Universidad Nacional José Faustino Sánchez Carrión

Facultad de Ingeniería Industrial, Sistemas e Informática

Escuela Profesional de Ingeniería Informática

Soluciones de ciberseguridad - Empresa Intecnia, Corp S.A.C y Safe Network S.A.C

Tesis

Para optar el Título Profesional de Ingeniero Informático

Autor

Wilson Zacarias Diaz Cordova

Asesor

Ing. Javier Alberto Manrique Quiñonez

Huacho - Perú

2025

UNIVERSIDAD NACIONAL
JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

LICENCIADA

(Resolución de Consejo Directivo N° 012-2020-SUNEDU/CD de fecha 27/01/2020

Facultad de Ingeniería Industrial, Sistemas e Informática
Escuela Profesional de Ingeniería Informática

METADATOS

DATOS DEL AUTOR (ES):		
APELLIDOS Y NOMBRES	**DNI**	**FECHA DE SUSTENTACIÓN**
Wilson Zacarias Diaz Cordova	46222553	27/12/2024
DATOS DEL ASESOR:		
APELLIDOS Y NOMBRES	**DNI**	**CÓDIGO ORCID**
Javier Alberto Manrique Quiñonez	15646920	0000-0001-9789-9881
DATOS DE LOS MIEMBROS DE JURADOS – PREGRADO/POSGRADO-MAESTRÍA-DOCTORADO:		
APELLIDOS Y NOMBRES	**DNI**	**CÓDIGO ORCID**
Carlos Enrique Bernal Valladares	15614554	0000-0002-7421-9537
Eddy Ivan Quispe Soto	15760232	0009-0004-1671-8524
Ulises Robert Martínez Chafalote	15616588	0000-0002-9523-308X

Díaz Córdova Wilson Zacarías 2024-088082

Soluciones de Ciberseguridad Empresa Intecnia Corp S.A.C. y Safe Network S.A.C.

Quick Submit

Quick Submit

Facultad de Ingeniería Industrial, Sistemas e Informática

Detalles del documento

Identificador de la entrega
trn:oid:::1:3116950967

Fecha de entrega
16 dic 2024, 2:32 p.m. GMT-5

Fecha de descarga
16 dic 2024, 2:33 p.m. GMT-5

Nombre de archivo
rdova_Wilson_Zacar_as_-_Informe_de_suficiencia_profesional.docx

Tamaño de archivo
2.6 MB

59 Páginas

9,460 Palabras

54,254 Caracteres

11% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Fuentes principales

10% Fuentes de Internet

0% Publicaciones

4% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.° de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

FACULTAD DE INGENIERÍA INDUSTRIAL SISTEMAS E INFORMÁTICA

ESCUELA RPOFESIONAL DE INGENIERÍA INFORMÁTICA

Soluciones de Ciberseguridad

Empresa Intecnia Corp S.A.C. y Safe Network S.A.C.

Sustentado y aprobado ante el Jurado Evaluador

PRESIDENTE Ing. Carlos Enrique Bernal Valladares	SECRETARIO Ing. Eddy Iván Quispe Soto
VOCAL Ing. Ulises Robert Martínez Chafalote	ASESOR Ing. Javier Alberto Manrique Quiñonez

HUACHO – PERÚ
2024

Dedicatoria

Dedicado a mis padres, a mi querida esposa

y a mis 2 grandiosos hijos.

Agradecimientos

A Dios, a mi familia, a mi asesor y a las personas que fueron parte de esta experiencia en cada una de las empresas.

Índice

Índice de figuras

Índice de Anexos

Resumen

Este informe detalla mi recorrido laboral en Intecnia Corp S.A.C. y Safe Network SAC, donde desempeñé cargos como Ingeniero de Preventa de Seguridad e Ingeniero de Soluciones de T.I. (Tecnología de Información) respectivamente y lo cual son cargos muy afines o similares.

En el Capítulo I comienza con un análisis detallado de la empresa Intecnia Corp S.A.C., desde sus inicios hasta la actualidad. Se presenta la principal línea de negocio de la empresa, su visión, misión, la cartera de clientes a nivel nacional e información de interés. Además, se detallan las funciones y actividades desarrolladas durante mi permanencia en el departamento de Ingeniería, desempeñando el rol de Ingeniero de Preventa de Seguridad.

En el Capítulo II continua mi experiencia laboral, pero ahora en la empresa Safe Network S.A.C. donde desempeñe un cargo similar llamado Ingeniero de Soluciones de T.I. Este capítulo incluye la describe la principal línea de negocio de la empresa, su visión, misión, la cartera de clientes a nivel nacional. Además, se detallan las funciones y actividades desarrolladas en esa empresa.

El Capítulo III se centra en las conclusiones y recomendaciones extraídas de mi experiencia laboral en ambas empresas. Destaco los aprendizajes clave adquiridos durante este periodo resaltando cómo estas vivencias han contribuido significativamente a mi crecimiento profesional. Además, presento recomendaciones que buscan abordar los desafíos presentes a esta línea de negocio. Estas sugerencias se basan en la experiencia acumulada durante mi trayectoria y están dirigidas a proporcionar una guía útil para futuros profesionales que desempeñen roles similares.

Palabras claves: Experiencia laboral, la cartera de clientes a nivel nacional y funciones

Abstract

This report details my work history at Intecnia Corp S.A.C. and Safe Network S.A.C., where I held positions as Security Pre-Sales Engineer and IT Solutions Engineer. (Information Technology) respectively and which are very related or similar positions.

Chapter I begins with a detailed analysis of the company Intecnia Corp S.A.C., from its beginnings to the present. The company's main line of business, its vision, mission, national client portfolio and information of interest are presented. In addition, the functions and activities developed during my stay in the Engineering department are detailed, performing the role of Security Pre-Sales Engineer.

In Chapter II my work experience continues, but now in the company Safe Network S.A.C. where I hold a similar position called IT Solutions Engineer, this chapter includes a description of the company's main line of business, its vision, mission, and client portfolio nationwide. In addition, the functions and activities carried out in that company are detailed.

Chapter III focuses on the conclusions and recommendations drawn from my work experience in both companies. I highlight the key learnings acquired during this period, highlighting how these experiences have contributed significantly to my professional growth, and I also present recommendations that seek to address the challenges present in this line of business. These suggestions are based on the experience accumulated during my career and are aimed at providing useful guidance for future professionals who perform similar roles.

Keywords: Work experience, national client portfolio and functions

Introducción

La ciberseguridad ha ganado relevancia en el entorno empresarial donde la información viaja por la red local e internet y por ello las empresas deben proteger sus activos ante amenazas sofisticadas o desconocidas. La evolución de las amenazas digitales ha originado una preocupación en todas las empresas porque día a día se incrementan ataques que pueden ser phishing, ataques sin archivos, ransomware e intrusiones avanzadas. Todo esto ha aumentado la importancia de implementar soluciones de ciberseguridad completas y robustas.

Las empresas Intecnia corp S.A.C. y Safe Network S.A.C. se caracterizan por brindar soluciones de empresas líderes de ciberseguridad.

La empresa Intecnia Corp S.A.C. es el máximo representante de Bitdefender en el Perú, teniendo la total distribución de todas las soluciones desde productos de uso personal hasta soluciones corporativas. Su principal labor de esta empresa es la de formar resellers o canales certificados que puedan comercializar las soluciones de Bitdefender y teniendo una cobertura nacional de más de 50 canales de venta y más de 3000 empresas clientes licenciadas con Bitdefender.

La empresa Safe Network S.A.C. es un canal Silver de Bitdefender asociada al Country Partner de Bitdefender (Intecnia Corp S.A.C.), actúa como un distribuidor de sus soluciones corporativas, esta empresa cuenta con todas las certificaciones comerciales y técnicas de Bitdefender, cuenta con aproximadamente 40 empresas como clientes.

Desempeñar cada una de las funciones en cada una de estas empresas me ayudó a conocer diferentes tipos de tecnología, desde la administración de servidores hasta la administración de plataformas virtuales o en nube (Cloud Services).

El presente informe detallo mi experiencia laboral en cada empresa, las dificultades, el compromiso y metas alcanzadas durante mi permanencia en ellas.

Empresa Intecnia Corp S.A.C.

1.1 Datos de la organización

1.1.1 Descripción del origen de Intecnia Corp S.A.C.

Intecnia Corp S.A.C. es una sociedad anónima cerrada que comenzó sus operaciones el 1 de noviembre de 2012 consolidándose como una empresa líder de soluciones de ciberseguridad.

Dentro de las marcas que ha representado tenemos a Kaspersky y actualmente representa a nivel nacional a Bitdefender una solución líder en ciberseguridad.

Intecnia Corp S.A.C. opera un sistema de canales (Bronze, Silver y Gold), lo que subraya el compromiso con la expansión y la difusión de la marca. En la estructura de canales de distribución, la empresa cuenta con más de 50 empresas dedicadas a distribuir soluciones de Bitdefender.

Además, Intecnia Corp S.A.C. ha consolidado alianzas estratégicas con los más importantes mayoristas del país, entre ellos se destacan empresas reconocidas internacionalmente como Grupo Deltron S.A., PC Link e Intcomex. La presencia en estos importantes mayoristas posiciona a la empresa en un lugar privilegiado para llegar a una amplia gama de clientes y usuarios finales.

1.1.2 Misión y visión de Intecnia Corp S.A.C.

La misión de la empresa se expresa de la siguiente manera: “Brindar soluciones tecnológicas innovadoras que complementen/impulsen de forma positiva la vida digital moderna de las familias y fortalezcan las operaciones y actividades de las empresas peruanas”.

La visión de la empresa se expresa de la siguiente manera “Queremos que las personas se desarrollen con libertad en el mundo digital, sintiéndose protegidas y donde el

conocimiento de tecnología aplicada a la educación esté siempre al alcance de las nuevas generaciones, sin distinción".

Los valores que considera la empresa como pilares de su organización son "honestidad, resiliencia, compromiso, innovación y unión."

1.1.3 Datos Generales de la Empresa

1.1.3.1 Nombre comercial

Razón Social: Intecnia Corp S.A.C.

Registro único de contribuyente (R.U.C.): 20550187664

Dirección: Av. Javier Prado Este Nro. 175 Interior 1201 urb. Fundo Conde de San Isidro Lima - Lima - San Isidro

Actividades económicas: Otras Actividades de Tecnología de la Información y de Servicios Informáticos

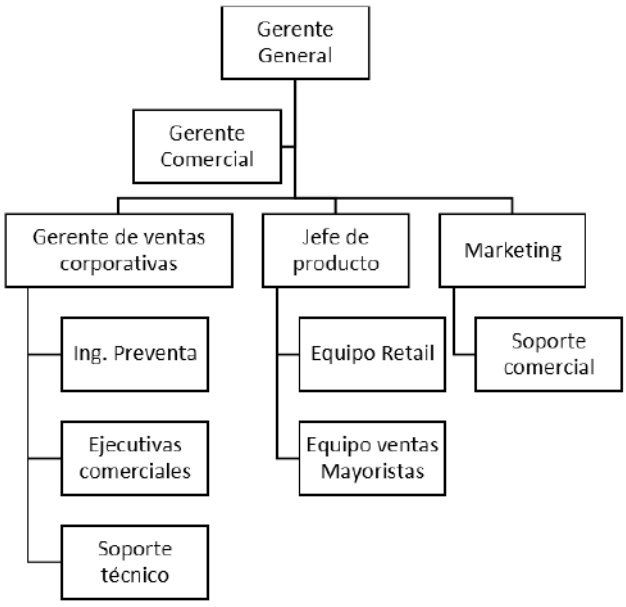
Página web: https://intecniacorp.pe

1.1.3.2 Organigrama

El organigrama se presenta en la figura 1.

Figura 1

Organigrama de Intecnia Corp S.A.C.



1.1.4 Tamaño de la empresa

Intecnia Corp S.A.C. Al cierre del 2022 contaba con más de 25 colaboradores.

1.1.5 Giro del negocio

Intecnia Corp S.A.C. su principal giro de negocio es el de comercializar y representar a nivel nacional a Bitdefender que una empresa líder mundial de software de seguridad informática.

1.1.6 Mercados que atiende

Intecnia Corp S.A.C. abarca un mercado amplio y ofrece soluciones de ciberseguridad de Bitdefender a nivel nacional. Su cartera está dirigida a una amplia gama de clientes, desde empresas privadas hasta entidades gubernamentales, instituciones de salud, entidades financieras, instituciones educativas y más.

