PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS Y COMPUTACIÓN

"PROPUESTA METODOLÓGICA PARA LA IMPLEMENTACIÓN DE UN MODELO DE NEGOCIO PARA LA PRESTACIÓN DE SERVICIOS ESTRATÉGICOS DE CIBERSEGURIDAD"

AUTOR

PIERRE LUIGY CAMINO MOLINA

DIRECTORA: ING. SUYANA ARCOS

QUITO DM, 2021

DEDICATORIA

Dedicado a todas las personas que hoy amo y a las que amaré en el futuro.

AGRADECIMIENTO

A Dios, por guiar mis pasos.

A mis amados padres Patricio Camino y Alexandra Molina, ustedes han sido la base elemental de mi formación y quienes siempre estuvieron a mi lado para celebrar mis triunfos y levantarme en mis tropiezos. Gracias a la vida por ser mis padres.

A mi hermano Jean Camino, quien ha sido mi ejemplo. Quiero agradecerte por tu apoyo incondicional en todas las etapas de mi vida.

A Melissa Vélez, la mujer que hoy amo, por compartir conmigo la increíble persona que eres.

A mis amigos por acompañarme en todas las alegrías y tristezas que vivimos juntos.

A mi tutora la Ing. Susana Arcos por sus consejos que fueron siempre útiles para culminar este trabajo.

Y a todos mis profesores por formarme con excelencia y profesionalidad.

Tabla de Contenidos

DEDICATORIA 2

AGRADECIMIENTO 3

CAPÍTULO I 1

1. INTRODUCCIÓN 1

1.1 Justificación 1

1.2 Planteamiento del problema 2

1.2.1 Objetivos 3

1.2.2 Objetivo General 3

1.2.3 Objetivos Específicos 3

2. MARCO TEÓRICO 4

2.1 Controles del anexo del estándar ISO 27002 4

2.1.1 Políticas de seguridad de la información 4

2.1.2 Organización de la seguridad de la información 4

2.1.3 Seguridad de los recursos humanos 5

2.1.4 Gestión de activos 5

2.1.5 Control de accesos 6

2.1.6 Criptografía – Cifrado y gestión de claves 7

2.1.7 Seguridad física y ambiental 7

2.1.8 Seguridad operacional 8

2.1.9 Seguridad de las comunicaciones 9

2.1.10 Adquisición, desarrollo y mantenimiento de sistemas 10

2.1.11 Relación con los proveedores 11

2.1.12 Gestión de incidentes de seguridad de la información 11

2.1.13 Aspectos de seguridad de la información en la gestión de la continuidad del negocio 12

2.1.14 Cumplimiento 12

2.2 ITIL V4 13

2.2.1 ITIL Service Value System (SVS) 13

2.3 CMMI 17

2.3.1 Inicial 17

2.3.2 Gestionado 17

2.3.3 Definido 17

2.3.4 Cuantitativamente gestionado 18
2.3.5 Optimizado 18
CAPÍTULO II 19
3. CIBERSEGURIDAD 19
3.1 ISO 27032 19
3.2 Definiciones y conceptos fundamentales 20
3.2.1 Seguridad de la información 21
3.2.2 Ciber riesgos 22
3.3 Tendencias 26
3.3.1 Ciberseguridad como una estrategia de negocio 26
3.3.2 Ciberataques 27
3.3.3 Iniciativas de ciberseguridad en las empresas 28
3.3.4 Situación actual de la ciberseguridad en el Ecuador y Latinoamérica 30
3.3.5 Panorama de amenazas cibernéticas en el Ecuador 32
CAPÍTULO III 33
4. MODELO DE NEGOCIO 33
4.1 Estudio de los requerimientos de mercado 33
4.1.1 Metodología 34
4.1.2 Encuestas y Entrevistas 35
4.1.3 Identificación y análisis de los servicios. 36
4.1.4 Resumen y criterios de inclusión de los servicios en el catálogo. 64
4.2 Estructura organizacional de una empresa de ciberseguridad 67
4.2.1 Propuesta de valor de la ciberseguridad como negocio 69
4.2.2 Los Proveedores. 70
4.2.3 Los Clientes 72
4.2.4 Cómo se inicia un negocio de ciberseguridad 73
4.3 Portafolio de servicios de ciberseguridad 76
4.3.1 Desarrollo del catálogo de servicios de ciberseguridad basado en ITIL V4. 78
CAPÍTULO IV 96
5. PROPUESTA DE IMPLEMENTACIÓN ESTRATÉGICA DE LOS SERVICIOS DE CIBERSEGURIDAD 96
5.1 Estrategia de mercado 96
5.1.1 Marketing para la ciberseguridad. 96

5.1.2 Cómo ofrecer servicios de ciberseguridad 97

5.2 Evaluación del nivel de madurez de ciberseguridad basado en el estándar ISO 27002 y CMMI 98

5.3 Planificación de la implementación estratégica de acuerdo con los servicios de ciberseguridad del catálogo 104

5.4 Beneficios de implementar la ciberseguridad de manera estratégica 107

5.4.1 Análisis Financiero 108

6. CONCLUSIONES Y RECOMENDACIONES 112

6.1 Conclusiones 112

6.2 Recomendaciones 113

7. BIBLIOGRAFÍA 114

8. ANEXOS 117

8.1 Glosario de términos. 117

8.2 Estructura de las encuestas realizadas. 119

8.3 Evidencia de las encuestas realizadas 129

8.4 Justificación del presupuesto y proyecciones de inversión. 130

CAPÍTULO I

1. INTRODUCCIÓN

1.1 Justificación

En la actualidad la inversión que realizan las empresas en generar un crecimiento y renovación digital por medio de las TIC (Tecnologías de la Información y Comunicación) es cada vez mayor y por ende el riesgo cibernético asociado también aumenta.

El mercado mundial de la ciberseguridad mueve alrededor de USD 97 billones al año, y en Latinoamérica alrededor de 3 billones de dólares, con un crecimiento proyectado de 12% anual hasta el 2021 (International Data Corporation, 2017), razón por la cual las empresas la están empezando a considerar como un elemento importante dentro de la estrategia de innovación tecnológica. Sin embargo, hoy en día el mercado ecuatoriano presenta varias limitaciones y obstáculos dado que la incorporación de un entorno digital con un alto nivel de madurez en ciberseguridad suele tener costos elevados debido a la falta de una estrategia cibernética que aporte valor al negocio dentro del proceso de implementación, además de la falta de personal capacitado en el área.

Por lo anterior mencionado el presente plan de disertación propone una metodología para formar una empresa de ciberseguridad que contemple estos desafíos desde un catálogo de servicios y una visión estratégica de implementación basada en los anexos del estándar de seguridad ISO 27002 (International Organization for Standardization) y el sistema de madurez de capacidades CMMI (Capability Maturity Model Integration) buscando la mejor alternativa en costo beneficio para el contexto de cada empresa, transformando así el problema en oportunidades de crecimiento económico y participación en el mercado ecuatoriano.

1.2 Planteamiento del problema

Durante los últimos 4 años en el Ecuador se ha registrado un aumento significativo en la aceptación e incorporación tecnológica a nivel corporativo e individual, no solo por las nuevas TIC emergentes sino también por la emergencia sanitaria del COVID -19. Ante este problema emergente y para garantizar su continuidad las empresas más representativas de la economía ecuatoriana como son las organizaciones financieras, entidades comerciales privadas e instituciones públicas han o se encuentran en proceso de automatizar sus servicios. En consecuencia, al desarrollo de esta transformación digital empresarial se han generado problemas de ciberseguridad especialmente para la banca ecuatoriana.

Por otro lado, existe un déficit de profesionales en el área de ciberseguridad, haciendo que los negocios ya existentes en el Ecuador contemplen ciertas limitantes operativas en sus servicios sin lograr aportar un nivel de madurez robusto a sus clientes.

En base a lo mencionado, se requiere de una solución viable e innovadora para los negocios que se hallan inmersos en este problema de ciberseguridad.

En función a la problemática ya descrita se plantea la siguiente pregunta principal:

- ¿Qué se necesita para implementar un modelo de negocio en ciberseguridad?

Y las siguientes preguntas secundarias:

- ¿Cuáles son los requerimientos actuales de ciberseguridad en el mercado ecuatoriano?
- ¿Cuáles son los servicios de ciberseguridad que podrían satisfacer las necesidades del mercado?
- ¿Cuál es el costo beneficio que obtienen las empresas al incorporar estratégicamente la ciberseguridad?
- ¿Cómo se implementa un plan estratégico de ciberseguridad?

1.2.1 Objetivos

1.2.2 Objetivo General

Proponer una metodología para implementar un modelo de negocio para la prestación de servicios de ciberseguridad.

1.2.3 Objetivos Específicos

- Identificar los requerimientos actuales de ciberseguridad en el mercado ecuatoriano.
- Desarrollar un catálogo de servicios de ciberseguridad que cubra las principales necesidades del entorno.
- Analizar el costo beneficio de la implementación de cada servicio de ciberseguridad propuesto.
- Definir un plan estratégico para la implementación de servicios de ciberseguridad.

2. MARCO TEÓRICO

2.1 Controles del anexo del estándar ISO 27002

Hoy en día la información y los sistemas de información están ligados a los objetivos de negocio particulares de cada empresa, cada vez aumenta el uso y transferencia de datos entre redes corporativas internas y externas lo cual viene acompañado de riesgos inherentes a los que se exponen los sistemas de información.

Para garantizar la seguridad de la información se han establecido estándares y normativas que las empresas deben cumplir para certificar un manejo adecuado de la información corporativa y la de sus clientes. Es así como la ISO por sus siglas en inglés International Organization for Standardization, líder emisor de estándares internacionales, en colaboración con la IEC (Comisión Electrotécnica Internacional) proponen el estándar ISO 27002 la cual tiene como objetivo proveer una guía distribuida en 14 dominios, 35 objetivos de control y 114 controles (ISO/IEC, 2013) para que las empresas puedan lograr una adecuada gestión de sus sistemas de información.

2.1.1 Políticas de seguridad de la información

La alta directiva debe definir, documentar y comunicar las políticas de seguridad de la información a todo el personal pertinente y a las partes externas de interés.

Su objetivo de control es la de establecer directrices en seguridad de la información por medio de los siguientes controles:

- Conjunto de políticas para la seguridad de la información. (ISO/IEC, 2013)
- Revisión de las políticas para seguridad de la información. (ISO/IEC, 2013)

2.1.2 Organización de la seguridad de la información

Se gestiona las operaciones de seguridad de la información a través de un marco de trabajo.

Este dominio posee dos objetivos de control, el primero se refiere a la organización interna en el cual se definen los siguientes controles:

- Asignación de responsabilidades para la seguridad de la información. (ISO/IEC, 2013)
- Segregación de tareas. (ISO/IEC, 2013)
- Contacto con las autoridades. (ISO/IEC, 2013)
- Contacto con los grupos de interés especial. (ISO/IEC, 2013)

- Seguridad de la información en la gestión de proyectos. (ISO/IEC, 2013)

El segundo objetivo se encarga de garantizar las herramientas necesarias para la seguridad en el uso de dispositivos móviles y teletrabajo por medio de los siguientes controles:

- Políticas de uso de dispositivos para la movilidad. (ISO/IEC, 2013)
- Teletrabajo. (ISO/IEC, 2013)

2.1.3 Seguridad de los recursos humanos

Las organizaciones deben garantizar la seguridad de la información en la gestión del recurso humano en todo su ciclo de vida dentro de la compañía que comprende objetivos de control desde la selección y contratación hasta la finalización del contrato y salida. A continuación, se detalla los controles de seguridad por etapas.

Antes de la contratación (ISO/IEC, 2013):

- Investigación de antecedentes. (ISO/IEC, 2013)
- Términos y condiciones de contrato. (ISO/IEC, 2013)

Durante la contratación (ISO/IEC, 2013):

- Responsabilidades de gestión. (ISO/IEC, 2013)
- Concienciación, educación y capacitación en seguridad de la información. (ISO/IEC, 2013)
- Proceso disciplinario. (ISO/IEC, 2013)

Cese o cambio de puesto de trabajo (ISO/IEC, 2013):

- Cese o cambio de puesto de trabajo. (ISO/IEC, 2013)

2.1.4 Gestión de activos

Se debe justificar la existencia de los activos de información dentro de una organización, así como asignar un responsable que coordine su protección y mantenimiento. Por medio de la clasificación de activos se debe generar un inventario de activos de información en el cual se muestra los propietarios y características relevantes de cada activo.

Al asignar la responsabilidad sobre un activo se debe considerar los siguientes controles (ISO/IEC, 2013):

- Inventario de activos. (ISO/IEC, 2013)
- Propiedad de los activos. (ISO/IEC, 2013)
- Uso aceptable de los activos. (ISO/IEC, 2013)
- Devolución de activos. (ISO/IEC, 2013)

Para gestionar la clasificación de la información se establece (ISO/IEC, 2013):

- Directrices de clasificación. (ISO/IEC, 2013)
- Etiquetado y manipulado de la información. (ISO/IEC, 2013)
- Manipulación de activos. (ISO/IEC, 2013)

Dentro del proceso de soporte y mantenimiento se definen los siguientes controles (ISO/IEC, 2013):

- Gestión de soporte extraíble. (ISO/IEC, 2013)
- Eliminación de soportes. (ISO/IEC, 2013)
- Soportes físicos en tránsito. (ISO/IEC, 2013)

2.1.5 Control de accesos

Uno de los principales objetivos de la ISO 27002 es controlar el acceso a la información por medio de restricciones y controles alineados a los objetivos de cada negocio entre los cuales tenemos:

Requisitos del negocio para el control de accesos (ISO/IEC, 2013):

- Política de control de accesos. (ISO/IEC, 2013)
- Control de acceso a las redes y servicios asociados. (ISO/IEC, 2013)

Gestión de acceso a usuarios (ISO/IEC, 2013):

- Gestión de altas y bajas en el registro de usuarios. (ISO/IEC, 2013)
- Gestión de los derechos de acceso asignados a los usuarios. (ISO/IEC, 2013)
- Gestión de los derechos de acceso con privilegios especiales. (ISO/IEC, 2013)
- Gestión de la información confidencial de autenticación de usuarios. (ISO/IEC, 2013)

- Revisión de los derechos de acceso de los usuarios. (ISO/IEC, 2013)
- Retirada o adaptación de los derechos de acceso. (ISO/IEC, 2013)

Responsabilidades del usuario:

- Uso de información confidencial para la autenticación. (ISO/IEC, 2013)

Control de acceso a sistemas y aplicaciones (ISO/IEC, 2013):

- Restricción del acceso a la información. (ISO/IEC, 2013)
- Procedimientos seguros de inicio de sesión. (ISO/IEC, 2013)
- Gestión de contraseñas de usuario. (ISO/IEC, 2013)
- Uso de herramientas de administración de sistemas. (ISO/IEC, 2013)
- Control de acceso al código fuente de los programas. (ISO/IEC, 2013)

2.1.6 Criptografía – Cifrado y gestión de claves

La ISO 27002 establece que deben utilizarse controles de criptografía y regulación de contraseñas para proteger la información confidencial y crítica contra cualquier acceso no autorizado.

Controles criptográficos (ISO/IEC, 2013):

- Política de uso de los controles criptográficos. (ISO/IEC, 2013)
- Gestión de claves. (ISO/IEC, 2013)

La implementación de estos controles se basa en un análisis de riesgos, por lo cual, el nivel de protección varía según las necesidades de cada negocio.

2.1.7 Seguridad física y ambiental

La gestión de la seguridad física es la primera línea de defensa para acceder a los sistemas de información, por eso es importante considerar los siguientes controles y objetivos de seguridad.

Áreas seguras (ISO/IEC, 2013):

- Perímetro de seguridad física. (ISO/IEC, 2013)

- Controles físicos de entrada. (ISO/IEC, 2013)
- Seguridad de oficinas, despachos y recursos. (ISO/IEC, 2013)
- Protección contra las amenazas externas y ambientales. (ISO/IEC, 2013)
- El trabajo en áreas seguras. (ISO/IEC, 2013)
- Áreas de acceso público, carga y descarga. (ISO/IEC, 2013)

Seguridad de los equipos (ISO/IEC, 2013):

- Emplazamiento y protección de equipos. (ISO/IEC, 2013)
- Instalaciones de suministro. (ISO/IEC, 2013)
- Seguridad de cableado. (ISO/IEC, 2013)
- Mantenimiento de los equipos. (ISO/IEC, 2013)
- Salida de activos fuera de las dependencias de la empresa. (ISO/IEC, 2013)
- Seguridad de los equipos y activos fuera de las instalaciones. (ISO/IEC, 2013)
- Reutilización o retirada segura de dispositivos de almacenamiento. (ISO/IEC, 2013)
- Equipo informático de usuario desatendido. (ISO/IEC, 2013)
- Política de puesto de trabajo despejado y bloqueo de pantalla. (ISO/IEC, 2013)

2.1.8 Seguridad operacional

El flujo de cualquier empresa es su parte operativa la cual debe estar protegida para poder mantener el procesamiento y manejo de información adecuado dentro de sus labores cotidianas. Para lograr una seguridad operacional óptima la ISO 27002 establece los siguientes controles.

Responsabilidad y procedimientos de operación (ISO/IEC, 2013):

- Documentación de procedimientos de operación. (ISO/IEC, 2013)
- Gestión de cambios. (ISO/IEC, 2013)
- Gestión de capacidades. (ISO/IEC, 2013)
- Separación de entornos de desarrollo, pruebas y producción. (ISO/IEC, 2013)

Protección contra código malicioso (ISO/IEC, 2013):

- Controles contra el código malicioso. (ISO/IEC, 2013)

Copias de seguridad (ISO/IEC, 2013):

- Copias de seguridad de la información. (ISO/IEC, 2013)

Registro de actividades y supervisión (ISO/IEC, 2013):

- Registro de eventos de actividad. (ISO/IEC, 2013)
- Protección de los registros de información. (ISO/IEC, 2013)
- Registros de actividad del administrador y operador del sistema. (ISO/IEC, 2013)
- Sincronización de relojes. (ISO/IEC, 2013)

Control de software en explotación (ISO/IEC, 2013):

- Instalación de software en sistemas en producción. (ISO/IEC, 2013)

Gestión de vulnerabilidades técnicas (ISO/IEC, 2013):

- Gestión de las vulnerabilidades técnicas. (ISO/IEC, 2013)
- Restricciones en la instalación de software. (ISO/IEC, 2013)

Consideraciones de las auditorías de los sistemas de información (ISO/IEC, 2013):

- Controles de auditoría de los sistemas de información. (ISO/IEC, 2013)

2.1.9 Seguridad de las comunicaciones

Proteger los canales por donde se transmite la información es de vital importancia para una seguridad cibernética en cualquier organización. Este dominio se enfoca en garantizar la seguridad y proteger el intercambio de información en cualquier escala de datos. Los controles que se deben implementar son los siguientes.

Gestión de seguridad en las redes (ISO/IEC, 2013):

- Control de red. (ISO/IEC, 2013)
- Mecanismos de seguridad asociados a servicios de red. (ISO/IEC, 2013)
- Segregación de redes. (ISO/IEC, 2013)

Intercambio de información con partes externas (ISO/IEC, 2013):

- Políticas y procedimientos de intercambio de información. (ISO/IEC, 2013)
- Acuerdos de intercambio. (ISO/IEC, 2013)
- Mensajería electrónica. (ISO/IEC, 2013)
- Acuerdos de confidencialidad y secreto. (ISO/IEC, 2013)

2.1.10 Adquisición, desarrollo y mantenimiento de sistemas

La seguridad debe ser abordada de forma global y transversal dentro de cada organización, es decir, debe estar presente en todas las unidades que conforman la administración de los sistemas de información. Para cumplir con este objetivo se definen los siguientes controles.

Requisitos de seguridad de los sistemas de información (ISO/IEC, 2013) :

- Análisis y especificaciones de los requisitos de seguridad. (ISO/IEC, 2013)
- Seguridad de las comunicaciones en servicios accesibles por redes públicas. (ISO/IEC, 2013)
- Protección de las transacciones por redes telemáticas. (ISO/IEC, 2013)

Seguridad en los procesos de desarrollo y soporte (ISO/IEC, 2013) :

- Políticas de desarrollo seguro de software. (ISO/IEC, 2013)
- Procedimientos de control de cambios en los sistemas. (ISO/IEC, 2013)
- Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. (ISO/IEC, 2013)
- Restricciones a los cambios en los paquetes de software. (ISO/IEC, 2013)
- Uso de principios de ingeniería en protección de sistemas. (ISO/IEC, 2013)
- Seguridad en entornos de desarrollo. (ISO/IEC, 2013)
- Externalización del desarrollo de software. (ISO/IEC, 2013)
- Pruebas de funcionalidad durante el desarrollo de los sistemas.
- Pruebas de aceptación. (ISO/IEC, 2013)

2.1.11 Relación con los proveedores

Se debe establecer controles de seguridad al momento de tener relaciones con terceras partes, sean clientes o proveedores, la información que se maneje en estos casos debe estar protegida. La ISO 27002 define los siguientes objetivos de control.

Seguridad de la información en las relaciones con suministradores (ISO/IEC, 2013):

- Política de seguridad de la información para suministradores. (ISO/IEC, 2013)
- Tratamiento de riesgo dentro de acuerdos de suministradores. (ISO/IEC, 2013)
- Cadena de suministro en tecnologías de la información y comunicaciones. (ISO/IEC, 2013)

Gestión de prestación del servicio por suministradores (ISO/IEC, 2013):

- Supervisión y revisión de los servicios prestados por terceros. (ISO/IEC, 2013)
- Gestión de cambios en los servicios prestados por terceros. (ISO/IEC, 2013)

2.1.12 Gestión de incidentes de seguridad de la información

Uno de los puntos más importantes dentro de la seguridad de la información es la capacidad de resiliencia de una empresa ante un incidente de seguridad garantizando una respuesta rápida y eficiente ante un evento que pueda comprometer la seguridad de los sistemas de información. Se establecen los siguientes controles de seguridad

Gestión de incidentes de seguridad de la información y mejoras (ISO/IEC, 2013):

- Responsabilidades y procedimientos. (ISO/IEC, 2013)
- Notificación de los eventos de seguridad de la información. (ISO/IEC, 2013)
- Notificación de puntos débiles de la seguridad. (ISO/IEC, 2013)
- Valoración de eventos de seguridad de la información y toma de decisiones. (ISO/IEC, 2013)
- Respuesta a los incidentes de seguridad. (ISO/IEC, 2013)
- Aprendizaje de los incidentes de seguridad de la información. (ISO/IEC, 2013)
- Recopilación de evidencias. (ISO/IEC, 2013)

2.1.13 Aspectos de seguridad de la información en la gestión de la continuidad del negocio

En este dominio se establecen los controles necesarios para que el negocio sea capaz de recuperar su información y continuar con sus labores operativas en el menor tiempo posible. Entre estos controles tenemos.

Continuidad de la seguridad de la información (ISO/IEC, 2013):

- Planificación de la continuidad de la seguridad de la información. (ISO/IEC, 2013)
- Implantación de la continuidad de la seguridad de la información. (ISO/IEC, 2013)
- Verificación, revisión y evaluación de la continuidad de la seguridad de la información. (ISO/IEC, 2013)

Redundancias (ISO/IEC, 2013):

- Disponibilidad de instalaciones para el procesamiento de la información. (ISO/IEC, 2013)

2.1.14 Cumplimiento

Para garantizar que los controles antes definidos se cumplan es necesario establecer aspectos legislativos, normativas y políticas aplicables al giro del negocio, escalables, fáciles de monitorear y sujetos a actualizaciones periódicas. Entre los controles que se deben implementar tenemos:

Cumplimiento de los requisitos legales y contractuales (ISO/IEC, 2013):

- Identificación de la legislación aplicable. (ISO/IEC, 2013)
- Derecho de propiedad intelectual (DPI). (ISO/IEC, 2013)
- Protección de los registros de la organización. (ISO/IEC, 2013)
- Protección de datos y privacidad de la información personal. (ISO/IEC, 2013)
- Regulación de los controles criptográficos. (ISO/IEC, 2013)

Revisiones de la seguridad de la información (ISO/IEC, 2013):

- Revisión independiente de la seguridad de la información. (ISO/IEC, 2013)
- Cumplimiento de las políticas y normas de seguridad. (ISO/IEC, 2013)
- Comprobación de cumplimiento. (ISO/IEC, 2013)

2.2 ITIL V4

ITIL 4 es la última versión del marco de trabajo ITIL publicada en febrero del 2019. (AXELOS, 2019). Esta nueva versión de ITIL se centra en reunir a diferentes partes interesadas en una organización para coclear valor para los usuarios finales. Con la llegada de nuevos marcos como VeriSM, SIAM y FitSM en el panorama de la gestión de servicios de TI, existía la necesidad de que la versión anterior de ITIL (ITIL v3) fuera más refinada en la forma en que se aborda la gestión de servicios como un habilitador para las empresas. (AXELOS, 2019). Esta versión presenta facilidad en el manejo con relación a su predecesora, ya que, en lugar de idealizar procesos de implementación, ahora entrega soluciones a medida de cualquier organización por medio de prácticas divididas en dos componentes: The Four Dimensions Model e ITIL Service Value System.

Dentro del presente trabajo de titulación se tomó como referencia el ITIL Service Value System para el diseño del catálogo de servicios de ciberseguridad.

2.2.1 ITIL Service Value System (SVS)

El Sistema de valor de servicio SVS de ITIL es un marco de referencia para la gestión y diseño de servicios dentro de una organización. El SVS describe las entradas al sistema, los diferentes elementos de la empresa que están directamente involucrados en la creación de valor y las salidas para lograr los objetivos comerciales. (AXELOS, 2019).

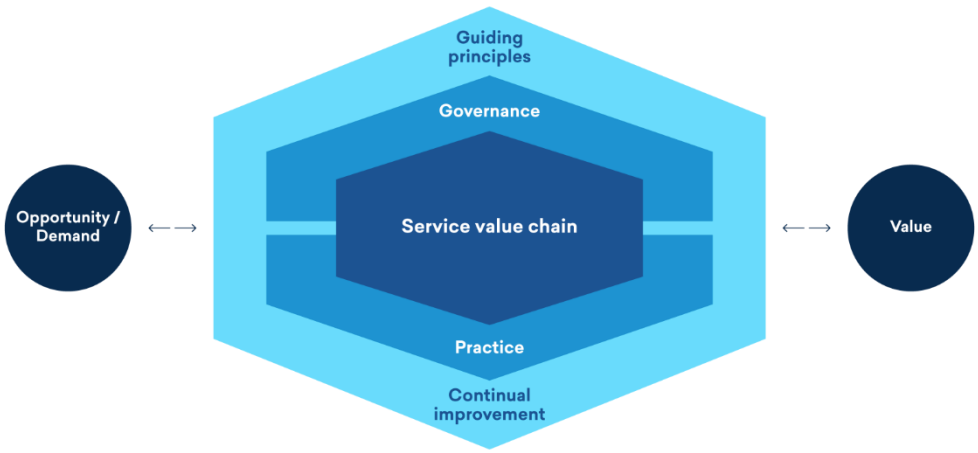


Figura 1. ITIL Service Value System (SVS). (AXELOS, 2019)

2.2.1.1 Oportunidad / Demanda

Oportunidad hace referencia a toda situación que pueda aportar valor al usuario final. Demanda es la necesidad de un producto o servicio en un determinado mercado. Las empresas deben mantener estos dos elementos a lo largo de su proceso de implementación del SVS, sin embargo, no se debe capitalizar en todas las oportunidades ni enfocarse en satisfacer todas las necesidades.

2.2.1.2 Principios Guía

Son un conjunto de recomendaciones que orienta a las empresas dentro de la gestión de los servicios alineados a sus objetivos, estrategias y estructura organizacional. (AXELOS, 2019) define siete principios guías dentro del libro básico de ITIL 4:

- Enfocarse en el valor.
- Empieza donde te encuentras.
- Progresa iterativamente con retroalimentación.
- Colabora y promueve la visibilidad.
- Piensa y trabaja de forma holística, es decir, considerar los servicios como un todo.
- Manténlo simple y práctico.
- Optimiza y automatiza.

2.2.1.3 Gobierno

Independientemente del tamaño de una organización, todas son dirigidas por una o varias personas denominadas la alta directiva o C-suite quienes son los encargados de supervisar, evaluar, dirigir y monitorear las actividades que se realizan en la cadena de valor dentro del proceso de gestión de los servicios.

2.2.1.4 Cadena de Valor

Se la describe como un conjunto de seis actividades clave que de manera conjunta aportan valor al usuario final. Estas actividades están basadas en prácticas de gestión de ITIL y se relacionan unas con otras de la siguiente manera.

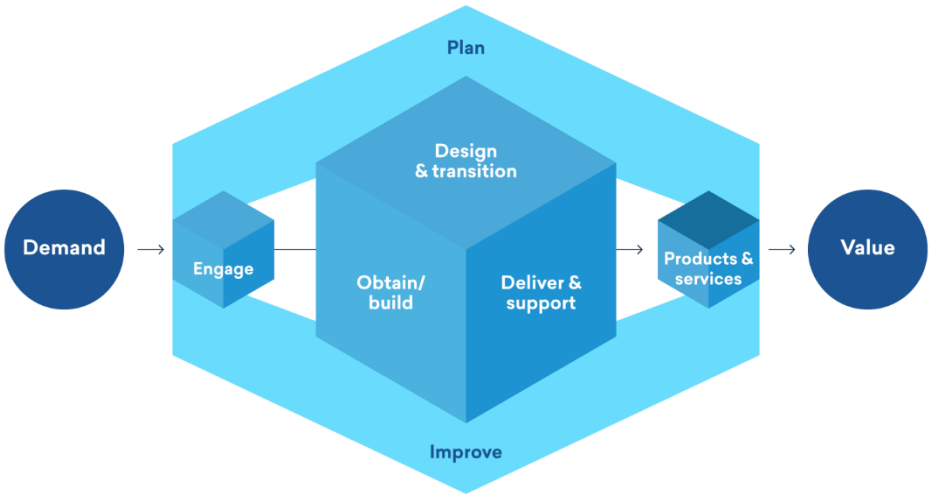


Figura 2. ITIL Service Value Chain. (AXELOS, 2019)

A continuación, se presenta un listado de las actividades que se describen en la cadena de valor de servicio de ITIL:

2.2.1.4.1 **Planificación:** La fase de creación de planes, políticas, estándares y la dirección del flujo de valor de los servicios. (AXELOS, 2019)

2.2.1.4.2 **Mejora:** Asegurar un crecimiento y mejora continua de las prácticas, productos y servicios que ofrece una empresa. (AXELOS, 2019)

2.2.1.4.3 **Compromiso:** Establecer buenas relaciones con las partes interesadas, involucradas o también llamados stakeholders y usuarios finales para proveer transparencia y un entendimiento claro de los servicios. (AXELOS, 2019)

2.2.1.4.4 **Diseño y Transición:** Los productos o servicios desarrollados deben cumplir las demandas de los stakeholders. (AXELOS, 2019)

2.2.1.4.5 **Obtener / Construir:** Garantizar la disponibilidad de los componentes que ayudarán a proveer el servicio tales como hardware, software, etc. (AXELOS, 2019)

2.2.1.4.6 **Entrega y Soporte:** Asegurarse de que el servicio es entregado y respaldado por un SLA (Service Level Agreement) de tal manera que cumpla las expectativas de los stakeholders. (AXELOS, 2019)

2.2.1.5 Mejora Continua

La idea central de la mejora continua (IC) en el contexto de la gestión de servicios es buscar constantemente oportunidades para mejorar la eficacia y la eficiencia de los servicios de TI que habilitan los procesos de negocio. (Freshworks Inc, 2019). En esta etapa debe ser transversal a todos los procesos de negocio de una organización, se debe mejorar continuamente las unidades operativas, productos, servicios, relaciones, etc.

2.2.1.6 Prácticas

La práctica de gestión de ITIL en ITIL 4 es un conjunto de recursos organizacionales diseñados para realizar un trabajo o lograr un objetivo. (AXELOS, 2019).

Cada etapa consta de un conjunto de procesos o funciones que están alineados con la estructura organizativa de TI. ITIL 4, por otro lado, describe "prácticas" en lugar de procesos, aunque estas dos palabras se usan indistintamente, significan cosas completamente diferentes en el contexto de la gestión de servicios de TI. (Freshworks Inc, 2019).

El ITIL SVS incluye 14 prácticas de administración general, 17 prácticas de gestión de servicios y 3 prácticas de gestión técnica.

Tabla 1

Prácticas de gestión ITIL 4

PRÁCTICAS DE ADMINISTRACIÓN GENERAL	PRÁCTICAS DE GESTIÓN DE SERVICIO	PRÁCTICAS DE GESTIÓN TÉCNICA
ADMINISTRACIÓN DE LA ARQUITECTURA	GESTIÓN DE DISPONIBILIDAD	GESTIÓN DE DESPLIEGUE
MEJORA CONTINUA	ANÁLISIS DE NEGOCIO	ADMINISTRACIÓN DE PLATAFORMAS E INFRAESTRUCTURA
GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	GESTIÓN DE CAPACIDAD Y DESEMPEÑO	DESPLIEGUE Y ADMINISTRACIÓN DE SOFTWARE
GESTIÓN DE CONOCIMIENTO	CONTROL DE CAMBIOS	
MÉTRICAS Y REPORTE	GESTIÓN DE INCIDENTES	
GESTIÓN DE CAMBIO ORGANIZACIONAL	GESTIÓN DE ACTIVOS DE TI	
GESTIÓN DE PORTAFOLIO	GESTIÓN DE EVENTOS Y MONITOREO	
GESTIÓN DE PROYECTOS	GESTIÓN DE PROBLEMAS	
GESTIÓN DE RELACIONES	GESTIÓN DE ENTREGA	
GESTIÓN DE RIESGOS	GESTIÓN DE CATÁLOGO DE SERVICIOS	

GESTIÓN DE SERVICIOS FINANCIEROS	GESTIÓN DE SERVICIOS DE CONFIGURACIÓN
GESTIÓN DE ESTRATÉGIA	GESTIÓN DE CONTINUIDAD DEL NEGOCIO
GESTIÓN DE PROVEEDORES	DISEÑO DE SERVICIOS
GESTIÓN DE PERSONAL Y EQUIPO DE TRABAJO	GESTIÓN DEL NIVEL DE SERVICIO
	GESTIÓN DE SOLICITUD DEL SERVICIO
	VALIDACIÓN Y PRUEBAS DEL SERVICIO

Tabla 1. Prácticas de gestión ITIL 4 en la cual se incluyen 14 prácticas de administración general, 17 prácticas de gestión de servicios y 3 prácticas de gestión técnica.

2.3 CMMI

El modelo de madurez de capacidades de integración o por sus siglas en inglés CMMI (Capability Maturity Model Integration) es un marco de trabajo que detalla las buenas prácticas en el desarrollo y mantenimiento de software, como también en la obtención de información para efectuar auditorías de productos y servicios.

CMMI no es una metodología. CMMI nos dice qué buenas prácticas implementar, pero no nos dice exactamente cómo. Es un "framework", un conjunto de buenas prácticas organizadas por capacidades críticas de negocio con el objetivo de mejorar su rendimiento. (Deloitte, 2021).

El principal objetivo de CMMI es el de evaluar la madurez de cualquier proceso dentro de una compañía para así poder definir procesos de mejora.

En el presente trabajo se utilizó CMMI para medir el nivel de madurez de los controles de ciberseguridad establecidos en la normativa ISO 27002 categorizándolos en 5 fases o niveles de madurez los cuales se dividen de la siguiente manera:

2.3.1 Inicial

El proceso es informal, existe menor calidad y un riesgo alto.

2.3.2 Gestionado

Presenta un nivel básico en la gestión de proyectos, existe baja calidad y alto riesgo

2.3.3 Definido

Se estandarizan y documentan los procesos, la calidad es media con un riesgo medio tolerable.

