

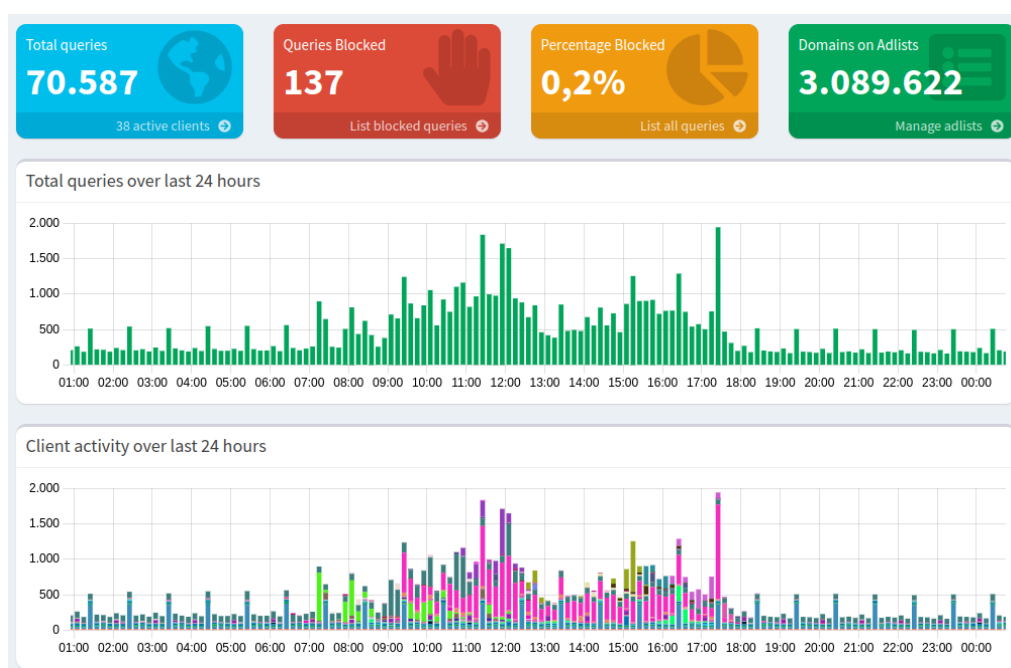
10.5.2 Generación de Listas en SecNet:

SecNet utiliza dos tipos de listas para proteger a sus clientes: listas de IPs y listas de dominios. Ambas se generan a partir de la combinación de información de honeypots propios y de fuentes externas de inteligencia de amenazas, principalmente OTX. El proceso de generación de listas es automatizado y se realiza en el servidor web de SecNet cada 8 horas, y cada 24 horas la lista reducida de IPs.

1. Listas de IPs:

- Honeypots: SecNet configura reglas de firewall en los routers Mikrotik de sus clientes para actuar como honeypots de baja interacción. Estas reglas escuchan tráfico en puertos específicos (web, ftp, bases de datos, etc.) y registran las IPs que intentan acceder a ellos. Estas IPs se consideran potencialmente maliciosas y se agregan a una lista temporal de bloqueo.
- OTX: SecNet consulta la plataforma OTX (Open Threat Exchange) de AlienVault para obtener información sobre amenazas, incluyendo IPs maliciosas, URLs y hashes de malware. Esta información se utiliza para enriquecer la lista de IPs. Se priorizan los indicadores con mayor riesgo según OTX.
- Procesamiento: Las IPs recopiladas de los honeypots y de OTX se procesan para eliminar falsos positivos y se agregan a la lista principal de bloqueo. Para optimizar el rendimiento de los routers Mikrotik, la lista se convierte a formato de subredes /24, reduciendo el número de registros.
- Listas reducidas: Se generan listas reducidas con información de OTX de los últimos 30 días, considerando el nivel de riesgo de los indicadores. Estas listas se utilizan en routers con menos recursos de hardware para evitar sobrecargas.

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	



Dashboard del panel de gestión de DNS

10.5.3 ¿Qué es OTX?

OTX¹⁴ (Open Threat Exchange) es una plataforma avanzada de intercambio de información sobre amenazas cibernéticas desarrollada por AlienVault, que ahora forma parte de AT&T Cybersecurity. Esta plataforma global permite a los usuarios compartir y recibir datos de amenazas en tiempo real, fomentando así una comunidad colaborativa de defensores contra las ciberamenazas.

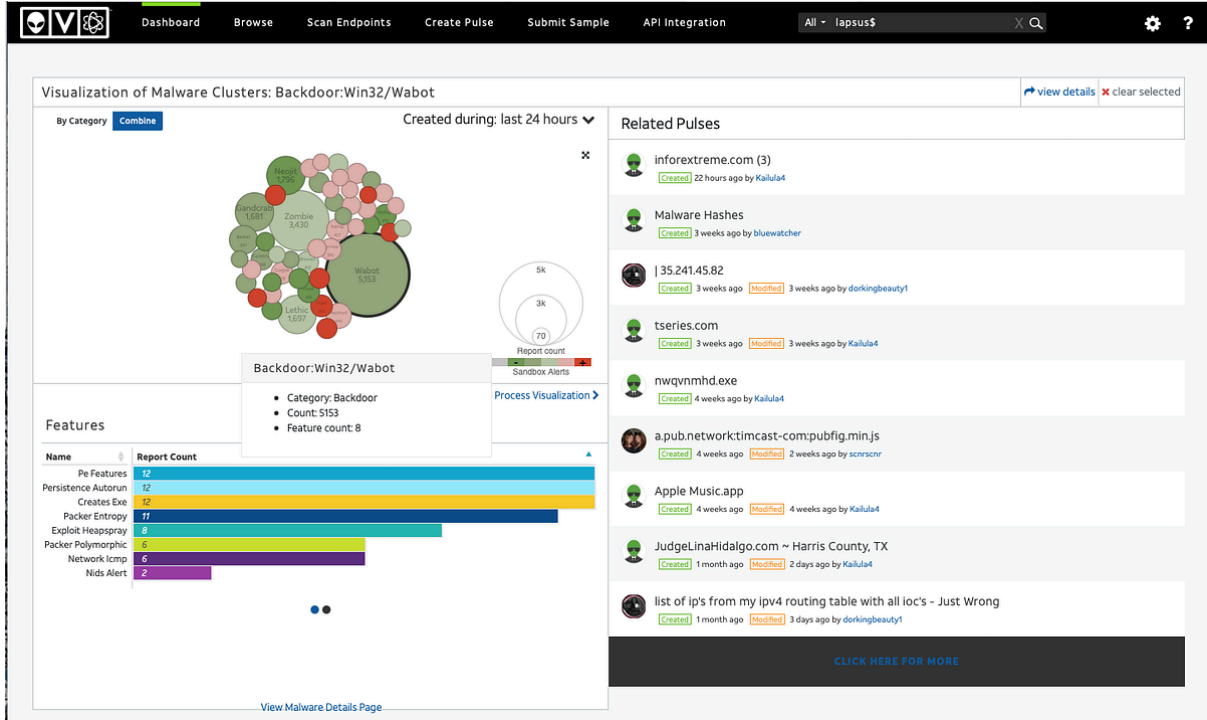
La importancia de OTX en el ámbito de la ciberseguridad radica en su capacidad para democratizar el acceso a la información de inteligencia sobre amenazas, lo que tradicionalmente había sido un recurso disponible sólo para organizaciones con grandes presupuestos. Al ofrecer acceso gratuito, OTX permite que incluso las empresas más pequeñas puedan beneficiarse de la inteligencia de amenazas actualizada, lo que ayuda a nivelar el campo de juego en la lucha contra los ciberdelincuentes.