1.1.7 Principales productos

Los productos o servicios que brinda Intecnia Corp S.A.C. son:

a) Bitdefender Gravityzone (Producto/servicio principal)

Bitdefender Gravityzone ofrece una amplia gama de soluciones de ciberseguridad dentro de los cuales podemos encontrar los siguientes beneficios y características:

- Es una solución líder en las pruebas independientes de AV-TEST
- Es una solución líder en las pruebas independiente de AV-Comparatives
- Es una solución como visionario en el cuadrante Mágico de Gartner.
- Es una solución líder en el cuadrante de The Forrester Wave.
- Es una solución reconocida y líder en MitreAtt&CK
- Es una solución ampliamente reconocida mundialmente, plataforma centralizada y unificada.
- Solución multiplataforma (Windows, Linux, Mac Os, Android y iOS)

- Solución altamente escalable puede soportar más de 50 mil equipos administrados.
- Solución con consola de administración única para pc, servidores, escritorios virtuales, servidores virtuales, dispositivos móviles.
- Solución con Interfaz Web y descentralizada permite el acceso desde cualquier equipo solo con conexión a internet.
- Solución que no impacta en los recursos del sistema operativo.
- Solución con EDR + XDR para ampliar la visibilidad de los ataques en la compañía.

Bitdefender tiene 03 soluciones base y 04 soluciones complementarias, dentro de ellas tenemos:

Bitdefender Gravityzone Business Security. - Es la solución estándar enfocada para pequeñas y medianas empresas, desde esta solución se pueden encontrar características de protección antimalware y anti-ransomware además ofrece un control para usuarios como control web, control de aplicaciones, control de dispositivos y gestión de riesgos.

Bitdefender Gravityzone Business Security Premium. – Es solución de gama media, esta presentación contiene lo mencionado en la versión Business Security y se agrega tecnologías de Sandboxing, Machine Learning, protección contra Fileless y cuenta con un sensor de investigación forense de ataques.

Esta presentación está enfocada en las medianas empresas que buscan una solución más completa.

Bitdefender Gravityzone Business Security Enterprise. – Es la solución top de Bitdefender contiene lo mencionado en la versión Business y Premium. Esta solución además agrega funcionalidad EDR (Endpoint Detection and Response) y XDR (eXtended

Detection and Response) que son herramientas útiles para analistas de seguridad, donde pueden identificar y analizar el origen de los ataques y crear tareas de remediación.

Con el XDR correlaciona los eventos de seguridad en la red para identificar que equipos están siendo comprometidos en el ataque.

Bitdefender Gravityzone Full-Disk Encryption. – Es una solución complemento que cifra las unidades de disco duro locales de los equipos portátiles con el fin de salvaguardar la información del equipo en caso de pérdida o robo, a través de su integración con la tecnología BitLocker de Microsoft y FileVault de Mac hace que sea imposible de acceder a los datos del equipo sin tener la contraseña ya que estos utilizan patrones de cifrado de grado militar.

Bitdefender Gravityzone Security for Email. – Es una solución complemento que integra tecnologías de protección antimalware, anti-phishing, anti-spoofing y anti-spam para correos electrónicos y se integra con plataforma de Google Platform y Office 365 (Exchange Server en Cloud). Esta solución funciona como un Gatewey filtrando los correos antes de su ingreso al servidor del cliente.

Bitdefender Gravityzone for Mobile. – Es una solución complemento en la que podemos administrar dispositivos móviles ya sea Android o iOS, esto nos permite poder gestionar los dispositivos desde la misma consola de Bitdefender, esta solución presenta características de antimalware y geolocalización.

Bitdefender Gravityzone Patch Management. - Es una solución complemento que nos permite actualizar los parches o actualizaciones críticas, importantes y opcionales del sistema operativo y las aplicaciones instaladas en los equipos informáticos como por ejemplo Microsoft Office, Autodesk Autocad, Adobe; etc.

Esta configuración o tarea se realiza de manera centralizada desde un servidor cache de

actualizaciones, se puede programar para que las descargas sean de madrugada y el aplicado de parches en horario de oficina.

b) Soluciones STEAM

Son productos o soluciones STEAM (Ciencia, tecnología, ingeniería, arte y matemáticas) enfocado en el desarrollo del pensamiento computacional, lógico, cognitivo y creativo de escolares a través del desarrollo de proyectos de robótica, programación y electrónica.

Intecnia Corp S.A.C. representa a Matatalab, Microduino, Crowbits y Snap Circuits.

1.1.8 Procesos del negocio

Intecnia Corp SAC funciona en torno a cuatro procesos clave: gestión de canales, gestión de preventa, gestión de ventas y gestión de postventa.

Los procesos de negocio en el nivel macroprocesos se muestra en la figura 2.

Los procesos estratégicos son:

- Dirección de la empresa o alta dirección.

Los procesos operativos son:

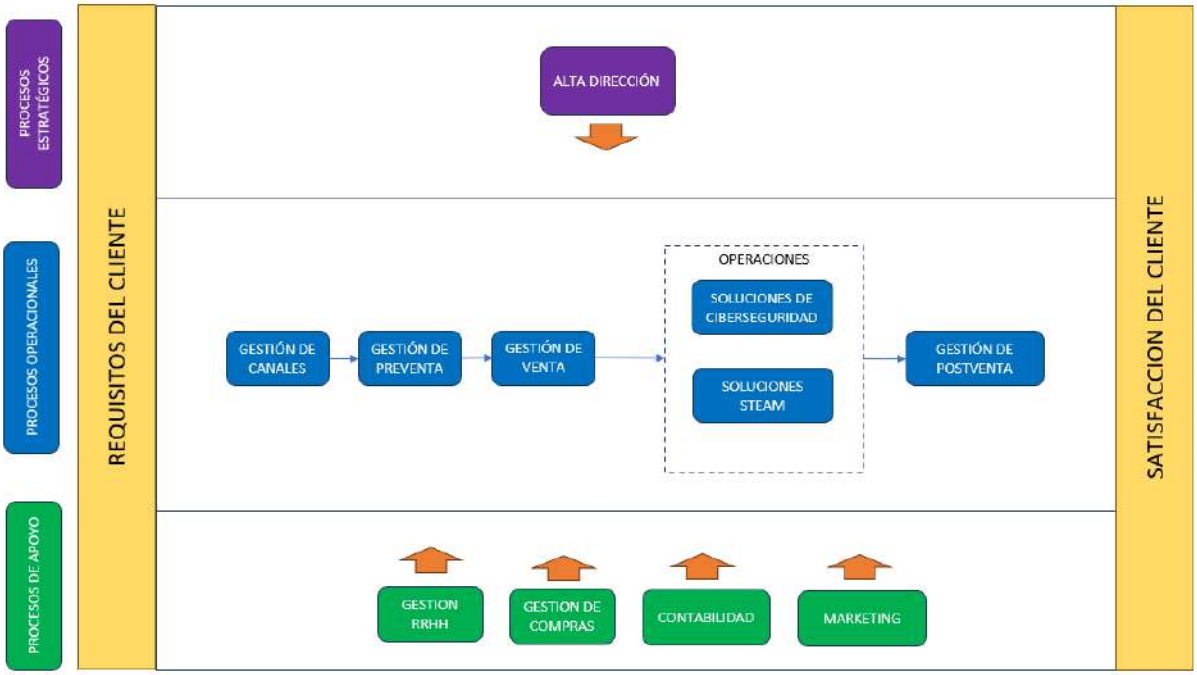
- Gestión de canales
- Gestión de preventa
- Gestión de venta
- Gestión de postventa

Los procesos de soporte son:

- Gestión de RRHH
- Gestión de compras
- Gestión de contabilidad
- Marketing

Figura 2

Mapa de procesos de Intecnia Corp SAC



a) Gestión de canales

La gestión de canales es un proceso clave en Intecnia Corp S.A.C., centrado en la formación y desarrollo de nuevos canales de distribución. Este proceso es fundamental para ampliar el alcance de sus soluciones. Involucra la identificación de posibles socios, la capacitación de nuevos distribuidores y el establecimiento de relaciones sólidas para asegurar un flujo constante de productos y servicios hacia el mercado.

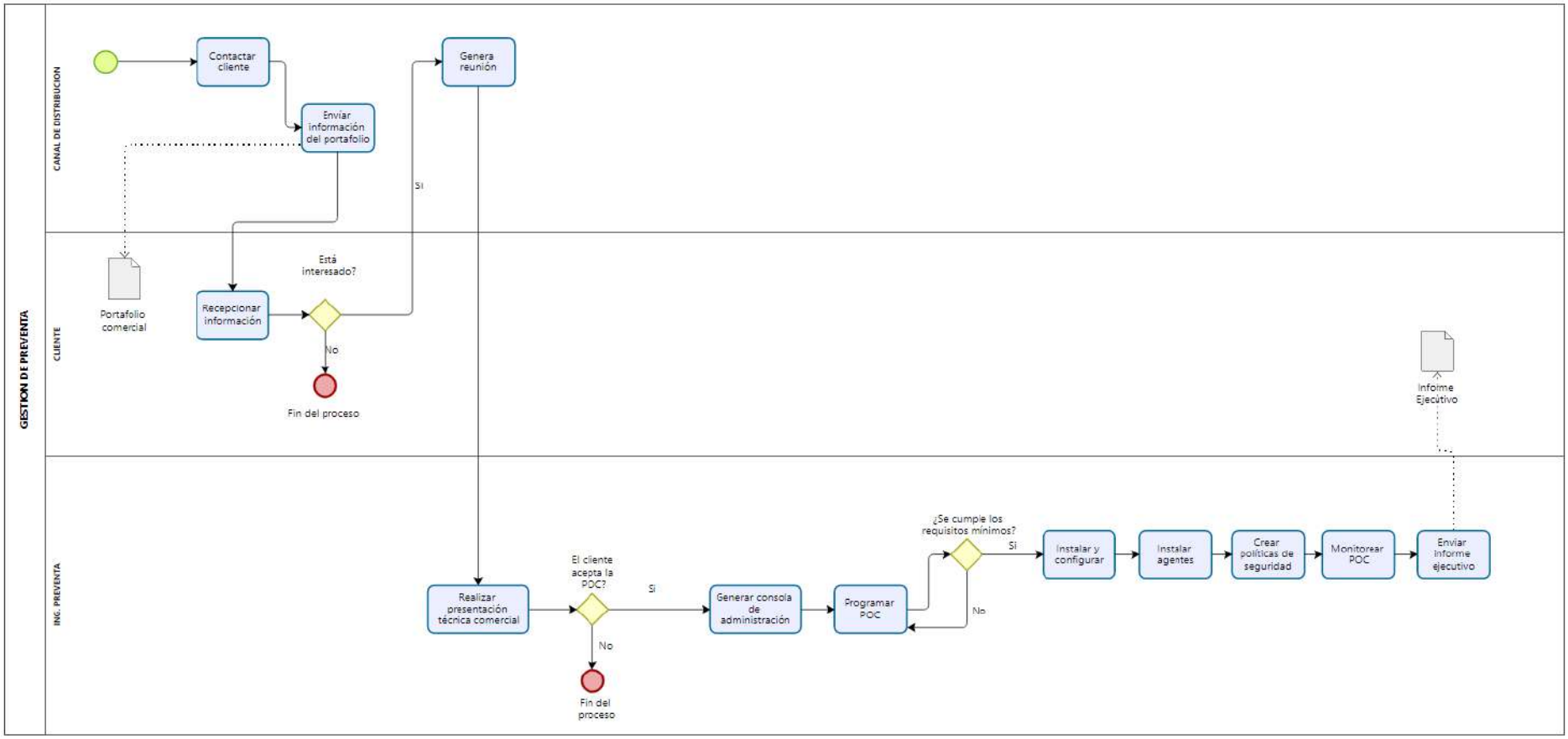
b) Gestión de preventa

La gestión de preventa es el proceso más importante dentro de Intecnia Corp SAC. Aquí es donde se realiza presentaciones técnicas de las soluciones para mostrar su valor y funcionalidad a los clientes potenciales. Durante este proceso, generamos pruebas de concepto (POC) en la infraestructura del cliente para demostrar que la solución puede ayudar al cliente mejorar su postura de seguridad.