2.3.4 Cuantitativamente gestionado

Los procesos están debidamente formalizados, existe un control y monitoreo gestionado del flujo de trabajo, la calidad es mayor con riesgos menores.

2.3.5 Optimizado

Se lo define como un flujo de trabajo ideal y alcanzable a largo plazo. Aquí existe la máxima calidad posible con riesgos menores y casi inexistentes.

CAPÍTULO II

3. CIBERSEGURIDAD

3.1 ISO 27032

La norma internacional ISO / IEC 27032 tiene como objetivo enfatizar el papel de los diferentes elementos en el ciberespacio, con respecto a la seguridad de la información, la seguridad de la red e Internet y la protección de la infraestructura de información crítica (CIIP). ISO / IEC 27032 como estándar internacional proporciona un marco de políticas para abordar el establecimiento de confiabilidad, colaboración, intercambio de información y orientación técnica para la integración del sistema entre las partes interesadas en el ciberespacio. (PECB, 2021).

El estándar ISO / IEC 27032 es esencial para que lo utilicen todas las empresas. El riesgo de amenazas a la seguridad aumenta a diario a medida que dependemos más del ciberespacio. Sin embargo, la norma ISO / IEC 27032 proporciona pautas con respecto a la protección y la sostenibilidad a largo plazo de los procesos comerciales. (PECB, 2021). De acuerdo con (PECB, 2021), esta norma internacional proporciona los siguientes beneficios:

- Una descripción general de la ciberseguridad.
- Una explicación de la relación entre la ciberseguridad y otros tipos de seguridad.
- Una definición de las partes interesadas y una descripción de sus roles en la ciberseguridad.
- Orientación para abordar problemas comunes de ciberseguridad.
- Un marco que permita a las partes interesadas colaborar en la resolución de problemas de ciberseguridad.

El acceso a los recursos de la ISO / IEC 27032 está autorizado únicamente a aquellas personas e instituciones que paguen el acceso a la documentación disponible en la OBP (Online Browsing Platform) del sitio web oficial de la ISO, razón por la cual se decidió desarrollar el presente trabajo con los recursos de libre uso del estándar ISO 27002 el cual incluye 14 dominios, 35 objetivos de control y 114 controles los cuales fueron detallados en la sección 2.1.

3.2 Definiciones y conceptos fundamentales

La ciberseguridad es una de las áreas más importantes dentro del campo de las tecnologías de información ya que vivimos en un mundo cada vez más digitalizado donde debemos proteger nuestra información y los componentes asociados con su manipulación y transmisión para construir un entorno seguro y robusto.

(Thakur & Al-Sakib, 2020) en su libro "Cybersecurity Fundamentals: A Real-World Perspective" definen a la ciberseguridad como la protección del software, hardware y las fuentes de datos conectados y almacenados en el internet, desde un individuo hasta una gran corporación, todos están involucrados en la seguridad de su información.

El alcance de la ciberseguridad no se limita a la protección de software o hardware, esta cubre los procesos de comportamiento humano hasta las operaciones tecnológicas que impactan directa o indirectamente la seguridad de los recursos y activos valiosos que almacenan, utilizan, transportan e interconectan datos.

La ciberseguridad no es un proceso de auditoría que se realiza dentro un periodo determinado, es un proceso continuo de concientización en seguridad cibernética, planificación estratégica, implementación, monitoreo y evaluación constante.

La importancia de la ciberseguridad reside en cubrir las necesidades tanto en individuos, familias, organizaciones, gobiernos y negocios de distinta índole. De acuerdo con los últimos análisis de (Gartner, 2018), se espera que el gasto total global en el campo de la ciberseguridad supere los $ 124 billones de dólares en los próximos 3 años, esto solo evidencia que la información es un activo con un valor comercial cada vez más alto y es tarea de los profesionales de la ciberseguridad garantizar un ciberespacio seguro para la información que reside en este ambiente digital, es decir que, la ciberseguridad es un componente más de la seguridad de la información, en la Figura 3 tenemos una mejor apreciación de lo expuesto anteriormente.



Figura 3. Difference between Information Security and Cyber Security. (GeeksforGeeks, 2020)

3.2.1 Seguridad de la información

La información es el conjunto de datos agrupados de tal forma que tengan sentido, se ha mencionado que la información cada vez más se transforma en un activo valioso para las organizaciones ya que en las manos equivocadas pueden generar impactos negativos en el ámbito financiero, legal y reputacional de una empresa.

La seguridad de la información nace como un concepto cuyo objetivo es el de generar controles, medidas y procesos técnicos y humanos para proteger la información cumpliendo los tres principios de seguridad informática, también llamada la triada CID por sus siglas (Confidencialidad, Integridad y Disponibilidad) a la cual hace referencia la Figura 4.



Figura 4. Principios de la seguridad informática: Confidencialidad, Integridad y Disponibilidad de la información. (Fandom, 2021)

3.2.1.1 Integridad

Hace referencia a la inalterabilidad de la información certificando que esta es completa y exacta, algunos controles que garantizan la integridad de la información son:

- Permisos de archivos.
- Control de acceso de usuarios.

3.2.1.2 Confidencialidad

Se asegura que la información sea accedida solamente por los usuarios que tienen autorización de hacerlo permitiéndoles manipularla. Algunos métodos de control de confidencialidad son:

- Cifrado y encriptación de datos.
- Identificación de usuarios.
- Gestión de contraseñas.
- Controles de autenticación.

3.2.1.3 Disponibilidad

La información debe estar disponible siempre que un usuario autorizado lo requiera, para cumplir con este objetivo es importante tomar en cuenta las siguientes consideraciones:

- Mantenimientos preventivos.
- Reparaciones de hardware.
- Actualizaciones de software.
- Conectividad adecuada.
- Plan de respuesta a incidentes.

3.2.2 Ciber riesgos

(ACIS, 2019) establece que los ciber riesgos surgen de la convergencia tecnológica entre el mundo físico y el lógico, apalancada por la densidad digital que lo rodea, es decir, de las nuevas conexiones e interfaces que generan datos sobre la condición particular del objeto. Estos riesgos, en su naturaleza diferentes a los tecnológicos, establecen un nuevo paradigma de gestión, que demanda una vista interdisciplinar y sistémica para comprender los retos de las tensiones a las cuales se ven sometidas las organizaciones en un escenario global.

Para entender un poco mejor este tipo de riesgos, es necesario definir ciertos componentes que los integran, (Dion, 2020) define los siguientes conceptos fundamentales y sus respectivas categorías:

3.2.2.1 Activo

Un activo es cualquier ítem que tenga valor para la organización, estos pueden ser tangibles o intangibles. (Dion, 2020)

3.2.2.2 Vulnerabilidad

Cualquier debilidad en el diseño del sistema, documentación, implementación, código de software, o falta de mantenimiento preventivo. Las vulnerabilidades son factores internos. (Dion, 2020)

3.2.2.3 Amenaza

Las amenazas son factores externos los cuales no podemos evitar que se produzcan, pero sí podemos gestionarlas y mitigarlas. (Dion, 2020)

3.2.2.3.1 Tipos de Amenaza

- **Amenaza Adversaria:**

  Personas u organizaciones que intentan irrumpir y dañar su red o su negocio (Dion, 2020), los más importantes pueden ser:

  - Internos de confianza
  - Competidores, proveedores, clientes
  - Compañeros de negocio
  - Ciber criminales
  - Estados o naciones

- **Amenaza Accidental:**

  Ocurre cuando alguien comete un error que daña la seguridad del sistema, los mismos que se los pude evitar definiendo y comunicando apropiadamente los procesos operativos y capacitando adecuadamente al personal. (Dion, 2020).

- **Amenaza Estructural:**

  Ocurre cuando fallan los equipos, el software o los controles físicos, lo cual podemos evitar con mantenimientos programados, equipos de contingencia, software de regulación, etc. (Dion, 2020).

- **Amenaza Ambiental:**

  Ocasionados por desastres naturales, estas amenazas se pueden gestionar por medio de sistemas de alta disponibilidad y un plan apropiado de continuidad de negocio. (Dion, 2020).

3.2.2.4 Riesgo

(E-SPIN, 2019) define un riesgo como la probabilidad de manifestación de una amenaza, no hay riesgo si no existe una vulnerabilidad y una amenaza. En la Figura 5 se aprecia de mejor manera esta relación.



Figura 5. Componentes de un riesgo. (E-SPIN, 2019)

3.2.2.4.1 Gestión de Riesgos

Uno de los principales objetivos de cualquier negocio a manera de complemento a su misión y visión debe ser reducir el riesgo asociado a sus distintas actividades operativas eligiendo un control apropiado.

Según (Dion, 2020) el riesgo se puede:

- **Aceptar:**

  Cuando sea lo suficientemente bajo como para no aplicar contramedidas, o ya se hayan aplicado contramedidas adecuadas. (Dion, 2020).

- **Transferir**:

  Si la organización no puede permitirse aceptar, evitar o mitigar el riesgo, puede transferirlo a una empresa aseguradora. (Dion, 2020).

- **Mitigar:**

  Minimizar los riesgos hasta un nivel aceptable agregando controles de riesgo. (Dion, 2020).

- **Evitar:**

  El riesgo es demasiado alto para aceptarlo, por lo que se cambia la configuración o el diseño del sistema para evitar el riesgo asociado con una vulnerabilidad específica, lo cual tiene consecuencias operativas. (Dion, 2020).

3.2.2.4.2 Tipos de Riesgo

(Dion, 2020) define cinco tipos de riesgo dentro de una organización:

- **Riesgo Estratégico:**

  Es el resultado directo de operar con una industria específica, en un momento específico al establecer relaciones estratégicas de negocio. (Dion, 2020).

- **Riesgo de Cumplimiento:**

  Ocasionado por el incumplimiento de leyes legislativas y regulaciones burocráticas. (Dion, 2020).

- **Riesgo Financiero:**

  Relacionado con presupuestos y aspectos financieros, generalmente dinero. (Dion, 2020).

- **Riesgo Operacional:**

  Como resultado de fallas internas de procesos, personas o sistemas internos. (Dion, 2020).

- **Riesgo Reputacional:**

  Pérdida de la reputación de una empresa o de la comunidad por fallas de productos, demandas o publicidad negativa. La reputación tarda mucho en construirse y solo un día para perderla. (Dion, 2020).

3.3 Tendencias

3.3.1 Ciberseguridad como una estrategia de negocio

Muchas veces la función principal de la ciberseguridad es confundida con reducir el riesgo operativo al eliminar programa maligno (programa maligno) y protegerse contra hackers o delincuentes informáticos, pero la ciberseguridad se posiciona netamente en la alta directiva como un factor de crecimiento estratégico.

Hoy en día la seguridad y gobierno de la información es muy compleja de gestionar ya que el panorama de amenazas aumenta generando cada vez más vulnerabilidades.

Al desarrollar nuevos productos y servicios, una empresa debe encontrar el equilibrio adecuado entre innovación y riesgo. En la mayoría de los casos, cuanto más se incrementa la seguridad, menos fácil de usar y conveniente se vuelve el producto o servicio. Una postura sólida en materia de ciberseguridad es esencial para garantizar que la innovación no se vea restringida debido a problemas de seguridad. Una estrategia de ciberseguridad sólida debe promover la innovación y la confianza del cliente, ambos esenciales para un crecimiento continuo. Una estrategia de ciberseguridad bien desarrollada mantiene en marcha las ruedas operativas del negocio. (X.Martin, 2019).

Se necesita una estrategia de ciberseguridad eficaz para que esta actué como soporte de los demás objetivos de negocio de una empresa mejorando la integridad del producto o servicio, la experiencia del cliente, las operaciones, el cumplimiento legal, la reputación de la marca y la confianza de los inversionistas. Las necesidades básicas de una estrategia de seguridad y bienestar cibernético incluyen: planificación minuciosa, delegación, un sistema para monitorear el cumplimiento y la supervisión de la alta directiva.

A largo plazo, la junta directiva debe comprender y considerar las implicaciones comerciales estratégicas de la ciberseguridad, fomentar una cultura corporativa consciente del riesgo cibernético y coordinar la implementación de las prácticas de seguridad en todos los procesos operativos y administrativos.

La ciberseguridad puede ser una ventaja competitiva para cualquier organización si incluye la protección de datos personales dentro de sus relaciones laborales, para obtener más negocios, todas las empresas deben ganarse la confianza de los clientes. Un solo incidente de menor impacto de

ciberseguridad puede volverse viral, provocando una pérdida rápida y generalizada de la confianza de los clientes.

(X.Martin, 2019) menciona que, para competir y ganar en el mundo impulsado por la tecnología de hoy, las empresas necesitan tener la seguridad cibernética correcta. Y las juntas directivas deben proporcionar la supervisión para garantizar que lleguen allí.

3.3.2 Ciberataques

Los ciberataques han sido calificados como el quinto riesgo mejor calificado en 2020 y se han convertido en la nueva norma en los sectores público y privado. Esta industria de riesgo continuará creciendo en 2021, ya que se espera que los ciberataques de IoT (Internet de las Cosas) por sí solos se dupliquen para 2025. (Foro Económico Mundial, 2020).

3.3.2.1 Costo del cibercrimen

La industria del cibercrimen ha cobrado relevancia en los últimos años debido al crecimiento exponencial de la tecnología. Algunas investigaciones estadísticas como la realizada por (Cybersecurity Ventures , 2021) reflejan que el delito cibernético costará a las empresas de todo el mundo un estimado de 10,5 trillones de dólares anuales para 2025, frente a los 3 trillones de dólares de 2015. Con una tasa de crecimiento del 15 por ciento interanual, representando así la mayor transferencia de riqueza económica de la historia.

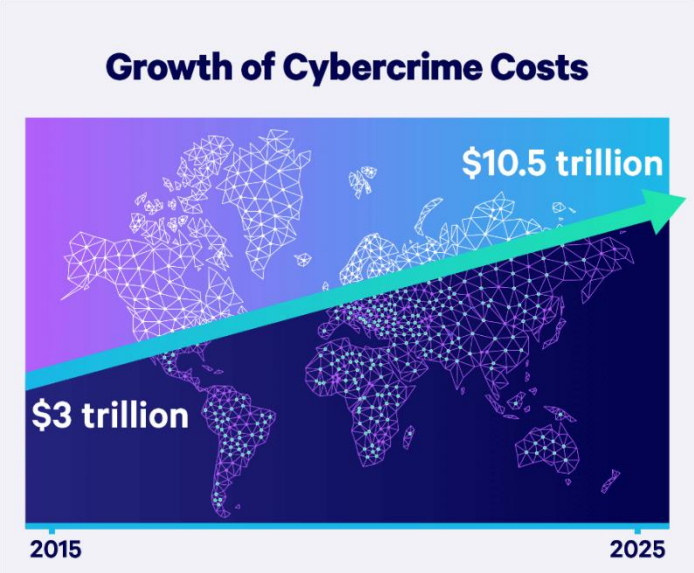


Figura 6. Growth of Cybercrime Costs. (Cybersecurity Ventures, 2021)

3.3.2.2 Impacto

Los ciberataques afectan a todas las organizaciones, particularmente a las pequeñas y medianas empresas, interrumpiendo sus operaciones y causando daños severos a sus activos de T.I. más importantes muchas veces sin la capacidad de recuperarse. Según un estudio del ciber crimen realizado por (Accenture, 2019), el 43% de los ciberataques están dirigidos a pequeñas empresas, pero solo el 14% están preparados para defenderse.

Según un reporte de ciberseguridad realizado por (Ponemon, 2019), los principales problemas que enfrentan las empresas de esta escala son los siguientes:

- Medidas de seguridad insuficientes: el 45% dice que sus procesos son ineficientes para mitigar los ataques.
- Frecuencia de los ataques: el 66% ha experimentado un ciberataque en los últimos 12 meses.
- Antecedentes de los ataques: el 69% dice que los ciberataques son cada vez más dirigidos.

3.3.3 Iniciativas de ciberseguridad en las empresas

Toda empresa que tome en serio sus objetivos de negocio tiene que invertir en ciberseguridad.

La ciberseguridad es una gran preocupación para las pequeñas y medianas empresas. Las amenazas a la seguridad cibernética se han ampliado en 2021 desde la pandemia COVID-19 y la consecuente realidad de "Trabajo remoto" que se ha creado en todo el mundo. (Cyber Management Alliance, 2021).

A continuación, se presenta algunas iniciativas que las empresas están adoptando para mantener la seguridad de sus activos:

3.3.3.1 Educación corporativa del ciber riesgo

Las empresas están capacitando periódicamente a sus empleados sobre los conceptos básicos de la ciberseguridad, también se los mantiene actualizados con todas las amenazas cibernéticas a las que se expone su empresa.

Las amenazas internas son una de las principales causas de vulnerabilidades en la actualidad, por eso cada miembro de la organización debe conocer a quien reportar un inconveniente y los procedimientos adecuados de cómo hacerlo.

Los miembros de la alta directiva establecen planes sólidos de respuesta a incidentes contra ataques cibernéticos, generalmente se trata de un documento detalla claramente las acciones que todos los empleados deben cumplir en caso de un ataque.

3.3.3.2 Inversión en seguridad

Las organizaciones se han visto en la necesidad de incorporar un software de seguridad adecuado para el funcionamiento eficiente de su empresa. Se realizan inversiones en antivirus, filtros antispam (correo basura) y antispyware (software de espionaje) y se mantienen al día con los parches y actualizaciones.

Las empresas están destinando un presupuesto para realizar copias de seguridad de los datos y administrar contraseñas por medio de un gestor de claves que, en lugar de las contraseñas normales se exige que estas sean frases o un conjunto de palabras, lo que hace que sea más difícil de descifrar.

La autenticación multifactor es otra tendencia que también es fundamental para una mayor seguridad, consiste en un doble chequeo de la identidad de una persona validando algo que el usuario sabe con algo que él tiene o es. Un ejemplo claro de esto es el uso de contraseñas y la confirmación por medio de un mensaje de texto al celular del usuario.

3.3.3.3 Encriptación de datos

Hoy en día es de vital importancia cifrar todos los datos que tenga en el espacio corporativo, esto hace que sea más difícil para los delincuentes informáticos robarlo, destruirlo o manipularlo.

Es una buena idea instalar un proxy (servidor intermediario) para cifrar sus datos. También obtienen otros beneficios. Proxy residencial, por ejemplo, proporciona anonimato en línea. Los piratas informáticos no pueden ver ni rastrear sus actividades en línea, lo que hace que sus datos sean más seguros. (Cyber Management Alliance, 2021).

En la Figura 2.4 se aprecia de mejor manera la encriptación por medio de un proxy.

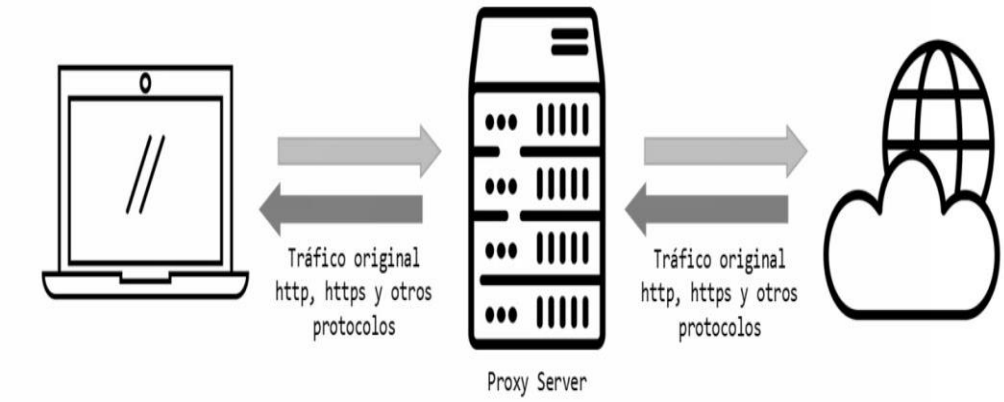


Figura 7. Funcionamiento de un proxy. (ESET, 2020)

3.3.3.4 Monitoreo de la actividad en línea

Consiste en llevar un registro de las actividades de los empleados cuando están en línea. Se debe limitar el acceso a sitios no aptos dentro del espacio laboral.

3.3.4 Situación actual de la ciberseguridad en el Ecuador y Latinoamérica

Ante la emergente necesidad de ser seguros en el ciberespacio, países de todo el mundo han empezado a incorporar la ciberseguridad como un proceso fundamental dentro de la estrategia de crecimiento de cualquier negocio.

A nivel Latinoamérica la situación no es muy diferente. “La persistente escasez de habilidades y los cambios regulatorios impulsan todavía más el continuo crecimiento del mercado de los servicios de ciberseguridad. Los factores principales para el gasto de ciberseguridad son los riesgos de ciberataques, las necesidades comerciales, los cambios en la industria y los resguardos de la privacidad de la información” (Gartner, 2018).

“En el Ecuador, dichas temáticas (ampliamente discutidas) se han focalizado en una dimensión pragmática.” (Vargas, Reyes, & Recalde, 2017).

Si bien Ecuador aún no cuenta con una estrategia de seguridad cibernética, sí ha logrado hacer avances significativos en la mejora de sus capacidades cibernéticas y en el enfrentamiento de amenazas, apoyado por el establecimiento de un grupo de trabajo para el desarrollo de la estrategia nacional de ciberseguridad. (OEA & BID, 2020)

La situación de gobierno y cumplimiento de ciberseguridad se encuentra dando sus primeros pasos en el país estableciendo políticas de seguridad de la información que este año han dado origen a la Estrategia Nacional de Ciberseguridad a la cual deberán estar alineadas ciertas empresas para reducir el aumento de los riesgos informáticos.

De acuerdo con un estudio sobre el estado de la ciberseguridad en el Ecuador realizado por (Deloitte, 2020) concluyeron que existen aspectos alentadores que reflejan un leve, pero sostenido crecimiento en la importancia que la gestión de ciberseguridad tiene en las compañías, pero existen otras realidades como la demora en la aprobación de normatividad, la restricción de recursos y la falta de entendimiento de lo que requiere una gestión efectiva de ciber-riesgos para tener una práctica madura y que sea un referente a nivel regional.

3.3.5 Panorama de amenazas cibernéticas en el Ecuador

Según el (Foro Económico Mundial, 2020), la ciberseguridad se encuentra en el top 5 de los riesgos globales por lo que se evidencia la necesidad de las empresas por incluir procesos de seguridad en sus objetivos de negocio.

En el Ecuador, las empresas cada vez son más propensas a tener una brecha de seguridad ya que el panorama de ciberamenazas es cada vez más extenso, en la Tabla 2 se mencionan las principales amenazas que pueden detonar los riesgos corporativos.

Tabla 2: Panorama de Ciber amenazas en el Ecuador

	Ciberamenazas en Ecuador	**Desviación de la clasificación según tendencias internacionales**	**Ciberamenaza 2018 de la *ENISA (European Union Agency for Cybersecurity)**
1	Suplantación de identidad	↑	Software malicioso
2	Correo no deseado	↑	Ataques basados en la web
3	Software malicioso	↓	Ataques de aplicaciones web
4	Fuga de información	↑	Suplantación de identidad
5	Amenaza interna	↑	Negación de Servicio
6	Manipulación física/daño/robo/pérdida	↑	Correo no deseado
7	Robo de identidad	↑	Redes de bots
8	Ataques de aplicaciones web	↓	Violación de datos
9	Programa de secuestro de datos	↑	Amenaza Interna
10	Negación de servicio	↓	Manipulación física/daño/robo/pérdida
11	Ataques basados en la web	↓	Fuga de información
12	Violación de datos	↓	Robo de identidad
13	Redes de bots	↓	Minería de criptomonedas maliciosa.
14	Minería de criptomonedas maliciosa	↓	Programa de secuestro de datos
15	Espionaje cibernético	→	Espionaje cibernético

Tabla 2. Nota: Las flechas ↑ y ↓ representan el aumento o disminución de la posición de las amenazas indicando de inicio a fin las más comunes con respecto al año 2018.

CAPÍTULO III

4. MODELO DE NEGOCIO

Con el fin de proponer un modelo de negocio para la prestación de servicios de ciberseguridad, este capítulo fue desarrollado como producto de la revisión de la literatura de la siguiente lista de autores:

- Lecciones en Estrategia, Hacia una gestión de excelencia. (Arnoldo Hax, 2018).
- How to Write a Cybersecurity Business Plan. (Martins, 2021).
- Startup Myths and Models. (Virk, 2020).
- Business Knowledge Blueprints. (Ross, 2020).

4.1 Estudio de los requerimientos de mercado

Para realizar un análisis objetivo de los requerimientos en ciberseguridad que requiere el mercado ecuatoriano es necesario conocer las necesidades de los clientes que pertenecen a distintas industrias para lo cual es necesario ciertas consideraciones que ayudarán a definir mejor los potenciales nichos de mercado.

- **Segmentación:** Como primer paso se debe desglosar el mercado en grupos más pequeños, de modo que se pueda trabajar de mejor manera con la información, es importante que el grupo de segmentación cumpla con algunos requisitos:
    - Ser definibles (que tengan características similares),
    - Ser alcanzables (que pertenezcan al mercado),
    - Ser homogéneos (que sus componentes no sean demasiado diversos entre sí)
    - Ser rentables (que sean considerados como posibles clientes para el negocio).

  Una vez realizado este proceso, se obtienen segmentos de mercado los cuales después de un proceso de análisis pueden convertirse en nichos de mercado donde el modelo de negocio propuesto puede ingresar a competir y obtener resultados rentables.
- **Objetivo:** El segundo paso del análisis consiste en definir cuáles son los segmentos objetivos, sus características y el cómo son las personas que componen estos grupos, tener un entendimiento más profundo de los objetivos nos ayuda significativamente para orientar los servicios a satisfacer sus necesidades.
- **Posicionamiento:** El tercer paso consiste en planificar el posicionamiento de los servicios en los nichos de mercado identificados. El objetivo primordial del modelo de negocio que se propone no solo es comercializar servicios, sino hacerlo a través de los canales más adecuados para alcanzar al cliente final adecuado y de manera eficaz y eficiente.

  Es importante mencionar que con el posicionamiento no sólo se obtiene mayor beneficio económico, sino que también permite mantenerse competitivo en el mercado a mediano y largo plazo.

4.1.1 Metodología

Para el desarrollo de la propuesta metodológica para la implementación de un modelo de negocio para la prestación de servicios estratégicos de ciberseguridad se utilizó la metodología investigativa ya que brinda una búsqueda sistemática partiendo del planteamiento del problema y estableciendo hipótesis y objetivos claros para evitar dejar hechos a la casualidad, dentro de esta metodología se utilizó el siguiente tipo de investigación:

Investigación de laboratorio o experimental:

Se ocupa de la orientación dirigida a los cambios y desarrollos, tanto de la esfera de las ciencias naturales como de las sociales. El control adecuado es el factor esencial del método utilizado. Esta investigación se presenta mediante la manipulación de variables no comprobada referentes al grado de aceptación en el mercado, los tiempos y costos de implementación de cada servicio propuesto que conforman el proceso de implementación de un modelo de negocio que ofrece servicios de ciberseguridad, en condiciones rigurosamente controladas, con el fin de escribir de qué modo y por qué causa se produce una situación o acontecimiento particular. Este tipo de investigación presenta las siguientes etapas:

- Presencia de un problema para el cual sea realizada una revisión bibliográfica.
- Identificación y definición del problema.
- Definición de hipótesis y variables para el tratamiento de estas.
- Diseño del plan experimental.
- Prueba de confiabilidad de los datos.
- Realización del experimento.
- Tratamiento de datos.

4.1.2 Encuestas y Entrevistas

Para poder identificar aquellos servicios que tienen mayor aceptación en el mercado, es necesario un método de recolección de datos para poder relacionarla y obtener información valiosa.

La encuesta se define como el proceso de interrogar a un determinado grupo de personas para obtener datos sobre un servicio, esta información refleja las opiniones, comportamiento o conocimiento de la muestra seleccionada. Los tipos más comunes de encuestas son: cuestionarios escritos, entrevistas personales o telefónicas, grupos focales y encuestas en línea.

Las encuestas son una valiosa herramienta de recopilación y análisis de datos que se utilizan comúnmente con clientes y empleados, para descubrir necesidades o evaluar la satisfacción.

El objetivo de las encuestas realizadas es conocer y priorizar aquellos servicios en el área de ciberseguridad categorizados en 3 dominios (Prevención, Detección y Respuesta) que aplican a los principales nichos de mercado en el Ecuador, para cumplir con este objetivo las encuestas serán dirigidas a gerentes de sistemas y profesionales de T.I. de distintas empresas.

Según un reporte de estudios sectoriales de la (Superintendencia de Compañías, Valores y Seguros del Ecuador, 2021) y de acuerdo con una publicación de (BuenTrip Hub, 2020) se establece que a la fecha en el Ecuador existen aproximadamente 300 empresas públicas y privadas que brindan servicios informáticos, para lo cual se tomó este valor como la población total para definir el tamaño de muestra poblacional del presente estudio.

La fórmula aplicada fue la propuesta por (Larry, 2005):

$$n = \frac{\mathrm{N} * Z^2 * \mathrm{p} * \mathrm{q}}{e^2 * (N-1) + Z^2 * \mathrm{p} * \mathrm{q}}$$

En donde:

n = es el tamaño de la muestra poblacional a obtener.

N = es el tamaño de la población total.

p y q = representan la desviación estándar de la población. En caso de desconocer este dato es común utilizar un valor constante que equivale a 0.5.

Z = es el valor obtenido mediante niveles de confianza. Su valor es una constante, por lo general se tienen dos valores dependiendo el grado de confianza que se desee siendo 99% el valor más alto (este valor equivale a 2.58) y 90% (1.645) el valor mínimo aceptado para considerar la investigación como confiable.

e = representa el límite aceptable de error muestral, generalmente va del 1% (0.01) al 9% (0.09), siendo 5% (0.5) el valor estándar usado en las investigaciones.

Parámetro	Valor Establecido
N	300
Z	1.645
P	50.00%
Q	50.00%
e	8.20%

Tamaño de muestra "n" =
75.53

Tabla 3. Cálculo de muestra poblacional

Una vez establecido los valores adecuados, se procede a realizar la sustitución de los valores y aplicación de la fórmula para obtener el tamaño de la muestra poblacional correspondiente al universo finito determinado.

Ya realizado el proceso matemático, se obtendrá la muestra, la cual como se mencionó al principio, nos ayudará a realizar una investigación válida y completa.

4.1.3 Identificación y análisis de los servicios.

Para el análisis de las encuestas realizadas y en base a la metodología planteada, se ha decidido relacionar los datos de las variables obtenidas en base a dos bloques de análisis y a las respuestas obtenidas en 77 encuestas realizadas.

Para el primer bloque se utilizó la escala de Likert para analizar la importancia que le asignaron las personas encuestadas a cada servicio de ciberseguridad propuesto.

Para el análisis del segundo bloque se realizaron tablas de contingencia lo cual ayudó a relacionar las variables categóricas correspondientes a: la disposición a implementar los servicios y los rangos de precios y tiempos de implementación propuestos para poder así determinar qué servicios de ciberseguridad tienen mayor aceptación. Cabe mencionar que este tipo de método estadístico viene acompañado de una medida de asociación “Chi cuadrado” y la “V de Cramer” los cuales respaldan la fiabilidad del análisis.

A continuación, se describen los métodos mencionados:

Escala de Likert sobre la importancia de un factor

La Escala de Likert es una escala de calificación que nos permite medir actitudes, reacciones y comportamientos de las personas, este método estadístico relaciona variables categóricas generalmente vinculadas con el nivel de acuerdo, grado de importancia o frecuencia de una actividad.

La escala de Likert es un tipo de medición utilizado principalmente en la investigación de mercados para la comprensión del grado de importancia y la posible aceptación de un producto o servicio en el mercado. (Muguira, ¿Qué es la escala de Likert y cómo utilizarla?, 2020).

Esta escala requiere un grupo de posibles respuestas de 5, 7 y hasta 9 elementos donde siempre debe existir una opción neutral.

Para el presente caso de estudio, se ha optado por utilizar escalas de importancia categorizadas en cinco posibles respuestas (Muy importante, Importante, Moderadamente Importante, Poco Importante o Nada Importancia).

(Muguira, ¿Qué es la escala de Likert y cómo utilizarla?, 2020) define las siguientes ventajas al utilizar este método estadístico:

- Es una escala de fácil aplicación y diseño.
- Puede utilizar ítems que no tienen relación con la expresión.
- Ofrece una graduación de la opinión de las personas encuestadas.
- Produce mediciones de calidad (precisas y que minimizan el error de medición)
- Permite realizar los análisis necesarios para alcanzar los objetivos de la investigación.
- Se pueden hacer comparaciones con evaluaciones anteriores del servicio o con servicios similares (benchmarking).
- Muy sencilla de contestar.
- A diferencia de una simple pregunta de “sí” / “no”, la escala de Likert permite a los encuestados calificar sus respuestas.

Tablas de Contingencia

Las tablas de contingencia son herramientas de análisis estadístico que consisten en relacionar filas y columnas de datos en términos de conteos de frecuencia con el objetivo de representar en un resumen la relación entre diferentes variables categóricas.

Esta herramienta ha sido uno de los pilares para la industria de la investigación de mercados ya que al analizar relaciones entre variables permite realizar un estudio de mercado efectivo, examinando la información recopilada en encuestas.

La información sin procesar puede ser difícil de interpretar. Incluso para pequeños conjuntos de datos, es demasiado fácil obtener resultados incorrectos con solo mirar los datos. La tabla ofrece un método simple de agrupar variables, que minimiza el potencial de confusión o error al proporcionar resultados claros (Muguira, 2020).

(Muguira, 2020) define las siguientes ventajas al utilizar este método estadístico:

- Facilita la lectura de los datos recolectados, ya que permite agruparlos cuando aún se encuentran sin procesar, lo que disminuye el margen de error al realizar un informe de investigación.
- Gracias a la tabla de contingencia es posible realizar gráficas que permitan visualizar la información fácilmente para su comprensión.
- A diferencia de otros métodos estadísticos de análisis de datos, la tabla de contingencia permite ahorrar tiempo durante la correlación de variables.
- Las tablas ofrecen resultados claros y precisos que permiten tomar mejores decisiones y crear estrategias basadas en datos.

Estadística Chi Cuadrado

(Stine & Foster, 2018) definen lo siguiente con respecto al Chi Cuadrado:

- Es una medida de asociación en una tabla de contingencia.
- Calculado sobre la base de una comparación de la contingencia observada a una tabla artificial con los mismos totales marginales.
- Cuanto mayor sea el chi-cuadrado, mayor será la cantidad de asociación.

V de Cramer

(Stine & Foster, 2018) definen lo siguiente con respecto a la V de Cramer:

- La estadística Chi Cuadrado es difícil de interpretar.
- La V de Cramer es una medida de asociación más interpretable. Se deriva de la estadística Chi Cuadrado
- V de Cramer varía en valores desde 0 (las variables no están asociadas) a 1 (las variables están perfectamente asociadas)

Análisis y resultados del Bloque 1:

El objetivo de este bloque de análisis fue el identificar aquellos servicios que presentan un mayor grado de importancia, lo cual complementa la selección de los servicios con mayor aceptación en el mercado para ser incluidos y desarrollados en el catálogo de servicios propuesto.

Para realizar el análisis se asignaron valores de medición a cada una de las opciones de grado de importancia de los servicios como se describe en la Tabla 4.

Tabla 4: Tabulación del grado de importancia de los servicios

	Grado de Importancia	Nivel
1	Muy Importante	5
2	Importante	4
3	Moderadamente Importante	3
4	Poco Importante	2
5	Nada Importante	1

Tabla 4. Nota: La tabulación incluye el valor 3 como el punto neutro de selección lo cual mejora el análisis de las encuestas.

Adicionalmente, se estableció como umbral de aceptación aquellos servicios que obtuvieron un valor promedio de importancia mayor a cuatro, lo cual hace referencia a todos los elementos con un grado de importancia mayor o igual a “Importante”.