Usuarios de todo tipo, desde investigadores independientes y pequeñas empresas hasta grandes corporaciones y organismos gubernamentales, utilizan OTX para compartir hallazgos, alertar sobre nuevas vulnerabilidades y discutir tendencias emergentes en ciberseguridad. Esta plataforma no solo sirve como un repositorio de datos, sino también

¹⁴ <https://cybersecurity.att.com/open-threat-exchange>

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

como un foro para el intercambio de ideas y estrategias, reforzando la defensa colectiva contra amenazas comunes.



Características Principales

Amplia Base de Datos de Indicadores de Compromiso (IoCs): OTX cuenta con una de las bases de datos más grandes y diversas de indicadores de compromiso, que incluye direcciones IP, URLs, hashes de archivos y más. Estos IoCs son contribuidos por una comunidad global, lo que asegura que la información sea actual y relevante.

Interfaz Intuitiva y Accesible: La plataforma ofrece una interfaz de usuario clara y fácil de navegar, lo que permite a los usuarios buscar, filtrar y analizar la inteligencia sobre amenazas de manera eficiente. Esto facilita a los usuarios de todos los niveles técnicos el aprovechamiento de los datos para proteger sus sistemas.

Pulse Reports: Los usuarios pueden crear y compartir "Pulses", que son informes que agrupan información relacionada con amenazas específicas, incluyendo descripciones detalladas, IoCs, y tácticas, técnicas y procedimientos (TTPs) de los atacantes. Estos informes ayudan a otros usuarios a entender rápidamente la naturaleza de una amenaza y cómo mitigarla.

Integraciones con Herramientas de Seguridad: OTX se integra fácilmente con una variedad de herramientas de seguridad, incluyendo SIEMs, firewalls, y sistemas de

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

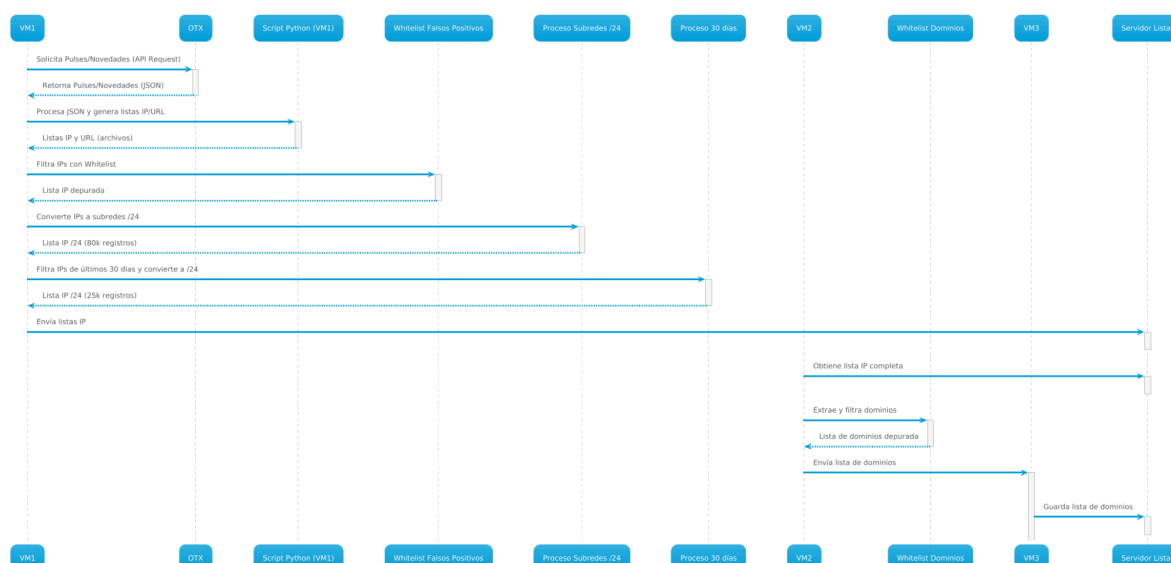
detección de intrusiones. Esto permite que los IoCs de OTX se utilicen directamente en herramientas de seguridad para mejorar la detección y respuesta automática a las amenazas.

API Robusta: La plataforma proporciona una API potente que permite a los desarrolladores y a las aplicaciones de terceros interactuar con OTX para automatizar la recolección y análisis de datos, ampliando las capacidades de las soluciones de seguridad existentes.

10.5.4 Otras fuentes de datos

Además de OTX, se utilizan los datos provenientes de la red de alertas (honeypots) y diversas fuentes open source. Todas son procesadas mediante scripts de python para validar su calidad. A mediano plazo, dentro de los gastos operativos del año 2 y 3, se incluye un costo mensual por suscripción a listas de pago sobre Inteligencia de Amenazas para aumentar aún más la calidad de detección.

10.5.5 Diagrama de secuencia

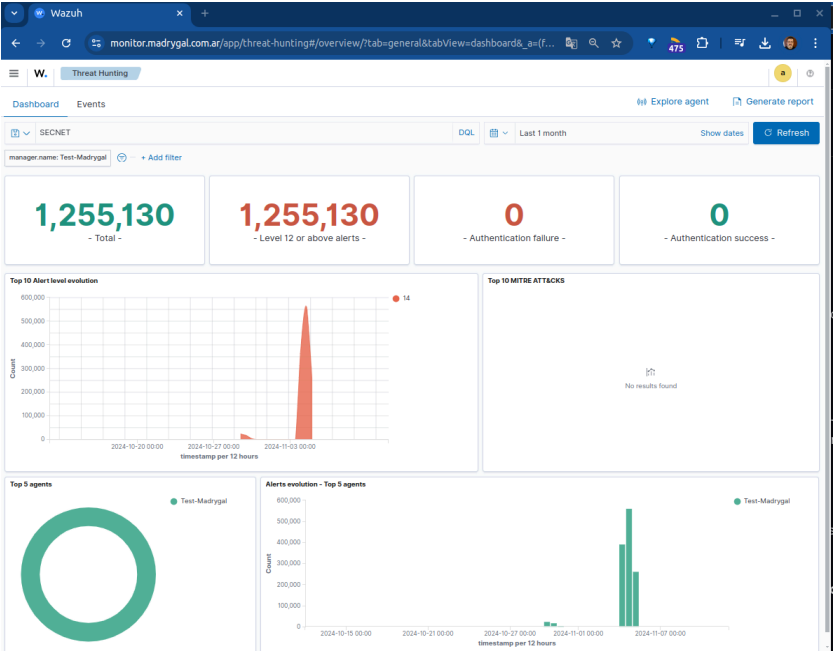
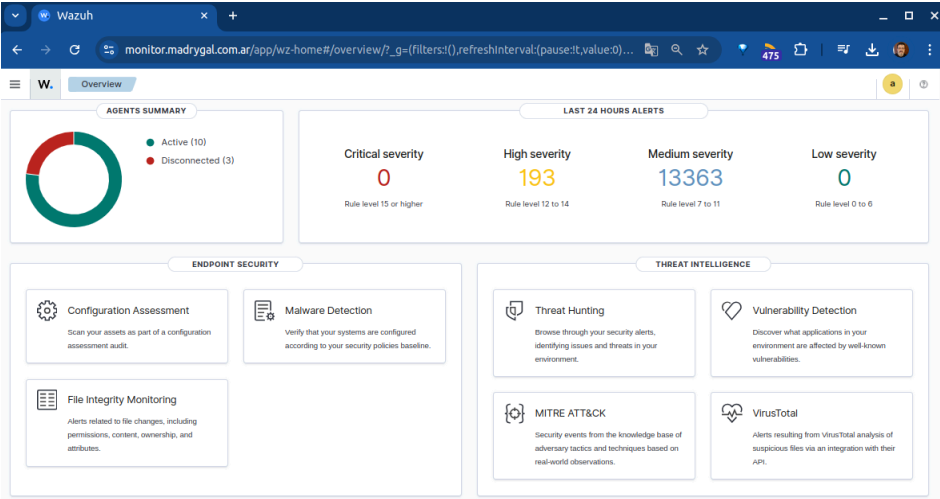