La descripción del proceso preventa se visualiza en la figura 3.

Figura 3

Proceso de gestión de preventa de Intecnia Corp S.A.C.



En esta parte es donde el ingeniero preventa de seguridad desempeña un papel crucial y toma el mayor protagonismo. Su responsabilidad principal es realizar presentaciones técnicas para destacar las características más importantes de la solución ofrecida. Durante estas presentaciones, el ingeniero preventa debe abordar y resolver todas las dudas técnicas del jefe de sistemas o de los especialistas de seguridad de la información.

Además, es fundamental que el ingeniero preventa o de soluciones de T.I. busque realizar la famosa prueba de concepto (POC). Esta POC permite demostrar de manera práctica cómo la solución puede integrarse y funcionar en el entorno del cliente.

El ingeniero preventa o de soluciones de TI es responsable de implementar y supervisar la prueba de concepto (POC).

Esta etapa finaliza cuando la solución puesta en POC fue de agrado del ingeniero y recibe la aprobación del área usuaria para su compra.

c) Gestión de venta

Este proceso se inicia cuando el cliente está interesado en la solución y solicita una cotización a su canal de ventas, por su parte el canal de ventas debe comunicar a Intecnia Corp. S.A.C. el interés y debe solicitar la protección de cuenta, que significa que el canal de distribución tiene todo el derecho de atender al cliente.

Intecnia Corp S.A.C. envía la cotización al canal de ventas y este a su vez hace la cotización al cliente final, una vez que el cliente final acepta la propuesta genera una orden de compra que es el documento formal donde se especifica el nombre de la solución, cantidad de equipos a proteger y el tiempo de la licencia.

Una vez que el canal de distribución recibe la orden de compra por parte del cliente, debe generar una orden de compra a favor de Intecnia Corp S.A.C.

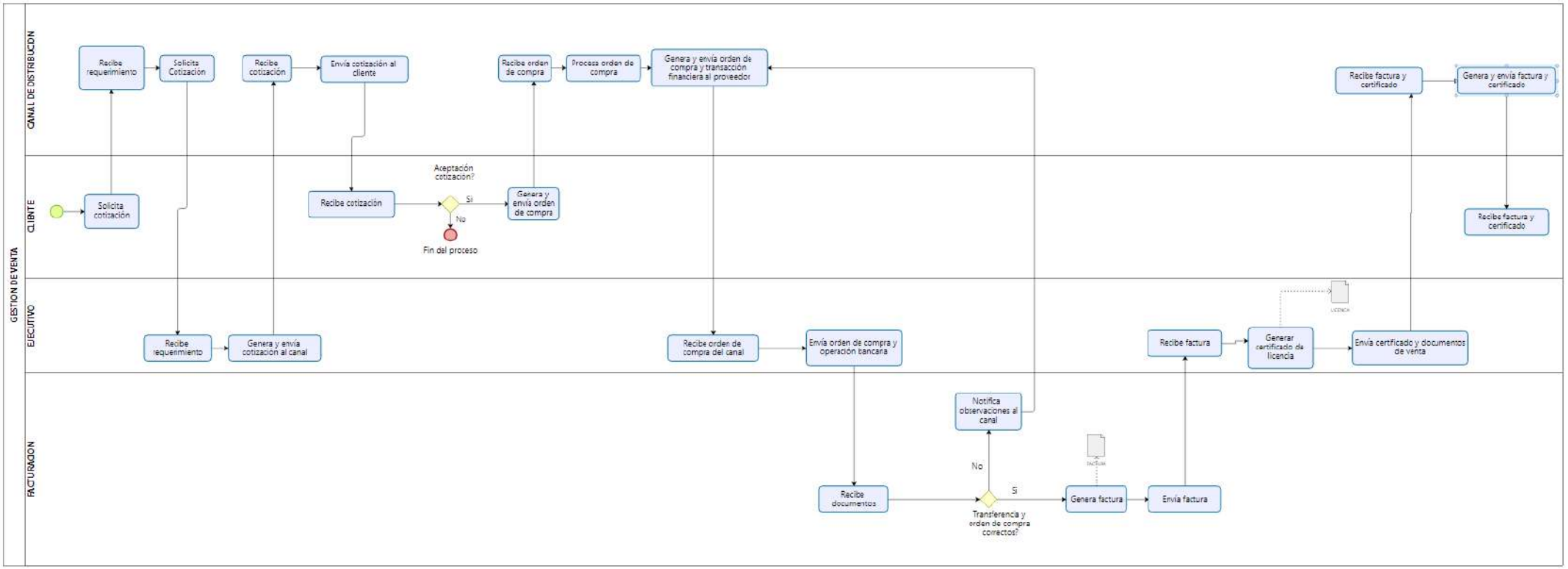
Al recibir la orden de compra Intecnia Corp S.A.C. lo procesa subiéndolo al sistema Bitdefender P.A.N (**Partner Advantage Network)** en este sistema se llena los datos del

canal y del cliente final y como resultado se emite un certificado de licencia el cual es enviado junto con la factura electrónica al canal de distribución, finalmente el canal de distribución envía este certificado junto con su factura al cliente final.

El proceso de gestión de venta se visualiza en la figura 4.

Figura 4

Proceso de gestión de venta de Intecnia Corp S.A.C.



Todo ingeniero preventa es medido por la cantidad de proyectos concretados, cada Q (trimestre), por lo cual asignaba una cuota de venta el cual tenía que cumplirse como un mínimo de 75%.

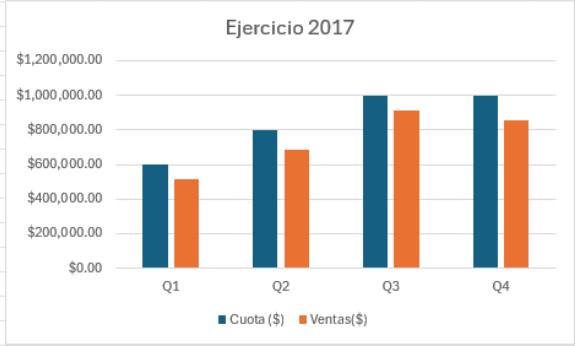
Siempre se cumplió con la cuota asignada. En la figura 5 podemos observar un simulado de las cuotas asignadas por Q (Trimestre) y sus resultados al final de este. Por temas de confidencialidad de la información no puede mostrar datos financieros, pero puedo simular o acercarse a un aproximado.

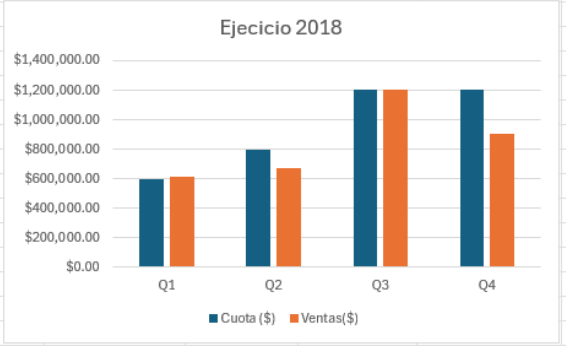
Figura 5

Cuotas de venta Intecnia Corp S.A.C.

Año	Trimestre	Prospectos	Crecimiento prospectos (%)	Cuota ($)	Ventas($)	% Cumplimiento	Prospectos Convertidos	% Prospectos Ganados	Ventas Totales ($)
2017	Q1	60		$600,000.00	$512,495.00	85%	50	83%	$512,495.00
2017	Q2	79	31.67%	$800,000.00	$688,256.00	86%	69	87%	$1,200,751.00
2017	Q3	92	16.46%	$1,000,000.00	$909,685.00	91%	83	90%	$2,110,436.00
2017	Q4	109	18.48%	$1,000,000.00	$853,399.00	85%	99	91%	$2,963,835.00

Año	Trimestre	Prospectos	Crecimiento prospectos (%)	Cuota ($)	Ventas($)	% Cumplimiento	Prospectos Convertidos	% Prospectos Ganados	Ventas Totales ($)
2018	Q1	75		$600,000.00	$609,005.00	102%	74	99%	$609,005.00
2018	Q2	99	32.00%	$800,000.00	$670,566.00	84%	82	83%	$1,279,571.00
2018	Q3	106	7.07%	$1,200,000.00	$1,200,990.00	100%	103	97%	$2,480,561.00
2018	Q4	115	8.49%	$1,200,000.00	$905,563.00	75%	82	71%	$3,386,124.00





d) Postventa

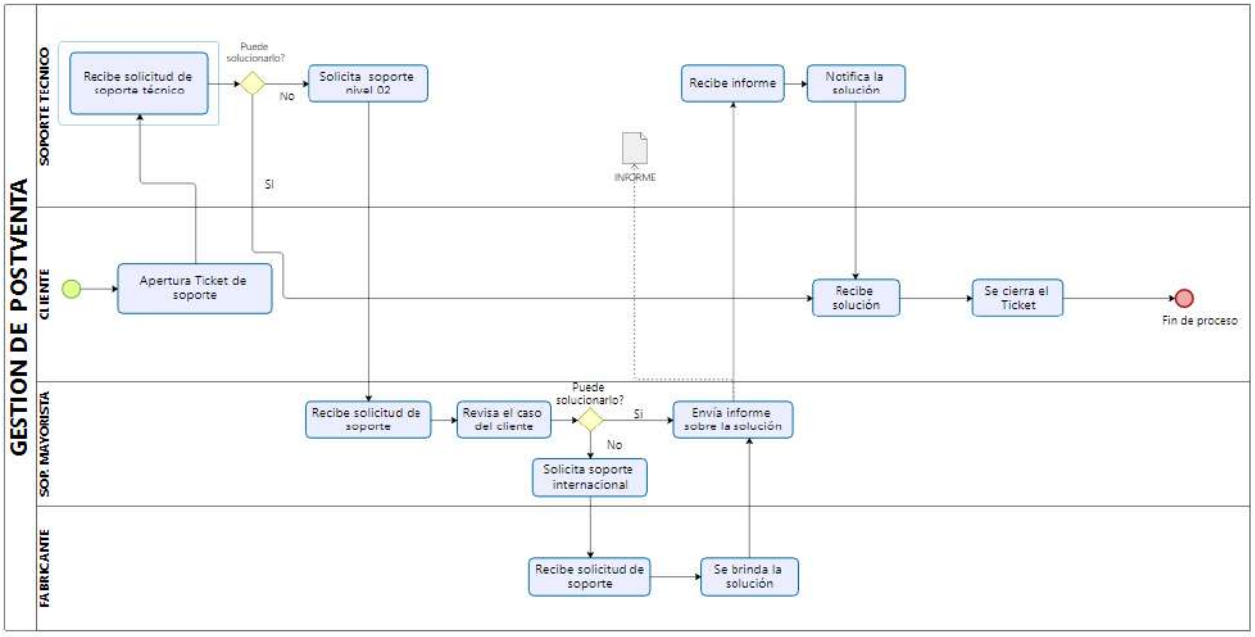
El servicio postventa consiste en proporcionar soporte técnico al cliente para resolver los incidentes que puedan surgir durante la vigencia de la licencia. Este servicio es crucial, ya que asegura la renovación del contrato o del servicio.

Intecnia Corp S.A.C. supervisa el proceso a través de sus canales de distribución para garantizar que el cliente reciba un soporte adecuado y asegurar las renovaciones anuales.

En la figura 6 podemos observar el proceso de gestión de la postventa. En la figura 6 se muestra el subproceso postventa.

Figura 6

proceso de postventa de Intecnia Corp S.A.C.



1.1.9 Clientes

Por motivos de acuerdos de confidencialidad, no se proporciona una lista específica de clientes. Sin embargo, puedo mencionar que Bitdefender está presente en todos los sectores, es tal así que la UNJFSC en un momento usó Bitdefender para proteger sus más de 1000 equipos entre ellos servidores y computadoras.

1.2 Funciones del puesto de trabajo

1.2.1 Puesto desempeñado.

Ingeniero de preventa de seguridad en Intecnia Corp S.A.C.)

Según Care, J., & Bohlig, A. (2013). Indica que el arte de ser un ingeniero preventas consultivo es encontrar ese número, la dirección en la que necesita moverse y en qué medida, y cuánto vale ese movimiento para alguien importante que tiene un presupuesto, afirma que es un profesional especializado en la intersección entre la tecnología y las ventas.