Los resultados indican que aquellos servicios con un mayor nivel de importancia fueron los siguientes:

Tabla 5: Servicios con Mayor Nivel de Importancia

	Servicio	Puntaje
1	Gestión Estratégica de un CISO como servicio	4.18
2	Gestión de accesos y contraseñas	4.29
3	Mitigación de Ataques	4.30
4	Evaluaciones de Seguridad de la Información	4.09
5	Capacitación en Ciberseguridad	4.12
6	Seguridad Endpoint	4.05
7	Sistema de Monitoreo de Amenazas	4.08

Tabla 5. Nota: El criterio de selección del grado de importancia fue aquellos servicios con un puntaje mayor o igual a 4.

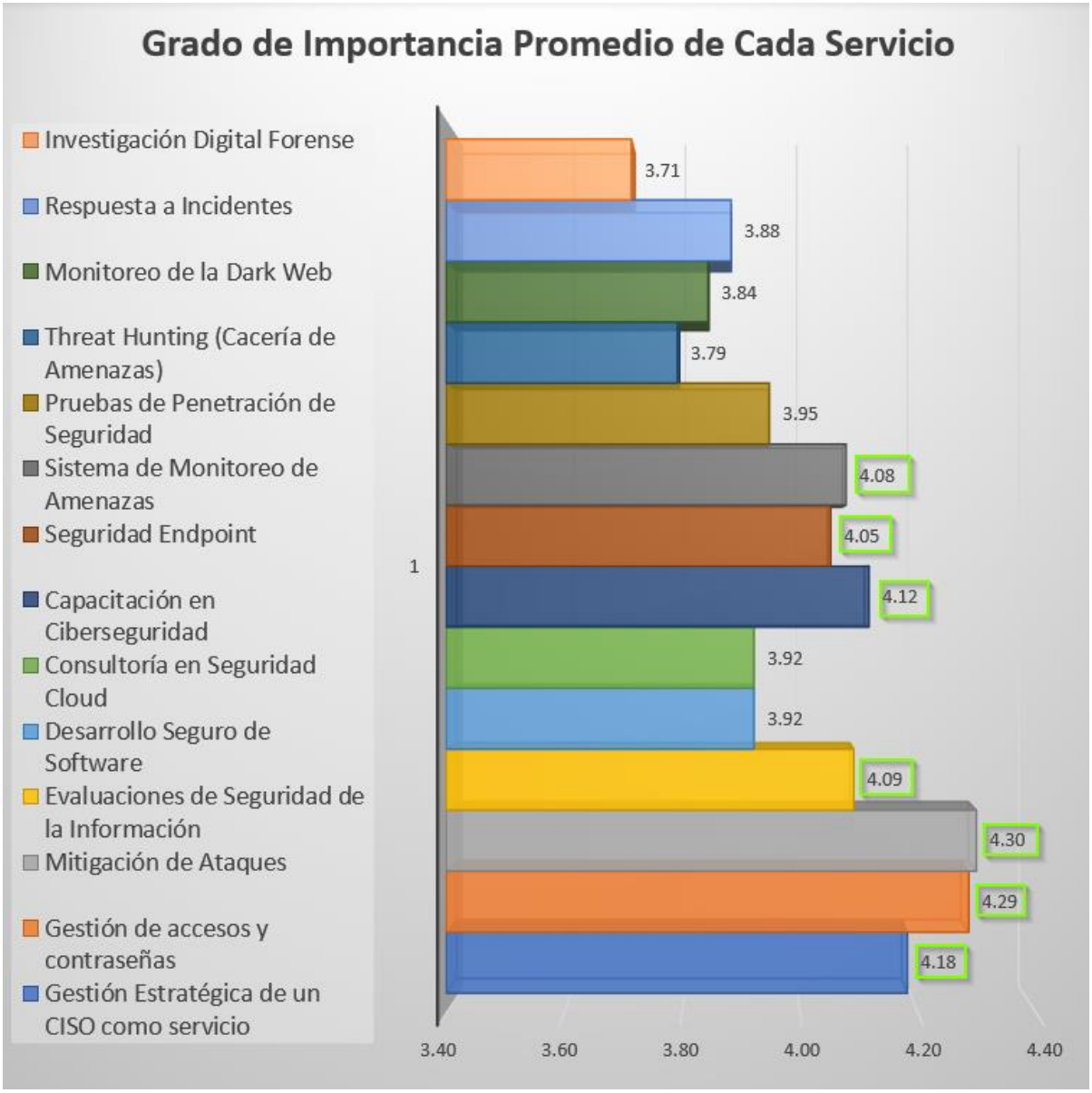


Figura 8. Grado de importancia Promedio de Cada Servicio de Ciberseguridad. Nota: Se evidencia que, en promedio, los servicios catalogados como más importantes son: Gestión Estratégica de un CISO como servicio, Gestión de accesos y contraseñas, Mitigación de Ataques, Evaluación de Seguridad de la información, Capacitación en Ciberseguridad, Seguridad Endpoint y Sistema de Monitoreo de Amenazas.

A continuación, se presenta el porcentaje del grado de importancia general e individual que se obtuvo de los servicios de ciberseguridad propuestos en las encuestas.



Figura 9. Grado de importancia General de los Servicios de Ciberseguridad. Nota: Generalmente, más del 70% de los encuestados estuvo de acuerdo en que los servicios de ciberseguridad tienen un alto grado de importancia.



Figura 10.Porcentajes del grado de Importancia del servicio Gestión Estratégica de un CISO como servicio. Nota: Se evidencia que la opción predominante es la de Muy Importante con un porcentaje de 42.86%, más del 70% de los encuestados lo considera mayor o igual a importante.

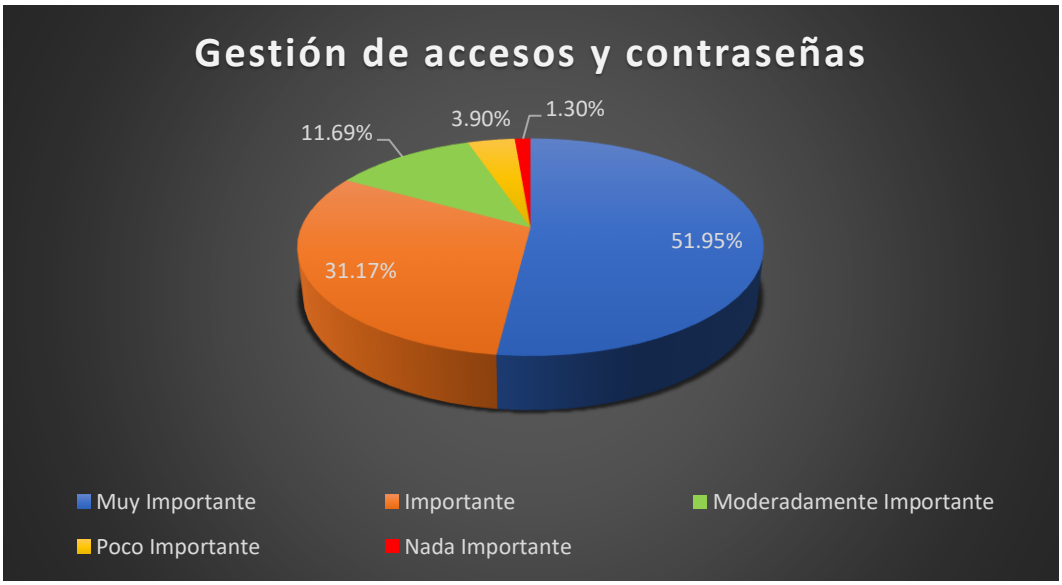


Figura 11. Porcentajes del grado de Importancia del servicio Gestión de accesos y contraseñas. Nota: Se evidencia que la opción predominante es la de Muy Importante con un porcentaje de 51.95%, más del 80% de los encuestados lo considera mayor o igual a importante.

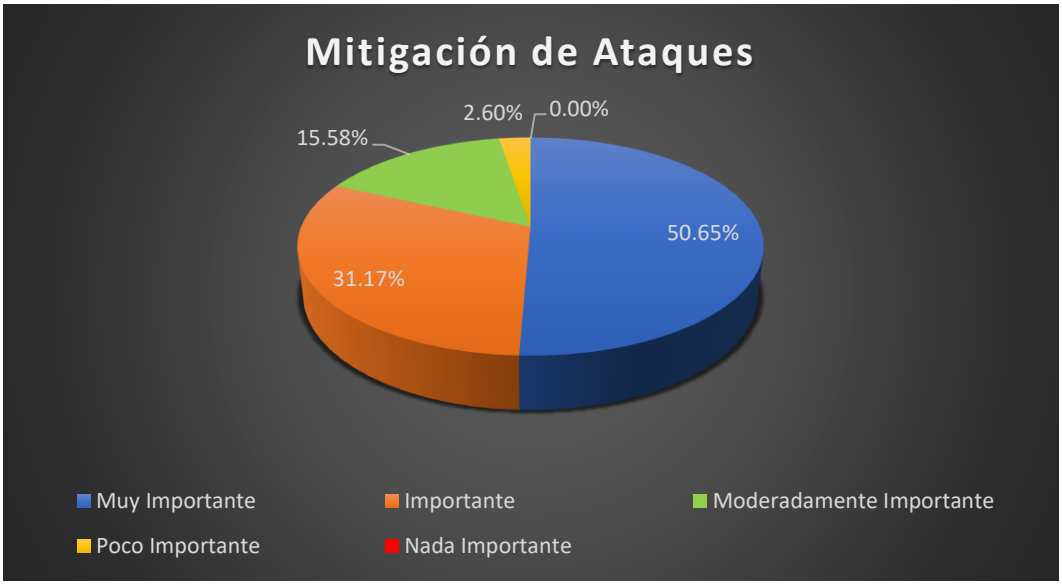


Figura 12. Porcentajes del grado de Importancia del servicio Mitigación de Ataques. Nota: Se evidencia que la opción predominante es la de Muy Importante con un porcentaje de 50.65%, más del 80% de los encuestados lo considera mayor o igual a importante.

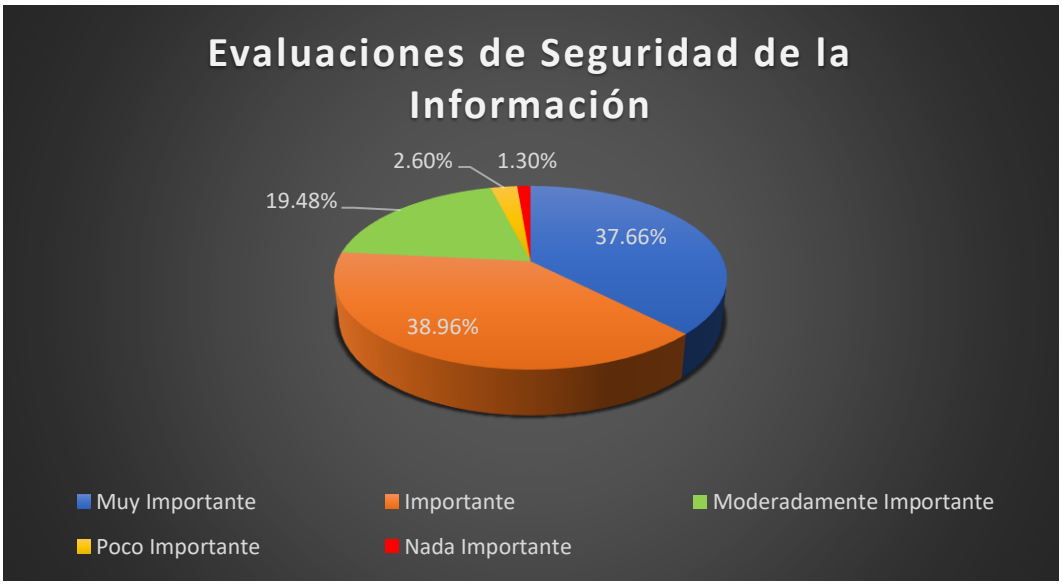


Figura 13. Porcentajes del grado de Importancia del servicio Evaluación de Seguridad de la Información. Nota: Se evidencia que la opción predominante es la de Importante con un porcentaje de 38.96%, más del 75% de los encuestados lo considera mayor o igual a importante.

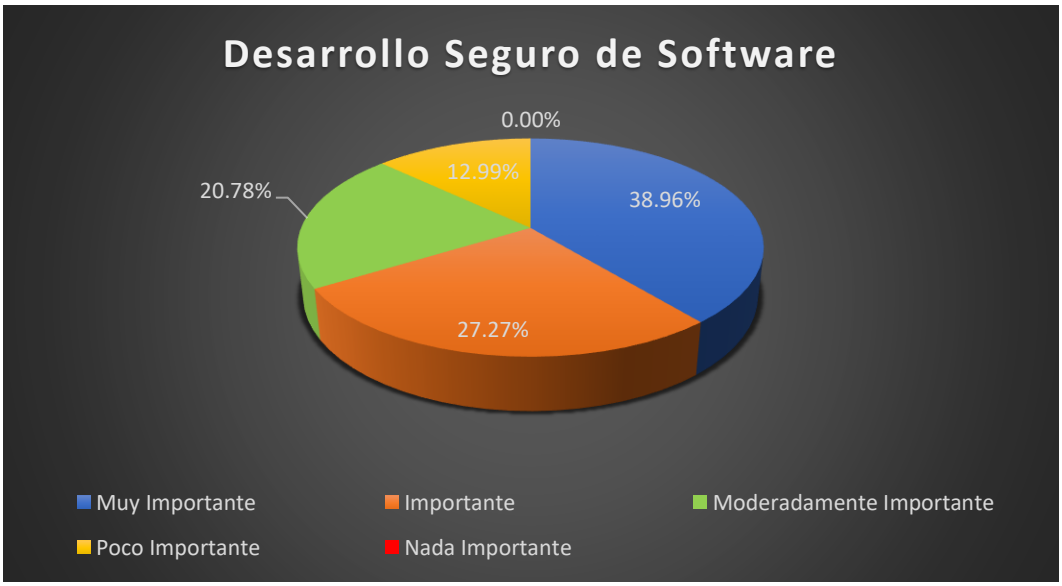


Figura 14.Porcentajes del grado de Importancia del servicio Desarrollo Seguro de Software. Nota: Se evidencia que la opción predominante es la de Muy Importante con un porcentaje de 38.96%, más del 65% de los encuestados lo considera mayor o igual a importante.

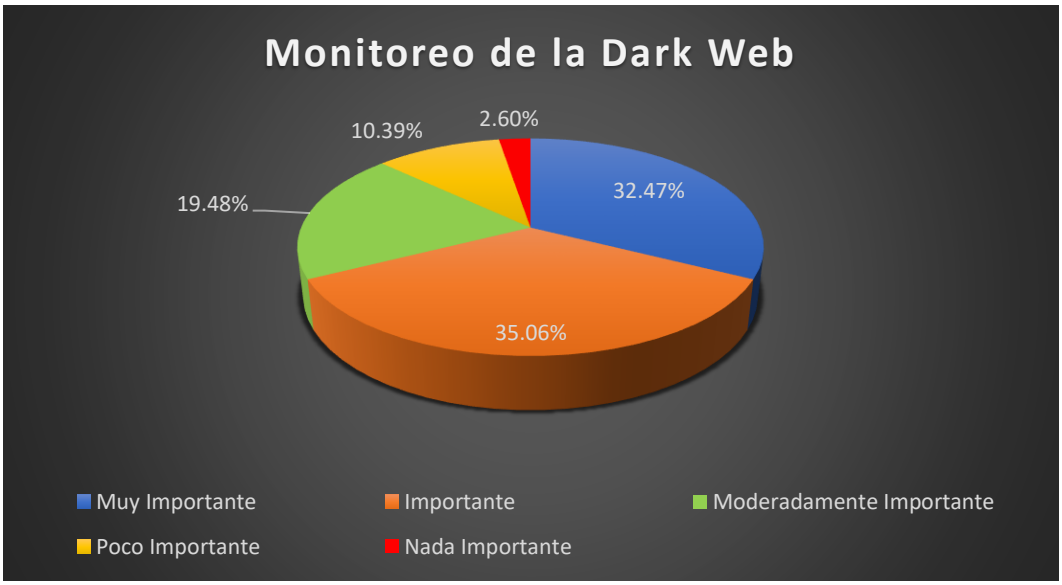


Figura 15. Porcentajes del grado de Importancia del servicio Monitoreo de la Dark Web. Nota: Se evidencia que la opción predominante es la de Importante con un porcentaje de 35.06%, más del 65% de los encuestados lo considera mayor o igual a importante.

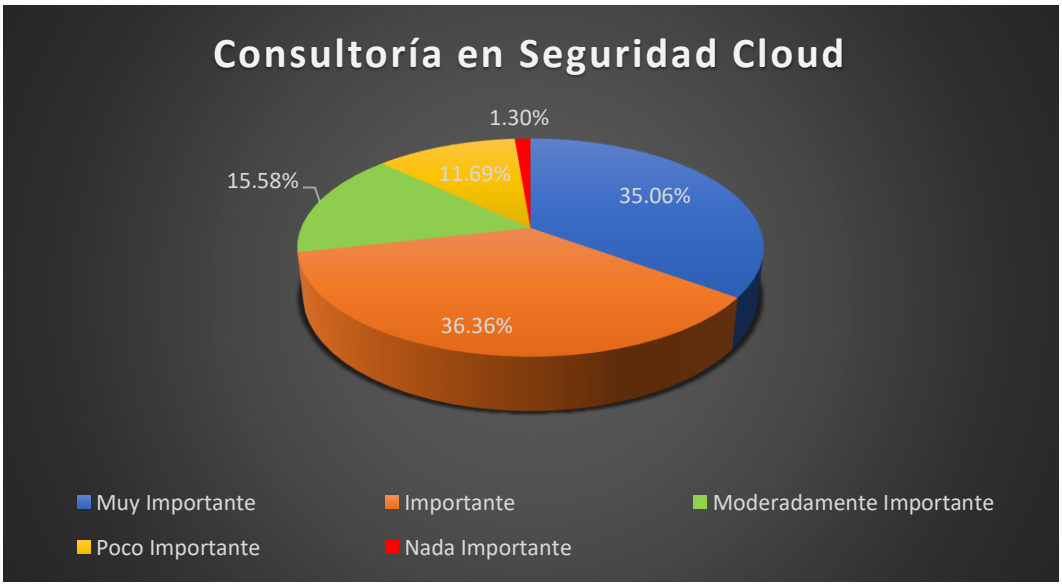


Figura 16. Porcentaje del grado de importancia del servicio Consultoría en Seguridad Cloud. Nota: Se evidencia que la opción predominante es la de Importante con un porcentaje de 36.36%, más del 70% de los encuestados lo considera mayor o igual a importante.

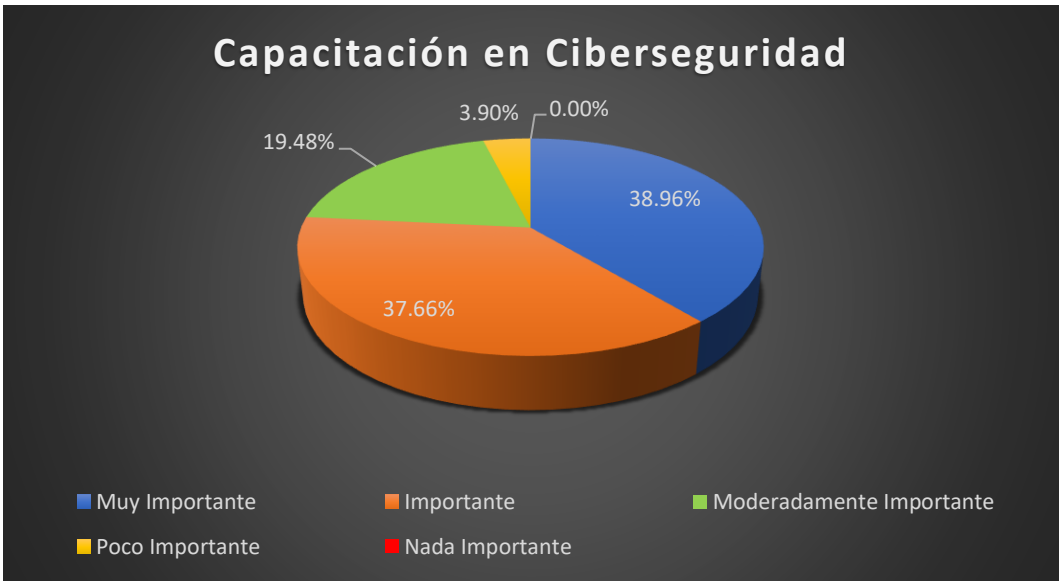


Figura 17. Porcentajes del grado de Importancia del servicio Capacitación en Ciberseguridad. Nota: Se evidencia que la opción predominante es la de Muy Importante con un porcentaje de 38.96%, más del 75% de los encuestados lo considera mayor o igual a importante.

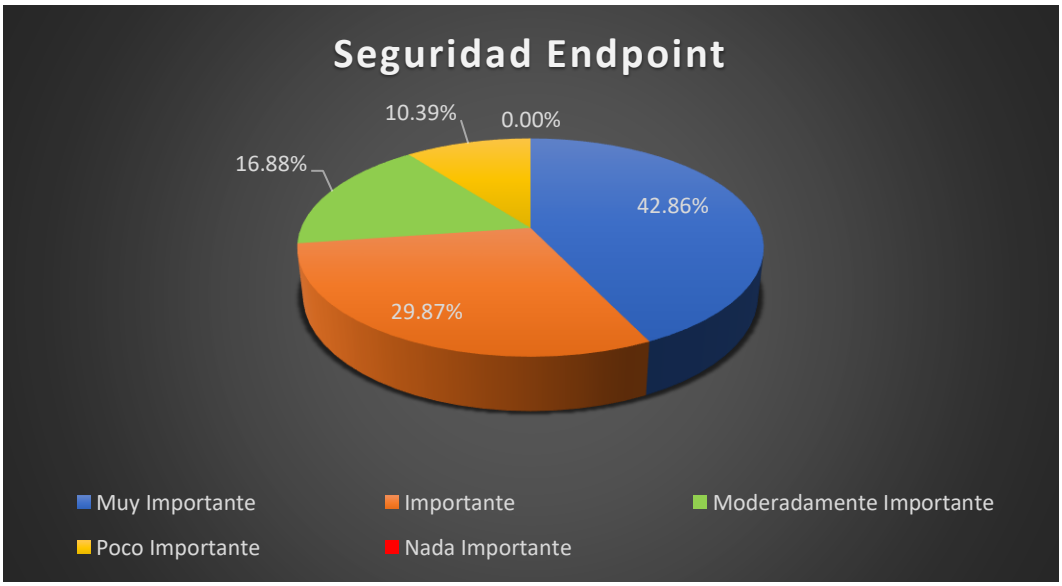


Figura 18. Porcentajes del grado de Importancia del servicio Seguridad Endpoint. Nota: Se evidencia que la opción predominante es la de Muy Importante con un porcentaje de 42.86%, más del 70% de los encuestados lo considera mayor o igual a importante.

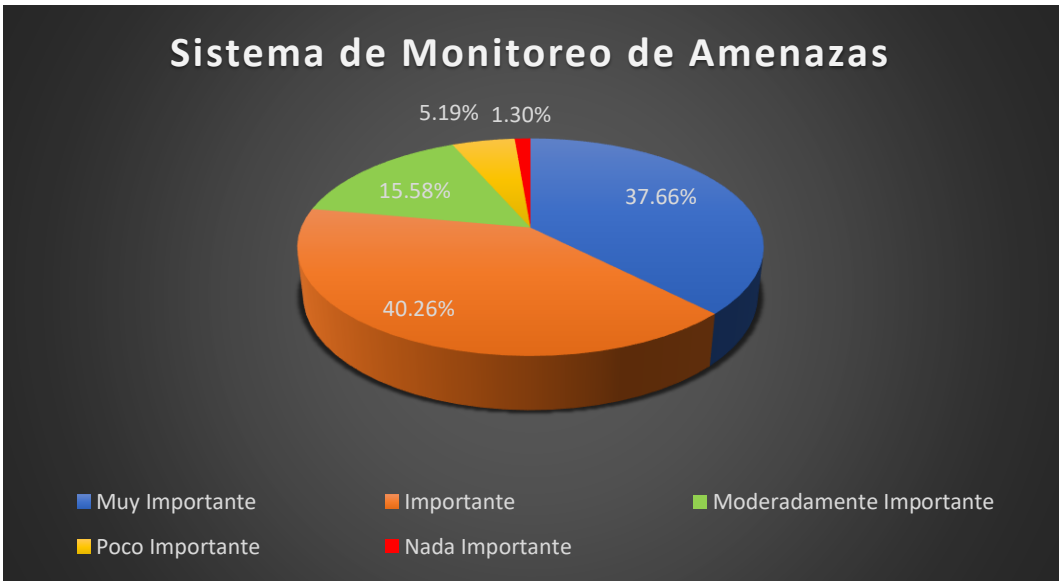


Figura 19. Porcentajes del grado de Importancia del servicio Sistema de Monitoreo de Amenazas. Nota: Se evidencia que la opción predominante es la de Importante con un porcentaje de 40.26%, más del 75% de los encuestados lo considera mayor o igual a importante.

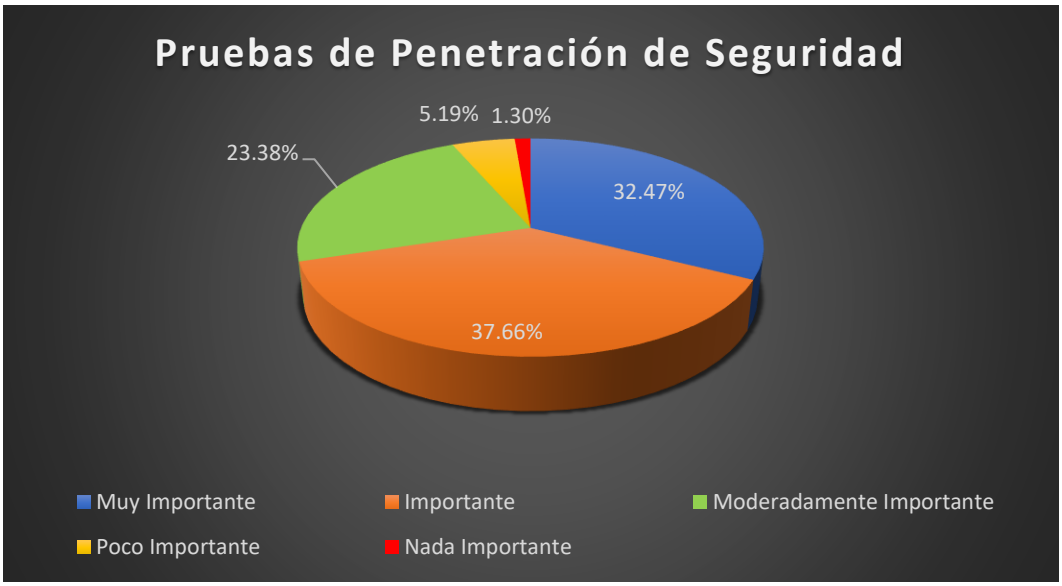


Figura 20. Porcentaje de grado de importancia del servicio Pruebas de Penetración de Seguridad. Nota: Se evidencia que la opción predominante es la de Importante con un porcentaje de 37.66%, más del 65% de los encuestados lo considera mayor o igual a importante.

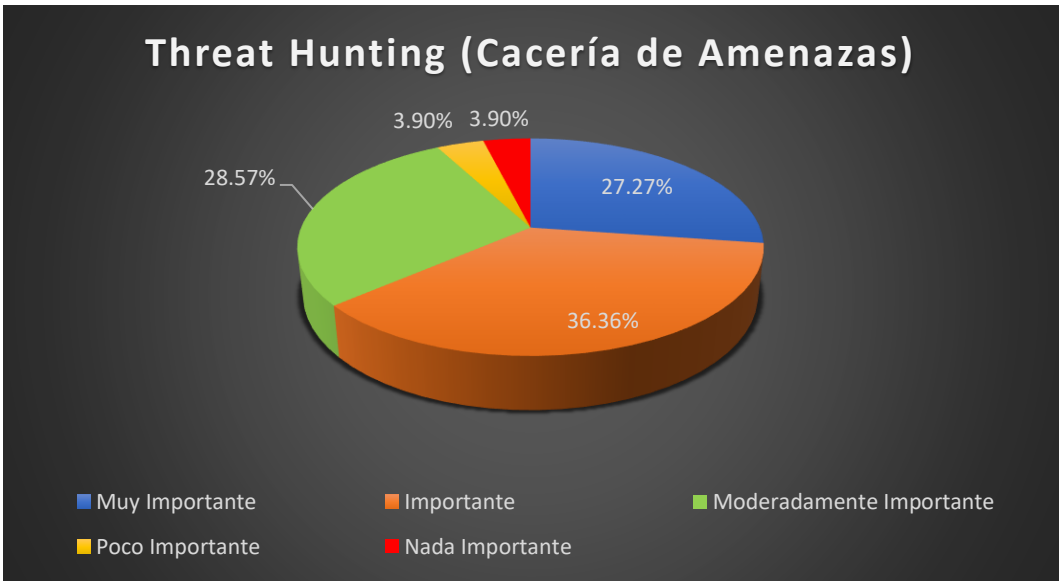


Figura 21. Porcentajes del grado de Importancia del servicio Threat Hunting (Cacería de Amenazas). Nota: Se evidencia que la opción predominante es la de Importante con un porcentaje de 36.36%, más del 60% de los encuestados lo considera mayor o igual a importante.



Figura 22. Porcentajes del grado de Importancia del servicio Investigación Digital Forense. Nota: Se evidencia que la opción predominante es la de Importante con un porcentaje de 33.77%, más del 60% de los encuestados lo considera mayor o igual a importante.



Figura 23. Porcentajes del grado de Importancia del servicio Respuesta a Incidentes. Nota: Se evidencia que la opción predominante es la de Importante con un porcentaje de 31.17%, más del 60% de los encuestados lo considera mayor o igual a importante.

Análisis y resultados del Bloque 2:

El objetivo de este bloque de análisis fue el identificar los tiempos de implementación y precios que el mercado está dispuesto a pagar para cada uno de los servicios de ciberseguridad propuestos en las encuestas. El análisis se realizó por medio de tablas de contingencia que reflejan la relación entre las siguientes variables categóricas:

- Disposición a implementar el servicio.
- Rango de tiempo de implementación y precio.

Para poder complementar la selección de aquellos servicios que son más rentables incorporar en el catálogo se midió el grado de asociación de las variables categóricas por medio de la Prueba Chi Cuadrado y la V de Cramer lo cual refleja la efectividad de la asociación propuesta.

A continuación, se presenta el análisis individual de las tablas de contingencia realizadas.

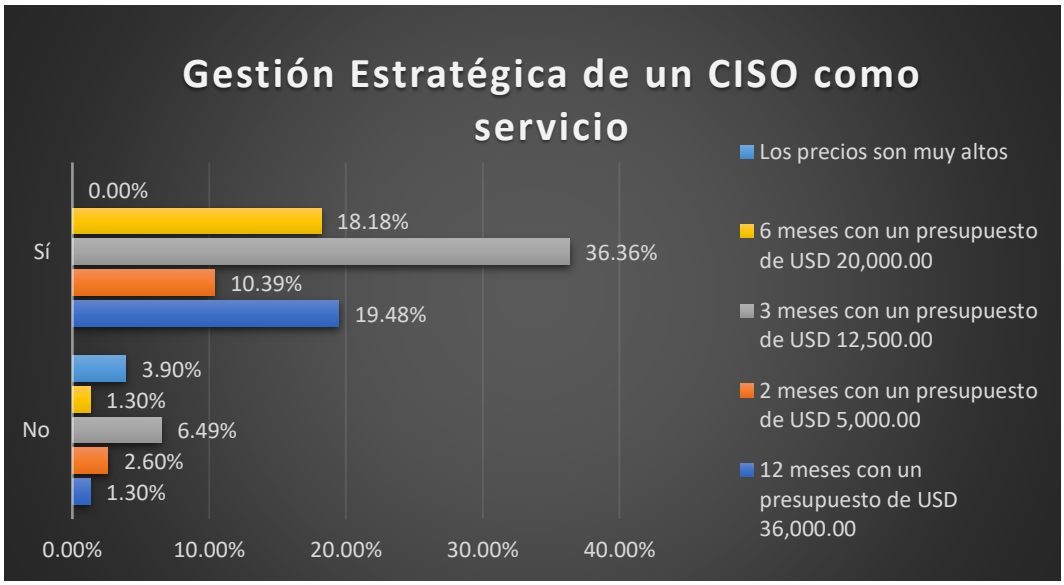


Figura 24. Porcentajes de rango de tiempo de implementación y precio de Gestión estratégica de un CISO como servicio. Nota: Se evidencia que la opción predominante es la de Sí implementaría el servicio con 3 meses de tiempo de implementación y un presupuesto de USD 12,500 con un porcentaje de 36.36%.

Datos Reales

Gestión Estratégica de un CISO como servicio	Rango de tiempo de implementación y costo estimado					
Implementación	**12 meses con un presupuesto de USD 36,000.00**	**2 meses con un presupuesto de USD 5,000.00**	**3 meses con un presupuesto de USD 12,500.00**	**6 meses con un presupuesto de USD 20,000.00**	**Los precios son muy altos**	**TOTAL**
No	1	2	5	1	3	12
Sí	15	8	28	14		65
TOTAL	**16**	**10**	**33**	**15**	**3**	**77**

Tabla 6. Datos reales de la tabla de contingencia del servicio Gestión estratégica de un CISO como servicio. Nota: Estos valores representan los números obtenidos en las encuestas realizadas.

Datos Esperados

Gestión Estratégica de un CISO como servicio	Rango de tiempo de implementación y costo estimado					
Implementación	**12 meses con un presupuesto de USD 36,000.00**	**2 meses con un presupuesto de USD 5,000.00**	**3 meses con un presupuesto de USD 12,500.00**	**6 meses con un presupuesto de USD 20,000.00**	**Los precios son muy altos**	**TOTAL**
No	2	2	5	2	0	12
Sí	14	8	28	13	3	65
TOTAL	**16**	**10**	**33**	**15**	**3**	**77**

Tabla 7. Datos esperados de la tabla de contingencia del servicio Gestión estratégica de un CISO como servicio. Nota: Estos valores representan los números que esperaríamos obtener en nuestro conjunto de datos basados en tablas de contingencia. Más detalle del análisis en la sección 4.1.4.

Prueba Chi Cuadrado: 18.37 **V de Cramer:** 0.49

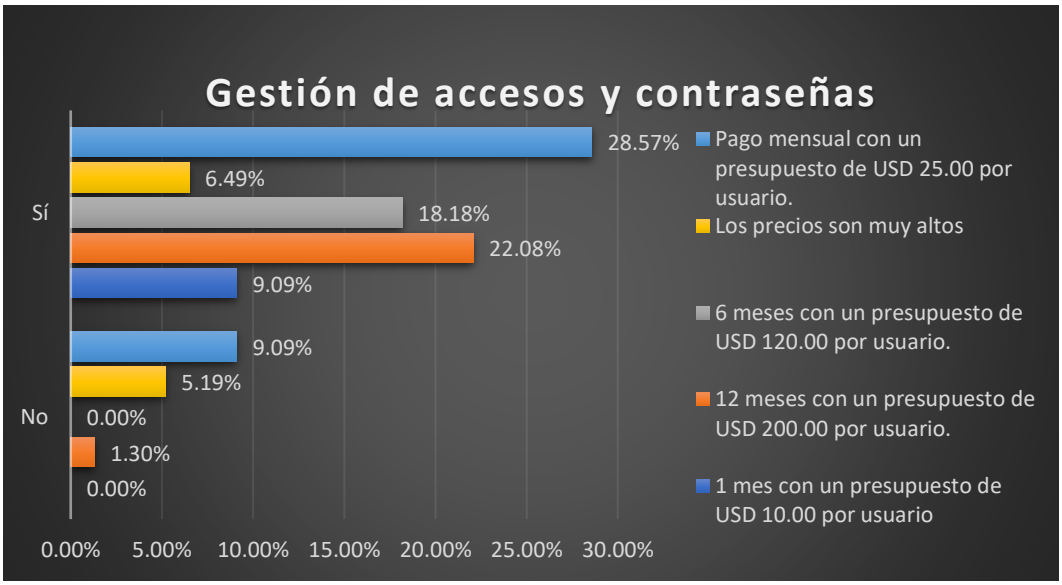


Figura 25. Porcentajes de rango de tiempo de implementación y precio de Gestión de accesos y contraseñas. Nota: Se evidencia que la opción predominante es la de Sí implementaría el servicio con 1 mes de tiempo de implementación y un presupuesto de USD 25 por usuario con un porcentaje de 28.57%.