10.5.6 Interface de usuario

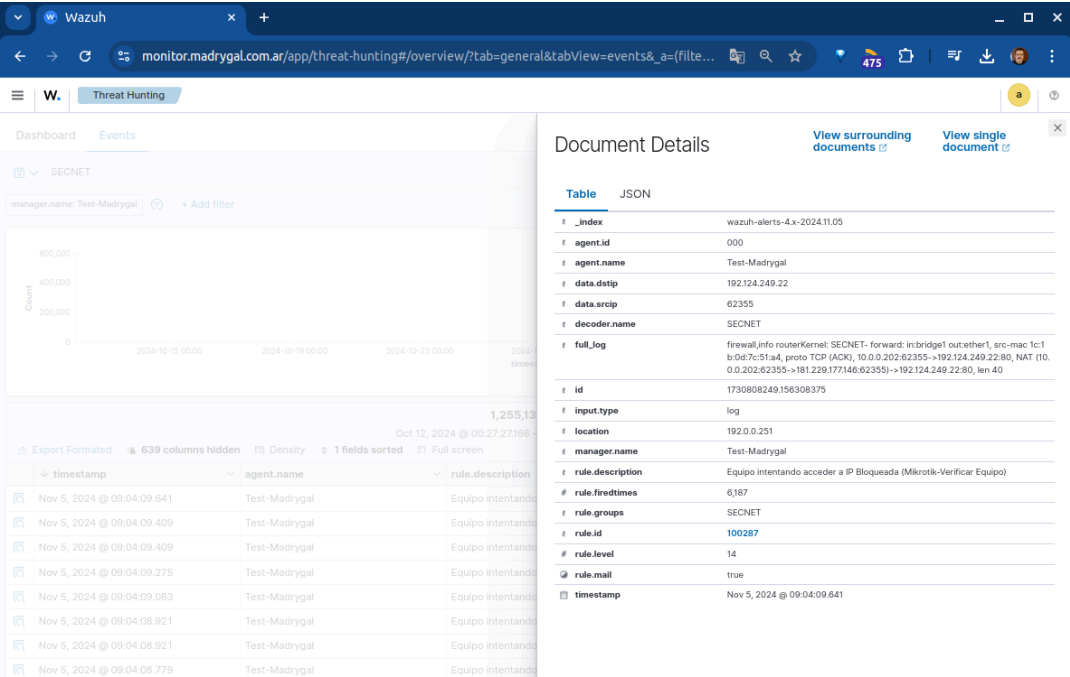
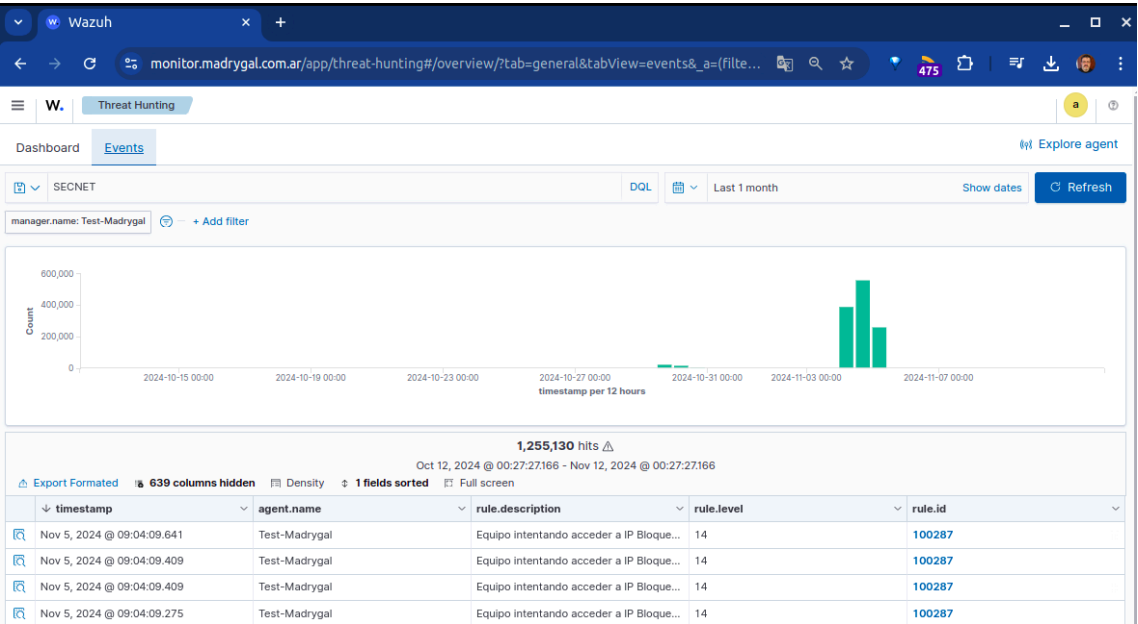
El sistema no tiene una interfaz de usuario sino que se accede a los dashboards de Wazuh específicos del dispositivo suscriptor. Si la empresa dispone de varios equipos, puede