Según Romero (2024), indica que “Estos profesionales sirven como puente entre la experiencia técnica y las estrategias de ventas efectivas” y “realizan demostraciones de productos para mostrar cómo la solución propuesta aborda las necesidades del cliente”.

Este cargo lo desempeñe en desde el 2015 hasta julio del 2019. Para fines de este documento se considera las siguientes fechas de enero 2017 a Julio 2019 (ver el Anexo A).

Según Dr. Tuuli Bell (2021), indica además que los ingenieros preventa pueden desarrollar empatía y creatividad para abordar problemas comerciales complejos mediante soluciones técnicas.

1.2.2 Funciones

Las funciones que desempeñe con ingeniero preventa de seguridad en Intecnia Corp S.A.C. son:

- Testear y evaluar toda la suite de ciberseguridad de Bitdefender.
- Presentar las soluciones de Bitdefender a los clientes de los distintos canales de distribución como apoyo técnico.
- Capacitar al equipo de soporte técnico de los canales de distribución en el manejo total de la plataforma incluyendo la instalación en arquitecturas complejas.
- Realizar pruebas de concepto (POC) de las soluciones en la infraestructura del cliente.
- Proporcionar soporte para toda la suite de Bitdefender en incidentes complejos.
- Formar parte del equipo de ingenieros en ferias tecnológicas.
- Validar las solicitudes de propuesta (RFP) o términos de referencia (TDR) de las entidades gubernamentales.

1.2.3 Actividades desarrolladas en el puesto

1.2.3.1 Explorar y evaluar soluciones de ciberseguridad

Según Moyle y Kelley (2020). Definen la **evaluación de soluciones de ciberseguridad** como el proceso sistemático de analizar y valorar diferentes herramientas y tecnologías de seguridad para determinar su efectividad en la protección de sistemas informáticos. Este proceso implica evaluar la capacidad de cada solución para mitigar riesgos específicos, integrarse adecuadamente en la infraestructura existente, y cumplir con los requisitos de seguridad organizacionales. La evaluación también considera factores como la facilidad de implementación, el costo y el impacto en el rendimiento del sistema.

Según IBM (s.f.), Las pruebas de software consisten en evaluar y verificar que un producto o aplicación de software cumple con su propósito previsto. Aunque esta práctica comenzó en el ámbito del desarrollo de software, también puede aplicarse a la evaluación de sistemas para entender su funcionalidad. Este proceso requiere tiempo para revisar la documentación del sistema, comprender su integración con otros sistemas y analizar su comportamiento en diversas arquitecturas. Así, el proceso de prueba se transforma en una exploración minuciosa que proporciona un conocimiento profundo sobre el sistema y su funcionamiento.

Mi tarea dentro de la empresa consistió en una revisión completa de todas las soluciones ofrecidas por Bitdefender. Este proceso incluyó un análisis detallado de todas las funciones y componentes. Además, me enfoqué en estudiar cómo se implementan estas soluciones en diferentes arquitecturas, tanto en su formato On-premise como en su formato Cloud.

Cada empresa tiene una infraestructura informática diferente, algunos por regulación no permiten el uso de servicios en nube o Cloud y es donde se tiene que desplegar un Virtual Appliance en los hipervisores de los clientes, en este caso podría tratarse de VMware, Citrix, Hyper-V y en casos más complejos en Linux con KVM, es tal así que necesitaba

conocer cómo se implementa máquinas virtuales en cada uno de estos servicios, ello me llevó a tener un laboratorio bastante completo.

Esta tarea no solo me permitió comprender cómo cada solución se ajusta a diferentes arquitecturas, sino también identificar sus ventajas y limitaciones en función de los requisitos específicos de cada entorno.

Además, con todo este conocimiento logré aprobar todas las certificaciones impartidas por la marca. (Ver Anexo B)

1.2.3.2 Presentar las soluciones de Bitdefender a los clientes de los distintos canales de distribución como apoyo técnico.

Según Carmine Gallo (2009), Steve Jobs tenía una habilidad especial al momento de hacer sus presentaciones o de comunicar, el autor nos indica que para vender ideas o productos debemos ser efectivos, planificar de manera eficaz, desarrollar mensajes y titulares convincentes.

Según Zendesk (2023), El concepto de presentación de ventas se refiere a una breve reunión, ya sea virtual o en persona, en la que un representante de ventas expone su solución a un cliente potencial o existente con el objetivo de persuadirlo para que efectúe una compra de una determinada solución o servicio.

Es decir, no solo se describe el producto o servicio; también se le mostrará al cliente cómo resuelves un problema o como satisface las necesidades y, en conclusión , cómo se realiza mejor que la competencia.

En tal sentido era importante que como Ingeniero preventa de seguridad sea claro con mis ideas, conceptos y sobre todo mostrar beneficios de usar Bitdefender como un producto diferencial.

En esta tarea hubo muchas presentaciones técnicas comerciales con diferentes empresas, entre ellas del sector privado como el sector gobierno.

Muchas de estas empresas vienen de usar plataformas del tipo Cliente-Servidor una arquitectura bastante obsoleta para estos servicios, si bien es cierto Cloud ya no es un concepto nuevo, pero aún hay profesionales que no se atreven a migrar a estos servicios y optan por tener plataformas instaladas en sus ambientes o arquitectura informática.

Las presentaciones que realizábamos lo hacíamos directamente al área usuaria, en este caso jefes de TI, jefes de infraestructura, analistas de seguridad, la comunicación era bastante técnica y muchas de las preguntas comunes que realizaban eran:

- ¿La solución va ralentizar mis operaciones?
- ¿La solución está presente en el Cuadrante de Gartner?
- ¿Cómo es forma de despliegue, se hace por AD o manual?
- ¿Si la solución protege de Ransomware?
- ¿Puedo bloquear páginas web a usuarios externos?

Estas preguntas eran bastante comunes y teníamos que darles una buena respuesta para seguir captando el interés, finalmente terminábamos invitando al ingeniero a probar nuestras soluciones.

1.2.3.3 Capacitar al equipo de soporte técnico de los canales de distribución en el manejo total de la plataforma incluyendo la instalación en arquitecturas complejas.

Según Fagel (2007). Subraya la importancia de asegurarse de que los entrenamientos no solo sean teóricos, sino que permitan a los técnicos aplicar directamente lo aprendido en su entorno de trabajo.

Según Indeed (2024), El adiestramiento y desarrollo de los empleados es crucial para preservar la competitividad de una empresa. El éxito de estos programas en gran medida depende de las técnicas de capacitación utilizadas. Aunque el instructor pueda ser muy competente, si emplea métodos obsoletos o que no se ajustan al estilo de aprendizaje de los participantes, es poco probable que se logren buenos resultados.

En este contexto, era importante proporcionar capacitación clara y precisa, dado que el soporte técnico actuaba como el soporte de primer nivel de asistencia para los clientes. Además, era fundamental asegurar que los técnicos lograran la certificación necesaria para que los canales de distribución mantuvieran su rango.

1.2.3.4 Realizar pruebas de concepto (POC) de las soluciones en la infraestructura del cliente.

Según Chernenko (2021) Indica que una POC es un piloto/ensayo, que tiene como objetivo probar un producto o servicio de TI antes de tomar una decisión de compra.

Según Asana (2023), Una prueba de concepto (POC) se realiza para validar la viabilidad de un producto, método o propuesta. Su objetivo es mostrar por qué tu idea será efectiva en la práctica, brindando a las partes interesadas e inversores la confianza necesaria para proceder con el proyecto.

Bajo este contexto realizar pruebas de concepto en la infraestructura del cliente era muy importante porque permite demostrar de manera concreta cómo nuestra solución empieza a funcionar en su parque informático o infraestructura. Este enfoque práctico no solo facilita una comprensión clara de nuestra oferta, sino que también fortalece la confianza del cliente.

Hemos comprobado que esta etapa es decisiva para el éxito en ventas. Según nuestras estadísticas, de cada 10 pruebas de concepto realizadas, 8 se convierten en ventas efectivas. Esto resalta la importancia de ejecutar la prueba de concepto al inicio del proyecto.

1.2.3.5 Proporcionar soporte para toda la suite de Bitdefender en incidentes complejos

Según Zendesk. (2023). El soporte técnico es el departamento de una empresa responsable de resolver problemas o inconvenientes que los clientes puedan enfrentar después de haber adquirido un producto.

El soporte técnico para casos complejos implicaba un análisis detallado de la situación o incidente. A menudo, estos problemas eran causados por migraciones, bloqueos de puertos durante actualizaciones o problemas de instalación. Aunque muchos de estos casos se resolvían rápidamente, los incidentes más complicados requerían una comunicación directa con el soporte del fabricante, generalmente en inglés. En tales situaciones, era necesario enviar todos los reportes y registros solicitados para identificar la causa del problema. Para estos casos complejos, contábamos con un plazo de hasta 72 horas para resolver el incidente.

1.2.3.6 Formar parte del equipo de ingenieros en ferias tecnológicas.

Según Estudiar Organización de Eventos (s.f.), Las ferias tecnológicas se han convertido en eventos clave y vibrantes en el campo de la innovación y el avance tecnológico. No solo celebran los desarrollos tecnológicos, sino que también actúan como un importante punto de encuentro para profesionales, empresas y aficionados del sector. En un entorno donde la tecnología progresa rápidamente, estas ferias son fundamentales al ofrecer una plataforma para el lanzamiento de nuevos productos, la demostración de innovaciones y la creación de redes que pueden conducir a colaboraciones y oportunidades de negocio.

Como ingeniero preventa de seguridad, mi presencia en las ferias tecnológicas era esencial. En estos eventos, ingenieros, jefes de sistemas y otros profesionales técnicos participaban activamente, planteando preguntas técnicas y complejas que resultaban difíciles de responder para los comerciales. Mi responsabilidad era explicar de manera clara y práctica las soluciones de Bitdefender, destacando cómo estas podían proteger de manera efectiva los equipos de los clientes (ver Anexo C)

1.2.3.7 Validar las solicitudes de propuesta (RFP) o términos de referencia (TDR) de las entidades gubernamentales.

Según Michael Asner (1995) Indica que un **(RFP)** es un documento formal que una organización utiliza para solicitar propuestas detalladas de proveedores externos con el fin de adquirir bienes, servicios o soluciones.

Según Unique (2019), Una solicitud de propuesta (RFP, por sus siglas en inglés) es un documento creado dentro de una empresa para solicitar a varios proveedores que presenten sus mejores soluciones y presupuestos para satisfacer necesidades específicas.

En este contexto, una RFP (Request for Proposal) o TDR (Términos de Referencia) se utiliza comúnmente en entidades gubernamentales para solicitar servicios o la compra de bienes. Nuestro proceso implicaba revisar toda la documentación proporcionada por la OSCE (Organismo Supervisor de las Contrataciones del Estado), específicamente filtrada para servicios de ciberseguridad. El objetivo era asegurar que las soluciones de Bitdefender cumplieran con las especificaciones técnicas detalladas en el TDR.

Frecuentemente, encontrábamos que no cumplíamos con todos los requisitos mencionados. En tales casos, era necesario presentar preguntas y aclaraciones para adaptar las características de Bitdefender y permitir que nuestra solución se ajustara a los criterios del TDR y pudiera competir efectivamente.

Aunque Intecnia Corp SAC no participaba directamente en estos procesos, ya que distribuye sus productos a través de canales o resellers, mi función incluía brindar apoyo técnico a estas empresas que sí participaban en las licitaciones. Mi rol era importante para asegurar que los socios pudieran presentar nuestras soluciones de manera competitiva y cumplir con los requisitos especificados en las RFP o TDR.

1.3 Dificultades para desempeñar el puesto

Para alcanzar estos logros, enfrenté desafíos significativos. Tuve que adquirir un amplio conjunto de habilidades técnicas, lo que me llevó a completar cursos en áreas como CCNA, Implementación de Exchange Server, Linux, plataforma Cloud; etc.

Otra de las dificultades presentadas, era el manejo del idioma inglés, casi todas las certificaciones y documentación está en ese idioma y era una de las debilidades que tenía.

1.4 Contribuciones de la formación académica en el desempeño del puesto

El conocimiento adquirido en la UNJFSC fue base para entender los conceptos básicos de que es una topología de red, que son servidores, que es Cloud entre otros conceptos clave para el mundo de la ciberseguridad.