Datos Reales

Gestión de accesos y contraseñas	Rango de tiempo de implementación y costo estimado					
Implementación	**1 mes con un presupuesto de USD 10.00 por usuario**	**12 meses con un presupuesto de USD 200.00 por usuario.**	**6 meses con un presupuesto de USD 120.00 por usuario.**	**Los precios son muy altos**	**Pago mensual con un presupuesto de USD 25.00 por usuario.**	**TOTAL**
No		1		4	7	12
Sí	7	17	14	5	22	65
TOTAL	**7**	**18**	**14**	**9**	**29**	**77**

Tabla 8. Datos reales de la tabla de contingencia del servicio Gestión de accesos y contraseñas. Nota: Estos valores representan los números obtenidos en las encuestas realizadas.

Datos Esperados

Gestión de accesos y contraseñas	Rango de tiempo de implementación y costo estimado					
Implementación	**1 mes con un presupuesto de USD 10.00 por usuario**	**12 meses con un presupuesto de USD 200.00 por usuario.**	**6 meses con un presupuesto de USD 120.00 por usuario.**	**Los precios son muy altos**	**Pago mensual con un presupuesto de USD 25.00 por usuario.**	**TOTAL**
No	1	3	2	1	5	12
Sí	6	15	12	8	24	65
TOTAL	**7**	**18**	**14**	**9**	**29**	**77**

Tabla 9. Datos esperados de la tabla de contingencia del servicio Gestión de accesos y contraseñas. Nota: Estos valores representan los números que esperaríamos obtener en nuestro conjunto de datos basados en tablas de contingencia. Más detalle del análisis en la sección 4.1.4.

Prueba Chi Cuadrado: 12.56 **V de Cramer:** 0.40

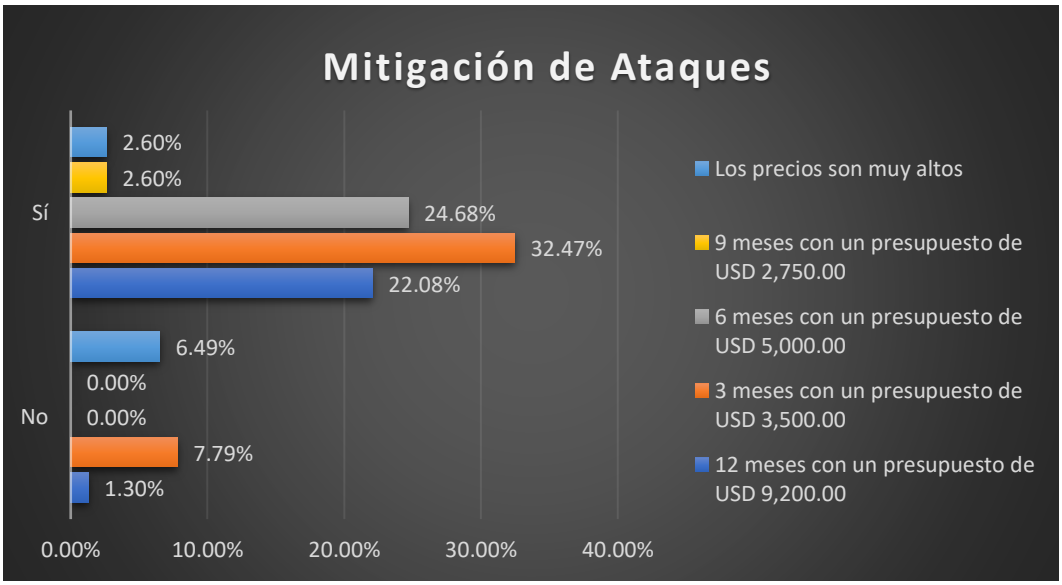


Figura 26. Porcentajes de rango de tiempo de implementación y precio de Mitigación de Ataques. Nota: Se evidencia que la opción predominante es la de Sí implementaría el servicio con 3 meses de tiempo de implementación y un presupuesto de USD 3,500 con un porcentaje de 32.47%.

Datos Reales

Mitigación de Ataques	Rango de tiempo de implementación y costo estimado					
Implementación	**12 meses con un presupuesto de USD 9,200.00**	**3 meses con un presupuesto de USD 3,500.00**	**6 meses con un presupuesto de USD 5,000.00**	**9 meses con un presupuesto de USD 2,750.00**	**Los precios son muy altos**	**TOTAL**
No	1	6			5	12
Sí	17	25	19	2	2	65
TOTAL	**18**	**31**	**19**	**2**	**7**	**77**

Tabla 10. Datos reales de la tabla de contingencia del servicio Mitigación de Ataques. Nota: Estos valores representan los números obtenidos en las encuestas realizadas.

Datos Esperados

Mitigación de Ataques	Rango de tiempo de implementación y costo estimado					
Implementación	**12 meses con un presupuesto de USD 9,200.00**	**3 meses con un presupuesto de USD 3,500.00**	**6 meses con un presupuesto de USD 5,000.00**	**9 meses con un presupuesto de USD 2,750.00**	**Los precios son muy altos**	**TOTAL**
No	3	5	3	0	1	12
Sí	15	26	16	2	6	65
TOTAL	**18**	**31**	**19**	**2**	**7**	**77**

Tabla 11. Datos esperados de la tabla de contingencia del servicio Mitigación de Ataques. Nota: Estos valores representan los números que esperaríamos obtener en nuestro conjunto de datos basados en tablas de contingencia. Más detalle del análisis en la sección 4.1.4.

Prueba Chi Cuadrado: 22.18 **V de Cramer:** 0.54

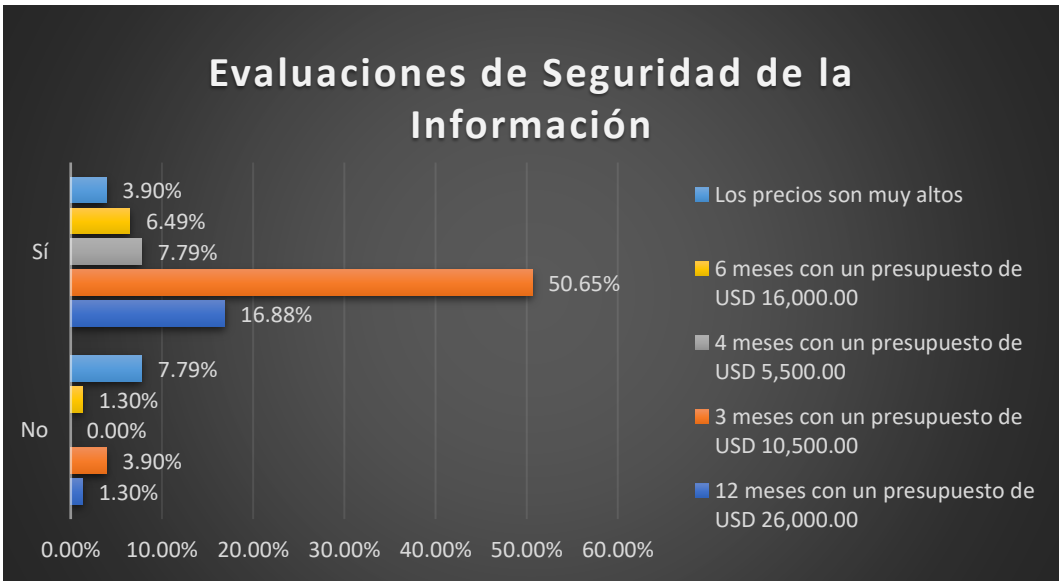


Figura 27. Porcentajes de rango de tiempo de implementación y precio de Evaluación de Seguridad de la Información. Nota: Se evidencia que la opción predominante es la de Sí implementaría el servicio con 3 meses de tiempo de implementación y un presupuesto de USD 10,500 con un porcentaje de 50.65%.

Datos Reales

Evaluaciones de Seguridad de la Información	Rango de tiempo de implementación y costo estimado					
Implementación	**12 meses con un presupuesto de USD 26,000.00**	**3 meses con un presupuesto de USD 10,500.00**	**4 meses con un presupuesto de USD 5,500.00**	**6 meses con un presupuesto de USD 16,000.00**	**Los precios son muy altos**	**TOTAL**
No	1	3		1	6	11
Sí	13	39	6	5	3	66
TOTAL	**14**	**42**	**6**	**6**	**9**	**77**

Tabla 12. Datos reales de la tabla de contingencia del servicio Evaluación de Seguridad de la Información. Nota: Estos valores representan los números obtenidos en las encuestas realizadas.

Datos Esperados

Evaluaciones de Seguridad de la Información	Rango de tiempo de implementación y costo estimado					
Implementación	**12 meses con un presupuesto de USD 26,000.00**	**3 meses con un presupuesto de USD 10,500.00**	**4 meses con un presupuesto de USD 5,500.00**	**6 meses con un presupuesto de USD 16,000.00**	**Los precios son muy altos**	**TOTAL**
No	2	6	1	1	1	11
Sí	12	36	5	5	8	66
TOTAL	**14**	**42**	**6**	**6**	**9**	**77**

Tabla 13. Datos esperados de la tabla de contingencia del servicio Evaluación de Seguridad de la Información. Nota: Estos valores representan los números que esperaríamos obtener en nuestro conjunto de datos basados en tablas de contingencia. Más detalle del análisis en la sección 4.1.4.

Prueba Chi Cuadrado: 23.53 **V de Cramer:** 0.55

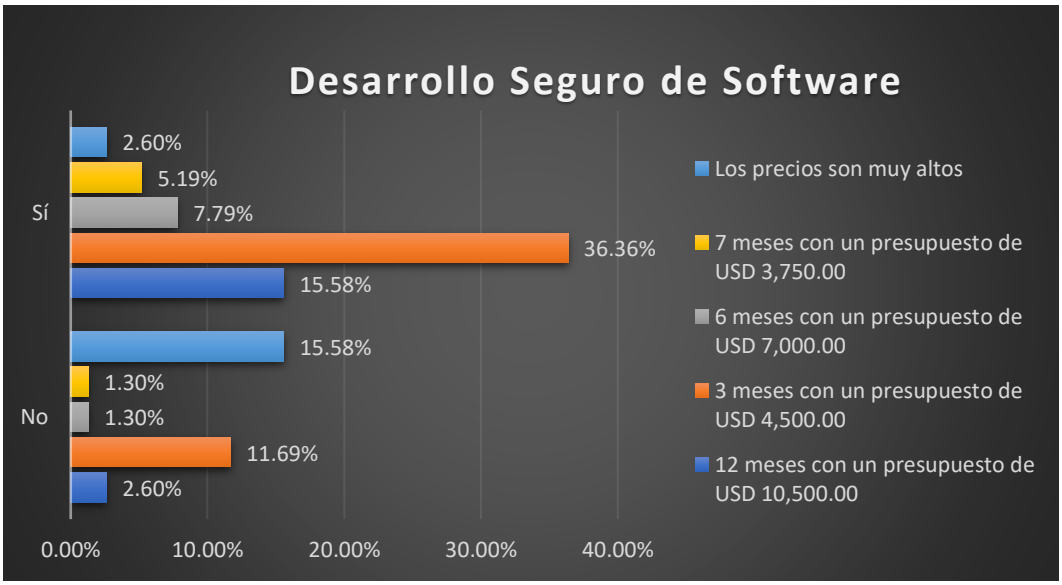


Figura 28. Porcentajes de rango de tiempo de implementación y precio de Desarrollo Seguro de Software. Nota: Se evidencia que la opción predominante es la de Sí implementaría el servicio con 3 meses de tiempo de implementación y un presupuesto de USD 4,500 con un porcentaje de 36.36%, sin embargo, el porcentaje de encuestados que no implementaría el servicio es mayor al 30%.

Datos Reales

Desarrollo Seguro de Software	Rango de tiempo de implementación y costo estimado					
Implementación	**12 meses con un presupuesto de USD 10,500.00**	**3 meses con un presupuesto de USD 4,500.00**	**6 meses con un presupuesto de USD 7,000.00**	**7 meses con un presupuesto de USD 3,750.00**	**Los precios son muy altos**	**TOTAL**
No	2	9	1	1	12	25
Sí	12	28	6	4	2	52
TOTAL	**14**	**37**	**7**	**5**	**14**	**77**

Tabla 14. Datos reales de la tabla de contingencia del servicio Desarrollo Seguro de Software. Nota: Estos valores representan los números obtenidos en las encuestas realizadas.

Datos Esperados

Desarrollo Seguro de Software	Rango de tiempo de implementación y costo estimado					
Implementación	**12 meses con un presupuesto de USD 10,500.00**	**3 meses con un presupuesto de USD 4,500.00**	**6 meses con un presupuesto de USD 7,000.00**	**7 meses con un presupuesto de USD 3,750.00**	**Los precios son muy altos**	**TOTAL**
No	5	12	2	2	5	25
Sí	9	25	5	3	9	52
TOTAL	**14**	**37**	**7**	**5**	**14**	**77**

Tabla 15. Datos esperados de la tabla de contingencia del servicio Desarrollo Seguro de Software. Nota: Estos valores representan los números que esperaríamos obtener en nuestro conjunto de datos basados en tablas de contingencia. Más detalle del análisis en la sección 4.1.4.

Prueba Chi Cuadrado: 22.74 **V de Cramer:** 0.54

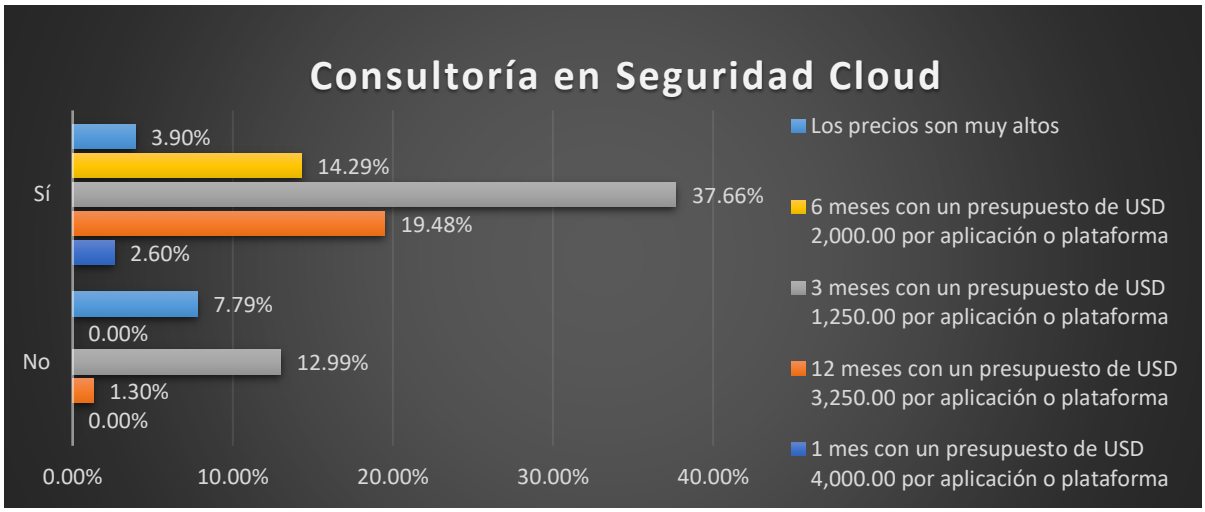


Figura 29. Porcentajes de rango de tiempo de implementación y precio de Consultoría en Seguridad Cloud. Nota: Se evidencia que la opción predominante es la de Sí implementaría el servicio con 3 meses de tiempo de implementación y un presupuesto de USD 1,250 con un porcentaje de 37.66%.

Datos Reales

Consultoría en Seguridad Cloud	Rango de tiempo de implementación y costo estimado					
Implementación	**1 mes con un presupuesto de USD 4,000.00 por aplicación o plataforma**	**12 meses con un presupuesto de USD 3,250.00 por aplicación o plataforma**	**3 meses con un presupuesto de USD 1,250.00 por aplicación o plataforma**	**6 meses con un presupuesto de USD 2,000.00 por aplicación o plataforma**	**Los precios son muy altos**	**TOTAL**
No		1	10		6	17
Sí	2	15	29	11	3	60
TOTAL	**2**	**16**	**39**	**11**	**9**	**77**

Tabla 16. Datos reales de la tabla de contingencia del servicio Consultoría en Seguridad Cloud. Nota: Estos valores representan los números obtenidos en las encuestas realizadas.

Datos Esperados

Consultoría en Seguridad Cloud	Rango de tiempo de implementación y costo estimado					
Implementación	**1 mes con un presupuesto de USD 4,000.00 por aplicación o plataforma**	**12 meses con un presupuesto de USD 3,250.00 por aplicación o plataforma**	**3 meses con un presupuesto de USD 1,250.00 por aplicación o plataforma**	**6 meses con un presupuesto de USD 2,000.00 por aplicación o plataforma**	**Los precios son muy altos**	**TOTAL**
No	0	4	9	2	2	17
Sí	2	12	30	9	7	60
TOTAL	**2**	**16**	**39**	**11**	**9**	**77**

Tabla 17. Datos esperados de la tabla de contingencia del servicio Consultoría en Seguridad Cloud. Nota: Estos valores representan los números que esperaríamos obtener en nuestro conjunto de datos basados en tablas de contingencia. Más detalle del análisis en la sección 4.1.4.

Prueba Chi Cuadrado: 16.70 **V de Cramer:** 0.47

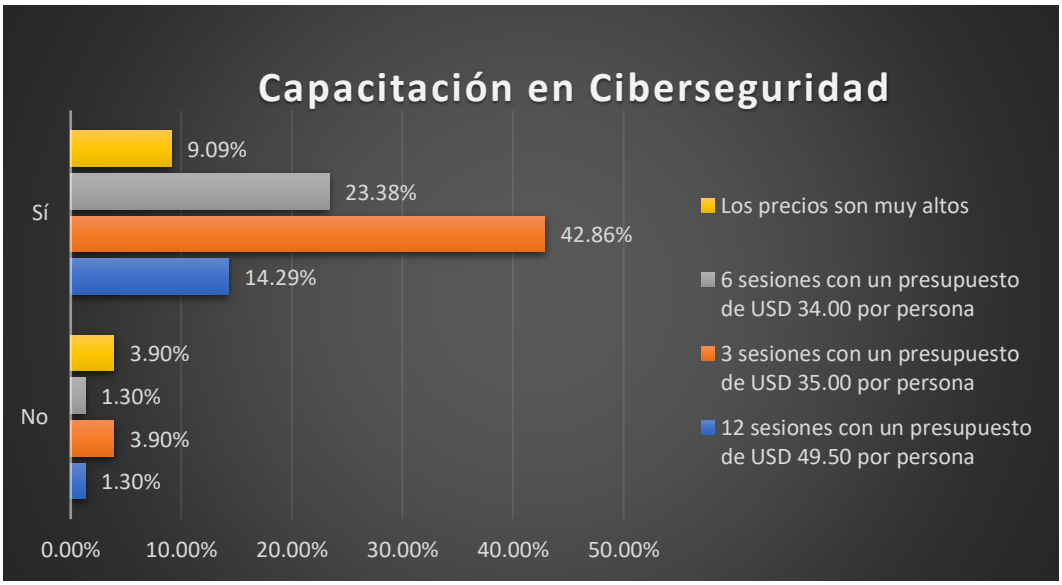


Figura 30. Porcentajes de rango de tiempo de implementación y precio de Capacitación en Ciberseguridad. Nota: Se evidencia que la opción predominante es la de Sí implementaría el servicio con 3 sesiones y un presupuesto de USD 35 por persona con un porcentaje de 42.86%.

Datos Reales

Capacitación en Ciberseguridad	Rango de tiempo de implementación y costo estimado				
Implementación	**12 sesiones con un presupuesto de USD 49.50 por persona**	**3 sesiones en con un presupuesto de USD 35.00 por persona**	**6 sesiones en con un presupuesto de USD 34.00 por persona**	**Los precios son muy altos**	**TOTAL**
No	1	3	1	3	8
Sí	11	33	18	7	69
TOTAL	**12**	**36**	**19**	**10**	**77**

Tabla 18. Datos reales de la tabla de contingencia del servicio Capacitación en Ciberseguridad. Nota: Estos valores representan los números obtenidos en las encuestas realizadas.

Datos Esperados

Capacitación en Ciberseguridad	Rango de tiempo de implementación y costo estimado				
Implementación	**12 sesiones con un presupuesto de USD 49.50 por persona**	**3 sesiones en con un presupuesto de USD 35.00 por persona**	**6 sesiones en con un presupuesto de USD 34.00 por persona**	**Los precios son muy altos**	**TOTAL**
No	1	4	2	1	8
Sí	11	32	17	9	69
TOTAL	**12**	**36**	**19**	**10**	**77**

Tabla 19. Datos esperados de la tabla de contingencia del servicio Capacitación en Ciberseguridad. Nota: Estos valores representan los números que esperaríamos obtener en nuestro conjunto de datos basados en tablas de contingencia. Más detalle del análisis en la sección 4.1.4.

Prueba Chi Cuadrado: 4.88 **V de Cramer:** 0.25

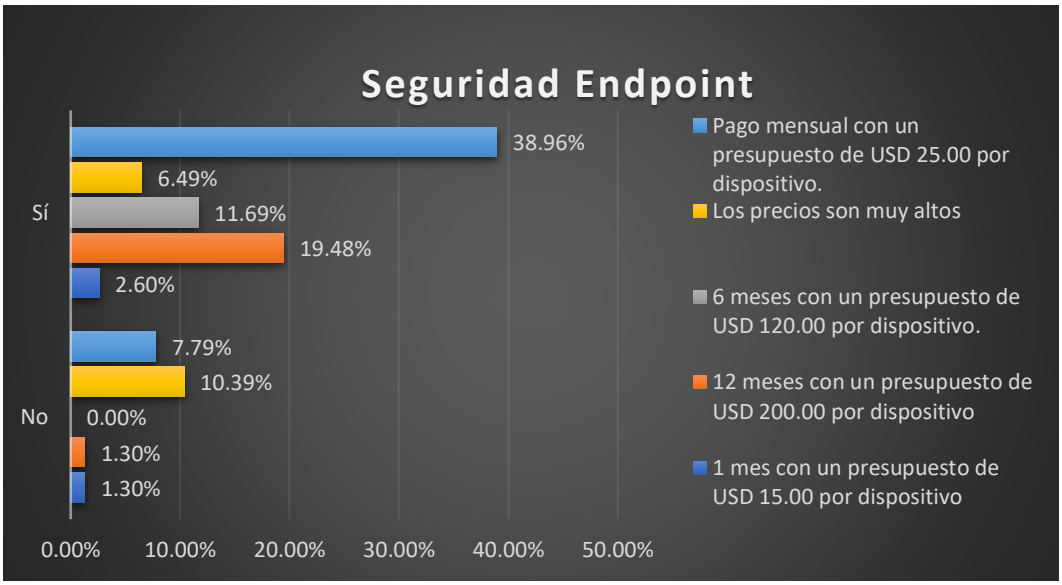


Figura 31. Porcentajes de rango de tiempo de implementación y precio de Seguridad Endpoint. Nota: Se evidencia que la opción predominante es la de Sí implementaría el servicio con 1 mes de tiempo de implementación y un presupuesto de USD 25 por dispositivo con un porcentaje de 38.96%.

Datos Reales

Seguridad Endpoint	Rango de tiempo de implementación y costo estimado					
Implementación	**1 mes con un presupuesto de USD 15.00 por dispositivo**	**12 meses con un presupuesto de USD 200.00 por dispositivo**	**6 meses con un presupuesto de USD 120.00 por dispositivo.**	**Los precios son muy altos**	**Pago mensual con un presupuesto de USD 25.00 por dispositivo.**	**TOTAL**
No	1.30%	1.30%	0.00%	10.39%	7.79%	20.78%
Sí	2.60%	19.48%	11.69%	6.49%	38.96%	79.22%
TOTAL	**3.90%**	**20.78%**	**11.69%**	**16.88%**	**46.75%**	**100.00%**

Tabla 20. Datos reales de la tabla de contingencia del servicio Seguridad Endpoint. Nota: Estos valores representan los números obtenidos en las encuestas realizadas.

Datos Esperados

Seguridad Endpoint	Rango de tiempo de implementación y costo estimado					
Implementación	**1 mes con un presupuesto de USD 15.00 por dispositivo**	**12 meses con un presupuesto de USD 200.00 por dispositivo**	**6 meses con un presupuesto de USD 120.00 por dispositivo.**	**Los precios son muy altos**	**Pago mensual con un presupuesto de USD 25.00 por dispositivo.**	**TOTAL**
No	1	3	2	2	7	16
Sí	2	13	7	7	29	61
TOTAL	**3**	**16**	**9**	**9**	**36**	**77**

Tabla 21. Datos esperados de la tabla de contingencia del servicio Seguridad Endpoint. Nota: Estos valores representan los números que esperaríamos obtener en nuestro conjunto de datos basados en tablas de contingencia. Más detalle del análisis en la sección 4.1.4.

Prueba Chi Cuadrado: 25.80 **V de Cramer:** 0.58

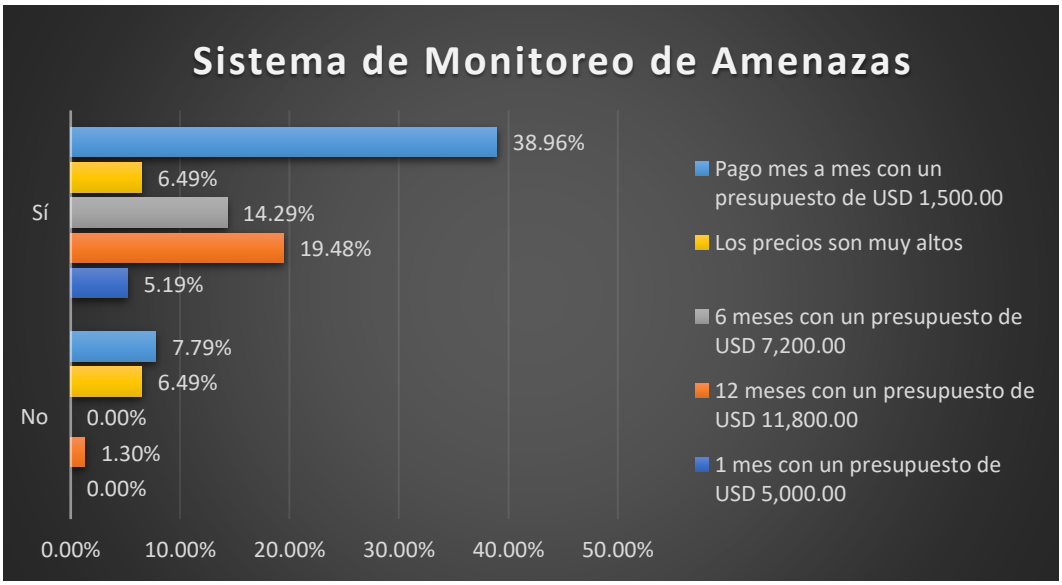


Figura 32. Porcentajes de rango de tiempo de implementación y precio de Sistema de Monitoreo de Amenazas. Nota: Se evidencia que la opción predominante es la de Sí implementaría el servicio con 1 mes de tiempo de implementación y un presupuesto de USD 1,500 con un porcentaje de 38.96%.

Datos Reales

Sistema de Monitoreo de Amenazas	Rango de tiempo de implementación y costo estimado					
Implementación	**1 mes con un presupuesto de USD 5,000.00**	**12 meses con un presupuesto de USD 11,800.00**	**6 meses con un presupuesto de USD 7,200.00**	**Los precios son muy altos**	**Pago mes a mes con un presupuesto de USD 1,500.00**	**TOTAL**
No		1		5	6	12
Sí	4	15	11	5	30	65
TOTAL	**4**	**16**	**11**	**10**	**36**	**77**

Tabla 22. Datos reales de la tabla de contingencia del servicio Sistema de Monitoreo de Amenazas. Nota: Estos valores representan los números obtenidos en las encuestas realizadas.

Datos Esperados

Sistema de Monitoreo de Amenazas	Rango de tiempo de implementación y costo estimado					
Implementación	**1 mes con un presupuesto de USD 5,000.00**	**12 meses con un presupuesto de USD 11,800.00**	**6 meses con un presupuesto de USD 7,200.00**	**Los precios son muy altos**	**Pago mes a mes con un presupuesto de USD 1,500.00**	**TOTAL**
No	1	2	2	2	6	12
Sí	3	14	9	8	30	65
TOTAL	**4**	**16**	**11**	**10**	**36**	**77**

Tabla 23. Datos esperados de la tabla de contingencia del servicio Sistema de Monitoreo de Amenazas. Nota: Estos valores representan los números que esperaríamos obtener en nuestro conjunto de datos basados en tablas de contingencia. Más detalle del análisis en la sección 4.1.4.

Prueba Chi Cuadrado: 12.86 **V de Cramer:** 0.41

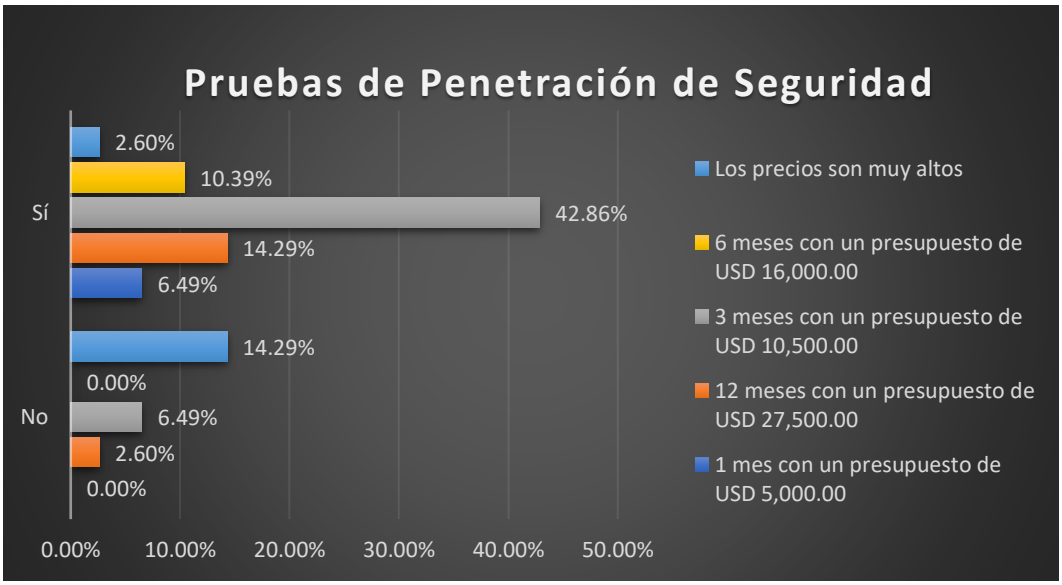


Figura 33. Porcentajes de rango de tiempo de implementación y precio de Pruebas de Penetración de Seguridad. Nota: Se evidencia que la opción predominante es la de Sí implementaría el servicio con 3 meses de tiempo de implementación y un presupuesto de USD 10,500 con un porcentaje de 42.86%.

Datos Reales

Pruebas de Penetración de Seguridad	Rango de tiempo de implementación y costo estimado					
Implementación	**1 mes con un presupuesto de USD 5,000.00**	**12 meses con un presupuesto de USD 27,500.00**	**3 meses con un presupuesto de USD 10,500.00**	**6 meses con un presupuesto de USD 16,000.00**	**Los precios son muy altos**	**TOTAL**
No		2	5		11	18
Sí	5	11	33	8	2	59
TOTAL	**5**	**13**	**38**	**8**	**13**	**77**

Tabla 24. Datos reales de la tabla de contingencia del servicio Pruebas de Penetración de Seguridad. Nota: Estos valores representan los números obtenidos en las encuestas realizadas.

Datos Esperados

Pruebas de Penetración de Seguridad	Rango de tiempo de implementación y costo estimado					
Implementación	**1 mes con un presupuesto de USD 5,000.00**	**12 meses con un presupuesto de USD 27,500.00**	**3 meses con un presupuesto de USD 10,500.00**	**6 meses con un presupuesto de USD 16,000.00**	**Los precios son muy altos**	**TOTAL**
No	1	3	9	2	3	18
Sí	4	10	29	6	10	59
TOTAL	**5**	**13**	**38**	**8**	**13**	**77**

Tabla 25. Datos esperados de la tabla de contingencia del servicio Pruebas de Penetración de Seguridad. Nota: Estos valores representan los números que esperaríamos obtener en nuestro conjunto de datos basados en tablas de contingencia. Más detalle del análisis en la sección 4.1.4.

Prueba Chi Cuadrado: 33.86 **V de Cramer:** 0.66

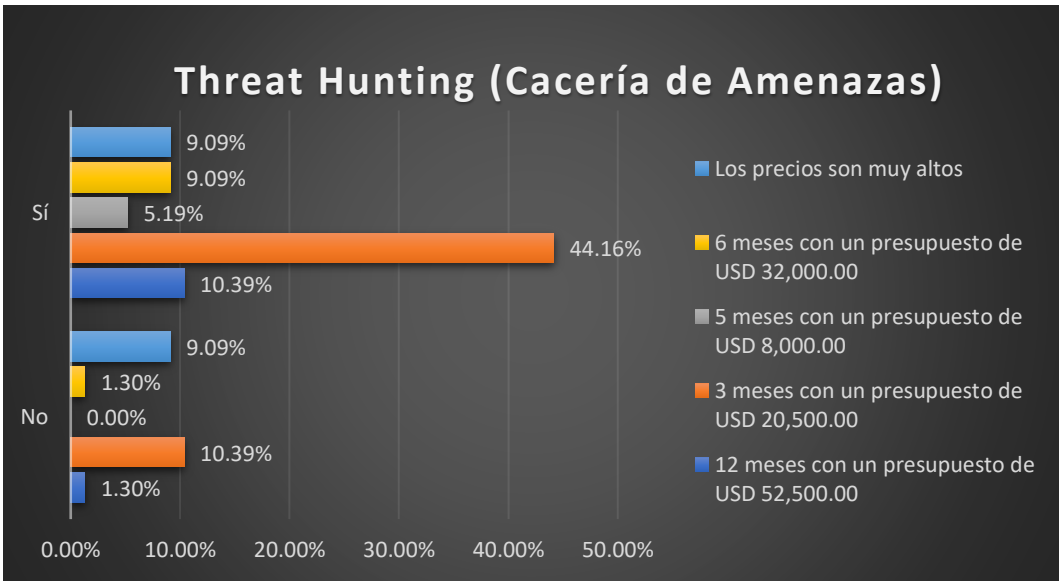


Figura 34. Porcentajes de rango de tiempo de implementación y precio de Threat Hunting (Cacería de Amenazas). Nota: Se evidencia que la opción predominante es la de Sí implementaría el servicio con 3 meses de tiempo de implementación y un presupuesto de USD 20,500 con un porcentaje de 44.16%.