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

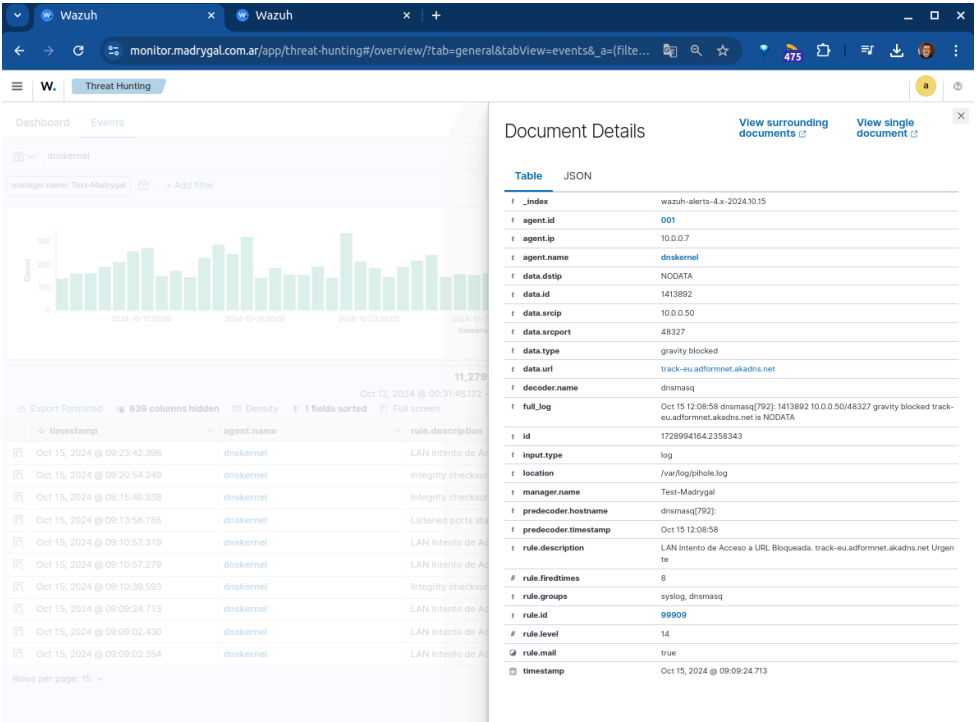
seleccionar el router o bien ver los eventos del conjunto luego de ingresar con las credenciales.



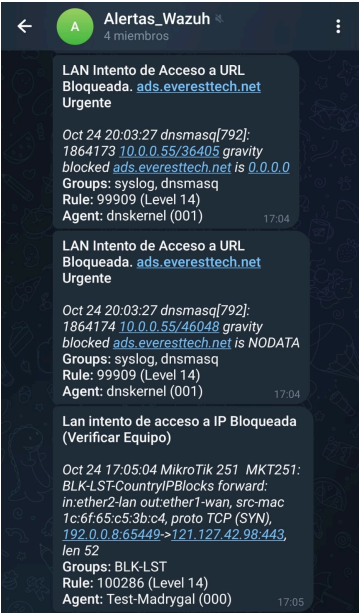
Dashboards informativos de cantidad y criticidad de eventos.



Alerta Wazuh por acceso a IP no autorizada



Alerta Wazuh por acceso a URL no autorizadas



Alerta Wazuh enviada a Telegram por acceso a URL y/o IP no autorizadas

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

D. Anexos

11 Contenido

11.1 Paper CONAISI

El siguiente paper de investigación (independiente del proyecto anterior) fue presentado y aprobado por el Congreso Nacional de Ingeniería informática y Sistemas de Información (CONAISI 2024).

Estrategias Metodológicas para la Modernización de Centros de Datos Gubernamentales

Fernando Andrés Corvalan¹, Alejandro Sartorio²

Universidad Abierta Interamericana¹, Facultad de Tecnología Informática.

CAETI - Universidad Abierta Interamericana², Facultad de Tecnología Informática.

Rosario, Argentina.

FernandoAndres.Corvalan@alumnos.uai.edu.ar¹, alejandro.sartorio@uai.edu.ar²

Abstract. Este trabajo propone un marco

metodológico para ser incluido en los procesos de definición de tecnologías y estrategias para centros de datos gubernamentales. Se realiza un análisis comparativo de las principales opciones tecnológicas, incluyendo mainframes, plataformas Open basadas en x86 y soluciones de computación en la nube.

El marco propuesto se basa en un enfoque por etapas, incluyendo: 1)Análisis de requisitos y contexto, considerando necesidades operativas, normativa aplicable (como la Ley de Software Libre 13.139 y la Ley de Protección de Datos Personales 25.326) y restricciones presupuestarias; 2)Evaluación de tecnologías disponibles en términos de eficiencia, escalabilidad, seguridad, flexibilidad y costo total de propiedad; 3)Diseño de la arquitectura tecnológica, integrando las soluciones seleccionadas y planificando aspectos de ciberseguridad; 4)Validación mediante pruebas de concepto; y 5)Implementación y gestión del cambio.

El estudio se enmarca en el contexto del gobierno de Santa Fe, Argentina, donde se evalúa el impacto de la legislación provincial y nacional en la modernización de la infraestructura de TI. Busca proporcionar a los responsables de tecnología una herramienta efectiva para la toma de decisiones estratégicas, asegurando la eficiencia, sustentabilidad, seguridad y soberanía tecnológica de los centros de datos gubernamentales.

Palabras Clave: *centros de datos, ciberseguridad, computación en la nube, gobierno electrónico, infraestructura crítica, mainframe, privacidad de datos, software de código abierto, virtualización*

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

 Outlook

[Trabajo de Cátedra de 4to Nivel en Adelante (TC4+)] CoNaiISI 2024: Decisión sobre su propuesta

Desde Director Trabajo de cátedra de 4to nivel en adelante <tc4.conaiisi@conaiisi.frc.utn.edu.ar>

Fecha Mar 15/10/2024 21:56

Para Corvalan, Fernando Andres <FernandoAndres.Corvalan@alumnos.uai.edu.ar>

Sr Fernando Andres Corvalan:

Felicitaciones!!!

Tenemos el agrado de informarle que ha finalizado la revisión de su envío con el título "Estrategias Metodológicas para la Modernización de Centros de Datos Gubernamentales" y que el mismo ha sido aceptado para ser presentado en la duodécima edición del CoNaiISI, que tendrá lugar los días 7 y 8 de Noviembre de 2024 en la ciudad de San Fernando del Valle de Catamarca, organizado por la Facultad de Tecnología y Ciencias Aplicadas de la Universidad Nacional de Catamarca, Argentina.

Deberá enviarnos el documento de su propuesta con las modificaciones sugeridas al final de este e-mail, si las hubiera (Versión Camera-Ready), en formato de documento portátil (PDF), siguiendo las normas indicadas en "<https://idi008.wixstudio.io/conaiisi-24>" y CON LA FILIACIÓN COMPLETA DE SUS AUTORES, antes del día 22-Oct-2024.

Para enviarnos el documento solicitado, por favor realice los siguientes pasos:

- A) Ingrese en el sistema de envíos, con el mismo usuario que utilizó para remitir la propuesta.
- B) Elija el rol de "Autor"
- C) Ingrese a la pestaña "Ya revisados" (o submenú "Ya revisados")
- D) Seleccione el trabajo con el título "Estrategias Metodológicas para la Modernización de Centros de Datos Gubernamentales".
- E) Ingrese en la pestaña "Revisión".
- F) Suba la Versión Camera-Ready en la sección "Decisión del Director".

De acuerdo a lo informado en la página principal del congreso, <https://idi008.wixstudio.io/conaiisi-24>, para garantizar la inclusión de este artículo en la publicación digital del CoNaiISI 2024, por lo menos un autor debe inscribirse en el congreso antes del 28-Oct-2024.

Oportunamente se publicará en el sitio web del congreso, el cronograma de desarrollo de actividades indicando fecha y lugar para la presentación oral.

Agradecemos su interés en el CoNaiISI 2024 y esperamos verlos en noviembre.

Cordiales saludos,

Director Trabajo de cátedra de 4to nivel en adelante
CoNaiISI
tc4.conaiisi@riisic.net.ar

Le agradeceremos no responder este mail, ya que esta dirección es utilizada sólo para envíos.