Además, lleve cursos complementarios en la Universidad Nacional de Ingeniería, cursos para entender la arquitectura de Windows Server, servicios como Active Directory, Hyper-V y sobre todo el servicio de Exchange Server, además complementé mis conocimientos con estudios de ambientes virtuales con Vmware y Citrix.

Así mismo para fortalecer mis conocimientos en seguridad de la información he llevado un diplomado en la SGSI ISO 27001:2013 (ver Anexo D), consiguiendo la certificación internacional como Auditor Interno SGSI 27001:2013 de AENOR. (ver Anexo E)

Además, hice estudios de maestría en Ingeniería Informática en la Universidad Ricardo Palma culminando satisfactoriamente los 4 ciclos académicos.

Además de llevar cursos libres en línea en plataformas como Udemy, análisis de malware, Ethical Hacking, entre otros.

1.5 Metas personales y formativas alcanzadas durante el desempeño del puesto

- El ocupar un puesto importante y clave en el Negocio de Intecnia Corp S.A.C.
- El haber sido la persona con más certificaciones internacionales de Bitdefender a nivel nacional.

- Haber conseguido la certificación del curso de Cisco CCNA.
- Haber conseguido el certificado como técnico en Windows Server y sus servicios.
- Haber realizado estudios de Diplomado en Seguridad de la información.
- Haber alcanzado el certificado como Auditor Interno en seguridad de la información SGSI ISO 27001:2013.
- Haber Realizado estudios de Maestría en Ingeniería informática en la URP.

Empresa Safe Network S.A.C.

2.1 Datos de la organización

2.1.1 Descripción del origen de Safe Network S.A.C.

Safe Network S.A.C. Es una empresa emergente dedicada exclusivamente a proporcionar soluciones integrales de ciberseguridad a empresas.

Es un canal de distribución de rango Silver de Bitdefender y cuenta con todas las certificaciones comerciales y técnicas impartidas por la marca. Cuenta con más de 50 clientes a nivel nacional que confían en sus soluciones y servicios.

Además, la empresa cuenta con alianzas estratégicas con diversas marcas de ciberseguridad para completar su portafolio, dentro de ellas también se ofrecen soluciones como DLP (Prevención de fuga de información) y soluciones de Backup.

La empresa ha formado alianzas y es un integrador de negocios, trabaja con los más grandes mayoristas de cómputo e infraestructura informática como por ejemplo tenemos a Deltron S.A., Ingram Micro, Intcomex, Adistec y muchos más.

La forma de trabajo de SAFE NETWORK SAC se enfoca en brindar un servicio de soporte postventa proactivo y rápido, sin colas de espera, mediante un eficiente sistema de tickets.

A la fecha SAFE NETWORK SAC ha dejado de operar y en su reemplazo nace DATASECURE PERU SAC quien se fundó con un nuevo capital y enfoque. Actualmente esta empresa asumió el cargo de todos los clientes de SAFE NETWORK SAC.

2.1.2 Misión y visión de Safe Network S.A.C.

La misión de la empresa se expresa de la siguiente manera: “Proporcionar a nuestros clientes soluciones integrales de ciberseguridad que garanticen la protección de su información y activos digitales. Nos comprometemos a ofrecer un soporte postventa rápido y eficiente”.

La visión de la empresa se expresa de la siguiente manera “Ser la empresa líder en soluciones de ciberseguridad en el mercado nacional, reconocida por su innovación constante, la excelencia en el servicio y la capacidad de anticipar y mitigar las amenazas digitales en un entorno en constante evolución”.

Los valores que considera la empresa como pilares de su organización son “honestidad, puntualidad, compromiso, innovación.”

2.1.3 Datos Generales de la Empresa

2.1.3.1 Nombre comercial

Razón Social: Safe Network S.A.C.

Registro único de contribuyente (R.U.C.): 20605050060

Dirección: Cal.Tiahuanaco Nro. 207 Urb. Los Chancas De Andahuaylas (G1 49 - 1era Etapa) Lima - Lima - Santa Anita

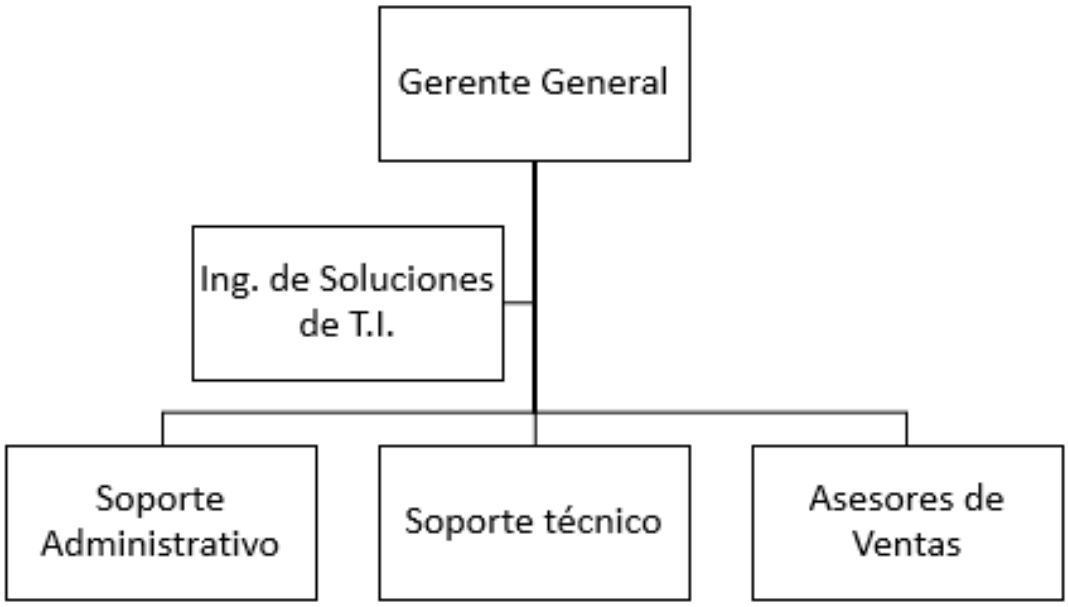
Actividades económicas: Consultoría de Informática y Gestión de Instalaciones Informáticas

Página web: https://safenetwork.pe

El organigrama de la empresa se presenta en la figura 7.

Figura 7

Organigrama de Safe Network S.A.C.



2.1.4 Tamaño de la empresa

Al cierre del 2022 contaba con 6 colaboradores.

2.1.5 Giro del negocio

Su principal giro de negocio es la de comercialización de soluciones de Ciberseguridad como Bitdefender, Eset, Kaspersky, Safetica y Attack Simulator además de la renovación de las suscripciones cada año.

2.1.6 Mercados que atiende

Safe Network S.A.C. Atiende al mercado privado explícitamente en el sector de la pequeña y mediana empresa de hasta 350 colaboradores en todos los rubros por ejemplo educación, gobierno, empresas privadas, transporte.

2.1.7 Principales productos

Los servicios o productos que brinda Intecnia Corp S.A.C. son:

a) Bitdefender Gravityzone

Bitdefender Gravityzone es la plataforma que permite administrar los puntos finales, desde esta plataforma podemos crear instaladores, aplicar, configurar políticas de seguridad, ver los incidentes de seguridad, ver los riesgos asociados a los equipos, hacer un control web, aplicaciones. También ofrece en su paquete o suite Enterprise un análisis forense de un ataque de red, donde se puede visualizar el tipo de ataque, la mitigación, las IPs remotas atacantes, los procesos creados, los equipos comprometidos e información detallada de cómo fue la causa raíz de un ataque.

Además, la plataforma genera reportes detallados de los eventos de seguridad recopilados. También permite gestionar las cuentas de administrador, asegurando que solo el personal autorizado tenga acceso a funciones críticas de seguridad.

b) Eset Protect Plataform

Eset Protect Plataform es la plataforma de gestión, esta solución protege a sus clientes contra Ransomware, phishing, amenazas de día cero y de ataques dirigidos.

Dentro de todo su portafolio podemos encontrar soluciones que cubren la necesidad de protección de punto final, protección para ambientes virtuales, protección para servidores de correo electrónico; entre otros.

Eset es una de las soluciones más premiadas del mercado, siendo Perú uno de los mercados que más clientes tiene.

c) Kaspersky Business

Kaspersky ofrece una gama de soluciones de ciberseguridad diseñadas para proteger a las empresas contra amenazas cibernéticas avanzadas. Estas soluciones están orientadas a garantizar la seguridad integral de la infraestructura de TI, incluyendo endpoints, servidores y redes.

Las soluciones de Kaspersky para empresas están orientadas a proporcionar una protección robusta y eficiente contra una variedad de amenazas cibernéticas. Ofrecen

herramientas para gestionar la seguridad desde una única plataforma, garantizando que todos los componentes de la infraestructura de TI estén protegidos y que la seguridad se mantenga operativa sin afectar el rendimiento del sistema. Estas soluciones están diseñadas para adaptarse a diferentes tamaños y tipos de empresas, desde pequeñas oficinas hasta grandes corporaciones, brindando flexibilidad y escalabilidad según las necesidades específicas de cada organización.

d) Safetica

Las soluciones de **Safetica** se centran en la protección de la información crítica de la empresa contra pérdidas y accesos no autorizados. Su enfoque integral en la prevención de pérdida de datos (DLP) ayuda a las organizaciones a proteger la integridad, confidencialidad y disponibilidad de la información sensible, mientras que sus herramientas de monitoreo y análisis proporcionan visibilidad sobre el uso y la seguridad de los datos. Safetica está diseñada para adaptarse a diferentes tamaños y tipos de organizaciones, ofreciendo flexibilidad en la implementación y escalabilidad en función de las necesidades de seguridad de cada empresa.

e) Fortinet

Los firewalls FortiGate de Fortinet son soluciones robustas de seguridad de red que combinan tecnologías avanzadas para proteger contra amenazas cibernéticas y optimizar el rendimiento de la red. Están diseñados para ofrecer una protección integral y escalable, adaptándose a las necesidades de redes empresariales de todos los tamaños. Con características como inspección profunda de paquetes, prevención de intrusiones, y capacidades de seguridad en la nube y SD-WAN, los firewalls FortiGate proporcionan una defensa efectiva contra una amplia gama de amenazas y permiten una gestión centralizada para facilitar la administración de la seguridad de la red.

2.1.8 Procesos del negocio

Safe Network SAC funciona en torno a tres procesos clave: gestión de preventa, gestión de ventas y gestión de postventa.

Los procesos de negocio en el nivel macroprocesos se muestra en la figura 8.

Los procesos estratégicos son:

- Dirección de la empresa o Gerencia General.

Los procesos operativos son:

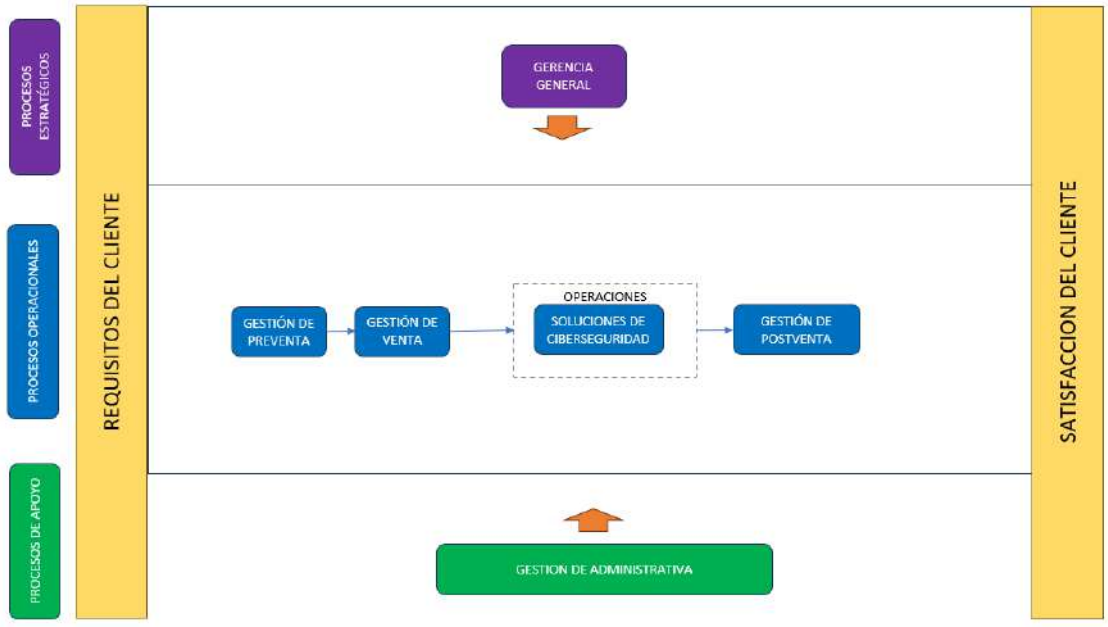
- Gestión de preventa
- Gestión de venta
- Gestión de postventa

Los procesos de soporte son:

- Gestión Administrativa

Figura 8

Organigrama de Safe Network S.A.C.



a) Pre-Venta

En esta parte es donde el Ingeniero de Soluciones de T.I. desempeña un papel importante, su responsabilidad principal es realizar presentaciones técnicas de todas las

soluciones ofrecidas por la empresa debe destacar las características más importantes de la solución ofrecida. Durante estas presentaciones, se debe abordar y resolver todas las dudas técnicas del jefe de sistemas o de los especialistas de seguridad de la información.