Datos Reales

Threat Hunting (Cacería de Amenazas)	Rango de tiempo de implementación y costo estimado					
Implementación	**12 meses con un presupuesto de USD 52,500.00**	**3 meses con un presupuesto de USD 20,500.00**	**5 meses con un presupuesto de USD 8,000.00**	**6 meses con un presupuesto de USD 32,000.00**	**Los precios son muy altos**	**TOTAL**
No	1	8		1	7	17
Sí	8	34	4	7	7	60
TOTAL	**9**	**42**	**4**	**8**	**14**	**77**

Tabla 26. Datos reales de la tabla de contingencia del servicio Threat Hunting (Cacería de Amenazas). Nota: Estos valores representan los números obtenidos en las encuestas realizadas.

Datos Esperados

Threat Hunting (Cacería de Amenazas)	Rango de tiempo de implementación y costo estimado					
Implementación	**12 meses con un presupuesto de USD 52,500.00**	**3 meses con un presupuesto de USD 20,500.00**	**5 meses con un presupuesto de USD 8,000.00**	**6 meses con un presupuesto de USD 32,000.00**	**Los precios son muy altos**	**TOTAL**
No	2	9	1	2	3	17
Sí	7	33	3	6	11	60
TOTAL	**9**	**42**	**4**	**8**	**14**	**77**

Tabla 27. Datos esperados de la tabla de contingencia del servicio Threat Hunting (Cacería de Amenazas). Nota: Estos valores representan los números que esperaríamos obtener en nuestro conjunto de datos basados en tablas de contingencia. Más detalle del análisis en la sección 4.1.4.

Prueba Chi Cuadrado: 8.76 **V de Cramer:** 0.34

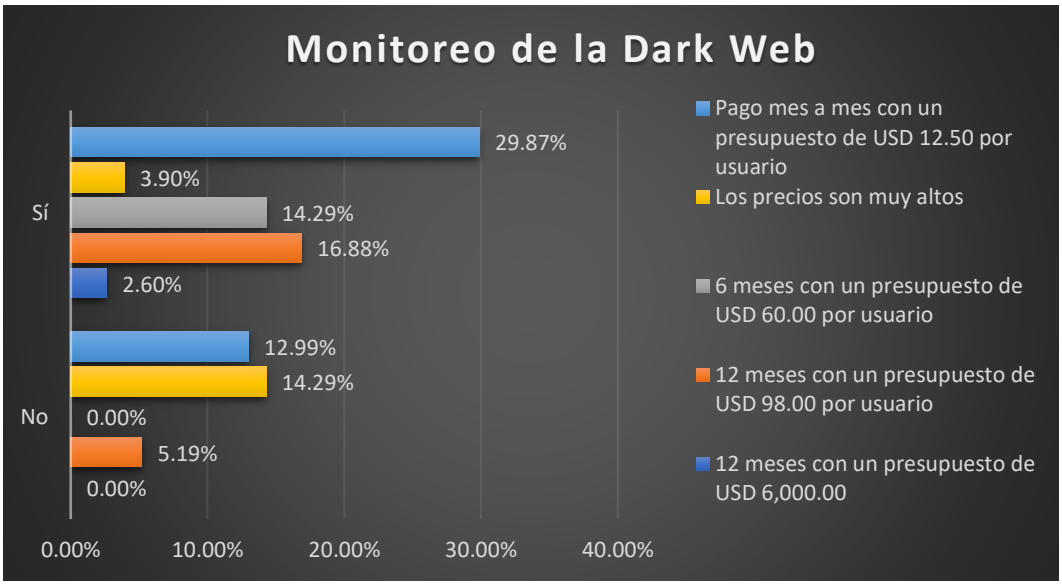


Figura 35. Porcentajes de rango de tiempo de implementación y precio de Monitoreo de la Dark Web. Nota: Se evidencia que la opción predominante es la de Sí implementaría el servicio con 1 mes de tiempo de implementación y un presupuesto de USD 12.50 por usuario con un porcentaje de 29.87%, sin embargo, el porcentaje de encuestados que no implementaría el servicio supera el 30%.

Datos Reales

Monitoreo de la Dark Web	Rango de tiempo de implementación y costo estimado					
Implementación	**12 meses con un presupuesto de USD 6,000.00**	**12 meses con un presupuesto de USD 98.00 por usuario**	**6 meses con un presupuesto de USD 60.00 por usuario**	**Los precios son muy altos**	**Pago mes a mes con un presupuesto de USD 12.50 por usuario**	**TOTAL**
No		4		11	10	25
Sí	2	13	11	3	23	52
TOTAL	**2**	**17**	**11**	**14**	**33**	**77**

Tabla 28. Datos reales de la tabla de contingencia del servicio Monitoreo de la Dark Web. Nota: Estos valores representan los números obtenidos en las encuestas realizadas.

Datos Esperados

Monitoreo de la Dark Web	Rango de tiempo de implementación y costo estimado					
Implementación	**12 meses con un presupuesto de USD 6,000.00**	**12 meses con un presupuesto de USD 98.00 por usuario**	**6 meses con un presupuesto de USD 60.00 por usuario**	**Los precios son muy altos**	**Pago mes a mes con un presupuesto de USD 12.50 por usuario**	**TOTAL**
No	1	6	4	5	11	25
Sí	1	11	7	9	22	52
TOTAL	**2**	**17**	**11**	**14**	**33**	**77**

Tabla 29. Datos esperados de la tabla de contingencia del servicio Monitoreo de la Dark Web. Nota: Estos valores representan los números que esperaríamos obtener en nuestro conjunto de datos basados en tablas de contingencia. Más detalle del análisis en la sección 4.1.4.

Prueba Chi Cuadrado: 20.51 **V de Cramer:** 0.52

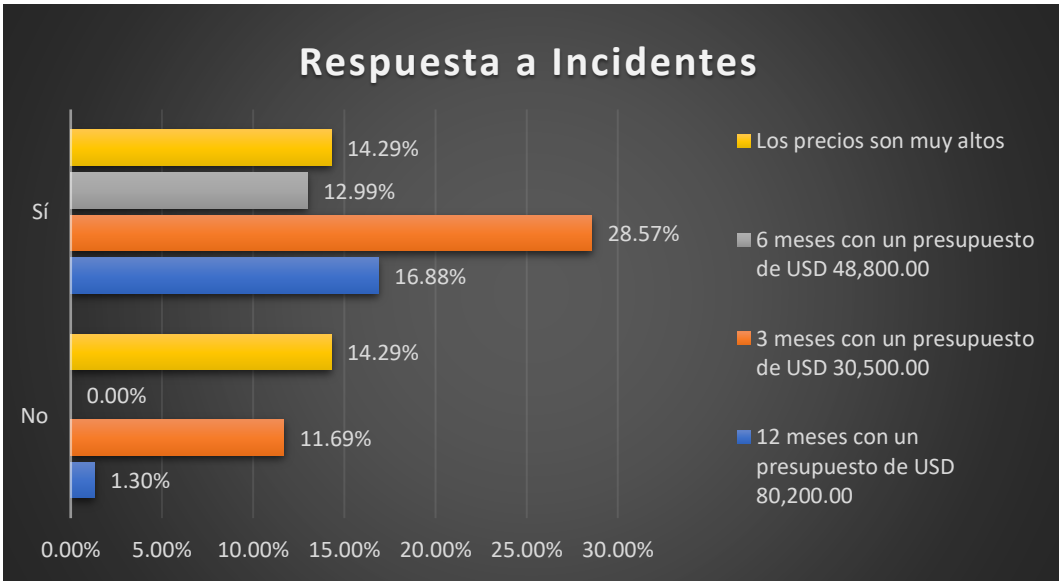


Figura 36. Porcentajes de rango de tiempo de implementación y precio de Respuesta a Incidentes. Nota: Se evidencia que la opción predominante es la de Sí implementaría el servicio con 3 meses de tiempo de implementación y un presupuesto de USD 30,500 con un porcentaje de 28.57%, sin embargo, el porcentaje de encuestados que no implementaría el servicio supera el 25%.

Datos Reales

Respuesta a Incidentes	Rango de tiempo de implementación y costo estimado				
Implementación	**12 meses con un presupuesto de USD 80,200.00**	**3 meses con un presupuesto de USD 30,500.00**	**6 meses con un presupuesto de USD 48,800.00**	**Los precios son muy altos**	**TOTAL**
No	1	9		11	21
Sí	13	22	10	11	56
TOTAL	**14**	**31**	**10**	**22**	**77**

Tabla 30. Datos reales de la tabla de contingencia del servicio Respuesta a Incidentes. Nota: Estos valores representan los números obtenidos en las encuestas realizadas.

Datos Esperados

Respuesta a Incidentes	Rango de tiempo de implementación y costo estimado				
Implementación	**12 meses con un presupuesto de USD 80,200.00**	**3 meses con un presupuesto de USD 30,500.00**	**6 meses con un presupuesto de USD 48,800.00**	**Los precios son muy altos**	**TOTAL**
No	4	8	3	6	21
Sí	10	23	7	16	56
TOTAL	**14**	**31**	**10**	**22**	**77**

Tabla 31. Datos esperados de la tabla de contingencia del servicio Respuesta a Incidentes. Nota: Estos valores representan los números que esperaríamos obtener en nuestro conjunto de datos basados en tablas de contingencia. Más detalle del análisis en la sección 4.1.4.

Prueba Chi Cuadrado: 12.39 **V de Cramer:** 0.40

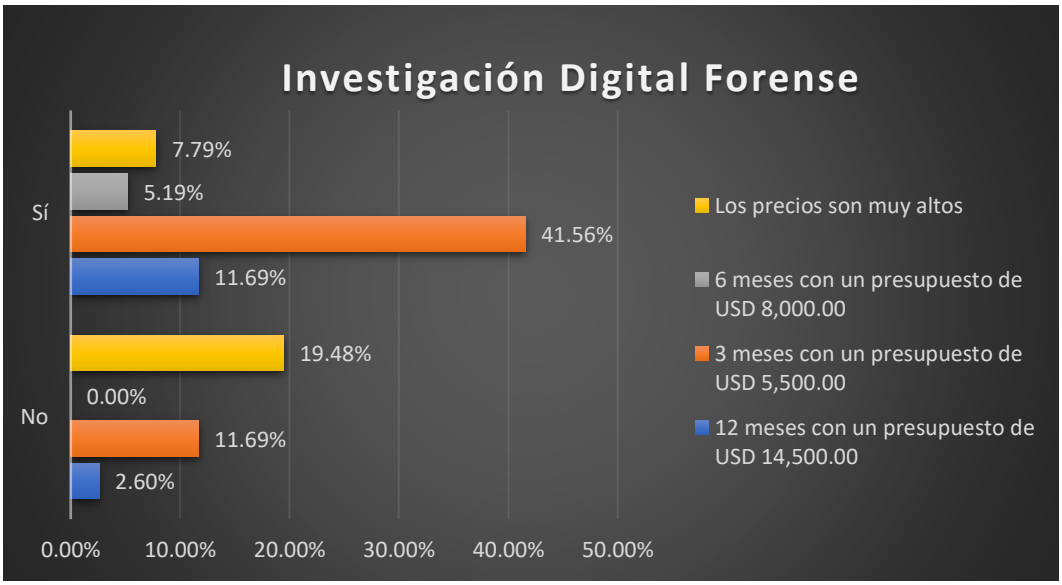


Figura 37. Porcentajes de rango de tiempo de implementación y precio de Investigación Digital Forense. Nota: Se evidencia que la opción predominante es la de Sí implementaría el servicio con 3 meses de tiempo de implementación y un presupuesto de USD 5,500 con un porcentaje de 41.56%, sin embargo, el porcentaje de encuestados que no implementaría el servicio supera el 30%.

Datos Reales

Investigación Digital Forense	Rango de tiempo de implementación y costo estimado				
Implementación	**12 meses con un presupuesto de USD 14,500.00**	**3 meses con un presupuesto de USD 5,500.00**	**6 meses con un presupuesto de USD 8,000.00**	**Los precios son muy altos**	**TOTAL**
No	2	9		15	26
Sí	9	32	4	6	51
TOTAL	**11**	**41**	**4**	**21**	**77**

Tabla 32. Datos reales de la tabla de contingencia del servicio Investigación Digital Forense. Nota: Estos valores representan los números obtenidos en las encuestas realizadas.

Datos Esperados

Investigación Digital Forense	Rango de tiempo de implementación y costo estimado				
Implementación	**12 meses con un presupuesto de USD 14,500.00**	**3 meses con un presupuesto de USD 5,500.00**	**6 meses con un presupuesto de USD 8,000.00**	**Los precios son muy altos**	**TOTAL**
No	4	14	1	7	26
Sí	7	27	3	14	51
TOTAL	**11**	**41**	**4**	**21**	**77**

Tabla 33. Datos esperados de la tabla de contingencia del servicio Investigación Digital Forense. Nota: Estos valores representan los números que esperaríamos obtener en nuestro conjunto de datos basados en tablas de contingencia. Más detalle del análisis en la sección 4.1.4.

Prueba Chi Cuadrado: 19.11 **V de Cramer:** 0.50

4.1.4 Resumen y criterios de inclusión de los servicios en el catálogo.

Para realizar la inclusión y el descarte de los servicios en el catálogo, se tomó en consideración los siguientes indicadores con su respectivo umbral de aceptación:

Tabla 34: Tabulación del criterio de aceptación según las buenas prácticas de (Stine & Foster, 2018)

	Indicador	Umbral de aceptación
1	Nivel de importancia	Mayor o igual a 4
2	Porcentaje de aceptación de implementación del servicio	Mayor o igual a 75%
3	Porcentaje de aceptación de implementación del servicio con el rango de tiempo y precio más aceptado	Mayor o igual a 30%
4	Nivel de asociación de las variables (V de Cramer)	Mayor o igual a 0.45

Tabla 34. Tabulación del criterio de aceptación según las buenas prácticas de (Stine & Foster, 2018) . Nota: Las variaciones en el criterio de inclusión depende del analista.

SERVICIO PROPUESTO	NIVEL DE IMPORTANCIA	RANGO DE TIEMPO DE IMPLEMENTACIÓN Y PRECIO MÁS ACEPTADO	PORCENTAJE DE ACEPTACIÓN DE IMPLEMENTACIÓN DEL SERVICIO	PORCENTAJE DE ACEPTACIÓN DE IMPLEMENTACIÓN DEL SERVICIO CON EL RANGO DE TIEMPO Y PRECIO MÁS ACEPTADO	NIVEL DE ASOCIACIÓN (V DE CRAMER)	SE INCLUYE AL CATÁLOGO DE SERVICIOS	COMENTARIOS
Gestión Estratégica de un CISO como servicio	4.18	3 meses con un presupuesto de USD 12,500.00	84.42%	30.70%	0.49	Sí	Este servicio superó todos los criterios de aceptación
Gestión de accesos y contraseñas	4.29	Pago mensual con un presupuesto de USD 25.00 por usuario.	84.42%	24.12%	0.40	Sí	Dado que su nivel de importancia es elevado y su nivel de asociación está ligeramente por debajo del criterio de aceptación, se lo incluye en el catálogo
Mitigación de Ataques	4.30	3 meses con un presupuesto de USD 3,500.00	84.42%	27.41%	0.54	Sí	Este servicio cumple con la mayoría de los criterios de aceptación
Evaluaciones de Seguridad de la Información	4.09	3 meses con un presupuesto de USD 10,500.00	85.71%	43.41%	0.55	Sí	Este servicio superó todos los criterios de aceptación
Desarrollo Seguro de Software	3.92	3 meses con un presupuesto de USD 4,500.00	67.53%	24.56%	0.54	No	El servicio no cumple con la mayoría de los criterios de aceptación pese a que su nivel de asociación es aceptable
Consultoría en Seguridad Cloud	3.92	3 meses con un presupuesto de USD 1,250.00 por aplicación o plataforma	77.92%	29.35%	0.47	Sí	Dado que su nivel de asociación es aceptable y su nivel de importancia se encuentra ligeramente por debajo del margen de aceptación, se lo incluye en el catálogo
Capacitación en Ciberseguridad	4.12	3 sesiones con un presupuesto de USD 35.00 por persona	89.61%	38.40%	0.25	No	Pese a que este servicio cumple con la mayoría de los criterios de aceptación, su nivel de asociación es demasiado bajo
Seguridad Endpoint	4.05	Pago mensual con un presupuesto de USD 25.00 por dispositivo.	79.22%	30.87%	0.58	Sí	Este servicio superó todos los criterios de aceptación

Sistema de Monitoreo de Amenazas	4.08	Pago mes a mes con un presupuesto de USD 1,500.00	84.42%	32.89%	0.41	Sí	Se incluye este servicio en el catálogo ya que su nivel de asociación está ligeramente por debajo del umbral de aceptación
Pruebas de Penetración de Seguridad	3.95	3 meses con un presupuesto de USD 10,500.00	76.62%	42.86%	0.66	Sí	Se incluye este servicio en el catálogo ya que su nivel de importancia está ligeramente por debajo del umbral de aceptación
Threat Hunting (Cacería de Amenazas)	3.79	3 meses con un presupuesto de USD 20,500.00	77.92%	34.41%	0.34	No	El nivel de asociación de este servicio es bajo
Monitoreo de la Dark Web	3.84	Pago mes a mes con un presupuesto de USD 12.50 por usuario	67.53%	20.17%	0.52	No	El servicio no cumple con la mayoría de los criterios de aceptación pese a que su nivel de asociación es aceptable
Respuesta a Incidentes	3.88	3 meses con un presupuesto de USD 30,500.00	72.73%	20.78%	0.40	No	El servicio no superó ninguno de los criterios de aceptación
Investigación Digital Forense	3.71	3 meses con un presupuesto de USD 5,500.00	66.23%	27.53%	0.50	No	El servicio no cumple con la mayoría de los criterios de aceptación pese a que su nivel de asociación es aceptable

Tabla 35. Resumen del análisis realizado.

4.2 Estructura organizacional de una empresa de ciberseguridad

Como parte de la propuesta metodológica para la implementación de un modelo de negocio para la prestación de servicios estratégicos de ciberseguridad que contempla el presente trabajo se incluye la estructura organizacional de una empresa de seguridad cibernética estándar, en esta sección se propone de manera general roles y responsabilidades jerarquizados que garantizan la formación de un equipo de trabajo sólido, eligiendo a los mejores colaboradores para que formen parte del negocio.

Primeramente, se debe mencionar que el equipo administrativo debe estar compuesto por profesionales que no solo poseen gran experiencia en la industria, sino que también estén dispuestos a trabajar para garantizar que el negocio alcance sus metas y objetivos.

Debido a que el modelo de negocio contempla diferentes servicios no convencionales, con el tiempo será necesario contratar más colaboradores para cubrir los diversos roles que surgirán.

Por lo tanto, a continuación, y en base a lo expuesto por (Martins, 2021), se exponen los roles y responsabilidades que conforman la estructura comercial propuesta para el modelo de negocio de ciberseguridad.

- **Director ejecutivo**

  Es el encargado de crear las políticas y estrategias adecuadas para guiar la dirección del negocio, delega responsabilidades y obligaciones al personal, se reúne y negocia con clientes para generar proyectos y establecer relaciones.

- **Gerente administrativo**

  Este rol debe asegurarse de que las funciones administrativas se realicen sin problemas, es un punto de unión entre el personal y el director ejecutivo, garantiza que el resto del personal cumpla con las políticas definidas por la empresa en todo momento, gestiona actividades administrativas del día a día.

- **Contador**

  Gestiona la información financiera tales como estados de cuenta, balances ejecutivos, roles de pago, se asegura que la empresa cumpla con las normativas financieras, desarrolla en conjunto con el gerente administrativo y el director ejecutivo presupuestos y estrategias financieras.

- **Gerente de Recursos Humanos**

  Administra el proceso de entrevista y contratación de empleados ideales para los cargos operativos de la empresa, crea políticas de recursos humanos y se asegura de que todo el personal las cumpla, coordina capacitaciones periódicas al personal y realiza evaluaciones de desempeño.

- **Gerente comercial**

  Desempeña actividades y estrategias comerciales en colaboración con el director ejecutivo, al ser esta una estructura organizacional para una empresa de ciberseguridad, este rol deberá tener un dominio de habilidades de técnicas y de negocio relacionadas con la seguridad cibernética, también es el encargado de gestionar contratos de negocio con el cliente.

- **Equipo de marketing y ventas**

  Este es un grupo de profesionales del marketing que son dirigidos por el gerente comercial, este equipo brinda apoyo en estrategias comerciales, elabora campañas publicitarias y se encarga de la expansión de marca del negocio.

- **Personal administrativo**

  Grupo formado por profesionales con conocimientos de administración de empresas que gestionará labores administrativas, tales como archivar, planificar y coordinar las actividades generales de la oficina, además de redactar los reportes correspondientes a los objetivos del negocio.

- **Personal operativo**

  Dentro de este grupo se encuentran profesionales técnicos de ciberseguridad los cuales bajo la guía del gerente comercial desarrollarán la implementación y gestión de los servicios propuestos en el catálogo.

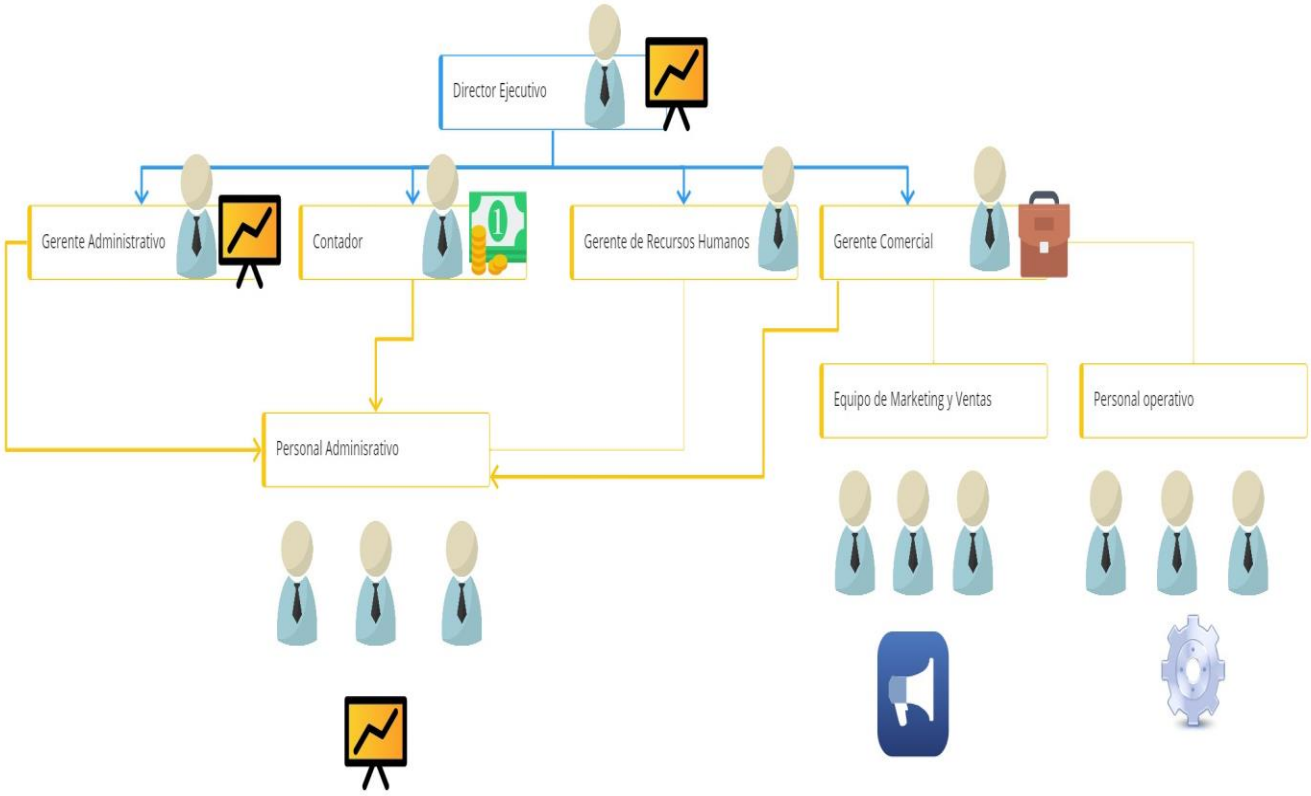


Figura 38. Elaboración propia

4.2.1 Propuesta de valor de la ciberseguridad como negocio

Los negocios de ciberseguridad atienden necesidades cotidianas y procesos complejos, de negocios o instituciones a través de acompañamiento en transformación digital, y la subcontratación de servicios de tecnologías de la información y comunicaciones. (Alfaro, 2020).

La propuesta de valor del modelo de negocio para la prestación de servicios de ciberseguridad que se describe en el presente trabajo consiste en implementar soluciones estratégicas de calidad, simples y eficientes que se ajusten a las necesidades de cada empresa por medio de un catálogo de servicios que tiene como alcance cubrir tres dominios de seguridad (Prevención, Detección y Respuesta).

Para cumplir con dicho objetivo, se ha tomado como referencia la cadena de valor descrita por (Alfaro, 2020) en la cual se integra procesos y transiciones entre distintos niveles comerciales para llegar al cliente final.

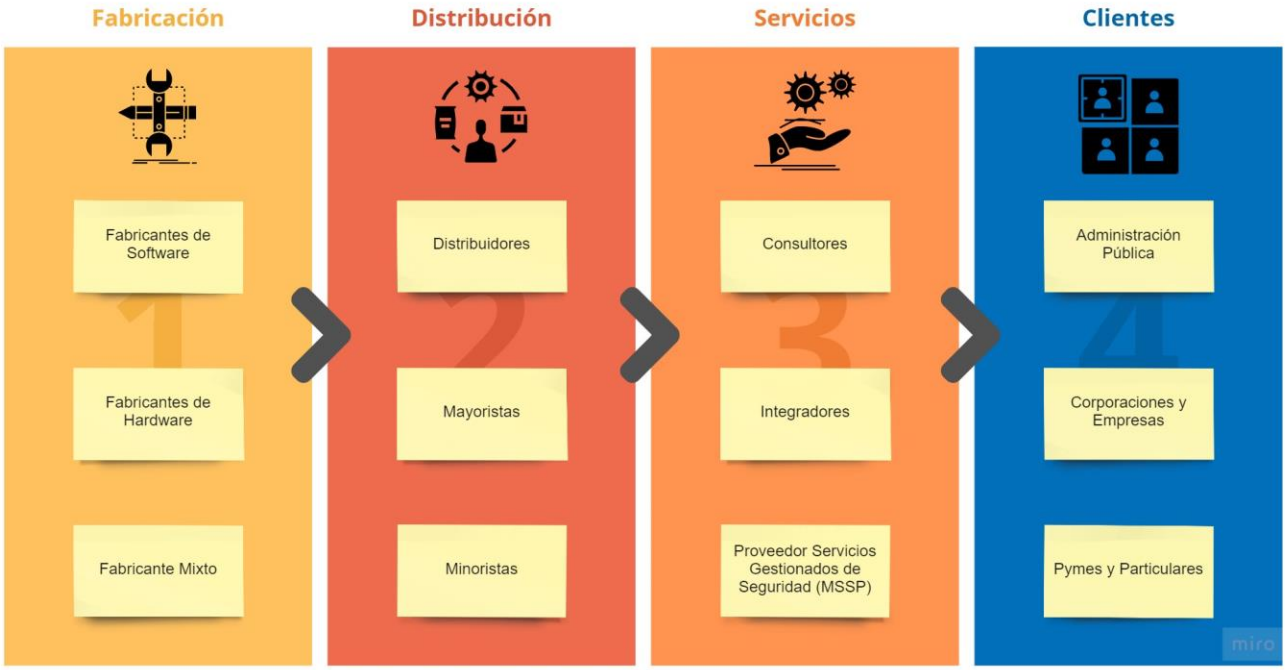


Figura 39. Cadena de Valor Servicios de Ciberseguridad. (Alfaro, 2020)

4.2.2 Los Proveedores.

4.2.2.1 Clasificación de Proveedores

Dentro de las etapas de la cadena de valor antes mencionada, se ha clasificado a los proveedores en los siguientes grupos:

Fabricantes:

Es aquel grupo de empresas que desarrollan soluciones de hardware de cifrado para garantizar la seguridad en la movilidad e interconexión de las redes corporativas. También se incluyen las empresas de desarrollo de software que crean soluciones digitales para garantizar la gestión y control de acceso e identidad de los usuarios.

Distribuidores de productos de ciberseguridad:

Este grupo está compuesto por empresas intermediarias entre el proceso de fabricación y prestación de los servicios. Se definen tres tipos de distribuidores:

- Distribuidores: Venden directamente a empresas de ciberseguridad o a clientes finales los productos de ciberseguridad. Pueden comercializar sus productos a los prestadores de servicios. (Alfaro, 2020).
- Mayoristas: Compran y venden productos de ciberseguridad a consultoras, a los integradores y a los proveedores de servicios gestionados de seguridad. Los mayoristas pueden estar especializados en seguridad TIC o bien, dedicarse a una actividad más genérica (informática, electrónica, etc.). (Alfaro, 2020)
- Minoristas: Son puntos de venta constituidos por tiendas físicas de informática, retail e incluso pequeñas consultorías enfocadas a Pymes y particulares. (Alfaro, 2020)

Proveedores de servicios gestionados de seguridad (MSSP):

Es en esta categoría donde se centra la propuesta de modelo de negocio del presente trabajo, las empresas de este tipo se dedican a gestionar y proveer distintos tipos de servicios de ciberseguridad. Los MSSP se categorizan en tres grupos:

- **Player de Nicho**: Estas empresas se enfocan en servir a un mercado o región local, por lo general este tipo de negocios son subcontratados por otras empresas proveedoras de Servicios de TI o MSS (Servicios de seguridad gestionados) para incorporar el conocimiento y la experiencia que estas empresas no poseen. (Gartner, 2018).
- **Telcos:** Son proveedores de conectividad y ancho de banda que administran y supervisan productos de seguridad de red, por lo general suelen proporcionar monitoreo remoto, tecnologías locales y servicios basados en la nube a través de sus conexiones a Internet. (Gartner, 2018).
- **TI:** Son proveedores de servicios de TI que generalmente administran dispositivos tecnológicos como parte de grandes iniciativas de outsourcing (tercerización de servicios) o integración de sistemas, donde tiene sentido que los clientes consuman MSS como parte de acuerdos generales de administración y monitoreo de infraestructura. (Gartner, 2018).

Además de las categorias anteriores, las empresas de consultoría de seguridad y algunos fabricantes de tecnologías son organizaciones que también ofrecen servicios de MSS ya que reconocen a este tipo de servicios fuentes de ingresos rentable, predecibles y de mayor crecimiento que los proyectos de consultoría por sí solos. También vale la pena señalar que muchos

subcontratistas de TI se están volviendo más activos como los MSSP, a través del desarrollo de habilidades en ciberseguridad o siendo partícipes de programas de partnership (Asociación de negocios) que ofrecen industrias mundiales líderes de TI como IBM, HP, CISCO, Oracle, Microsoft, entre otros.

Considerando la categorización anterior, en la Figura 40 podemos identificar en el mercado ecuatoriano algunos ejemplos de proveedores de servicios de TI y consultoras. (OEA & BID, 2020)



Figura 40. Elaboración propia basada en ejemplos de (OEA & BID, 2020).

4.2.3 Los Clientes

4.2.3.1 Clasificación de Clientes

A continuación, se detalla el último elemento de la cadena de valor antes descrita el cual corresponde a los clientes. De forma general y según (OEA & BID, 2020), la demanda de soluciones y servicios de ciberseguridad abarca tanto al sector público como privado los cuales se subdividen en los siguientes grupos comerciales:

- Industrial
- Comercial
- Automotriz
- Alimenticio
- Salud y Farmacéutica

- Construcción
- TI

4.2.4 Cómo se inicia un negocio de ciberseguridad

Para iniciar un negocio de ciberseguridad es necesario considerar las siguientes preguntas: ¿Qué servicios va a ofrecer el negocio?, ¿Cuál es el mercado?, ¿Quiénes son los clientes?, ¿Quién es la competencia?, ¿Cuál es la estrategia de ventas?, ¿Qué métodos de comercialización se utilizarán?, ¿Cuánto dinero se necesita para operar?, ¿Cómo se realiza el trabajo?, entre otros. A continuación, se presenta el detalle de los requerimientos y los costos que involucra iniciar un negocio de ciberseguridad.

4.2.4.1 Requerimientos para la puesta en marcha

El primer punto es obtener las certificaciones profesionales adecuadas, antes de que alguien contrate los servicios de un negocio, debe confiar en las capacidades técnicas de los profesionales que implementarán las soluciones. Una ingeniería en tecnología de la información, ciencias de la computación o un campo similar es un buen indicador de que se tiene las habilidades para iniciar un negocio de ciberseguridad, sin embargo, los títulos no brindan la experiencia del mundo real que los clientes anhelan. Las certificaciones ofrecen otra forma de desarrollar su credibilidad y señalar que sus habilidades son prácticas y relevantes.

Según (Insureon, 2021), estas son algunas de las certificaciones de ciberseguridad más populares y disponibles actualmente:

Tabla 34

Principales certificaciones para ciberseguridad

CERTIFICACIÓN	ORGANIZACIÓN EMISORA	PRECIO	NÚMERO DE PREGUNTAS	DETALLE
Certificación Certified Ethical Hacker	EC-Council	$100	125	Esta certificación se emite a los profesionales de ciberseguridad que prueban redes o sistemas y buscan debilidades de seguridad.
Certificación GIAC Security Essentials (GSEC)	Global Information Assurance Certification (GIAC)	$150	180	Valida el conocimiento de seguridad de la información de los profesionales de TI.
Profesional certificado en seguridad de sistemas de información (CISSP)	International Information Systems Security Certification Consortium (ISC)2	$699	150	Muestra su capacidad para diseñar, implementar y mantener un programa de ciberseguridad y sistemas de seguridad eficaces.
Profesional certificado en seguridad en la nube (CCSP)	International Information Systems Security Certification Consortium (ISC)2	$599	125	Muestra a los clientes potenciales que tiene las habilidades para diseñar, mantener y proteger los datos, las aplicaciones y la infraestructura de la nube.
Analista de ciberseguridad de CompTIA (CompTIA CySA +)	Asociación de la Industria de Tecnología de Computación (CompTIA)	$359	85	Evalúa las habilidades de detección de amenazas de los candidatos, la capacidad de analizar e interpretar datos y la capacidad de encontrar problemas de seguridad.
Certificado de ISACA en el gobierno de la TI empresarial (CGEIT)	Asociación de Auditoría y Control de Sistemas de Información (ISACA)	$760	150	Demuestra la capacidad de los examinados para auditar, controlar y proteger los sistemas de información.
Gerente de Seguridad de la Información Certificado (CISM)	Asociación de Auditoría y Control de Sistemas de Información (ISACA)	$760	150	Esta certificación demuestra que tiene la experiencia técnica para administrar los sistemas de información y la seguridad de TI

Tabla 36. Principales certificaciones para ciberseguridad. Esta tabla detalla los precios y número de preguntas que contiene cada certificación de ciberseguridad mencionada. (Insureon, 2021).

El segundo punto en el que un modelo de negocio debe enfocarse es en el marketing, un proyecto exitoso de este tipo empieza con el dueño del negocio el cual debe conocer sus servicios y las necesidades de sus clientes para así poder gestionar estrategias que determinen puntos de venta, atraigan a nuevos compradores y aumentan el número de ventas, este tema se explica con más detalle en la sección 4.4.1 y 4.4.2.

El siguiente paso debe ser la definir un presupuesto y coordinar la gestión financiera, la financiación puede ayudar a que su negocio repunte más allá del capital que se tenga designado para empezar el negocio, por eso es necesario explorar préstamos o convenios con inversionistas.

(Insureon, 2021) propone algunos consejos para administrar su dinero, que incluyen:

- Establezca objetivos de ingresos por ventas.
- Comprenda sus gastos operativos.
- Realice un seguimiento de su flujo de caja.
- Aparte dinero para un fondo de emergencia.

Otro paso fundamental es la contratación de empleados capacitados, para lo cual deben realizarse entrevistas exhaustivas y verificaciones de antecedentes de los empleados potenciales para verificar sus credenciales y experiencia.