Por cualquier duda o consulta, utilice el siguiente e-mail:

conaiisi@riisic.net.ar

Para información sobre el Congreso visite

<https://idi008.wixstudio.io/conaiisi-24>

--

Director eje Trabajo de cátedra de 4to nivel en adelante
Mail: tc4.conaiisi@riisic.net.ar

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Estrategias Metodológicas para la Modernización de Centros de Datos Gubernamentales

Fernando Andrés Corvalán¹, Alejandro Sartorio²

Universidad Abierta Interamericana¹, Facultad de Tecnología Informática.

*CAETI - Universidad Abierta Interamericana², Facultad de Tecnología Informática.
Rosario, Argentina.*

FernandoAndres.Corvalan@alumnos.uai.edu.ar¹, alejandro.sartorio@uai.edu.ar²

Abstract. Este trabajo propone un marco metodológico para ser incluido en los procesos de definición de tecnologías y estrategias para centros de datos gubernamentales. Se realiza un análisis comparativo de las principales opciones tecnológicas, incluyendo mainframes, plataformas Open basadas en x86 y soluciones de computación en la nube.

El marco propuesto se basa en un enfoque por etapas, incluyendo: 1)Análisis de requisitos y contexto, considerando necesidades operativas, normativa aplicable (como la Ley de Software Libre 13.139 y la Ley de Protección de Datos Personales 25.326) y restricciones presupuestarias; 2)Evaluación de tecnologías disponibles en términos de eficiencia, escalabilidad, seguridad, flexibilidad y costo total de propiedad; 3)Diseño de la arquitectura tecnológica, integrando las soluciones seleccionadas y planificando aspectos de ciberseguridad; 4)Validación mediante pruebas de concepto; y 5)Implementación y gestión del cambio.

El estudio se enmarca en el contexto del gobierno de Santa Fe, Argentina, donde se evalúa el impacto de la legislación provincial y nacional en la modernización de la infraestructura de TI. Busca proporcionar a los responsables de tecnología una herramienta efectiva para la toma de decisiones estratégicas, asegurando la eficiencia, sustentabilidad, seguridad y soberanía tecnológica de los centros de datos gubernamentales.

Palabras Clave: centros de datos, ciberseguridad, computación en la nube, gobierno electrónico, infraestructura crítica, mainframe, privacidad de datos, software de código abierto, virtualización

1.Introducción

En el contexto de la transformación digital que están experimentando los gobiernos, la modernización de la infraestructura tecnológica se ha vuelto un imperativo para

ofrecer servicios públicos eficientes, seguros y adaptados a las necesidades actuales de la ciudadanía. La selección de la tecnología y la arquitectura adecuadas es una decisión estratégica que no solo impacta en la capacidad operativa de las instituciones gubernamentales, sino que también determina su capacidad para cumplir con normativas estrictas, como las leyes de protección de datos y de software libre, así como para garantizar la soberanía tecnológica [1], [2].

Un ejemplo concreto de esta problemática se observa en el caso del gobierno de Santa Fe, Argentina, donde la implementación de la Ley de Software Libre 13.139 [3] ha presentado desafíos significativos. A pesar de la intención de fomentar la independencia tecnológica y la transparencia, la falta de un marco metodológico claro para seleccionar las tecnologías adecuadas ha generado dificultades en la integración de plataformas Open en los sistemas existentes, así como en el cumplimiento simultáneo de las normativas nacionales sobre protección de datos [4].

Sin embargo, la variedad de opciones disponibles, desde mainframes tradicionales hasta soluciones de computación en la nube y plataformas Open basadas en x86, presenta un desafío significativo para la toma de decisiones estratégicas en la modernización de la infraestructura tecnológica. La falta de un marco metodológico claro puede llevar a decisiones subóptimas, resultando en infraestructuras que no satisfacen completamente los requisitos de ciberseguridad, escalabilidad, eficiencia y costo-efectividad que demanda el entorno gubernamental.

 SecNeT Ciberseguridad para Empresas	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 111 de 120
---	--	-----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

En este escenario, surge la necesidad de una metodología que guíe el proceso de análisis y selección de tecnologías para la infraestructura gubernamental. Esta metodología debe considerar tanto los aspectos técnicos como los contextos normativos y presupuestarios, permitiendo a las administraciones públicas tomar decisiones informadas y alineadas con sus objetivos estratégicos.

El presente trabajo propone una metodología estructurada para abordar este desafío, ofreciendo una guía clara para la evaluación y selección de tecnologías en centros de datos gubernamentales. A través de un análisis comparativo de las principales opciones tecnológicas y la aplicación de esta metodología en el caso de la provincia de Santa Fe, Argentina, este estudio busca proporcionar a los responsables de tecnología del sector público una herramienta efectiva para la modernización de sus infraestructuras, asegurando así una mayor eficiencia, seguridad y sostenibilidad a largo plazo [5].

2. Estado del Arte: De los Mainframes a la Nube

La evolución de la tecnología de centros de datos ha sido vertiginosa en las últimas décadas, transitando desde los tradicionales mainframes, caracterizados por su robustez y confiabilidad de cinco nueves (99,999%), hasta la computación en la nube con sus promesas de flexibilidad y escalabilidad. En medio, un abanico de soluciones On Premise, con servidores físicos o virtualizados, de tecnologías propietarias hasta arquitecturas abiertas x86, con software open source o privativo. A continuación, se presenta un análisis de estas opciones, considerando las normativas relevantes para la gestión de datos en el sector público, y el impacto de su condicionamiento:

2.1. Mainframes: Legado en Entredicho

Las instituciones gubernamentales han utilizado tradicionalmente Mainframes debido a su capacidad para manejar grandes volúmenes de transacciones y su confiabilidad.

Sin embargo, su elevado costo y su falta de flexibilidad para adaptarse a las demandas tecnológicas han llevado a muchos gobiernos a explorar alternativas. Tal como lo describe Zlatanov [1], la tendencia actual se inclina hacia la adopción de soluciones más flexibles y escalables, como la computación en la nube. La arquitectura propietaria de los mainframes y su dependencia de un único proveedor: IBM, generan una serie de desventajas para los gobiernos:

- **Altos Costos de Propiedad:** Los mainframes se caracterizan por sus elevados costos de hardware, software, mantenimiento y personal especializado, dificultando su justificación en contextos de restricciones presupuestarias [2]. La incompatibilidad del software de mainframe con la Ley 13.139 de Software Libre de Santa Fe [3] exige un trámite de excepción para su adquisición e implementación.

- **Inflexibilidad y Resistencia al Cambio:** Su arquitectura cerrada limita la integración de nuevas tecnologías y la adaptación a las demandas cambiantes del entorno digital [5].

- **Riesgos de Seguridad:** La dependencia de un único proveedor y un ecosistema cerrado limita las opciones de seguridad y aumenta la vulnerabilidad a ciberataques. Requiere la implementación de capas de comunicaciones y ciberseguridad externas que elevan el costo operativo y la complejidad de administración.