Además, es fundamental que el Ingeniero de Soluciones de T.I. busque realizar la famosa Prueba de Concepto (POC). Esta POC permite demostrar de manera práctica cómo la solución puede integrarse y funcionar en el entorno del cliente.

El ingeniero de soluciones de TI es responsable de implementar y supervisar la Prueba de Concepto (POC).

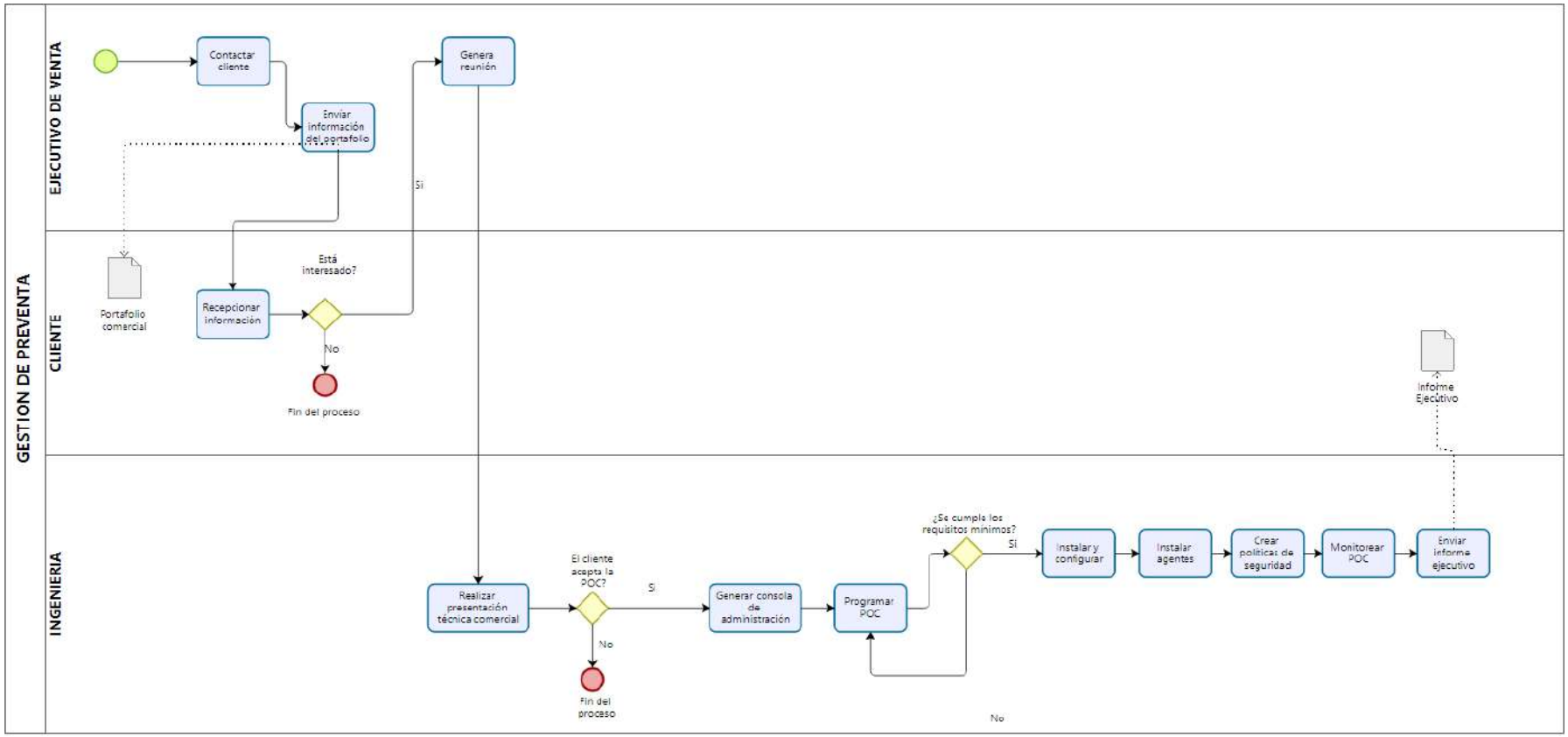
Esta etapa finaliza cuando la solución puesta en POC fue de agrado del ingeniero a cargo y recibe la aprobación del área usuaria para su compra.

Es importante mencionar que todo proyecto se debe registrar en el representante o mayorista con el fin de protección de cuenta final y que el canal tenga todo el derecho en venta y en renovaciones, esto se realizar antes de una prueba de conceptos.

El proceso de preventa se muestra en la figura 9.

Figura 9

Proceso de preventa de Safe Network S.A.C.



b) Venta

El proceso de venta depende mucho de la fase de la POC, en caso que la prueba de concepto haya resultado exitoso esta se convierte en una venta, por experiencia se tiene que de cada 10 POC 8 se vuelven ventas.

Para concretar una venta el cliente debe enviar una orden de compra en señal de su interés por el producto o servicio, Safe Network S.A.C. se comunica con el mayorista o representante enviando una orden de compra, luego de recibir el certificado de Licencia se procede a enviar al cliente con su respectiva factura.

Luego el Ing. de Soluciones de T.I. debe coordinar con el cliente todo el proceso de despliegue y capacitación de la solución contratada.

La figura 10 muestra la facturación de proyectos de Safe Network S.A.C. El proceso de venta se muestra en la figura 11.

Figura 10

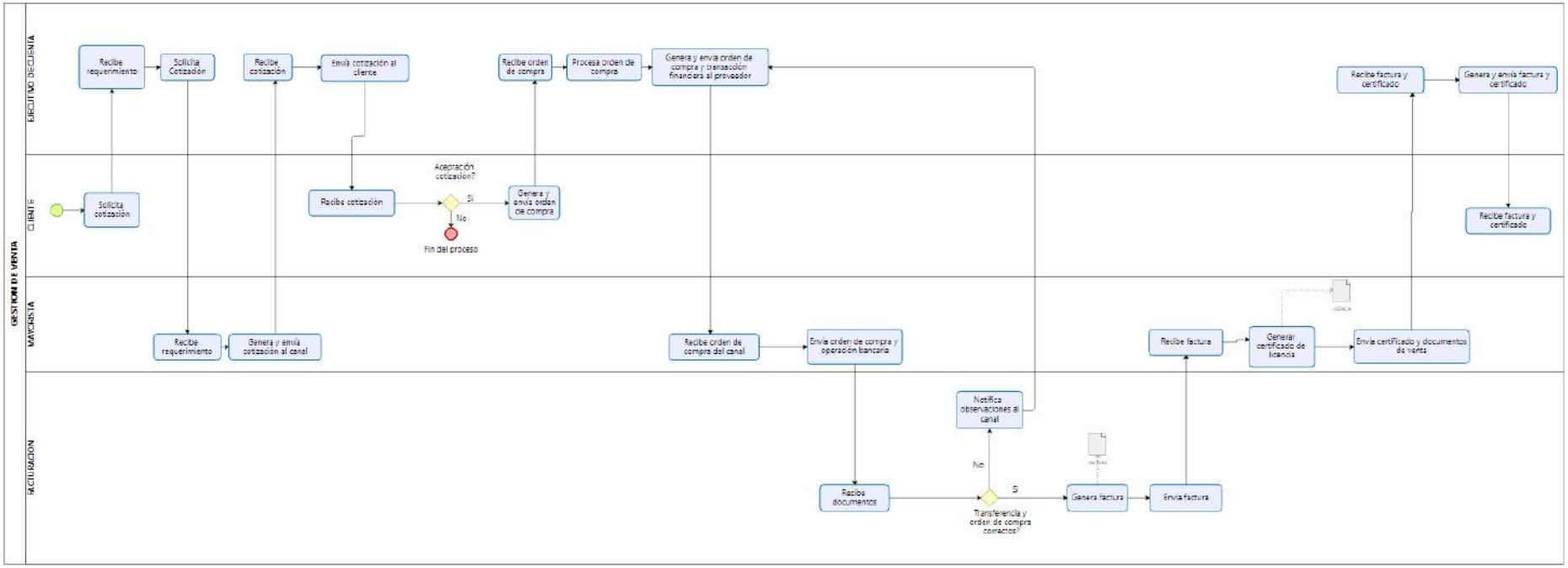
Facturación de proyectos de Safe Network S.A.C.

Descargar Reporte

Cliente	Tipo	N° Comprobante	F. Emisión	F. Vencimiento	Estado	Monto
REPRIND S.A.C RUC: 20102309180	Factura	F001-00000023	2020-05-11	2020-06-11	VALIDADO	USD 2,509.03
COMPAÑIA DE SEGUROS DE VIDA CAMARA S.A. RUC: 20554477721	Factura	F001-00000017	2020-01-29	2020-02-05	VALIDADO	USD 2,224.30
JELP CONSULTING E.I.R.L. RUC: 20605109803	Factura	F001-00000006	2019-09-24	2019-09-25	VALIDADO	USD 2,033.94
STAFF REPRESENTACIONES S.A. RUC: 20502253302	Factura	F001-00000010	2019-10-14	2019-12-14	VALIDADO	USD 1,982.40
MERCADEO COMERCIAL SA RUC: 20100525641	Factura	F001-00000002	2019-08-14	-	VALIDADO	USD 1,794.78
DEEPTEK S.A.C RUC: 20606262991	Factura	F001-00000045	2020-11-30	2020-11-30	Dado de baja	USD 1,770.00
DEEPTEK S.A.C RUC: 20606262991	Factura	F001-00000043	2020-11-30	2020-11-30	VALIDADO	USD 1,770.00
CASTILLO CORDOVA RICARDO BARTOLOME RUC: 10101133503	Factura	F001-00000041	2020-10-29	2020-10-29	VALIDADO	S/ 1,700.00
MERCADEO COMERCIAL SA RUC: 20100525641	Factura	F001-00000033	2020-08-10	2020-08-13	VALIDADO	USD 1,659.08
SUPERFISH S.A.C RUC: 20505102399	Factura	F001-00000031	2020-06-25	2020-07-25	VALIDADO	USD 1,604.80

Figura 11

Proceso de venta de Safe Network S.A.C.



c) Post-venta

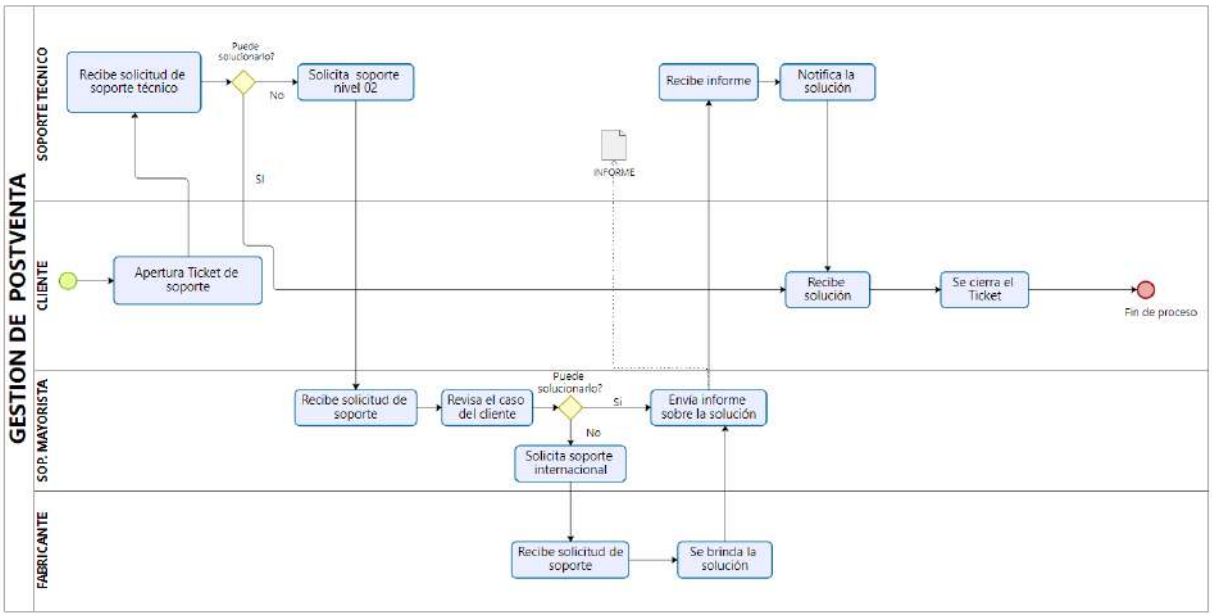
El proceso de postventa consiste en proporcionar soporte técnico al cliente para resolver los incidentes que puedan surgir, darle una atención oportuna y de calidad al cliente. Este servicio es crucial, ya que asegura la renovación del contrato o del servicio.