Finalmente se debe gestionar estrategias administrativas, hay que tener en cuenta que un nuevo negocio es una inversión a futuro, razón por la cuál será necesario establecer indicadores de rendimiento que nos ayuden a anticiparnos a circunstancias críticas para el negocio y poder tomar las mejores decisiones.

4.3 Portafolio de servicios de ciberseguridad

Los riesgos que representan las ciber amenazas para la reputación financiera, legal o de reputación de una empresa necesitan ser monitoreados y gestionados de forma estratégica.

La seguridad cibernética comienza con los usuarios y abarca posteriormente todos los aspectos de una organización.

La resiliencia cibernética ya no es opcional, es un componente esencial de la gestión de la información para proteger la mayoría de los activos valiosos: datos y procesos comerciales. (OPENTEXT, 2020)

Las mejores soluciones de seguridad de la información empresarial proporcionan una visibilidad profunda de la tecnología digital, también permiten una mayor automatización y contextualización de la seguridad de sus activos de información.

Con el fin de proponer un catálogo de servicios rentable y aceptado en el mercado ecuatoriano, se realizó un análisis cuyo objetivo fue evaluar la importancia y el rango de tiempos de implementación y precios que el mercado está dispuesto a asumir, inicialmente se consideró las siguientes áreas de servicio:

- Prevención
    - Gestión Estratégica de un CISO como servicio.
    - Gestión de accesos y contraseñas.
    - Mitigación de Ataques.
    - Evaluación de Seguridad de la información.
    - Desarrollo Seguro de Software.
    - Consultoría en Seguridad Cloud.
    - Capacitación en Ciberseguridad.
- Detección
    - Seguridad Endpoint.
    - Sistema de Monitoreo de Amenazas.
    - Pruebas de Penetración de Seguridad.
    - Threat Hunting (Cacería de Amenazas).
    - Monitoreo de la Dark Web.

- Respuesta
    - Respuesta a Incidentes.
    - Investigación Digital Forense.

Sin embargo, los resultados señalan que actualmente los servicios con mayor rentabilidad y aceptación cubren las siguientes áreas de la ciberseguridad:

- Prevención
    - Gestión Estratégica de un CISO como servicio.
    - Gestión de accesos y contraseñas.
    - Mitigación de Ataques.
    - Evaluación de Seguridad de la información.
    - Consultoría en Seguridad Cloud.
- Detección
    - Seguridad Endpoint.
    - Sistema de Monitoreo de Amenazas.
    - Pruebas de Penetración de Seguridad.

De esta manera, la siguiente sección contempla únicamente el desarrollo del portafolio de servicios en base a las áreas de ciberseguridad ya mencionadas.

4.3.1 Desarrollo del catálogo de servicios de ciberseguridad basado en ITIL V4.

Una vez documentada la parte teórica de ITIL V4 en la sección 2.2 del Capítulo I, se desarrolla y propone el siguiente catálogo de servicios, el cual cubre necesidades cibernéticas en los dominios de prevención y detección de amenazas.



Figura 41. Catálogo de servicios de ciberseguridad propuesto. Elaboración propia.

4.3.1.1 Servicios de Prevención.

4.3.1.1.1 Gestión Estratégica de un CISO como servicio.

Descripción

Un director de seguridad de la información (CISO) es el ejecutivo de alto nivel dentro de una organización responsable de establecer y mantener la visión, la estrategia y el programa de la empresa para garantizar que los activos y tecnologías de la información estén adecuadamente protegidos. (Fruhlinger, 2021). El rol de un CISO es crucial para una buena estrategia de ciberseguridad. Al no siempre contar con personas capacitadas para desempeñar este rol en las empresas y al ser limitado el presupuesto para ciberseguridad, se propone el desarrollo la Gestión Estratégica de un CISO como servicio.

Enfoque

El servicio de Gestión Estratégica de un CISO como servicio contempla una vasta experiencia en todos los componentes del espectro de ciberseguridad cuyo objetivo es comprender exactamente cuáles son sus necesidades de los clientes, teniendo en cuenta su presupuesto y las regulaciones específicas de la industria. Este servicio gestiona los siguientes aspectos:

- Liderazgo y orientación en seguridad de la información.
- Liderazgo / participación del comité directivo.
- Gestión de cumplimiento de seguridad.
- Desarrollo de políticas, procesos y procedimientos de seguridad.
- Capacitación y concientización sobre seguridad.
- Incidentes: identificar, informar y controlar.
- Gestión del presupuesto de seguridad de la información.
- Establecimiento de un plan de recuperación ante desastres y un plan de continuidad de negocio.
- Gestión de riesgos.

Flujo de Trabajo

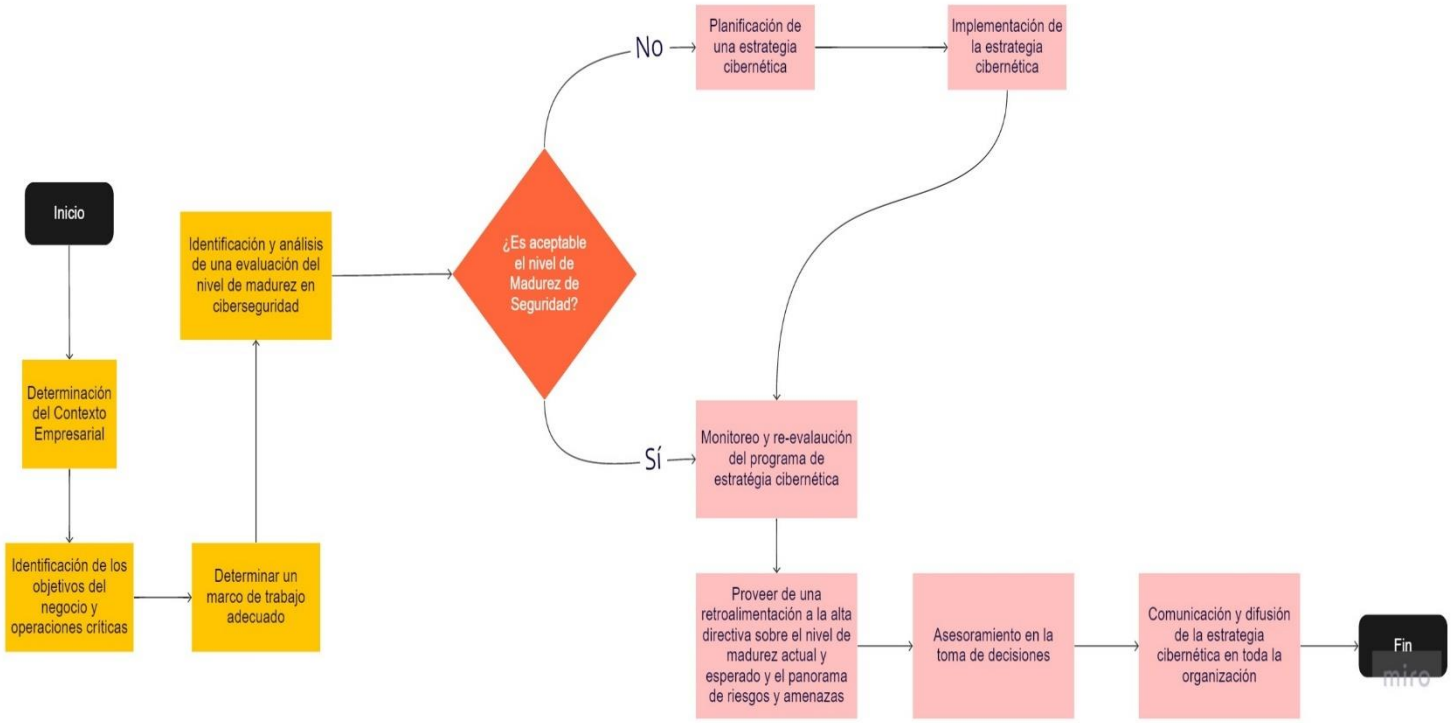


Figura 42. Flujo de Trabajo de Gestión Estratégica de un CISO como servicio. Elaboración propia

Tiempo de implementación y precio propuesto

En base al estudio de mercado realizado, se propone un tiempo de implementación de 3 meses con un presupuesto de $ 12,500.00.

Cabe mencionar que el rango de tiempo de implementación y precio dependerá siempre de los requerimientos de cada empresa.

Beneficios para el cliente

La Gestión Estratégica de un CISO como servicio brinda a las organizaciones los siguientes beneficios:

- Acceder a un grupo de profesionales experimentados y especializados en ciberseguridad.
- Acceder rápidamente a los recursos de gestión estratégica y eliminar la necesidad de atraer y retener talento.
- Reducir costos pagando únicamente por el soporte requerido.
- Reducir su riesgo mejorando su estrategia cibernética con una guía claramente definida.
- Lograr sus objetivos de seguridad de la información.

4.3.1.1.2 Gestión de Accesos y Contraseñas.

Descripción

Este servicio, en complemento con la Gestión estratégica de un CISO como servicio, ayuda a los clientes a proteger sus prácticas de gestión de identidad y accesos identificando todos los activos comerciales, aplicaciones, elementos de infraestructura y datos, y todas las personas que tienen acceso regular o administrativo a ellos.

Enfoque

El enfoque del servicio de Gestión de Accesos y Contraseñas contempla identificar potenciales formas de atacar o hacer un mal uso de los accesos y se desarrollar controles de compensación para todos los riesgos identificados.

Una parte fundamental de este servicio es educar a todo el equipo de trabajo a la interna del cliente sobre la importancia de no reutilizar las contraseñas y cómo usar un administrador de contraseñas de manera eficiente.

Flujo de Trabajo

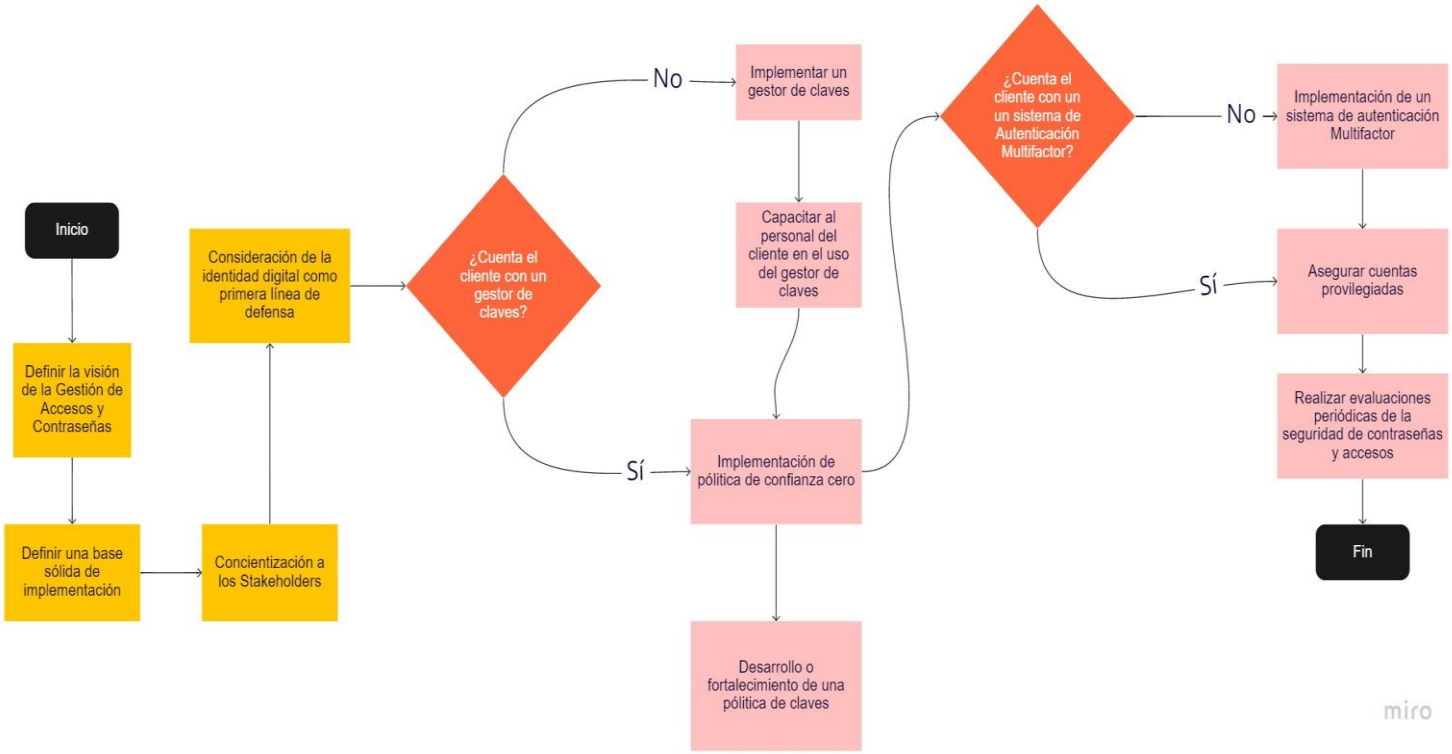


Figura 43. Flujo de Trabajo de Gestión de Accesos y Contraseñas. Elaboración Propia

Tiempo de implementación y precio propuesto

En base al estudio de mercado realizado, se propone un pago mensual con un presupuesto de $25.00 por usuario estableciendo un mínimo de 50 usuarios.

Cabe mencionar que el rango de tiempo de implementación y precio dependerá siempre de los requerimientos de cada empresa.

Beneficios para el cliente

El servicio de Gestión de Accesos y Contraseñas brinda a las organizaciones los siguientes beneficios:

- Eliminación de contraseñas débiles.
- Mitigación de amenazas internas.
- Seguridad Multifactor para el acceso mediante la autenticación de lo que un usuario es, lo que un usuario sabe o lo que un usuario tiene.
- Implementación de medidas de seguridad para cumplir con los requisitos regulatorios y de auditoría.
- La Gestión de Accesos y Contraseñas simplifica los procesos de registro, inicio de sesión y administración de usuarios para propietarios de aplicaciones, usuarios finales y administradores de sistemas, lo cual aumenta la productividad de la empresa.

4.3.1.1.3 Mitigación de Ataques.

Descripción

Cada empresa tiene un panorama de amenazas diferente debido a sus datos, clientes, competidores y recursos, los piratas informáticos pueden utilizar diferentes métodos de ataque para comprometer la seguridad de la empresa y lograr sus objetivos. El servicio de Mitigación de Ataques realiza una revisión de los controles de mitigación frente a 17 tipos de ciberataques.

Enfoque

El enfoque del servicio de Mitigación de Ataques contempla el desarrollo y revisión de controles en función de la prioridad comercial y el riesgo asociado a la siguiente lista de amenazas cibernéticas:

- Intrusiones contra redes.
- Infecciones por ransomware.
- Infecciones de malware.
- Divulgación no autorizada de información.
- Acceso no autorizado.

- Compromiso de cuentas.
- Abuso de privilegios.
- Cambios no autorizados de información, aplicaciones, sistemas o hardware.
- Violación de la política de seguridad de la información.
- Comportamiento sospechoso del sistema.
- Violación de la confidencialidad de la contraseña.
- Sabotaje / daño físico.
- Explotación de 0 días (Realizado por amenazas muy recientes).
- Ataques de phishing.
- Ataques de spear phishing.
- Violación del servicio web.
- Amenazas internas.

Flujo de Trabajo

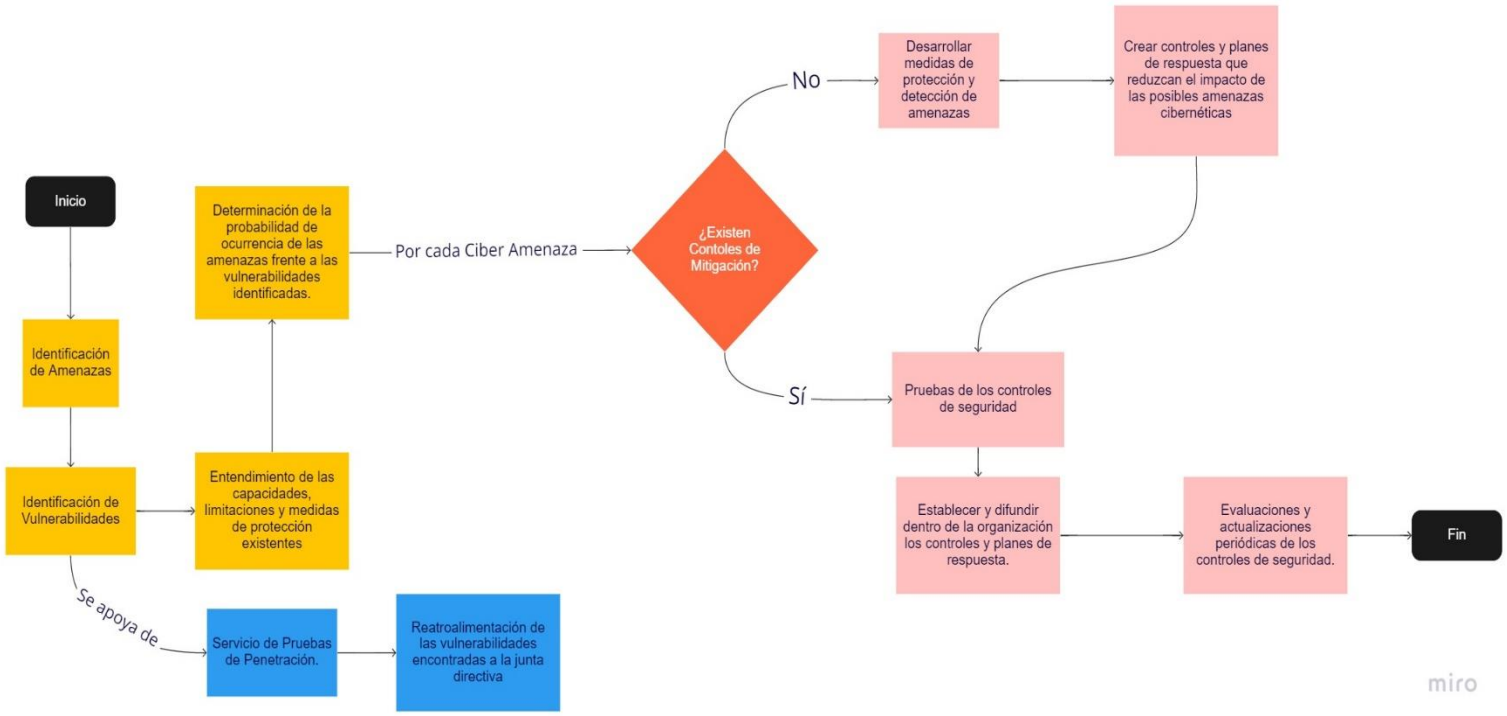


Figura 44. Flujo de Trabajo de Mitigación de Ataques. Elaboración Propia

Tiempo de implementación y precio propuesto

En base al estudio de mercado realizado, se propone un tiempo de implementación de 3 meses con un presupuesto de $3,500.00.

Cabe mencionar que el rango de tiempo de implementación y precio dependerá siempre de los requerimientos de cada empresa.

Beneficios para el cliente

El servicio de Mitigación de ataques brinda a las organizaciones los siguientes beneficios:

- Visión del panorama existente de vulnerabilidad y amenazas.
- Controles de seguridad sólidos.
- Mantener planes de acción ante una posible materialización de una amenaza.
- Actualizaciones periódicas de los controles de mitigación implementados.

4.3.1.1.4 Evaluación de Seguridad de la Información.

Descripción

Las Evaluaciones de Seguridad de la Información ayudan a conocer qué áreas de su negocio necesitan mayor protección y qué controles de la ISO 27002 conviene aplicar.

Enfoque

El enfoque del servicio de Evaluación de Seguridad de la Información brinda un detalle profundo sobre los niveles de madurez cibernética que tiene una organización. Esto incluye un plan de acción detallado con pasos a seguir y objetivos claros que se deben cumplir para mantenerse alejado de las brechas de seguridad que pueden tener impactos significativos de tiempo y dinero.

Flujo de Trabajo

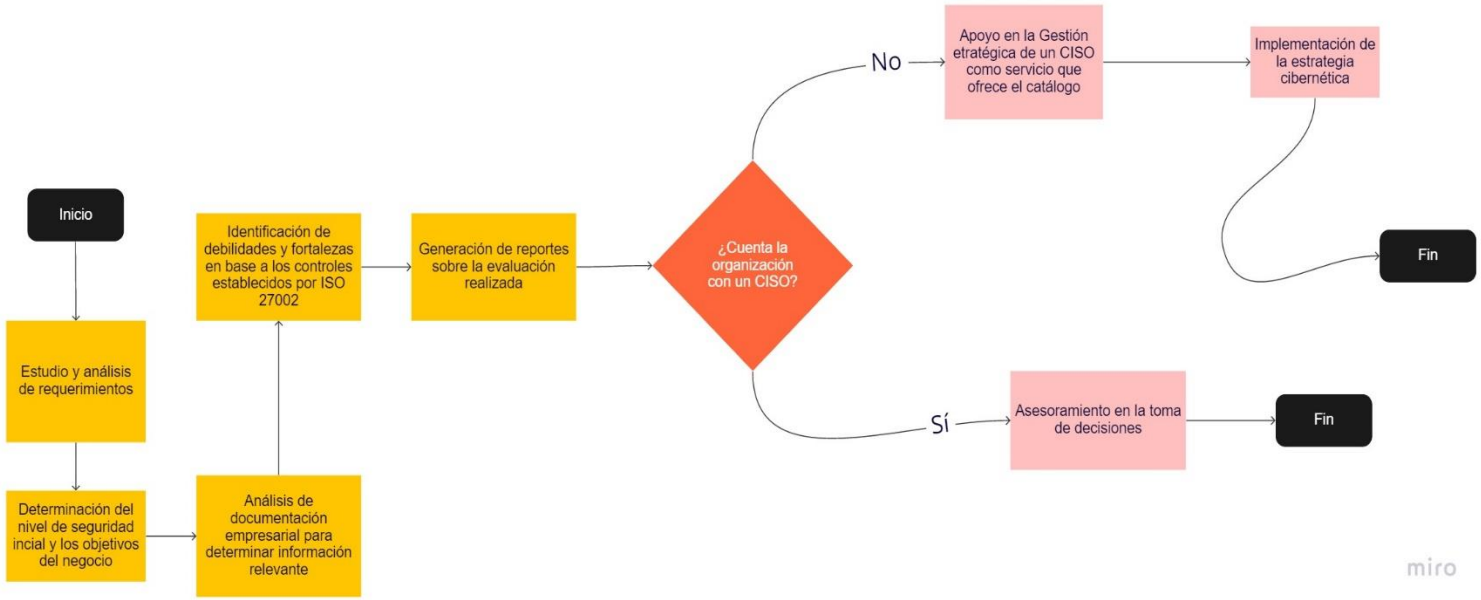


Figura 45. Flujo de Trabajo de Mitigación de Evaluación de Seguridad de la información. Elaboración propia.

Tiempo de implementación y precio propuesto

En base al estudio de mercado realizado, se propone un tiempo de implementación de 3 meses con un presupuesto de $ 10,500.00.

Cabe mencionar que el rango de tiempo de implementación y precio dependerá siempre de los requerimientos de cada empresa.

Beneficios para el cliente

El servicio de Evaluación de Seguridad de la información brinda a las organizaciones los siguientes beneficios:

- Noción y concientización de los riesgos de seguridad dentro de su entorno. Este es el beneficio más obvio y directo. No se puede solucionar un problema si no se sabe que existe.
- Ayudan a documentar el progreso realizado para proteger a la empresa.
- Es una manera fiable para demostrar el Due Diligence (Conceptos que implican la investigación de una empresa o persona previa a la firma de un contrato) de una empresa.

- Algunas industrias requieren evaluaciones de seguridad como condición de cumplimiento legislativo.

4.3.1.1.5 Consultoría en Seguridad Cloud.

Descripción

El servicio propuesto de Consultoría en Seguridad Cloud ayuda a los clientes en la configuración y migración de entornos locales tradicionales a la nube de forma segura. El servicio está diseñado para optimizar las configuraciones y evaluar las arquitecturas cloud aplicando las mejores prácticas de seguridad en la nube para brindar la tranquilidad de saber que el entorno Cloud del cliente es seguro dentro de los servicios que ofrecen los principales proveedores de tecnología cloud como son: AWS (Amazon Web Services), Azure y Google Cloud.

Enfoque

El servicio de Consultoría en Seguridad Cloud contempla los siguientes aspectos:

- Revisión de la configuración del entorno de la nube para identificar las vulnerabilidades de configuración y proporcionar orientación personalizada en áreas de mejora de la seguridad en la nube.
- Evaluación de la arquitectura de seguridad en la nube basada en el contexto único de cada empresa para desarrollar una estrategia de seguridad madura y una arquitectura cloud alineada al negocio.

Flujo de Trabajo

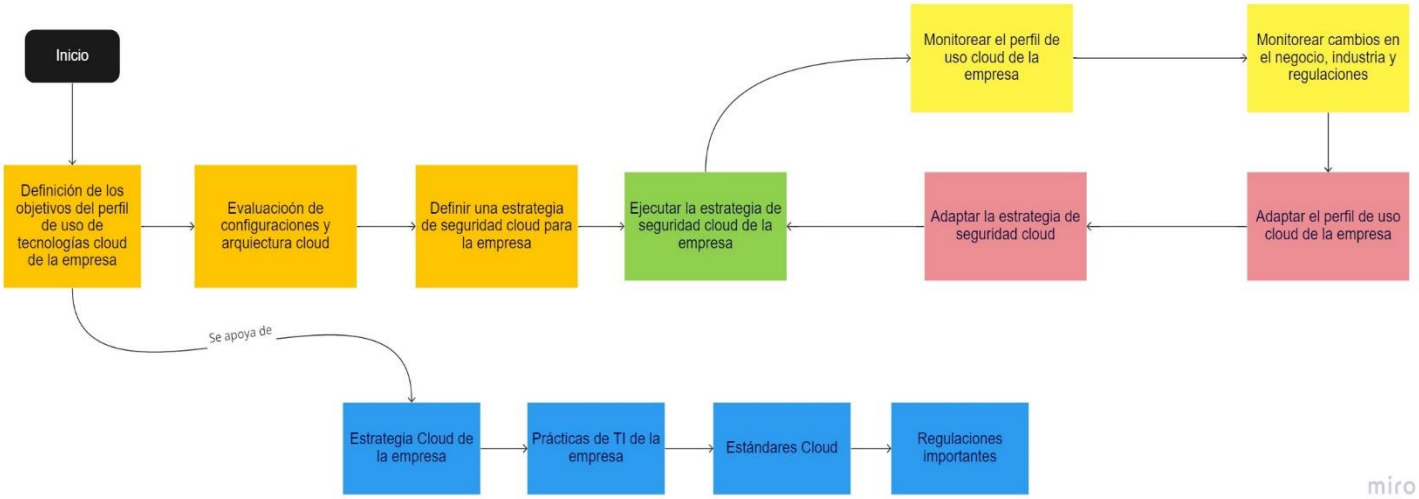


Figura 46. Flujo de Trabajo de Consultoría en Seguridad Cloud. Elaboración propia.

Tiempo de implementación y precio propuesto

En base al estudio de mercado realizado, se propone un tiempo de implementación de 3 meses con un presupuesto de $ 1,250.00 por aplicación o plataforma, estableciendo un mínimo de 3 aplicaciones con un máximo de 200 líneas de código por módulo.

Cabe mencionar que el rango de tiempo de implementación y precio dependerá siempre de los requerimientos de cada empresa.

Beneficios para el cliente

El servicio de Consultoría en Seguridad Cloud brinda a las organizaciones los siguientes beneficios:

- Análisis exhaustivo de sistemas individuales basados en la nube y evaluación de todo su entorno para determinar el alcance total de posibles ataques.
- Análisis completo de los componentes internos y externos de su infraestructura alojada en la nube

- Identificación de problemas potenciales y orientación detallada sobre los mejores métodos para mitigarlos y resolverlos.
- Recomendaciones específicas y detalladas para mejorar su postura general de seguridad en la nube para ayudar a prevenir, detectar y recuperarse rápidamente de los incidentes.

4.3.1.2 Servicios de Detección.

4.3.1.2.1 Seguridad Endpoint.

Descripción

La seguridad de los dispositivos Endpoint es la práctica de proteger los puntos finales o los puntos de entrada de los dispositivos de los usuarios finales, como equipos de escritorio, portátiles y dispositivos móviles, para que no sean explotados por campañías y agentes malintencionados. Los sistemas de seguridad de terminales protegen estos terminales en una red o en la nube de las amenazas de ciberseguridad.

Enfoque

El servicio de Seguridad Endpoint contempla los siguientes aspectos:

- **Protección de dispositivos:** Incluye la protección antivirus y contra malware tanto para computadoras como para dispositivos móviles como teléfonos y tabletas, protegiéndolos principalmente contra ataques de tipo ransomware.
- **Controles de red:** El sistema de seguridad de Endpoint funciona como un firewall completo que filtra todo el tráfico entrante e identifica los riesgos potenciales.
- **Controles de aplicaciones:** Contempla la integración con los servidores de aplicaciones para monitorear y limitar el acceso al dispositivo Endpoint.
- **Controles de datos:** Incluye herramientas que ayudan a prevenir fugas de información y mejorar la seguridad de los datos con el cifrado de información confidencial.
- **Protecciones del navegador:** La Seguridad Endpoint incluye un filtro web para que el cliente pueda elegir a qué tipos de sitios pueden acceder sus usuarios corporativos mientras están conectados a la red.

Flujo de Trabajo

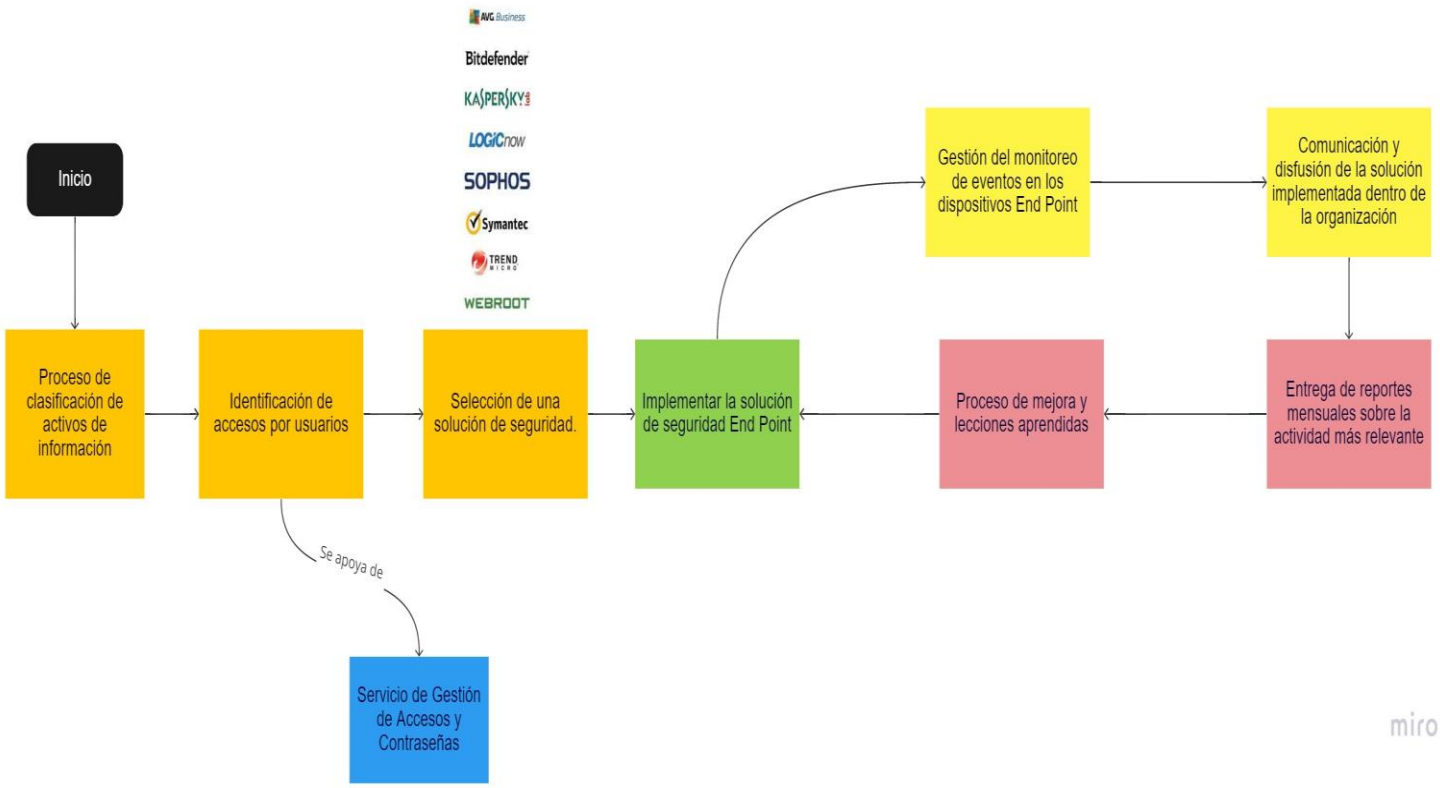


Figura 47. Flujo de Trabajo de Seguridad End Point. Elaboración propia.

Tiempo de implementación y precio propuesto

En base al estudio de mercado realizado, se propone un pago mensual con un presupuesto de $25.00 por dispositivo, estableciendo un mínimo de 50 dispositivos.

Cabe mencionar que el rango de tiempo de implementación y precio dependerá siempre de los requerimientos de cada empresa.

Beneficios para el cliente

El servicio de Seguridad Endpoint brinda a las organizaciones los siguientes beneficios:

- Seguridad y administración unificadas, los dispositivos críticos para la empresa como son los dispositivos móviles, terminales fijos y entornos de servidor, deben administrarse y protegerse fácilmente a través de un solo panel de control.
- Protección contra los principales vectores de amenazas.
- Mejor visibilidad de la actividad de los dispositivos finales.
- Protección de reputación empresarial, con la confianza que conlleva tener puntos finales altamente seguros, el cliente puede mantenerse fuera de los titulares negativos de prensa y mantener su reputación.

4.3.1.2.2 Sistema de Monitoreo de Amenazas.

Descripción

Un sistema de monitoreo de amenazas se apoya principalmente de un software llamado SIEM por sus siglas en inglés Security Information and Event Management el cual recopila datos de las diferentes tecnologías dentro de un sistema, monitorea y analiza esos datos en busca de anomalías y posibles riesgos de seguridad, y luego toma las medidas adecuadas contra esas amenazas.

Enfoque

El servicio de Sistema de Monitoreo de Amenazas propuesto proporciona visibilidad en tiempo real de comportamientos sospechosos o cambios de sistema no autorizados en la red del cliente. Esto permite a los profesionales de TI estar un paso por delante de posibles amenazas de seguridad y una variedad de diferentes violaciones de datos.

A medida que se recopilan y analizan los datos, se definen comportamientos sospechosos que activarán alertas, las cuales serán reportadas y mitigadas dependiendo el alcance del servicio establecido con el cliente.

Se consideran dos tipos principales de monitoreo cibernético: Monitoreo de dispositivos Endpoint y Monitoreo de red.