2.2. Computación en la Nube: Entre Promesas y Desafíos

La computación en la nube, con sus diferentes modalidades (pública, privada e híbrida), se presenta como una alternativa atractiva, ofreciendo escalabilidad, flexibilidad y un modelo de pago por uso “potencialmente” más económico, al menos en las primeras etapas. Sin embargo, esta transición no está exenta de desafíos, especialmente en lo que respecta a la gestión de datos sensibles y a los modelos de contratación basados en el consumo flexible y en moneda extranjera:

- **Soberanía de Datos:** La ubicación de los datos en servidores de proveedores externos, a

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

menudo fuera del territorio nacional, plantea serias preocupaciones sobre la soberanía de datos, un aspecto crucial para los gobiernos. Esta situación podría plantear desafíos de compatibilidad con las legislaciones nacionales de protección de datos, como la Ley 25.326 de Argentina.

– **Seguridad y Privacidad:** A pesar de los avances en seguridad en la nube, la cesión del control de los datos a un tercero siempre genera riesgos para la privacidad y la confidencialidad de la información. Esta variable, en el caso de gobiernos tiene un impacto superior respecto a la implementación en el sector privado, especialmente por el tipo de información ya que se incluyen desde datos médicos, hasta fiscales y/o prontuarios.

– **Costos Ocultos:** El modelo de pago por uso, si bien aparentemente atractivo, puede generar desvíos significativos en los costos previstos a largo plazo, especialmente en economías volátiles. Los costos ocultos, como la dependencia del proveedor, el ancho de banda y la seguridad adicional, pueden impactar significativamente en el presupuesto [6].

- **Contrataciones:** La Ley de Administración Pública presenta un obstáculo para la adopción de la nube en el sector público, ya que no contempla un formato adecuado para adquirir este tipo de servicios, especialmente en lo que respecta a los consumos elásticos (bajo demanda) en las licitaciones. Una excepción a esta limitación es ARSAT, el prestador estatal de telecomunicaciones y nube. Al ser una empresa pública, los organismos gubernamentales (nacionales, provinciales o municipales) pueden acceder a sus servicios sin necesidad de licitación. ARSAT ofrece dos modalidades: "pago por uso" (facturación posterior) y "reserva de uso" (pago adelantado a cuenta de consumo), siendo esta última más económica. Sin embargo, la contratación de servicios de otros proveedores, como AWS, Azure o Google, resulta inviable debido a las restricciones actuales para gestionar el consumo elástico en dólares en el marco de la normativa de compras públicas.

2.3. Plataformas Open x86 y la Ley de Software Libre: Un Camino hacia la Independencia Tecnológica

En el contexto de la administración pública, y en contraste con las soluciones de nube, las plataformas Open, basadas en la arquitectura Intel x86, han ganado popularidad debido a su compatibilidad con el software libre y a la posibilidad de construir centros de datos propios, reduciendo la dependencia de proveedores externos. La Ley de Software Libre 13.139 de la provincia de Santa Fe, Argentina, es un claro ejemplo de cómo la normativa puede impulsar la adopción de tecnologías abiertas en el sector público [3].

La adopción de software libre, como Linux, no solo reduce costos al evitar las licencias propietarias, sino que también fomenta la transparencia, la colaboración y la innovación, valores fundamentales para la gestión pública efectiva [5].

La virtualización, la orquestación de contenedores y las tecnologías serverless constituyen pilares para la eficiencia, simplifican la gestión, optimizan recursos y brindan alta disponibilidad y escalabilidad horizontal.

3. Marco Normativo Argentino para la Gestión de la Tecnología

La gestión de la tecnología en Argentina se rige por un marco normativo organizado en tres niveles: Nacional, Provincial y Municipal, cada uno con responsabilidades y competencias específicas. A nivel nacional, la Ley de Protección de Datos Personales N.º 25.326 [4] establece las bases para la protección de datos personales, mientras que la Estrategia Nacional de Ciberseguridad [7] y la Decisión Administrativa 641/2021 [8] establecen directrices en materia de ciberseguridad. Aunque la provincia de Santa Fe no adhiere a esta última normativa, las adquisiciones tecnológicas que hiciere financiadas por el Consejo Federal de Inversiones (CFI) sí se encuentran bajo su alcance.

Santa Fe, al igual que las demás provincias,

	Gestión Integral de ciberseguridad para Routers Mikrotik	Pág. 113 de 120
---	--	-----------------

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

goza de autonomía para legislar sobre tecnología, tal como lo demuestra la Ley de Software Libre N.º 13.139 [3], que impone la obligatoriedad del uso de software libre en la administración pública provincial, a diferencia de la legislación nacional, que no establece un carácter obligatorio en este aspecto.

La gestión de la tecnología en el poder ejecutivo de Santa Fe recae en el Ministerio de Gestión Pública, a través de la Secretaría de Tecnologías para la Gestión (STG) como organismo rector en tecnología. Si bien Santa Fe no cuenta con una normativa específica sobre ciberseguridad, las resoluciones sobre este tema las emite la STG. La Mesa Provincial de Ciberseguridad, experiencia única en el país donde trabajaron en conjunto los tres poderes del Estado provincial y las empresas de energía y servicios sanitarios como actores de infraestructura crítica y activa entre 2022 y 2023, sentó las bases para la unificación de políticas y estándares en la materia, buscando una gestión integral y coordinada de la ciberseguridad en el gobierno provincial de Santa Fe.

4. Metodología para la Definición de Tecnología y Arquitectura en Infraestructura Gubernamental: Un Enfoque por Etapas

La selección de la tecnología y la arquitectura para la infraestructura de TI gubernamental constituye una decisión estratégica que exige un enfoque metodológico riguroso [6]. Este enfoque debe considerar los aspectos técnicos, las necesidades operativas, el marco normativo, la seguridad, la sustentabilidad y las restricciones presupuestarias.

Para la construcción del consenso sobre los criterios de selección tecnológica, se ha elegido el método Delphi. Este método, basado en la consulta iterativa a un panel de expertos, se destaca por su capacidad para generar un consenso sólido y fundamentado en un entorno de anonimato y retroalimentación controlada. La naturaleza iterativa del Delphi permite refinar las opiniones de los expertos a medida que se analizan las perspectivas del grupo,

evitando la influencia grupal y la dominación de opiniones individuales. La flexibilidad geográfica del método facilita la participación de un grupo más diverso de expertos, enriqueciendo el análisis con una variedad de perspectivas y experiencias.

Para guiar este proceso de toma de decisiones, se propone la siguiente metodología de cinco etapas:

4.1. Análisis de Requerimientos y Contexto

Esta etapa se centra en comprender las necesidades específicas de la administración pública y su contexto operativo, normativo y presupuestario.

- **Recolección de Requerimientos:** A través de entrevistas y talleres con los responsables de las áreas clave del gobierno, se identificarán los requisitos funcionales y no funcionales de la infraestructura de TI.

- **Evaluación del Contexto Normativo:** Se analizarán las normativas locales, provinciales y nacionales aplicables, incluyendo la Ley de Software Libre 13.139 [3] en la provincia de Santa Fe y la Ley de Protección de Datos Personales 25.326 [4], para garantizar que la arquitectura cumpla con todas las regulaciones vigentes.

- **Análisis del Contexto Presupuestario:** Se evaluará el presupuesto disponible y las restricciones financieras, asegurando que la solución tecnológica propuesta sea viable desde un punto de vista económico y alineada a los requerimientos de contratación del organismo.

4.2. Evaluación de Tecnologías Disponibles

La segunda etapa se centra en la identificación de tecnologías y arquitecturas que potencialmente podrían satisfacer los requerimientos identificados, considerando sus características técnicas, de seguridad y costo.