Este proceso es importante porque genera liquidez con las renovaciones cada año, mientras más renovaciones se logre más ganancia habrá para la compañía.

El proceso de postventa se muestra en la figura 12.

Figura 10.

Proceso de postventa de Safe Network S.A.C.



2.1.9 Clientes

Por motivos de acuerdos de confidencialidad, no se proporciona una lista específica de clientes. Sin embargo, en la figura 10 podemos observar algunos de los clientes que tiene Safe Network S.A.C.

2.2 Funciones del puesto de trabajo

2.2.1 Puesto desempeñado.

Ingeniero de Soluciones de T.I.

Según Glassdoor (s.f.). Un ingeniero de soluciones se comunica con los clientes para comprender sus necesidades y colabora con diferentes departamentos, como los de redes, asistencia y operaciones, para asegurar que se implemente un plan que mejore la experiencia del cliente. Su rol implica gestionar diversos aspectos del proyecto, incluyendo la seguridad y el diseño. Además, el ingeniero de soluciones realiza investigaciones en tecnología avanzada y en mejores prácticas del sector para encontrar soluciones que sean rentables.

Este cargo lo desempeñe en Safe Network S.A.C. desde el octubre del 2019 hasta enero del 2021. (ver anexo A)

2.2.2 Funciones

Las funciones que desempeñe con Ingeniero de Soluciones de T.I. en Safe Network S.A.C. son:

- Realizar presentaciones comerciales y técnicas de las suites de soluciones ofrecidas por la empresa a los clientes.
- Llevar a cabo pruebas de concepto (POC) de las soluciones en los clientes de la empresa.
- Presentar Webinars sobre soluciones de ciberseguridad.
- Ofrecer charlas de concientización en seguridad de la información para los usuarios de las empresas clientes.
- Realizar análisis de vulnerabilidades en la infraestructura del cliente.
- Conducir pruebas de phishing controlado para evaluar a los colaboradores de la empresa cliente.

- Validar las solicitudes de propuesta (RFP) o términos de referencia (TDR) de las entidades gubernamentales.

2.2.3 Actividades desarrolladas en el puesto

2.2.3.1 Realizar presentaciones comerciales y técnicas de las suites de soluciones ofrecidas por la empresa a los clientes.

Esta actividad es muy similar a la que ejercía cuando hacía presentaciones técnicas de Bitdefender, la única diferencia en este punto es que como Ingeniero de Soluciones de T.I. tenía que presentar todo el portafolio de las soluciones de la empresa.

2.2.3.2 Llevar a cabo pruebas de concepto (POC) de las soluciones en los clientes de la empresa.

Esta actividad es muy similar a la que ejercía cuando realizaba POC de Bitdefender, la única diferencia en este punto es que como Ingeniero de Soluciones de T.I. tenía que realizar el POC de todas las marcas comercializadas.

2.2.3.3 Presentar Webinars sobre soluciones de ciberseguridad.

Según Akamai (s.f.), Las soluciones de ciberseguridad consisten en productos o servicios destinados a proteger los sistemas digitales y la información contra posibles ciberataques. Estas abarcan diversos elementos de seguridad, como cortafuegos, defensa frente a ataques DDoS, microsegmentación, protección de cuentas, seguridad en API, gestión de bots y seguridad para aplicaciones web.

En Safe Networks SAC, como empresa emergente, entendíamos la importancia de destacarnos en un mercado competitivo. Para lograrlo, implementamos una estrategia que incluía la organización de Webinars mensuales. Estos eventos en línea estaban diseñados para centrarse en temas de ciberseguridad y para presentar nuestras soluciones.

Cada Webinars ofrecía contenido valioso y actualizado sobre las últimas amenazas y tendencias en el ámbito de la ciberseguridad, sino que también destacaba nuestras

soluciones y cómo podían abordar los desafíos específicos de nuestros clientes. Estos eventos nos permitieron establecer nuestra presencia en el sector, educar a nuestros clientes potenciales y actuales, y consolidar nuestra reputación como expertos en tecnología y ciberseguridad.

2.2.3.4 Ofrecer charlas de concientización en seguridad de la información para los usuarios de las empresas clientes.

Según Kaspersky (s.f.), La charlar de concientización sobre seguridad es fundamental para empresas u organizaciones que buscan proteger sus datos de manera efectiva, disminuir los incidentes causados por errores humanos, reducir los costos de respuesta y garantizar que sus empleados sepan manejar de forma responsable la información de los clientes y navegar por Internet de manera segura.

Uno de los compromisos que ofrecíamos a nuestros clientes antes de realizar firmar cualquier contrato era la realización de charlas de concientización sobre seguridad de la información. Este servicio estaba orientado a para educar a todo el personal dente en las mejores prácticas de seguridad informática, con un enfoque especial en el reconocimiento de amenazas y riesgos comunes.

Nuestras charlas estaban orientadas a enseñar a los usuarios a identificar y evitar páginas web maliciosas, así como a detectar correos electrónicos potencialmente peligrosos o ataques de phishing. La seguridad de la información no solo depende de las herramientas tecnológicas, sino también de la capacitación adecuada de los empleados, quienes son una primera línea crucial de defensa contra las amenazas en línea.

Para asegurar una mayor efectividad y retención del conocimiento, diseñábamos estas sesiones de manera dinámica y participativa. Utilizábamos juegos interactivos, simulaciones prácticas y estudios de caso reales para ilustrar conceptos clave. Además,

incorporábamos ejemplos concretos y experiencias recientes para que los participantes pudieran relacionar la teoría con situaciones prácticas y cotidianas.

2.2.3.5 Realizar análisis de vulnerabilidades en la infraestructura del cliente.

Según IBM (2023), El análisis de vulnerabilidades, o evaluación de vulnerabilidades, es el proceso de examinar redes o activos de TI para identificar fallos, debilidades o vulnerabilidades de seguridad que podrían ser explotadas tanto por amenazas internas como externas.

Bajo este contexto, conocer nuestras vulnerabilidades es muy importante para mantener la seguridad de nuestra red, sin embargo, muchas de las empresas no se toman el tiempo en realizan esta tarea, Desde Safe Network SAC implementamos un servicio sin costo para nuevos clientes, este servicio consistía en analizar sus principales servicios con la finalidad de buscar vulnerabilidades y buscar la solución. Gracias a esta iniciativa logramos captar la atención de muchos clientes y subimos rápidamente de nivel hasta lograr ser Silver en Bitdefender.

2.2.3.6 Conducir pruebas o test de phishing controlado para evaluar a los colaboradores de la empresa cliente.

Según Hadnagy (2018). Indica que Phishing es suplantación de identidad y se define como el acto de enviar correos electrónicos maliciosos que pretenden ser de fuentes confiables.

Según Nsit (2024), Las pruebas de phishing consisten en enviar correos electrónicos falsos que se hacen pasar por mensajes legítimos, con la intención de que los destinatarios sean engañados y proporcionen información sensible, como contraseñas, datos bancarios o información personal.

Uno de los servicios de valor agregado que ofrecíamos a nuestros nuevos clientes consistía en crear un entorno controlado para enviar correos electrónicos tipo phishing, con

el objetivo de medir la respuesta de los usuarios. A través de esta actividad, podíamos identificar qué usuarios abrían los correos, cuáles hacían clic en los enlaces, quiénes completaban formularios y quiénes descargaban y ejecutaban los archivos adjuntos. Este enfoque no solo captó la atención de nuestros clientes, sino que también nos permitió posicionarnos como sus proveedores de servicios tecnológicos y de ciberseguridad.

A la fecha son pocas empresas que realizan este servicio y es uno de los puntos más fuertes que tiene la empresa.

2.2.3.7 Validar las solicitudes de propuesta (RFP) o términos de referencia (TDR) de las entidades gubernamentales.

Esta actividad es similar la que hacía en Intecnia Corp S.A.C. y se fundamenta en el mismo proceso, la única diferencia es que no usábamos el recurso de ingeniería del representante, es decir nosotros nos encargábamos de revisar los TDRs, armar las preguntas y luego de la apertura de las bases hacer nuestra cotización formal.

2.3 Dificultades para desempeñar el puesto

Este nuevo reto de pasar de Ing. Preventa de Seguridad a Ing. de Soluciones de T.I. y de ver una sola marca a ver muchas marcas o soluciones era un desafío bastante grande porque tenía que dominar todas las soluciones del portafolio de la empresa.

Al ser una empresa nueva y emergente muchas veces nos dificultaba llegar a contactar con las empresas y en los primeros meses ese fue problema hasta que llegamos a contratar con nuestros primeros clientes.

Además, una de las dificultades que teníamos era que no estábamos certificados para poder comercializar los productos y tuve que llevar todos los cursos para conseguir las certificaciones y convertirnos en un distribuidor autorizado.

2.4 Contribuciones de la formación académica en el desempeño del puesto

El conocimiento adquirido en la UNJFSC fue base para entender los conceptos básicos de que es una topología de red, que son servidores, que es Cloud entre otros conceptos clave para el mundo de la ciberseguridad.

Además, lleve cursos complementarios en la Universidad Nacional de Ingeniería, cursos para entender la arquitectura de Windows Server, servicios como Active Directory, Hyper-V y sobre todo el servicio de Exchange Server, además complementé mis conocimientos con estudios de ambientes virtuales con Vmware y Citrix.

Así mismo para fortalecer mis conocimientos en Seguridad de la Información he llevado un diplomado en la SGSI ISO 27001:2013, consiguiendo la certificación internacional como Auditor Interno SGSI 27001:2013 de AENOR.

Además, realicé estudios de maestría en Ingeniería Informática en la Universidad Ricardo Palma culminando satisfactoriamente los 4 ciclos académicos.

Además de llevar cursos libres en línea en plataformas como Udemy, análisis de malware, Ethical Hacking, entre otros.

2.5 Metas personales y formativas alcanzadas durante el desempeño del puesto

Las metas personales y formativas alcanzadas durante el desempeño del puesto tenemos:

- El haber conseguido todas las certificaciones que necesitaba la empresa para ser un canal de distribución de Bitdefender, Eset, Kaspersky.
- El haber conseguido los cierres de venta a través de la buena ejecución de las pruebas de concepto, llegando ser un canal Silver en Bitdefender y Bronce en el resto de marcas.
- El haber conseguido que SAFE NETWORK SAC sea la empresa canal con más certificaciones de Bitdefender.

Conclusiones y recomendaciones

3.1 Conclusiones

- Como ingeniero Pre-venta de seguridad y de soluciones de T.I. en empresas como INTECNIA CORP SAC y SAFE NETWORK S.A.C. respectivamente, he sido testigo de la importancia de que las empresas deben contar con soluciones de ciberseguridad avanzadas. A lo largo de mi experiencia, he podido observar cómo empresas peruanas y sobre todo de gobierno no se preocupan por la seguridad de su red, muchas de estas entidades abusan del uso de cracks o activadores dejando paso libre a los ataques e infecciones a sus equipos críticos.
- En estos cargos que he tenido durante mi experiencia profesional he comprendido que hay que estar siempre actualizados tanto en habilidades como en conocimientos. La rápida evolución del panorama tecnológico exige que estemos al tanto de las últimas tendencias y herramientas para poder ofrecer a nuestros clientes servicios y soluciones innovadoras.
- En Intecnia Corp SAC y Safe Network S.A.C., he tenido la oportunidad de colaborar estrechamente con un gran equipo, desde ingenieros, técnicos y expertos en ciberseguridad. Esta colaboración ha sido fundamental para seguir aprendiendo de esta hermosa línea de carrera y además me permitió conocer las diferentes formas o marcos de trabajo que podemos utilizar para proteger nuestros activos de información.
- Mi cargo como ingeniero preventa de seguridad y de soluciones de T.I. me ha ayudado en conseguir habilidades de comunicación y una capacidad para traducir conceptos técnicos complejos en términos comprensibles para los usuarios o clientes además también la capacidad de establecer relaciones sólidas y amicales con los clientes y proveedores.

3.2 Recomendaciones

- Es importante que quienes enfrenten desafíos similares a este informe y en el ámbito de la ciberseguridad se mantengan al actualizados en las últimas tendencias, como por ejemplo las nuevas tácticas y técnicas utilizadas por los ciberdelincuentes, Es crítico mantenerse actualizado en estos aspectos, ello te permitirá brindar información relevante y actualizada al cliente, demostrando así tu profundo conocimiento del tema y tu compromiso con la protección de sus sistemas y datos.
- Es importante estudiar diversas tecnologías, tanto físicas como en la nube. El manejo de estas tecnologías permitirá adaptar las pruebas de concepto a diferentes arquitecturas informáticas, asegurando así la viabilidad y eficacia de las soluciones propuestas.
- Para asegurar un correcto soporte técnico, es fundamental mantener una comunicación constante con el representante o la marca de la solución brindada al cliente. Esto garantizará un rápido escalamiento de incidentes, permitiendo así una pronta resolución de problemas y minimizando el tiempo de inactividad para los usuarios finales.
- En el tema de capacitaciones, es esencial comprender a fondo la solución o servicio para poder explicarla de manera fácil y sencilla. Esta comprensión profunda nos permitirá transmitir conceptos complejos de manera clara y comprensible para los técnicos y/o ingenieros, facilitando así su adopción y uso efectivo de la tecnología. Además, al dominar estos temas, estaremos mejor equipados para responder preguntas y resolver problemas durante la capacitación, garantizando una experiencia de aprendizaje enriquecedora para todos los involucrados.

Referencias bibliográficas

Alex R. (2024). Ing. de Preventa Recuperado de: https://www.alexromero.es/ingeniero-preventas-papel-fundamental/

Akamai. (s.f). What are cybersecurity solutions? Akamai. https://www.akamai.com/es/glossary/what-are-cybersecurity-solutions

Asana. (2023). Proof of concept: ¿Qué es y cómo implementarlo? Asana. https://asana.com/es/resources/proof-of-concept

Asner, M. (1995). *The request for proposal handbook*. McGraw-Hill. p.220

Care, J., & Bohlig, A. (2013). *Mastering Technical Sales: The Sales Engineer's Handbook*. Chapter 1, p. 68.

Chernenko, A. (2021). *POC (proof-of-concept) and its optimisation in a software company* (p. 1).

Dr Tuuli Bell. (2021). *An Introduction to the Art of Presales*

Estudiar Organización de Eventos. (s.f.). Qué son las ferias tecnológicas. Estudiar Organización de Eventos. https://estudiarorganizaciondeeventos.es/que-son-las-ferias-tecnologicas/

Fagel, M. J. (2007). *Training engineers and technicians*. CRC Press. p. 10.

Gallo, C. (2010). *The presentation secrets of Steve Jobs: How to be insanely great in front of any audience* (p. 20). McGraw-Hill.

Glassdoor. (s.f.). ¿Qué hace un ingeniero de soluciones? Glassdoor. https://www.glassdoor.com.ar/Profesion/ingeniero-de-soluciones-profesion_KO0,23.htm

Hadnagy, C. (2011). *The art of human hacking*. Wiley.p.229

IBM. (2023). ¿Qué es el análisis de vulnerabilidades? IBM. https://www.ibm.com/mx-es/topics/vulnerability-scanning#:~:text=Kosinski%2C%20Amber%20Forrest-,¿Qué%20es%20el%20análisis%20de%20vulnerabilidades%3F,externos%20o%20internos%20pueden%20aprovechar

IBM ¿Qué son las pruebas de software? | IBM. (s.f.). IBM - United States. https://www.ibm.com/es-es/topics/software-testing

Indeed. (2024). Técnicas para la capacitación de equipos: Mejora el rendimiento de tu personal. Indeed. https://mx.indeed.com/orientacion-profesional/desarrollo-profesional/tecnicas-capacitacion-equipo

Kaspersky. (s.f.). ¿Qué es la capacitación en concientización sobre seguridad? Kaspersky. https://latam.kaspersky.com/resource-center/definitions/what-is-security-awareness-training

NSIT. (2024). ¿Por qué las pruebas de phishing test son cruciales para tu empresa? NSIT. https://www.nsit.com.co/por-que-las-pruebas-de-phishing-test-son-cruciales-para-tu-empresa/

Unique. (2019). ¿Qué es RFP (request for proposal) o solicitud de propuesta? Unique. https://esunique.com/que-es-rfp-request-for-proposal-o-solicitud-de-propuesta/

Visión Tecnológica. (2023). Soluciones informáticas integrales: ¿Qué son y cómo funcionan? LinkedIn. https://www.linkedin.com/pulse/soluciones-informáticas-integrales-qué-son-y-cómo/

Zendesk. (2023). Niveles de soporte técnico: ¿Qué son y cómo gestionarlos? Zendesk. https://www.zendesk.com.mx/blog/niveles-soporte-tecnico/

Zendesk. (2023). Presentación de ventas: Estrategias para captar clientes. Zendesk. https://www.zendesk.com.mx/blog/presentacion-ventas/

ANEXOS / APENDICES

ANEXO A: Certificado Único Laboral para Personas Adultas

PERÚ | Ministerio de Trabajo y Promoción del Empleo

República del Perú — Firma Digital

Firmado digitalmente por: Ministerio de Trabajo y Promoción del Empleo
Motivo: Servidor de Agente automatizado.
Fecha: 12/09/2023 08:39:46-0500

septiembre 12, 2023 / 08:39

20237404529

CERTIADULTO – Certificado Único Laboral para Personas Adultas

El Ministerio de Trabajo y Promoción del Empleo CERTIFICA que en la Plataforma de Interoperabilidad del Estado (PIDE) y el Sistema de Planillas Electrónicas se registra la siguiente información:

IDENTIDAD: Validación - RENIEC

Nombres	:	WILSON ZACARIAS
Apellidos	:	DIAZ CORDOVA
Fecha de nacimiento	:	22/03/1990
DNI	:	46222553
Domicilio	:	

ANTECEDENTES POLICIALES: Validación - PNP

No registra antecedentes.

ANTECEDENTES JUDICIALES: Validación - INPE

El registro consultado está observado

ANTECEDENTES PENALES: Validación – Poder Judicial

No registra antecedentes.

TRAYECTORIA EDUCATIVA RESPECTO A FORMACIÓN UNIVERSITARIA: Validación - SUNEDU

No se puede presentar información solicitada debido a incovenientes con el sistema SUNEDU.

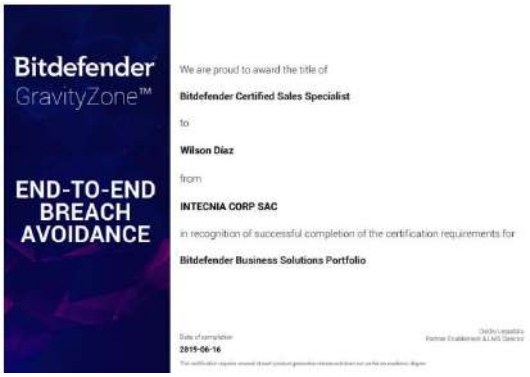
TRAYECTORIA EDUCATIVA RESPECTO A EDUCACIÓN SUPERIOR PEDAGÓGICA, TECNOLÓGICA Y ARTÍSTICA: Validación – MINEDU

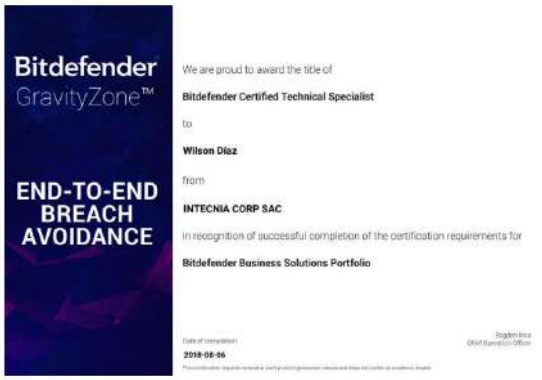
No se registra información sistematizada para el DNI consultado.

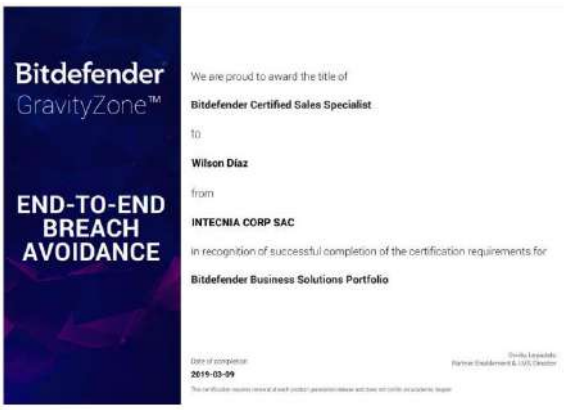
EXPERIENCIA LABORAL: Validación - MTPE

Ruc	Razón Social	Desde	Hasta
20605050060	SAFE NETWORK S.A.C.	15/10/2019	08/01/2021
20550187664	INTECNIA CORP S.A.C	02/01/2019	31/07/2019
20550187664	INTECNIA CORP S.A.C	01/01/2015	30/11/2018

ANEXO B: Certificados de Bitdefender.







ANEXO C: Eventos Bitdefender

ANEXO D: Diplomado en Seguridad de la Información.

BS grupo

DIPLOMA

Se Otorga el siguiente Diploma a:

Don: WILSON ZACARIAS DIAZ CORDOVA

Por haber completado en forma satisfactoria el Diplomado:

"SEGURIDAD DE LA INFORMACIÓN ISO 27001:2013"

Desarrollado desde el 7 de Marzo de 2017 al 15 de Julio de 2017,
con una duración de 60 horas cronológicas,
en el cual se desarrolló el siguiente temario (detallado al reverso).

Lima, Agosto del 2017

BS GRUPO DIRECTOR AREA DE CAPACITACIÓN

ING. OSCAR QUINTANILLA PEREZ
Director Académico
BS GRUPO S.A.C

BS GRUPO GERENTE AREA DE CAPACITACIÓN

ING. JIMMY QUINTANILLA PEREZ
Gerente General
BS GRUPO S.A.C

936181BA57620317P0

ANEXO E: Certificación ISO SGSI 27001: Seguridad de la Información.

AENOR

Otorga el presente

CERTIFICADO

A: WILSON ZACARÍAS DIAZ CÓRDOVA

Por haber aprobado el curso de:

AUDITOR INTERNO EN SISTEMAS DE SEGURIDAD EN TECNOLOGÍAS DE LA INFORMACIÓN ISO 27001:2013

Realizado los días 18 y 19 de noviembre de 2017 en la ciudad de Lima con una duración de 16 horas.

Pedro J. Fernández García
Director General
AENOR PERÚ

N° Registro APE/17/2049

27 de noviembre de 2017

AENOR AENOR AENOR AENOR AENOR AENOR AENOR AENOR AENOR AENOR AENOR AENOR AENOR