- **Revisión de Tecnologías Existentes:** Se analizarán las opciones disponibles, incluyendo mainframes, plataformas Open basadas en x86, y soluciones de computación en la nube (pública, privada e híbrida).

- **Análisis Comparativo:** Se realizará un análisis comparativo basado en criterios clave

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

como eficiencia, escalabilidad, seguridad, flexibilidad, costo total de propiedad (TCO) y cumplimiento normativo.

- **Estudio de Casos:** Se revisarán casos de estudio y experiencias de otras administraciones públicas que hayan implementado soluciones similares, para identificar lecciones aprendidas y buenas prácticas.

4.3. Diseño de la Arquitectura Tecnológica

Con base en los resultados de las etapas anteriores, se diseñará una arquitectura tecnológica que satisfaga los requerimientos del gobierno y se alinee con las tecnologías seleccionadas.

- **Modelado de la Arquitectura:** Se utilizarán herramientas de modelado arquitectónico, como TOGAF o ArchiMate, para diseñar la arquitectura tecnológica, especificando componentes clave como servidores, redes, almacenamiento y aplicaciones.

- **Integración de Tecnologías:** Se garantizará la compatibilidad de la arquitectura con las tecnologías y sistemas existentes, incluyendo plataformas legacy, y se considerará la escalabilidad futura.

- **Planificación de Seguridad:** Se incorporarán medidas de seguridad desde el diseño, incluyendo control de acceso, cifrado y sistemas de prevención de intrusiones, en cumplimiento con la normativa de ciberseguridad vigente.

4.4. Validación y Prueba de Concepto

Se validará la viabilidad técnica y operativa de la arquitectura propuesta a través de pruebas en un entorno controlado.

- **Desarrollo de una Prueba de Concepto (PoC):** Se implementará una PoC para validar que la arquitectura propuesta cumple con los requisitos operativos y de seguridad.

- **Evaluación de Resultados:** Se analizarán los resultados de la PoC para identificar posibles

problemas o áreas de mejora, y ajustar el diseño de la arquitectura según sea necesario. Se presentarán los resultados de la PoC a las partes interesadas (stakeholders), clave para obtener retroalimentación y asegurar la aceptación del proyecto.

4.5. Implementación y Gestión del Cambio

Finalmente, se implementará la arquitectura tecnológica y se gestionará el cambio hacia la nueva infraestructura.

- **Planificación de la Implementación:** Se desarrollará un plan de implementación detallado, incluyendo cronogramas, recursos necesarios y gestión de riesgos.

- **Gestión del Cambio:** Se implementará un plan de gestión del cambio para minimizar la resistencia y asegurar una transición fluida, incluyendo comunicación constante con los usuarios finales y soporte técnico.

- **Monitoreo y Optimización Continua:** Se establecerá un sistema de monitoreo continuo para asegurar el rendimiento óptimo de la infraestructura y se realizarán revisiones periódicas para identificar áreas de mejora y adaptar la infraestructura a las nuevas necesidades.

4.6. La gestión de riesgos: Será un componente integral de la metodología. Se implementará un proceso para la identificación, análisis y mitigación de los riesgos asociados a la modernización de la infraestructura. Los riesgos serán categorizados y priorizados mediante una matriz de riesgo, considerando su impacto potencial y probabilidad de ocurrencia. Se diseñarán estrategias de mitigación, incluyendo medidas preventivas, planes de contingencia y mecanismos de control. El plan de gestión de riesgos se revisará periódicamente para adaptarlo a las nuevas necesidades y realidades del entorno

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

Tabla 1. Checklist para la Definición de Tecnología y Arquitectura en Infraestructura Gubernamental

Etapa	Actividad	Checklist	Val.	Evento - Riesgo - Mitigación
1. Análisis de Requerimientos y Contexto	Requerimiento	¿Se identificaron y documentaron los requisitos funcionales y no funcionales de la infraestructura?	☐ Sí ☒ No 50%	Evento: Identificación parcial de requisitos. Riesgo: Posibles problemas de funcionalidad. Mitigación: Revisión y complementación de los requisitos.
	Marco Normativo	¿Se analizó la normativa aplicable (Ley de Software Libre 13.139 [3], Ley de Protección de Datos Personales 25.326 [4], etc.)?	☒ Sí ☐ No ___%	Evento: Análisis completo de la normativa aplicable. Riesgo: Mínimo riesgo legal. Mitigación: Mantener un monitoreo de actualizaciones legales.
	Presupuesto	¿Se evaluó el presupuesto disponible, las restricciones financieras y la viabilidad económica de las opciones?	☒ Sí ☐ No ___%	Evento: Evaluación completa del presupuesto. Riesgo: Riesgo económico bajo. Mitigación: Seguimiento de gastos.
2. Evaluación de Tecnologías Disponibles	Tecnologías	¿Se analizaron todas las opciones tecnológicas relevantes (Mainframes, plataformas Open x86, nube púb/priv/híbrida)?	☐ Sí ☐ No ☒ 60%	Evento: Análisis parcial de opciones tecnológicas. Riesgo: Posibles limitaciones en la elección de tecnologías. Mitigación: Ampliar el análisis a otras tecnologías faltantes.
	Análisis Comparativo	¿Se compararon las tecnologías en base a criterios de eficiencia, escalabilidad, seguridad, flexibilidad, TCO y cumplimiento normativo?	☐ Sí ☐ No ☒ 40%	Evento: Comparación parcial de tecnologías. Riesgo: Posibles riesgos de rendimiento, seguridad o costo. Mitigación: Completar la comparación de tecnologías.
	Estudios de Caso	¿Se revisaron estudios de casos y se identificaron lecciones aprendidas de implementaciones similares?	☐ Sí ☒ No ___%	Evento: Falta de revisión de estudios de casos. Riesgo: Riesgo de repetir errores. Mitigación: Buscar y estudiar casos de implementación similares.
3. Diseño de la Arquitectura Tecnológica	Modelado	¿Se diseñó la arquitectura con una herramienta adecuada (TOGAF, ArchiMate), detallando los componentes clave?	☒ Sí ☐ No ___%	Evento: Diseño completo de la arquitectura. Riesgo: Bajo riesgo de errores en la implementación. Mitigación: Revisar y asegurar la coherencia del diseño.
	Integración y Escalabilidad	¿Se aseguró la compatibilidad con sistemas legacy y se consideró la escalabilidad futura?	☐ Sí ☒ No ___%	Evento: Falta de consideración de la escalabilidad y/o compatibilidad. Riesgo: Posibles problemas de rendimiento o compatibilidad con sistemas actuales.

 Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

				Mitigación: Reconsiderar la escalabilidad a futuro en el diseño y opciones de compatibilidad.
	Seguridad	¿Se incorporaron medidas de seguridad y se alineó el diseño con la normativa de ciberseguridad?	☐ Sí ☒ No ☐ ___%	Evento: Falta de medidas de seguridad. Riesgo: Vulnerabilidades de seguridad. Mitigación: Incorporar medidas de seguridad robustas en el diseño para cumplir con la normativa actual.
4. Validación y Prueba de Concepto	PoC	¿Se implementó y evaluó una Prueba de Concepto (PoC) para validar la arquitectura?	☐ Sí ☒ No ☐ ___%	Evento: Falta de prueba de concepto. Riesgo: Posibles errores en la implementación. Mitigación: Implementar y evaluar una prueba de concepto.
	Stakeholders	¿Se presentaron los resultados de la PoC a los stakeholders y se obtuvo su retroalimentación?	☐ Sí ☒ No ☐ ___%	Evento: Falta de presentación de resultados de la PoC. Riesgo: Rechazo del proyecto por parte de los stakeholders. Mitigación: Presentar los resultados a los stakeholders y obtener su retroalimentación.
5. Implementación y Gestión del Cambio	Planificación	¿Se elaboró un plan de implementación detallado?	☒ Sí ☐ No ☐ ___%	Evento: Plan de implementación detallado. Riesgo: Riesgo de retraso bajo. Mitigación: Revisar y asegurar la coherencia del plan.
	Gestión del Cambio	¿Se implementó un plan de gestión del cambio, incluyendo comunicación con los usuarios y soporte técnico?	☐ Sí ☒ No ☐ ___%	Evento: Falta plan de gestión del cambio. Riesgo: Resistencia al cambio por parte de los usuarios. Mitigación: Implementar un plan de gestión del cambio.
	Monitoreo y Optimización	¿Se implementó un sistema de monitoreo y se planificaron revisiones para optimizar la infraestructura?	☐ Sí ☒ No ☐ ___%	Evento: Falta de sistema de monitoreo. Riesgo: Problemas de rendimiento o seguridad. Mitigación: Implementar un sistema de monitoreo.

5. Framework de trabajo:

Para gestionar y evaluar el avance en cada etapa del proceso de modernización de los centros de datos, se utilizará un checklist como el presentado en la Tabla 1. Este documento servirá como herramienta de control para asegurar que se completen todas las actividades necesarias en cada etapa e identificar de forma temprana riesgos potenciales.

El análisis de las respuestas del checklist, como se ejemplifica en la Tabla 1, permitirá:

- Evaluar el nivel de avance del proyecto en cada etapa, identificando las actividades completadas y las pendientes.- Detectar y

analizar riesgos en términos de su impacto potencial y probabilidad de ocurrencia.

- Definir medidas de mitigación para los riesgos identificados, incluyendo acciones preventivas, planes de contingencia y mecanismos de control.

- Facilitar la toma de decisiones informadas sobre el curso del proyecto, permitiendo ajustar el plan según sea necesario para alcanzar los objetivos propuestos.

5.1 Análisis de las respuestas de Tabla 1

En este ejemplo, la última columna analiza las respuestas al campo “Valoración”, determinando los riesgos tecnológicos, financieros, legales y operativos, así como las medidas de mitigación, en función del

	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

cumplimiento. El análisis de la Tabla 1 revela un avance significativo en la planificación del proyecto de modernización. Se evidencia que gran parte de los requisitos para la implementación del proyecto se han cubierto. Sin embargo, existen algunas áreas donde se detectan riesgos que requieren atención. La identificación de requisitos aún no está completa, lo que podría generar problemas de funcionalidad si no se aborda a tiempo. Es fundamental considerar la escalabilidad y retrocompatibilidad en el diseño para asegurar la interoperabilidad con sistemas legacy y la capacidad de adaptación a nuevas tecnologías. La ciberseguridad también representa un punto crítico, ya que el diseño actual carece de medidas de seguridad robustas para evitar ataques y pérdida de datos. La falta de pruebas de concepto aumenta el riesgo de errores en la implementación, cuya solución podría preverse. La ausencia de un plan de gestión del cambio podría generar resistencia por parte de los usuarios y dificultar la transición a la nueva infraestructura. Se recomienda diseñar un plan que contemple estrategias de comunicación, capacitación y soporte técnico para asegurar una adopción fluida de la nueva tecnología. No disponer de un sistema de monitoreo podría acarrear problemas de rendimiento o seguridad en el futuro. Para mitigar estos riesgos y asegurar el éxito de la implementación, es fundamental completar la identificación de requisitos. Si se toman estas medidas, el proyecto tendrá altas probabilidades de éxito.

6. Conclusión: Este trabajo propone una metodología estructurada y exhaustiva para abordar el desafío de la selección de tecnologías y arquitecturas para los centros de datos gubernamentales. A través de un análisis comparativo de las principales opciones tecnológicas, como Mainframes, plataformas Open x86 y soluciones de computación en la nube, y la aplicación de un enfoque por etapas basado en el método Delphi, este estudio busca proporcionar a los responsables de tecnología del sector público una herramienta efectiva para la modernización de sus infraestructuras.

La metodología propuesta considera aspectos clave como los requisitos funcionales y no funcionales, el contexto normativo (como la Ley de Software Libre 13.139 y la Ley de Protección de Datos Personales 25.326), las restricciones presupuestarias y los criterios de eficiencia, escalabilidad, seguridad, flexibilidad y costo total de propiedad (TCO). Además, el estudio destaca la importancia de integrar las tecnologías seleccionadas con los sistemas existentes, planificar minuciosamente la seguridad desde el diseño y llevar a cabo pruebas de concepto para validar la viabilidad técnica y operativa de la arquitectura propuesta. En el contexto de gobierno, en este caso el de Santa Fe, Argentina, este trabajo brinda una herramienta valiosa para la toma de decisiones estratégicas en la modernización de los centros de datos, asegurando así la eficiencia, seguridad y soberanía e independencia tecnológicas.

Referencias

- [1] N. Zlatanov, "The data center evolution from Mainframe to Cloud," *ResearchGate, IEEE Computer Society*, 2016. DOI: 10.13140/RG.2.1.4103.8489.
- [2] L. Joyanes, "Computación en Nube (Cloud Computing) y Centros de Datos: La nueva revolución industrial ¿Cómo cambiará el trabajo en organizaciones y empresas?," *SOCIEDAD Y UTOPIA. Revista de Ciencias Sociales*, n.º 36, pp. 111-128, Nov. 2010.
- [3] H.C. Diputados de Santa Fe, Ley N.º 13.139. Software Libre en la Administración Pública Provincial, Santa Fe, Argentina, 2013. Disponible en: <https://www.santafe.gob.ar/normativa/getNorma.php?id=166534>
- [4] República Argentina. (2000). Ley de Protección de Datos Personales 25.326. Disponible en: <https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm>
- [5] L. Joyanes Aguilar, "Computación en nube (Cloud computing): El nuevo paradigma tecnológico para empresas y organizaciones en la sociedad del conocimiento". *ICADE: Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales*, no. 76, pp. 95-111, 2010.
- [6] S. D. Lowe, J. Green, & D. Davis, *Building a Modern Data Center: Principles and Strategies of Design*. ActualTech Media, 2016.
- [7] Jefatura de Gabinete de Ministros, Estrategia Nacional de Ciberseguridad. República Argentina, 2019. [En línea]. Disponible en: <https://www.boletinoficial.gob.ar/detalleAviso/primera/208317/20190528>

 UAI Universidad Abierta Interamericana	Corvalán, Fernando Andres Leg B00061099-T7	
Poncio Silvia Victoria Audoglio Pablo Andres	Trabajo Final - 12/2024	

[8] J.G.Ministros. Sec de Innovación Pública. Dir. Nac. de Ciberseguridad, DA 641/2021. Gestión de riesgos en la APN, Argentina, 2021.