Flujo de Trabajo

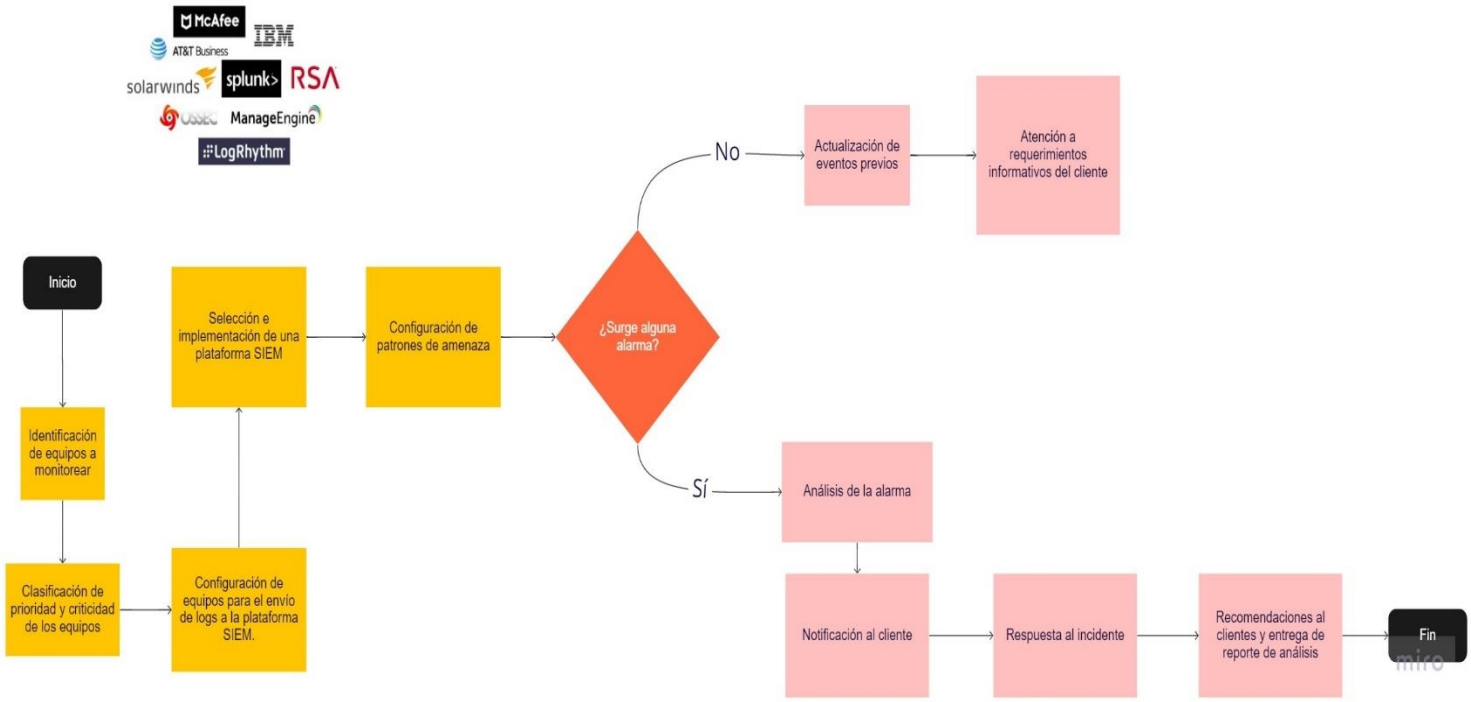


Figura 48. Flujo de Trabajo de Sistema de Monitoreo de Amenazas. Elaboración propia.

Tiempo de implementación y precio propuesto

En base al estudio de mercado realizado, se propone un tiempo de implementación de 3 meses con un pago mensual de $1,500.00.

Cabe mencionar que el rango de tiempo de implementación y precio dependerá siempre de los requerimientos de cada empresa.

Beneficios para el cliente

El servicio de Sistema de Monitoreo de Amenazas brinda a las organizaciones los siguientes beneficios:

- Una de las principales ventajas de los servicios de monitoreo de seguridad cibernética es que es una excelente manera de reducir el tiempo de inactividad de su empresa, una red en pleno funcionamiento es esencial para las operaciones comerciales diarias.
- Visibilidad total de las actividades que se realizan en toda la corporativa del cliente.
- Respuesta proactiva ante incidentes, no solo realizando un proceso de mitigación, sino que también proporciona un análisis de las incidencias detectadas y proponer acciones de mejora.

4.3.1.2.3 Pruebas de Penetración de Seguridad.

Descripción

Una prueba de penetración, también llamada hackeo ético, es una técnica de ciberseguridad que utilizan las organizaciones para identificar, probar y resaltar vulnerabilidades en su postura de seguridad. Estas pruebas de penetración a menudo las realizan hackers éticos. Estos empleados internos o terceros imitan las estrategias y acciones de un atacante para evaluar la capacidad de hackeo de los sistemas informáticos, la red o las aplicaciones web de una organización. Las organizaciones también pueden utilizar las pruebas de penetración para comprobar su cumplimiento de las normas legislativas.

Enfoque

El servicio propuesto de Pruebas de Penetración de Seguridad contempla los siguientes aspectos:

- Determinar la viabilidad de un conjunto particular de proveedores de ataques.
- Identificar las vulnerabilidades de riesgo que resultan de una combinación de vulnerabilidades de menor riesgo explotadas en una secuencia particular.
- Descubrir vulnerabilidades que pueden ser difíciles de detectar con aplicaciones de red automatizadas.

- Evaluar la magnitud de los posibles impactos comerciales y operativos de los ataques exitosos.
- Proporcionar evidencia para respaldar una mayor inversión en tecnología y personal de seguridad.

Flujo de Trabajo

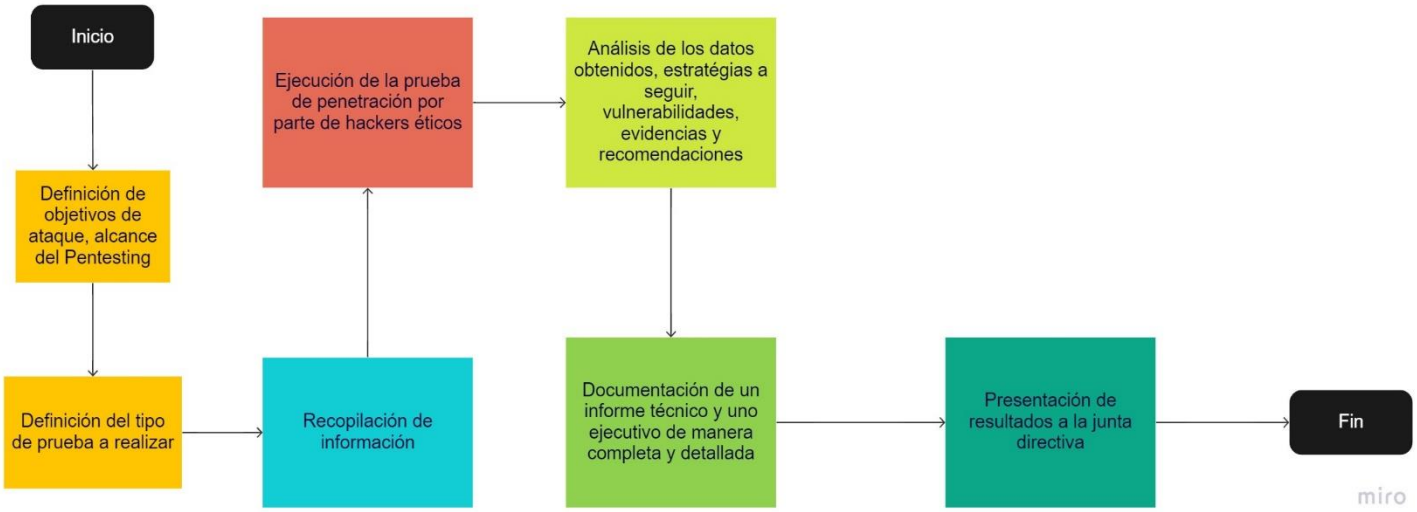


Figura 49. Flujo de Trabajo de Pruebas de Penetración de Seguridad. Elaboración propia basada en la Metodología Cyber kill Chain

Tiempo de implementación y precio propuesto

En base al estudio de mercado realizado, se propone un tiempo de implementación de 3 meses con un presupuesto de $10,500.00.

Cabe mencionar que el rango de tiempo de implementación y precio dependerá siempre de los requerimientos de cada empresa.

Beneficios para el cliente

El servicio de Pruebas de Penetración de Seguridad brinda a las organizaciones los siguientes beneficios:

- **Revelación de vulnerabilidades:** Las pruebas de penetración exploran las debilidades existentes en su sistema o configuraciones de aplicaciones e infraestructura de red. Incluso las acciones y hábitos de su personal que podrían conducir a violaciones de datos e infiltraciones maliciosas se investigan durante las pruebas de penetración. Un informe detalla las vulnerabilidades de seguridad encontradas para que el cliente sepa qué mejoras de software y hardware debe considerar o qué recomendaciones y políticas mejorarían la seguridad general de su empresa.
- **Muestra riesgos reales:** Los hackers éticos intentan explotar las vulnerabilidades identificadas, evidenciando lo que podría hacer un atacante en el "mundo real".
- **Garantizar la continuidad del negocio:** Para asegurarse de que sus operaciones comerciales estén en funcionamiento todo el tiempo, necesita disponibilidad de red, comunicaciones 24 horas al día, 7 días a la semana y acceso a recursos. Cada interrupción tendrá un impacto negativo en su negocio. Las pruebas de penetración revelan amenazas potenciales y ayudan a garantizar que sus operaciones no sufran un tiempo de inactividad inesperado o una pérdida de accesibilidad por una ciber amenaza.
- **Mantener la confianza reputacional:** Un ciberataque o violación de datos afecta negativamente la confianza y la lealtad de los clientes, proveedores y socios. Sin embargo, si la empresa del cliente es conocida por sus estrictas y sistemáticas revisiones de seguridad y pruebas de penetración, brindará confianza a todas sus partes interesadas.

CAPÍTULO IV

5. PROPUESTA DE IMPLEMENTACIÓN ESTRATÉGICA DE LOS SERVICIOS DE CIBERSEGURIDAD

5.1 Estrategia de mercado

5.1.1 Marketing para la ciberseguridad.

La importancia del marketing ha hecho que las empresas mantengan un presupuesto separado y creen políticas y estrategias que le permitan destacar en el mercado.

En vista de esto, en esta sección se describe una estrategia de marketing que complementa el análisis realizado en la sección 4.1.3.

(Porter, 2020) menciona que las ventas empiezan con la educación, relaciona al marketing como una expedición de pesca en la cual mientras más educación proveas a tus clientes, será más fácil venderles tus servicios. En ciberseguridad es común encontrarse a usuarios que no saben que tienen un problema hasta que este se vuelve catastrófico y la principal causa es precisamente la falta de conocimiento.

Dentro de cualquier proceso de comercialización es importante demostrar resultados y aportar valor. En el ámbito de la ciberseguridad se debe promocionar los servicios enfocándonos en protección de datos, gestión de riesgos y de cierta manera proporcionarles a los clientes la paz y confianza de que sus sistemas estarán protegidos.

De cierta manera el marketing de un servicio también se basa en construir confianza, especialmente en ciberseguridad ya que es un trabajo crítico que involucra la gestión de varios componentes que son de alta prioridad para las empresas, por lo cual es importante darles razones suficientes a los clientes para confiarnos su seguridad cibernética. (Porter, 2020) también define algunos puntos clave que ayudan a construir esta confianza:

- **Autoridad:** Participación en charlas, generación de contenido, involucramiento con la prensa, reconocimiento público.
- **Presencia Social:** Testimonios de clientes y casos de éxito.
- **Simpatía:** Buena imagen corporativa, se aconseja gestionar un sitio web seguro y que aporte contenido valioso.

- **Reciprocidad:** Es importante hacerle sentir al cliente que, en lugar de venderle algún servicio, se le está haciendo un acompañamiento para la solución de un problema y que estaremos dispuestos a ayudarlo en lo que podamos.
- **Consistencia:** Mantener contacto con clientes para brindar apoyo si es necesario.
- **Factor miedo:** El miedo a la pérdida de disponibilidad de los sistemas puede ser un factor de influencia para que los clientes inviertan en servicios de ciberseguridad que cubran su necesidad de ser seguros.

5.1.2 Cómo ofrecer servicios de ciberseguridad

En base a todo lo mencionado en esta sección, se definen a continuación las estrategias de comercialización de servicios de ciberseguridad propuestas;

- Presentar formalmente nuestra empresa de seguridad cibernética enviando una carta de presentación a las empresas que ya hemos identificado como potenciales clientes.
- Organizar un evento de lanzamiento de nuestra firma de seguridad cibernética de tal manera que genere conciencia sobre el valor de nuestros servicios.
- Utilizar plataformas de redes sociales y otras plataformas tecnológicas para comercializar el negocio de seguridad cibernética publicando contenido de valor por medio de infografías.
- Formar un equipo de marketing que de manera cíclica gestione los procesos y estrategias de marketing para atraer nuevos clientes y mantener una buena posición en el mercado.

5.2 Evaluación del nivel de madurez de ciberseguridad basado en el estándar ISO 27002 y CMMI

La información es uno de los activos más importantes de las empresas, pero no es asegurada como se merece. En los últimos años, el desarrollo de las tecnologías de la información ha incrementado la posibilidad de que se generen brechas de seguridad de la información. Con el fin de gestionar los riesgos emergentes, el presente trabajo de titulación propone como estrategia de implementación de los servicios de ciberseguridad una evaluación de capacidades de cibernéticas para conocer el nivel de madurez actual y deseado aplicable a la ciber resiliencia (capacidad de responder adecuadamente a un incidente de ciberseguridad) de cada empresa y así poder proponer soluciones estratégicas y personalizadas a las necesidades de cada industria.

Algunas empresas no dudan en invertir cierto porcentaje de su presupuesto en las tecnologías de la información, aunque la inversión en la seguridad de estas genera un gasto adicional enorme si no se gestiona de manera estratégica. Una evaluación de seguridad de la información es un requisito muy importante para todas las empresas y organizaciones porque se ha demostrado que ayuda a mejorar la eficacia y eficiencia de los procesos comerciales de las empresas reduciendo riesgos operacionales.

Dentro del asesoramiento y evaluación de seguridad de la información, hay varios marcos que se hacen referencia a la gobernanza internacional de la información y que han sido ampliamente aceptadas y probadas como lo es la familia de normativas ISO 27000. Para el presente trabajo se ha tomado como referencia el listado de objetivos y controles de seguridad definidos en la normativa ISO 27002 y en conjunto al modelo de integración de capacidades CMMI se propone una metodología de evaluación estratégica de seguridad de la información la cual sirve como base para la implementación de servicios de ciberseguridad.

Los pasos de la metodología para la evaluación de capacidades de ciberseguridad se pueden ver en la Figura 50.

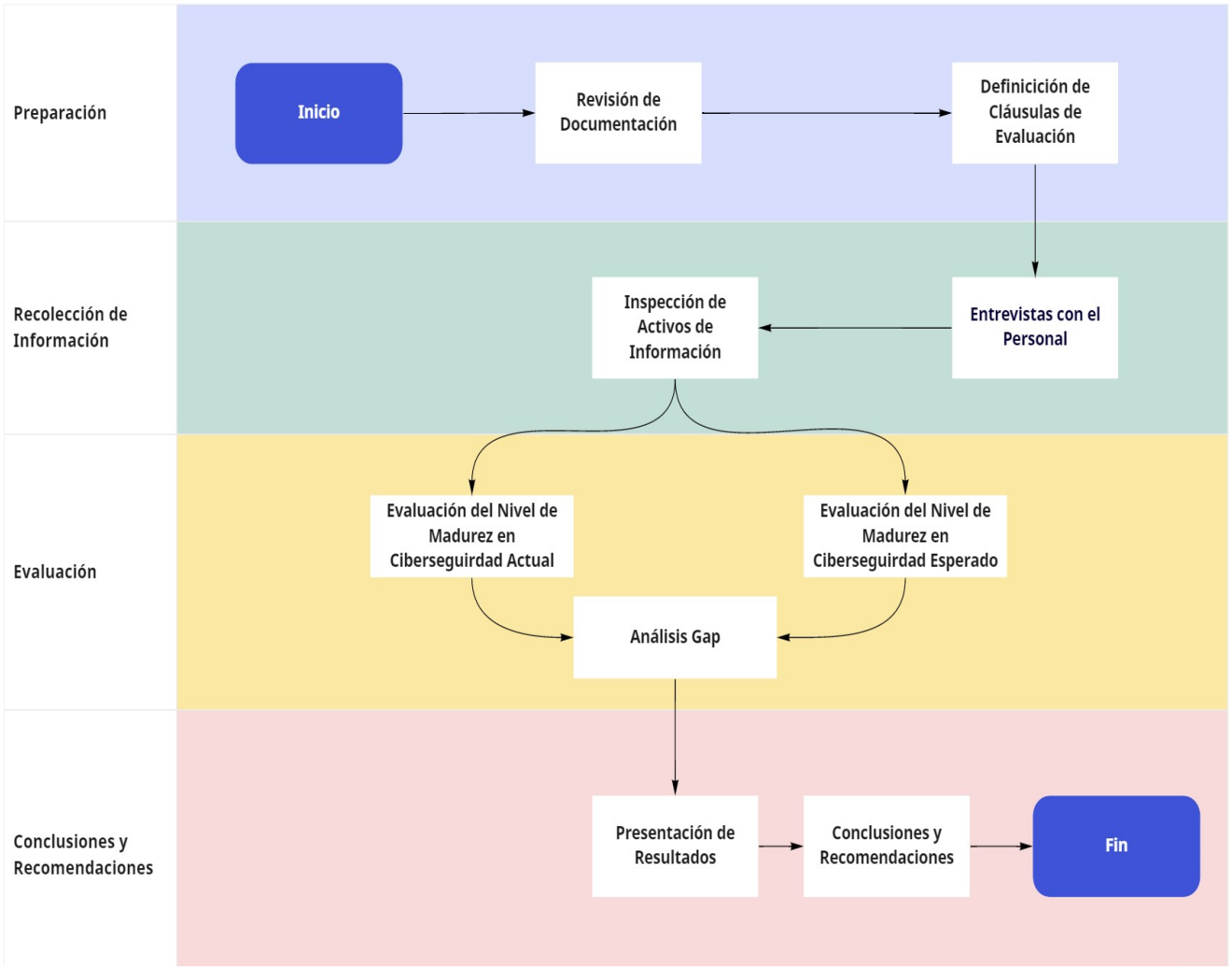


Figura 50. Proceso de Evaluación de Seguridad de la Información. Elaboración Propia.

Dentro de los procesos para la evaluación de seguridad de la información se contempla las siguientes fases:

- **Preparación:** Primeramente, se debe revisar el alcance de la evaluación tomando en cuenta los componentes del sistema críticos (Joyas de la Corona) que almacenen, procesen o transmitan información valiosa para el negocio. Las conexiones entre sistemas también deben ser incluidas en el alcance de la evaluación para verificar que los controles apropiados de seguridad estén implementados para prevenir que un atacante obtenga acceso a la información. Adicionalmente, existen otro tipo de sistemas que deben incluirse en el alcance de la evaluación como son aquellos sistemas proveedores de servicios de seguridad y generalmente todos los sistemas que puedan impactar de forma directa la seguridad de las joyas de la corona. Cabe mencionar que el alcance no se limita a evaluar tecnología, se incluye también procesos y personas.
    - **Personas:** Algunos ejemplos de los roles que deben incluirse en el alcance de la evaluación de seguridad son:
        - Administrador de redes.
        - Administrador de sistemas.
        - Personal de soporte de TI.
        - Desarrolladores de software.
        - Recursos humanos.
        - Oficiales de seguridad.
        - Personal de atención al cliente.
        - Personal de finanzas y contabilidad.
        - Supervisores y gerentes de cada área.
        - Gerentes generales y ejecutivos.

    - **Procesos:** Algunos ejemplos de los procesos que generalmente son incluidos en la evaluación de seguridad son:

        - Procesos y canales de pago.
        - Procesos de respaldo de la información.
        - Reportes periódicos.
        - Procesos legales.
        - Procesos de altas y bajas de personal.

    - **Tecnología:** Los activos tecnológicos generalmente incluidos en la evaluación de seguridad son:
        - Servidores, aplicaciones, redes y dispositivos móviles.
        - Sistemas de seguridad física.
        - Comunicaciones electrónicas.
        - Sitios de almacenamiento de respaldo.
        - Sistemas administrativos.
        - Sistemas de acceso remoto.

- **Recolección de información:** Antes de empezar con la fase de evaluación, es necesario obtener un entendimiento claro del tamaño y complejidad del entorno que será evaluado. Esto incluye la identificación de los tipos de componentes del sistema, la documentación pertinente, el personal involucrado y los procesos que serán analizados. Generalmente esta fase involucra conversaciones con varios representantes de la empresa con el fin de entender sus perspectivas y objetivos de seguridad. Obtener esta información antes de que inicie la evaluación de seguridad puede aumentar la efectividad en la estimación de tiempos y en la identificación de aquellos controles y requerimientos que aplican al contexto empresarial en cuestión mejorando así el resultado final.

- **Evaluación:** Dentro de esta fase se contempla la asignación de una calificación del nivel de madurez en ciberseguridad actual y esperado según el modelo de capacidades CMMI (Definido en el Capítulo I) para cada uno de los dominios de control que define la normativo ISO 27002 los cuales son:
    - Políticas de seguridad.
    - Aspectos organizativos de la Seguridad de la Información.

- Seguridad ligada a los Recursos Humanos.
- Gestión de activos.
- Control de accesos.
- Cifrado.
- Seguridad física y ambiental.
- Seguridad en la operativa.
- Seguridad en las telecomunicaciones.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- Relaciones con proveedores.
- Gestión de incidentes en la Seguridad de la Información.
- Aspectos de la Seguridad de la Información en la gestión de la continuidad de negocio.
- Cumplimiento.

Adicionalmente, se identifican brechas y fortalezas en cada dominio de control los cuales se incluyen en el reporte final de la evaluación de seguridad.

Una vez que se ha asignado la calificación de madurez en ciberseguridad actual y deseada, se realiza un análisis de brechas, o también conocido como análisis GAP, que existe entre estas dos unidades. Para una mejor visualización del análisis se propone realizar gráficos de radar para identificar claramente la diferencia existente entre el valor actual y el deseado del nivel de madurez en ciberseguridad de la empresa evaluada, así como se muestra en la Figura 51.



	CAPACIDAD	NIVEL ACTUAL	NIVEL DESEADO
1	POLÍTICAS DE SEGURIDAD	3	3.5
2	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	1.5	3
3	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	1	4
4	GESTIÓN DE ACTIVOS	3	4
5	CONTROL DE ACCESOS	1	2.5
6	CIFRADO	2.5	3.2
7	SEGURIDAD FÍSICA Y AMBIENTAL	1	3
8	SEGURIDAD OPERATIVA	2.5	3
9	SEGURIDAD EN LAS TELECOMUNICACIONES	1.5	3
10	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	2.8	3
11	RELACIONES CON PROVEEDORES	1	2
12	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	1.5	3.5
13	ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	1	3
14	CUMPLIMIENTO	1.5	3.5

Figura 51. Gráfico de Radar de Evaluación de Seguridad (Ejemplo No Oficial). Elaboración propia.

- **Conclusiones y Recomendaciones:** Para la fase final, se desarrolla y presenta un informe ejecutivo donde se detalla los hallazgos más importantes de la evaluación de seguridad realizada, así como un plan de implementación estratégica de los servicios propuestos en el catálogo que aplicarían al contexto empresarial para poder alcanzar el nivel de madurez deseado para cada uno de los controles de la ISO 27002.

  En la sección 5.3 se detalla el proceso para realizar la planificación estratégica de los servicios de ciberseguridad.

5.3 Planificación de la implementación estratégica de acuerdo con los servicios de ciberseguridad del catálogo

La seguridad cibernética total nunca se puede "lograr". En cambio, elaborar un programa de ciberseguridad es un proceso empresarial necesario que requiere esfuerzos a todos los niveles. Lograr un cambio de comportamiento es significativamente más desafiante que identificar e implementar un conjunto de políticas. El personal y la dirección no solo deben comprender las acciones necesarias y las razones para ellas, sino debe interiorizarse e integrarlos en su comportamiento regular. (The American Public Power Association, 2019).

El éxito de convertir los planes de acción en significativos requiere no solo la implementación de actividades sino la adopción de roles adicionales, responsabilidades y cambios de procesos, así como una combinación de liderazgo ejecutivo y gestión de estrategias. Se requiere capacitación y concientización, revisión y compromiso basados en riesgos, recompensas, disciplina para implementar un cambio significativo, estable y apropiado. (The American Public Power Association, 2019).

En base a la lectura del reporte publicado por (The American Public Power Association, 2019), se describe a continuación las siguientes etapas para desarrollar un plan de ciberseguridad, estas etapas proporcionan guías de prácticas cibernéticas responsables y seguras para que las organizaciones respondan a los incidentes de manera eficiente y efectiva.

Las etapas que se definen son las siguientes:

- **Etapa 1:** Evaluar los factores internos y externos que influyen en los problemas de ciberseguridad más urgentes e identificar oportunidades de mejora.
- **Etapa 2:** Formular un plan para mejorar la ciberseguridad en las áreas identificadas (Se recomienda la participación de un CISO en esta etapa).
- **Etapa 3:** Activar el plan llevando a cabo las actividades de control.
- **Etapa 4:** Integrar las prácticas definidas por el plan en la operación y gestión de riesgos de la organización y hacerlos parte de la cultura de la organización.

A la par del desarrollo del plan de ciberseguridad, debemos definir los servicios que se implementan como parte del proceso de mejora. La tabla muestra la relación entre los servicios del catálogo que en el análisis de mercado tuvieron mayor grado de aceptación y el correspondiente objetivo de control de la normativa ISO 27002 que gestiona.

Objetivos de Control ISO 27002 ↓	Gestión Estratégica de un CISO como servicio	Gestión de accesos y contraseñas	Mitigación de Ataques	Evaluaciones de Seguridad de la Información	Consultoría en Seguridad Cloud	Seguridad Endpoint	Sistema de Monitoreo de Amenazas	Pruebas de Penetración de Seguridad
Políticas de seguridad de la información	X							
Organización de la seguridad de la información	X			X				
Seguridad de los recursos humanos		X		X				
Gestión de activos	X			X				
Control de accesos	X	X		X		X		
Criptografía – Cifrado y gestión de claves	X	X		X		X		
Seguridad física y ambiental				X				

Seguridad operacional			X		X	X	X	X
Seguridad de las comunicaciones		X				X	X	X
Adquisición, desarrollo y mantenimiento de sistemas	X	X	X		X			X
Relación con los proveedores	X			X	X			
Gestión de incidentes de seguridad de la información							X	
Aspectos de seguridad de la información en la gestión de la continuidad del negocio	X		X	X				
Cumplimiento	X			X				

Tabla 37. Relación entre los servicios de ciberseguridad del catálogo propuesto y los objetivos de control de la normativa ISO 27002. Elaboración propia.

5.4 Beneficios de implementar la ciberseguridad de manera estratégica

La gestión de riesgos forma parte fundamental de todos los negocios, la estrategia cibernética puede ayudar a las organizaciones a alcanzar nuevos niveles de éxito por medio de una gestión integral de ciber riesgos el cual incluye un sólido componente de seguridad cibernética. Los avances tecnológicos significan que la seguridad cibernética sigue siendo un enfoque empresarial que requiere una atención seria.

Las empresas deben empezar a incorporar una estrategia de seguridad cibernética eficaz integrada en su política de gestión de riesgos. Con objetivos como la prevención de la pérdida de datos, mejores medidas de seguridad para proteger el sistema y los servicios de red y el control activo de los datos.

Las estrategias de seguridad cibernética pueden tener un gran impacto en la capacidad de una empresa para cumplir sus objetivos y métricas de rendimiento.

Estos son algunos de los beneficios de priorizar un plan de gestión de riesgos de seguridad cibernética de manera estratégica:

- **Mejora la reputación empresarial:** Ya sea que se trabaje con clientes o se venda a clientes, es importante tener en cuenta sus mejores intereses. Una de las mejores formas de generar confianza y desarrollar el negocio es asegurarse de que los datos estén protegidos. Las filtraciones de datos continúan amenazando a las empresas, les cuesta clientes y ganancias, y son noticia de manera negativa. Las organizaciones que priorizan de manera proactiva la seguridad de la información y los datos de sus clientes tienden a hacer más negocios, tener clientes más leales y experimentar más éxito a largo plazo.
- **Resguardo de los ingresos:** Las filtraciones de datos pueden provocar la pérdida de beneficios, así como multas y demandas. Las empresas que tienen una estrategia de gestión de riesgos de seguridad cibernética gastan recursos de la empresa, como la mano de obra de los empleados y el dinero en soluciones de software, pero esta es una inversión en el futuro de la empresa. Mejores medidas de seguridad pueden ayudar a las empresas a minimizar el riesgo de pérdidas inesperadas de recursos por un ataque informático.

- **Ventaja competitiva:** La seguridad cibernética puede abarcar todas las áreas de la empresa; además de proteger los datos de los clientes y empleados, las medidas de seguridad cibernética protegen la información patentada que puede ayudar a las empresas a salir adelante. La estrategia adecuada de gestión de riesgos de seguridad cibernética incluye garantizar que se otorguen los permisos adecuados a los empleados para que los equipos adecuados tengan acceso a los datos correctos. Además, ayuda a evitar que la información empresarial privada se filtre a otras empresas o competidores.

5.4.1 Análisis Financiero

A continuación, se presenta un análisis financiero el cual contempla los siguientes indicadores:

- **VAN (Valor Actual Neto):** El valor actual neto, o VAN, es un método para evaluar los gastos de capital, el VPN se utiliza para determinar si un proyecto o una inversión generarán beneficios y cuándo. El cálculo del VPN se utiliza con un período de tiempo específico para que la empresa pueda ver en qué punto específico pueden esperar un retorno de su inversión; El VAN se expresa como una cantidad en dólares en lugar de un porcentaje. En general, se cree que el VAN es más fácil de entender para las personas que no pertenecen al sector de la planificación financiera. (Indeed, 2021).

  Fórmula: **VAN = FC - (1 + i)** $^{-n}$ − inversión inicial = entrada de efectivo neta esperada recibida en cada período de tiempo

  - i = Tasa de descuento (tasa de rendimiento requerida por período de tiempo).
  - n = Número de períodos de tiempo.
  - FC = Flujo de caja neto.

- **TIR (Tasa Interna de Retorno):** La Tasa Interna de Retorno, o TIR, es un método utilizado para evaluar los gastos de capital. La TIR se utiliza para determinar la tasa de rendimiento de la inversión. Las empresas seleccionan una fecha de finalización y utilizan la TIR para calcular el porcentaje de retorno o pérdida en ese punto del proyecto. La TIR se expresa como un porcentaje en lugar de una cantidad en dólares. La TIR es una métrica compleja que se utiliza con mayor frecuencia dentro de la comunidad empresarial y no como una medida externa. (Indeed, 2021).

  Fórmula: TIR = [-I + [FC / (1 + X) ^ n]] = 0

  - -I = Inversión inicial.
  - FC = Flujo de caja neto.
  - (1 + X) = Tasa de descuento
  - n = periodo de tiempo

- **ROI (Retorno sobre la inversión):** El retorno sobre la inversión es un indicador que mide la relación entre la ganancia obtenida y la inversión de un negocio. Se lo conoce como ROI por sus siglas en inglés (Return Of Investment). Con el ROI puedes evaluar las finanzas de una empresa; si el valor es positivo, significa que obtuviste beneficios económicos por tu inversión; pero si es menor o igual a cero, su significado se traduce a que quienes invirtieron están perdiendo dinero. (Indeed, 2021).

  Fórmula: ROI = (Ganancia – Inversión) / Inversión.

La siguiente tabla muestra un análisis de pérdidas y ganancias suponiendo un incremento del 11% anual tanto en los ingresos como en los costos de venta. El detalle de donde se obtienen los valores de inversión se detalla en la sección de Anexos – 8.3 Justificación del presupuesto y proyecciones de inversión.

Estado de Situación económica o estado de Pérdidas y Ganancias con proyección a 5 años						
Concepto	**Fase inicial - momento 0**	**Año 1**	**Año2**	**Año 3**	**Año 4**	**Año 5**
(-) Inversión Activos Fijos	$ -79,850.00					
(-) Activos Intangibles	$ -21,500.00					
(-) CAPITAL DE TRABAJO	$ -35,595.57					
(+) CRÉDITO RECIBIDO	$ 61,350.00					
INGRESOS OPERACIONALES (Datos de Ingresos Esperados)		$ 200,000.00	$ 222,000.00	$ 246,420.00	$ 273,526.20	$ 303,614.08
(-) COSTOS DE VENTAS (Datos Esperados)		$ 135,373.60	$ 150,264.70	$ 166,793.81	$ 185,141.13	$ 205,506.66
(=) UTILIDAD BRUTA		**$ 64,626.40**	**$ 71,735.30**	**$ 79,626.19**	**$ 88,385.07**	**$ 98,107.43**
(-) Gastos No Operacionales						
(-) Gastos Financieros		$ 9,202.50	$ 7,837.63	$ 6,268.02	$ 4,462.98	$ 2,387.17
(-) Otros Gastos NO Operacionales		$ 7,008.68	$ 7,008.68	$ 7,008.68	$ 7,008.68	$ 7,008.68
(=) UTILIDADES ANTES DE LA PARTICIPACIÓN DE TRABAJADORES		**$ 48,415.22**	**$ 56,889.00**	**$ 66,349.49**	**$ 76,913.41**	**$ 88,711.57**
(-) 15% Participación de Empleados		$ 7,262.28	$ 8,533.35	$ 9,952.42	$ 11,537.01	$ 13,306.74
(=)UTILIDADES ANTES DE IMPUESTOS		**$ 41,152.94**	**$ 48,355.65**	**$ 56,397.06**	**$ 65,376.40**	**$ 75,404.84**
(-) 23% Impuestos a la Renta		$ 9,465.18	$ 11,121.80	$ 12,971.32	$ 15,036.57	$ 17,343.11
(=) UTILIDAD ANTES DE RESERVA LEGAL		**$ 31,687.76**	**$ 37,233.85**	**$ 43,425.74**	**$ 50,339.83**	**$ 58,061.72**
(-) 5% Reserva Legal		$ 1,584.39	$ 1,861.69	$ 2,171.29	$ 2,516.99	$ 2,903.09
(=)UTILIDAD NETA	**$ -75,595.57**	**$ 30,103.37**	**$ 35,372.16**	**$ 41,254.45**	**$ 47,822.84**	**$ 55,158.64**
EVALUACIÓN FINANCIERA						
Aplicar una tasa de interés anual	15.00%	0.15				
1.- VALOR NETO ACTUAL (VNA)						
VAN	$ 59,219.63		Promedio de ingresos netos anuales			
2.- TASA INTERNA DE RETORNO (TIR)			$ 41,942.29			
TIR	41%					
3.- RETORNO DE INVERSIÓN (ROI)			Tiempo de recuperación de la inversión			
ROI	0.78		1.802371007	≈ 2 años		

Tabla 38. Análisis de pérdidas y ganancias suponiendo un incremento del 11% anual tanto en los ingresos como en los costos de venta.

Al obtener un VAN positivo de $59,219.63, esto indica que el proyecto es viable, ya que el valor actual de los flujos es mayor al desembolso inicial de la inversión.

Para el TIR obtenido de 41%, se acepta el proyecto de inversión si el rendimiento de la empresa es mayor que el mínimo fijado como aceptable, en este caso la inversión es económicamente rentable.

Por último, el ROI al ser positivo con un valor de 0.78 es un indicador de que la inversión es viable. Si se tiene una expectativa de ganancias anuales netas promedio de $ 41,942.29, eso quiere decir que la inversión inicial de $ 75,595.57 se recuperará en un periodo menor a 2 años.

6. CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

Producto de la elaboración del presente trabajo de titulación se puede concluir que:

- El catálogo de servicios desarrollado es una propuesta adaptada a los requerimientos, necesidades y expectativas de los clientes, para lo cual se utilizó métodos de análisis estadístico y encuestas dirigidas a profesionales de T.I. con criterios de decisión empresarial.
- Con base en lo descrito en la tabla 35 (Resumen del análisis realizado), los servicios con mayor aceptación en el mercado corresponden al dominio de prevención de amenazas, evidenciando el potencial de negocio que tiene ofrecer este tipo de servicios.
- La propuesta de implementación estratégica de servicios de ciberseguridad basado en el sistema de niveles de madurez CMMI y los objetivos de control de la normativa ISO 27002 parte desde la ejecución del servicio de evaluación de seguridad del cual se obtiene un análisis GAP que permite identificar brechas y puntos específicos donde se requiere generar controles y mejoras que mitiguen los riesgos cibernéticos ofreciendo el beneficio a los clientes de priorizar sus recursos de seguridad en las áreas de mayor criticidad.
- Según el ROI de 0.78 obtenido en el análisis financiero y siendo este un primer estudio, se podría imaginar que la tendencia se mantiene para otros casos de estudio y así poder concluir que invertir en un negocio de ciberseguridad es un proyecto rentable en el que se espera recuperar el monto neto de la inversión inicial en un periodo aproximado de 2 años.
- Una vez analizados los conceptos y definiciones teóricos del estado actual de la ciberseguridad en el Ecuador correspondiente a las secciones 3.3.4 y 3.3.5, se puede considerar al Ecuador como un país inexperto en ciberseguridad y que al manejar una economía dolarizada es foco de atención para un amplio panorama de ciber amenazas.

6.2 Recomendaciones

Producto de la elaboración del presente trabajo de titulación se puede recomendar:

- Con base en la malla curricular de Ingeniería en Sistemas y Computación de la Facultad de Ingeniería de la Pontificia Universidad Católica del Ecuador que he cursado y al presente estudio realizado, se recomienda continuar con estudios estadísticos que abarquen un mayor alcance de análisis para determinar los requerimientos de mercado en servicios de ciberseguridad e instruir a los estudiantes de futuras generaciones con los conocimientos necesarios para cubrir las demandas de profesionales de ciberseguridad emergentes en el futuro.
- Se recomienda adaptar y mejorar el presente modelo de negocio propuesto para promover nuevas oportunidades de trabajo que contemplen la concientización y difusión de la importancia de la ciberseguridad en los entornos corporativos para reducir el riesgo y prevenir las ciber amenazas.
- Tomando como referencia inicial la presente propuesta metodológica, se recomienda generar nuevos modelos de negocio para las tecnologías emergentes como el internet de las cosas (IoT), domótica, realidad aumentada, entre otros, para poder desarrollar servicios competentes a las nuevas necesidades de ciberseguridad de un mundo cada vez más digitalizado.

7. BIBLIOGRAFÍA

Accenture. (2019). *Ninth Annual Cost of Cybercrime Study.* Accenture.

ACIS. (2019). *Ciberriesgo. Aprendizaje de un riesgo sistémico, emergente y disruptivo.* ACIS.

Alfaro, V. (2020). *ESTRATEGIA DE NEGOCIO PARA EL SERVICIO DE CIBERSEGURIDAD ENTEL S.A.* Santiago de Chile: Universidad de Chile.

Almeida, C. A., & Recalde, L. (2019). LA CIBERSEGURIDAD EN EL ECUADOR, UNA PROPUESTA DE. *Revista de Ciencias de Seguridad y Defensa*, 156.

Arnoldo Hax, N. M. (2018). *Lecciones en Estrategia, Hacia una gestión de excelencia.*

Arroyo Guardeño, D., Gayoso Martínez, V., & Hernández Encinas, L. (2020). *¿Qué sabemos de Ciberseguridad?* Madrid: Los Libros de la Catarata.

AXELOS. (2019). *WELCOME TO THE FUTURE OF ITIL*. Obtenido de AXELOS: https://www.axelos.com/welcome-to-itil-4

BuenTrip Hub. (2020). *Radar Tech Startup.*

Chávez, R. (2020). *ESTADO ACTUAL DE LA CIBERSEGURIDAD EN EL ECUADOR 2020.* Quito - Ecuador: Revista IT Ahora.

Comunicaciones. (22 de 07 de 2019). *Modelo CMMI, calidad y buenas prácticas en el desarrollo de software*. Obtenido de Globalbit: https://www.globalbit.co/2019/07/22/modelo-cmmi-calidad-y-buenas-practicas-en-el-desarrollo-de-software/

Cyber Management Alliance. (11 de Mayo de 2021). *Protect Your Business from Cyber Threats in 2021*. Obtenido de Cyber Managements Alliance: https://www.cm-alliance.com/cybersecurity-blog/protect-your-business-from-cyber-threats-in-2021

Cybersecurity Ventures . (2021). *Costs of Cybercrime* . Cybersecurity Ventures .

Deloitte. (2020). Estado Actual de Cibersiguridad Ecuador. *Revista IT Ahora*, 17-18.

Deloitte. (2021). *¿Qué es Capability Maturity Model Integration? (CMMI)*. Obtenido de Deloitte: https://www2.deloitte.com/es/es/pages/technology/articles/que-es-cmmi-capability-maturity-model-integration.html

Dion, J. (Junio de 2020). *Risk Management for Cybersecurity and IT Managers.* Obtenido de https://www.udemy.com/course/risk-management-for-cybersecurity/

EMBROKER. (April de 2021). *2021 Must-Know Cyber Attack Statistics and Trends*. Obtenido de EMBROKER: https://www.embroker.com/blog/cyber-attack-statistics/

ESET. (05 de Febrero de 2020). *Cuáles son las diferencias entre un Proxy y una VPN*. Obtenido de welivesecurity: https://www.welivesecurity.com/la-es/2020/02/05/diferencias-entre-proxy-vpn/

E-SPIN. (21 de August de 2019). *What is a Cyber Security Vulnerability Assessment?* Obtenido de E-SPIN: https://www.e-spincorp.com/what-is-a-cyber-security-vulnerability-assessment/

Fandom. (2021). *Principios de la seguridad informática: Confidencialidad, Integridad y Disponibilidad de la información*. Obtenido de Fandom.

Foro Económico Mundial. (2020). *Series Futuras: Ciberseguirdad, tecnologías emergentes y riesgo sistemático.* Ginebra: Foro Económico Mundial.

Freshworks Inc. (3 de Enero de 2019). *ITIL 4*. Obtenido de Freshservice: https://freshservice.com/itil/itil-4

Fruhlinger, J. (2021). *Does it matter who the CISO reports to?* PricewaterhouseCoopers.

Gartner. (2018). *Magic Quadrant for Managed Security Services.* Worldwide.

GeeksforGeeks. (30 de March de 2020). *Difference between Network Security and Cyber Security*. Obtenido de GeeksforGeeks: https://www.geeksforgeeks.org/difference-between-network-security-and-cyber-security/

IDC, International Data Corporation. (2017). *Cybersecurity Focus Leads to Security Spending Growth of Over 10%, Services Lead the Way.* New Jersey: IDC.

INCIBE. (2016). *Tendencias en el mercado de la Ciberseguridad.* Madrid: INCIBE.

Indeed. (15 de 09 de 2021). *Net Present Value (NPV) vs. Internal Rate of Return (IRR)*. Obtenido de Indeed: https://www.indeed.com/career-advice/career-development/npv-vs-irr

Insureon. (2021). *How to start a cybersecurity company*. Obtenido de Insureon: https://www.insureon.com/blog/how-to-get-into-the-cybersecurity-industry

ISO/IEC. (Agosto de 2013). *ISO/IEC 27002:2013*. Obtenido de ISO: https://www.iso.org/standard/54533.html

Larry, M. &. (2005).

Martins, A. T. (2021). *How to Write a Cyber Security Business Plan.* Obtenido de Profitableventure: https://www.profitableventure.com/cyber-security-business-plan/

Muguira, A. (2020). *¿Qué es la escala de Likert y cómo utilizarla?* Obtenido de Question Pro: https://www.questionpro.com/blog/es/que-es-la-escala-de-likert-y-como-utilizarla/amp/

Muguira, A. (2020). *¿Qué es una tabla de contingencia?* Obtenido de QuestionPro: https://www.questionpro.com/blog/es/que-es-una-tabla-de-contingencia/

NRD Cyber Security . (2019). *Panorama de Ciber amenazas en Ecuador.* Kaunas: NRD Cyber Security .

OEA & BID. (2020). *RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE.* Observatorio de Ciberseguridad.

OPENTEXT. (2020). *Security Services.*

PECB. (2021). *ISO/IEC 27032 Cyber Security Trainings.* PECB MAGAZINE.

Ponemon. (2019). *Read the 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses to learn how to protect your business.* State of Cybersecurity Report.

Porter, M. (2020). Cybersecuirty Marketing Simplified. (H. W. Networks, Entrevistador)

Ross, R. G. (2020). *Business Knowledge Blueprints: Enabling Your Data to Speak the Language of the Business.*

Stine, R., & Foster, D. (2018). *Statistics for Business.*

Superintendencia de Compañías, Valores y Seguros del Ecuador. (2021). *Estudios Sectoriales – SUPERCIAS.* Quito.

Thakur, K., & Al-Sakib, K. (2020). *Cibersecurity Fundamentals: A Real-World Perspective.* New Jersey: CRC Press.

The American Public Power Association. (2019). *Public Power Cybersecurity Roadmap.*

Vargas, R., Reyes, R., & Recalde, L. (2017). *Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa.* Sangolquí - Ecuador: URVIO. REVISTA LATINOAMERICANA DE ESTUDIOS DE SEGURIDAD (JUNIO-NOVIEMBRE) /.

Virk, R. (2020). *Startup Myths and Models.*

X.Martin, D. (2019). *Cybersecurity As A Business Strategy*. Obtenido de Corporate Board Member: https://boardmember.com/cybersecurity-as-a-business-strategy/

8. ANEXOS

8.1 Glosario de términos.

TIC: Tecnologías de la Información y Comunicación

ISO 27002: Estándar para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional.

CMMI: Modelo para la mejora y evaluación de procesos para el desarrollo, mantenimiento y operación de sistemas informáticos.

IEC: La Comisión Electrotécnica Internacional, es una organización de normalización en los campos: eléctrico, electrónico y tecnologías relacionadas.

Criptografía: Ámbito de la criptología que se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

DPI: Derecho de Propiedad Intelectual.

ITIL: La Biblioteca de Infraestructura de Tecnologías de Información es un conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general.

Stakeholder: También llamado "El interesado", "parte interesada" o "involucrado" es una persona, organización o empresa que tiene interés en una empresa u organización dada**.**

SLA: Acuerdo de nivel de servicio.

Framework: Marco de trabajo.

Hacker: Persona con grandes conocimientos de informática que se dedica a detectar fallos de seguridad en sistemas informáticos.

Malware: Programa maligno.

Spam: Correo no deseado.

Spyware: Programa destinado a violar la privacidad de un individuo.

Outsourcing: Herramienta que permite contratar a un proveedor externo a la empresa para la ejecución de actividades secundarias.

MSSP: Proveedores de Servicios de Seguridad Administrados.

MSS: Servicio de Seguridad Administrado.

Retail: Sector económico que engloba a las empresas especializadas en la comercialización masiva de productos o servicios uniformes a grandes cantidades de clientes.

Player nicho: Empresas enfocadas en servir a un mercado o región local.

Telcos: Proveedor de servicios de telecomunicaciones.

Due Diligence: Investigación de una empresa o persona previa a la firma de un contrato o una ley con cierta diligencia de cuidado.

SIEM: Sistema de Gestión de Eventos e Información de Seguridad es un sistema que centraliza el almacenamiento y la interpretación de los datos relevantes de seguridad.

Análisis GAP: Análisis que implica la comparación del desempeño real con el desempeño potencial o deseado.

DDoS: Ataque de denegación de servicio distribuido.

VAN: Valor Actual Neto.

TIR: Tasa Interna de Retorno.

ROI: Retorno sobre la inversión.

8.2 Estructura de las encuestas realizadas.

Encuesta para el estudio de los requerimientos de mercado en servicios de ciberseguridad

Empresa: _____

Nombre: _____

Cargo: _____

Teléfono: _____

E-mail: _____

El objetivo de la siguiente encuesta es conocer y priorizar aquellos servicios en el área de ciberseguridad categorizados en 3 dominios (Prevención, Detección y Respuesta) que aplican a los principales nichos de mercado en el Ecuador, para cumplir con este objetivo las encuestas serán dirigidas a gerentes de sistemas y profesionales de T.I. de distintas empresas.

A continuación, se le presentará una serie de preguntas que describen varios servicios de ciberseguridad, para responder debe considerar el grado de importancia que usted le asignaría a cada servicio, si lo implementaría dentro de su empresa, el monto que estaría dispuesto a pagar y el tiempo estimado de implementación. Marque con una x según su consideración o escriba sus costos y tiempos de implementación estimados donde observe este espacio en blanco "_____" si ninguna de las opciones propuestas va de acuerdo con su criterio.

Nota: Los precios y tiempos presentados en la cuesta son valores promedios, los costos y tiempos reales de implementación dependerán principalmente del tamaño del negocio, el tipo de industria a la que pertenece y sus objetivos.

Preguntas del dominio #1 (Prevención):

1. El rol de un CISO (Jefe de Seguridad de la Información) es crucial para una buena estrategia de ciberseguridad. Al no siempre contar con personas capacitadas para desempeñar este rol en las empresas y al ser limitado el presupuesto para ciberseguridad, ¿Qué tan importante consideraría ofrecer la **Gestión Estratégica de un CISO como servicio**?
    a) Nada Importante ☐
    b) Poco Importante ☐
    c) Moderadamente Importante ☐
    d) Importante ☐
    e) Muy Importante ☐

2. ¿Usted implementaría este servicio en su empresa?
    a) Sí ☐
    b) No ☐
3. Considerando que este tipo de servicio tiene un tiempo prolongado de implementación ¿Cuál sería el tiempo y costos estimados que usted consideraría adecuados para implementar este servicio?
    a) ☐ 3 meses con un presupuesto de USD 12,500.00
    b) ☐ 6 meses con un presupuesto de USD 20,000.00
    c) ☐ 12 meses con un presupuesto de USD 36,000.00
    d) ☐ _____ meses con un presupuesto de USD _____

4. Para la seguridad de un entorno corporativo es necesario saber cómo se está gestionando las contraseñas y los accesos, asegurarse de que el personal no esté reutilizando las mismas contraseñas en todas partes, saber quién tiene acceso a qué y por qué, saber si los delincuentes informáticos pueden robar fácilmente las contraseñas de los empleados. En base a lo mencionado anteriormente. ¿Qué tan importante consideraría ofrecer un servicio de **Gestión de accesos y contraseñas**?
    a) Nada Importante ☐
    b) Poco Importante ☐
    c) Moderadamente Importante ☐
    d) Importante ☐
    e) Muy Importante ☐

5. ¿Usted implementaría este servicio en su empresa?
    a) Sí ☐
    b) No ☐

6. Considerando que este tipo de servicio tiene un tiempo prolongado de implementación ¿Cuál sería el tiempo y costos estimados que usted consideraría adecuados para implementar este servicio?
    a) ☐ Pago mensual con un presupuesto de USD 25.00 por usuario.
    b) ☐ 6 meses con un presupuesto de USD 120.00 por usuario.
    c) ☐ 12 meses con un presupuesto de USD 200.00 por usuario.
    d) ☐ _____ meses con un presupuesto de USD _____

7. La **Mitigación de Ataques** es un servicio que verifica los controles de mitigación para varios tipos de ataques cibernéticos como: compromiso cuentas, acceso no autorizado, ransomware, intrusiones en la red, infecciones de malware, sabotaje, violaciones de las políticas de seguridad y más. ¿Cuál es el grado de importancia que le daría a este tipo de servicio?
    a) Nada Importante ☐
    b) Poco Importante ☐
    c) Moderadamente Importante ☐
    d) Importante ☐
    e) Muy Importante ☐

8. ¿Usted implementaría este servicio en su empresa?
    a) Sí ☐
    b) No ☐

9. Considerando que este tipo de servicio tiene un tiempo prolongado de implementación ¿Cuál sería el tiempo y costos estimados que usted consideraría adecuados para implementar este servicio?
    a) ☐ 3 meses con un presupuesto de USD 3,500.00
    b) ☐ 6 meses con un presupuesto de USD 5,000.00
    c) ☐ 12 meses con un presupuesto de USD 9,200.00
    d) ☐ _____ meses con un presupuesto de USD _____

10. Las **Evaluaciones de Seguridad de la Información** ayudan a conocer qué áreas de su negocio necesitan mayor protección y qué controles conviene aplicar. ¿Cuál es el grado de importancia que le daría a este tipo de servicio?
    a) Nada Importante ☐
    b) Poco Importante ☐
    c) Moderadamente Importante ☐
    d) Importante ☐
    e) Muy Importante ☐

11. ¿Usted implementaría este servicio en su empresa?
    a) Sí ☐
    b) No ☐

12. Considerando que este tipo de servicio tiene un tiempo prolongado de implementación ¿Cuál sería el tiempo y costos estimados que usted consideraría adecuados para implementar este servicio?
    a) ☐ 3 meses con un presupuesto de USD 10,500.00
    b) ☐ 6 meses con un presupuesto de USD 16,000.00
    c) ☐ 12 meses con un presupuesto de USD 26,000.00
    d) ☐ _____ meses con un presupuesto de USD _____

13. ¿En qué grado considera importante un servicio de **Desarrollo Seguro de Software** en el cual se brinde asesoramiento en la creación, desarrollo, integración, ¿despliegue y pruebas para gestionar las posibles vulnerabilidades y crear un entorno seguro de desarrollo?
    a) Nada Importante ☐
    b) Poco Importante ☐
    c) Moderadamente Importante ☐
    d) Importante ☐
    e) Muy Importante ☐

14. ¿Usted implementaría este servicio en su empresa?
    a) Sí ☐
    b) No ☐

15. Considerando que este tipo de servicio tiene un tiempo prolongado de implementación ¿Cuál sería el tiempo y costos estimados que usted consideraría adecuados para implementar este servicio?
    a) ☐ 3 meses con un presupuesto de USD 4,500.00
    b) ☐ 6 meses con un presupuesto de USD 7,000.00
    c) ☐ 12 meses con un presupuesto de USD 10,500.00
    d) ☐ _____ meses con un presupuesto de USD _____

16. Una de las tendencias actuales en tecnología son los servicios Cloud tales como Amazon Web Services, Azure y Google Cloud los cuales cuentan con cientos de configuraciones de seguridad. ¿En qué grado considera importante un servicio de **Consultoría en Seguridad Cloud** que ayude a configurar un entorno o migración segura a la nube?
    a) Nada Importante ☐
    b) Poco Importante ☐
    c) Moderadamente Importante ☐
    d) Importante ☐
    e) Muy Importante ☐

17. ¿Usted implementaría este servicio en su empresa?
    a) Sí ☐
    b) No ☐

18. Considerando que este tipo de servicio tiene un tiempo prolongado de implementación ¿Cuál sería el tiempo y costos estimados que usted consideraría adecuados para implementar este servicio?
    a) ☐ 3 meses con un presupuesto de USD 1,250.00 por aplicación o plataforma
    b) ☐ 6 meses con un presupuesto de USD 2,000.00 por aplicación o plataforma
    c) ☐ 12 meses con un presupuesto de USD 3,250.00 por aplicación o plataforma
    d) ☐ _____ meses con un presupuesto de USD _____ por aplicación o plataforma

19. Comúnmente el punto más débil dentro de una organización es el factor humano debido a la falta de capacitación en conceptos básicos de ciberseguridad. ¿En qué grado considera importante un servicio de **Capacitación en Ciberseguridad** para los empleados de una organización ayudando a convertirlos en una primera línea de defensa sólida?
    a) Nada Importante ☐
    b) Poco Importante ☐
    c) Moderadamente Importante ☐
    d) Importante ☐
    e) Muy Importante ☐

20. ¿Usted implementaría este servicio en su empresa?
    a) Sí ☐
    b) No ☐

21. ¿Cuál sería el tiempo y costos estimados que usted consideraría adecuados para implementar este servicio?
    a) ☐ 3 sesiones en con un presupuesto de USD 35.00 por persona
    b) ☐ 6 sesiones en con un presupuesto de USD 34.00 por persona
    c) ☐ 12 sesiones con un presupuesto de USD 49.50 por persona
    d) ☐ _____ sesiones con un presupuesto de USD _____ por persona

Preguntas del dominio #2 (Detección):

22. ¿En qué grado considera importante contar con un servicio de **Seguridad Endpoint** que a diferencia de un antivirus (El cual funciona con firmas de ataques ya registradas previamente), provee seguridad proactiva a dispositivos como laptops y celulares de ataques avanzados de hacking evitando la explotación de estos dispositivos a través de documentos maliciosos, scripts, vulnerabilidades recientes, etc?
    a) Nada Importante ☐
    b) Poco Importante ☐
    c) Moderadamente Importante ☐
    d) Importante ☐
    e) Muy Importante ☐

23. ¿Usted implementaría este servicio en su empresa?
    a) Sí ☐
    b) No ☐

24. ¿Cuál sería el tiempo y costos estimados que usted consideraría adecuados para implementar este servicio?
    a) ☐ Pago mensual con un presupuesto de USD 25.00 por dispositivo.
    b) ☐ 6 meses con un presupuesto de USD 120.00 por dispositivo.
    c) ☐ 12 meses con un presupuesto de USD 200.00 por dispositivo.
    d) ☐ _____ meses con un presupuesto de USD _____

25. ¿En qué grado considera importante contar con un **Sistema de Monitoreo de Amenazas** que le notifique cuando un sistema se vea comprometido o se haya violado la seguridad de este?
    a) Nada Importante ☐
    b) Poco Importante ☐
    c) Moderadamente Importante ☐
    d) Importante ☐
    e) Muy Importante ☐

26. ¿Usted implementaría este servicio en su empresa?
    a) Sí ☐
    b) No ☐

27. ¿Cuál sería el tiempo y costos estimados que usted consideraría adecuados para implementar este servicio?
    a) ☐ Pago mes a mes con un presupuesto de USD 1,500.00
    b) ☐ 6 meses con un presupuesto de USD 7,200.00
    c) ☐ 12 meses con un presupuesto de USD 11,800.00
    d) ☐ _____ meses con un presupuesto de USD _____

28. ¿En qué grado considera importante contar con un servicio de **Pruebas de Penetración de Seguridad**, en el cual profesionales con conocimientos de hacking ético asumen el rol de un atacante, penetran en los sistemas y realizan un informe detallado con las vulnerabilidades encontradas y los procedimientos realizados para hackear el sistema?
    a) Nada Importante ☐
    b) Poco Importante ☐
    c) Moderadamente Importante ☐
    d) Importante ☐
    e) Muy Importante ☐

29. ¿Usted implementaría este servicio en su empresa?
    a) Sí ☐
    b) No ☐

30. ¿Cuál sería el tiempo y costos estimados que usted consideraría adecuados para implementar este servicio?
    a) ☐ 3 meses con un presupuesto de USD 10,500.00
    b) ☐ 6 meses con un presupuesto de USD 16,000.00
    c) ☐ 12 meses con un presupuesto de USD 27,500.00
    d) ☐ _____ meses con un presupuesto de USD _____

31. Un delincuente informático, malware o cualquier otra amenaza cibernética puede permanecer dentro de un sistema por años sin ser detectado, esperando la oportunidad ideal para realizar su ataque. ¿En qué grado considera importante implementar un servicio de **Threat Hunting (Cacería de Amenazas)** para detectar y descubrir de manera proactiva cualquier intruso dentro de sus sistemas?
    a) Nada Importante ☐
    b) Poco Importante ☐
    c) Moderadamente Importante ☐
    d) Importante ☐
    e) Muy Importante ☐

32. ¿Usted implementaría este servicio en su empresa?
    a) Sí ☐
    b) No ☐

33. Considerando que este tipo de servicio tiene un tiempo prolongado de implementación y el nivel de especialización para proveer este servicio es alto ¿Cuál sería el tiempo y costos estimados que usted consideraría adecuados para implementar este servicio?
    a) ☐ 3 meses con un presupuesto de USD 20,500.00
    b) ☐ 6 meses con un presupuesto de USD 32,000.00
    c) ☐ 12 meses con un presupuesto de USD 52,500.00
    d) ☐ _____ meses con un presupuesto de USD _____

34. Muchas empresas han sufrido fuga o robo de información sin ni siquiera saberlo, esta información puede ser comercializada en la Dark Web (Red Oscura), un lugar de internet difícil de acceder y donde se comercializa ilegalmente la información robada por ciberdelincuentes, esto puede afectar gravemente la reputación de cualquier organización si su información cae en las manos equivocadas. ¿En qué grado considera importante un servicio de **Monitoreo de la Dark Web** para conocer si su información corporativa, como credenciales de acceso, nombres de usuario, contraseñas, etc, está comprometida?
    a) Nada Importante ☐
    b) Poco Importante ☐
    c) Moderadamente Importante ☐
    d) Importante ☐
    e) Muy Importante ☐

35. ¿Usted implementaría este servicio en su empresa?
    a) Sí ☐
    b) No ☐

36. ¿Cuál sería el tiempo y costos estimados que usted consideraría adecuados para implementar este servicio?
    a) ☐ Pago mes a mes con un presupuesto de USD 12.50 por usuario
    b) ☐ 6 meses con un presupuesto de USD 60.00 por usuario
    c) ☐ 12 meses con un presupuesto de USD 98.00 por usuario
    d) ☐ _____ meses con un presupuesto de USD _____ por usuario

Preguntas del dominio #3 (Respuesta):

37. Dentro de un sistema es imposible alcanzar una seguridad total del mismo, los incidentes pueden suceder en cualquier momento. ¿En qué grado considera importante contar con un servicio de **Respuesta a Incidentes** 24/7 que gestione y límite un impacto significativo independientemente de la escala del incidente de seguridad?
    a) Nada Importante ☐
    b) Poco Importante ☐
    c) Moderadamente Importante ☐
    d) Importante ☐
    e) Muy Importante ☐

38. ¿Usted implementaría este servicio en su empresa?
    a) Sí ☐
    b) No ☐

39. Considerando que este tipo de servicio tiene un tiempo prolongado de implementación y el nivel de especialización para proveer este servicio es alto. ¿Cuál sería el tiempo y costos estimados que usted consideraría adecuados para implementar este servicio?
    a) ☐ 3 meses con un presupuesto de USD 30,500.00
    b) ☐ 6 meses con un presupuesto de USD 48,800.00
    c) ☐ 12 meses con un presupuesto de USD 80,200.00
    d) ☐ _____ meses con un presupuesto de USD _____

40. La única manera de mejorar después de sufrir un incidente es investigar las causas que lo ocasionaron ¿Considera importante implementar un servicio de **Investigación Digital Forense** capaz de realizar análisis en la red, discos de memoria, dispositivos móviles y análisis de malware para conocer cuáles fueron las brechas de seguridad que generaron un incidente?
    a) Nada Importante ☐
    b) Poco Importante ☐
    c) Moderadamente Importante ☐
    d) Importante ☐
    e) Muy Importante ☐

41. ¿Usted implementaría este servicio en su empresa?
    a) Sí ☐
    b) No ☐

42. Considerando que este tipo de servicio tiene un tiempo prolongado de implementación ¿Cuál sería el tiempo y costos estimados que usted consideraría adecuados para implementar este servicio?
    a) ☐ 3 meses con un presupuesto de USD 5,500.00
    b) ☐ 6 meses con un presupuesto de USD 8,000.00
    c) ☐ 12 meses con un presupuesto de USD 14,500.00
    d) ☐ _____ meses con un presupuesto de USD _____

8.3 Evidencia de las encuestas realizadas

Para ver el repositorio de las encuestas acceder a los siguientes enlaces:

- https://docs.google.com/forms/d/1x-YfHFjod-utFiMUY0DBBAs6j5kVolQgD00bpqeybqA/edit?usp=sharing
- https://docs.google.com/spreadsheets/d/1gQagxnv-ZzPfEZ3_8_S9KLhKKCyqyZNH/edit?usp=sharing&ouid=102209464718506186306&rtpof=true&sd=true

8.4 Justificación del presupuesto y proyecciones de inversión.

ACTIVOS

ACTIVO FIJO	CARACTERÍSTICA	CANTIDAD	COSTO UNITARIO	COSTO TOTAL
VEHÍCULOS				
Camioneta	Toyota Hilux Cabina Simple 2.5 D-4D Manual 5v. GX 2.5 Diésel D-4D (Diésel) Manual 5 velocidades	2	$ 30,000.00	$ 60,000.00
TOTAL VEHÍCULOS				**$ 60,000.00**
MUEBLES Y ENSERES				
Estantería metálica	Estantes metálicos estándar	4	$ 1,500.00	$ 6,000.00
TOTAL MUEBLES Y ENSERES				**$ 6,000.00**
MUEBLES DE OFICINA				
Mesa de reuniones	Mesa con tablero de MDF y patas metálicas para reuniones de 8 personas	1	$ 320.00	$ 320.00
Escritorios estándar	Escritorios estándar con cajones y patas metálicas, tablero laminado con rudones	8	$ 270.00	$ 2,160.00
Escritorios en L	Escritorios en L - para estación de trabajo con patas metálicas, y tablero laminado con rudones	4	$ 350.00	$ 1,400.00
Sillas giratorias	Sillas giratorias con apoyabrazos tapizada en tela o cuerina	12	$ 85.00	$ 1,020.00

Sillas simples	Sillas simples tapizadas en corrosil, color negro de estructura en hierro niquelado.	10	$ 25.00	$ 250.00
TOTAL MUEBLES DE OFICINA				**$ 5,150.00**
EQUIPO DE OFICINA				$ -
Central Telefónica	Central telefónica “SIEMENS” apta para dos líneas simultáneas y con seis extensiones	1	$ 220.00	$ 220.00
TOTAL EQUIPO DE OFICINA				**$ 220.00**
EQUIPO DE COMPUTACIÓN				
COMPUTADORA	computadoras de escritorio Intel Corei 5, disco duro 500 gb, sata(expandible), memoria 8 gb, dvd writer 22 xl, lector de tarjetas sd 7-1 puertos usb 3.0, case atx 650w niutek, teclado, mouse y parlantes, monitor lcd lg-sansumg 18.5.	12	$ 620.00	$ 7,440.00
IMPRESORA	Impresoras multifunción a tinta continua Epson L355	4	$ 260.00	$ 1,040.00
TOTAL EQUIPO DE COMPUTACIÓN				**$ 8,480.00**
TOTAL ACTIVOS FIJOS	**COMPRENDE LA SUMATORIA DE LOS TOTALES DE VEHÍCULOS, MUEBLES Y ENSERES, MUEBLES DE OFICINA, EQUIPOS DE OFICINA Y EQUIPOS DE COMPUTACIÓN.**			**$ 79,850.00**

ACTIVO	VALOR TOTAL ($)	AÑOS DE VIDA ÚTIL	% DE DEPRECIACIÓN ANUAL	DEPRECIACIÓN POR AÑOS EXPRESADA EN DÓLARES ($)					VALOR RESIDUAL
				AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5	
VEHÍCULOS	$ 60,000.00	5	20%	12,000.00	12,000.00	12,000.00	12,000.00	12,000.00	$ -
MUEBLES Y ENSERES	$ 6,000.00	10	10%	600.00	600.00	600.00	600.00	600.00	$ 3,000.00
MUEBLES DE OFICINA	$ 5,150.00	10	10%	515.00	515.00	515.00	515.00	515.00	$ 2,575.00
EQUIPO DE OFICINA	$ 220.00	10	10%	22.00	22.00	22.00	22.00	22.00	$ 110.00
EQUIPO DE COMPUTACIÓN	$ 8,480.00	3	33.3333 %	2,826.67	2,826.67	2,826.67			$ 0.00
TOTAL DEPRECIACIÓN				15,963.67	15,963.67	15,963.67	13,137.00	13,137.00	5,685.00

ACTIVOS INTANGIBLES

RUBRO	COSTO TOTAL ($)
GASTOS DE CONSTITUCIÓN	$ 1,500.00
PATENTES Y MARCAS	$ 1,000.00
SISTEMAS INFORMÁTICOS (PARA GESTIÓN Y CONTABILIDAD)	$ 5,000.00
SISTEMAS INFORMÁTICOS (PARA OPERACIÓN)	$ 12,000.00
MARKETING Y PUBLICIDAD	$ 2,000.00
TOTAL	**$ 21,500.00**

DESCRIPCIÓN	VALOR ($)	PORCENTAJE DE AMORTIZACIÓN	AÑOS DE AMORTIZACIÓN	AMORTIZACIÓN POR AÑO EXPRESADA EN DÓLARES				
				AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5
GASTOS DE CONSTITUCIÓN	$ 1,500.00	25%	6	$ 250.00	$ 250.00	$ 250.00	$ 250.00	$ 250.00
PATENTES Y MARCAS	$ 1,000.00	25%	6	$ 166.67	$ 166.67	$ 166.67	$ 166.67	$ 166.67
SISTEMAS INFORMÁTICOS (PARA GESTIÓN Y CONTABILIDAD)	$ 5,000.00	25%	6	$ 833.33	$ 833.33	$ 833.33	$ 833.33	$ 833.33
SISTEMAS INFORMÁTICOS (PARA OPERACIÓN)	$ 12,000.00	25%	6	$ 833.33	$ 833.33	$ 833.33	$ 833.33	$ 833.33
MARKETING Y PUBLICIDAD	$ 2,000.00	25%	6	$ 2,000.00	$ 2,000.00	$ 2,000.00	$ 2,000.00	$ 2,000.00
TOTAL	**$ 21,500.00**	**25%**	**6**	**$ 4,083.33**	**$ 4,083.33**	**$ 4,083.33**	**$ 4,083.33**	**$ 4,083.33**

GASTOS ADMINISTRATIVOS	REQUERIMIENTOS
Arriendo oficina administrativa	$ 550 mensuales (de acuerdo con investigaciones del costo de oficinas aptas para la actividad económica propuesta, en el sector de la Mariana de Jesús)
Pago servicios básicos de la oficina (luz, agua, internet)	$ 80 mensuales (de acuerdo con el consumo de empresas similares, investigación llevada a cabo en el sector)
Pago de sueldo a un administrador general	$ 2000 mensuales (de acuerdo con el mercado laboral)
Pago de sueldo a un contador	$ 600 mensuales (de acuerdo con el mercado laboral)
Pago de sueldo a una secretaria recepcionista	$ 400 mensuales (de acuerdo con el mercado laboral)
Pago de sueldo a personal técnico	$ 700 mensuales por trabajador, se requiere mínimo 3 (de acuerdo con el mercado laboral)
Compra de suministros de oficina	$ 100 cada tres meses (no será tan necesario dado que se gestiona la mayoría de los documentos en un repositorio TEAMS)

Compra de activos menores	$ 100 cada tres meses (los activos menores, como se explicó en la presupuestación de activos fijos, son activos cuyo valor monetario es mínimo, ejemplo cuadros, floreros, adornos, manteles, y similares; de la misma forma se presupuestan en base a las necesidades internas de la empresa de estos artículos en relación con los precios en el mercado, respaldando con proformas los mismos.)
GASTOS DE VENTA	**REQUERIMIENTOS EN DÓLARES**
Pago sueldo a un jefe de ventas	$2000 mensuales más comisiones (de acuerdo con el mercado laboral)
Pago sueldo a vendedores	Se contará con dos vendedores, a cada uno se le pagará fijo $ 500 dólares (de acuerdo con el mercado laboral y el tamaño del mercado, en este caso).
Viáticos	Este rubro incluye movilización y gastos menores que requieren los vendedores para llevar a cabo su trabajo; de acuerdo con investigaciones de la actividad económica y específicamente para este ejemplo este rubro es de $ 1.500 mensuales
Suministros de limpieza	$15 mensuales, destinados a la compra de desinfectantes, trapeadores, ambientales y similares.

GASTOS DE ADMINISTRACIÓN			
CONCEPTO	**PARCIAL**	**PRESUPUESTO ANUAL**	**CÁLCULO**
Arriendo oficina administrativa		**$ 6,600.00**	$ 550 mensuales por 12 meses
Servicios básicos administración		**$ 960.00**	$ 80 mensuales por 12 meses
Sueldos y salarios personal administrativo		**$ 50,400.00**	Sumatoria de los sueldos anuales del personal del área
Pago de sueldo a un administrador general	$ 24,000.00		$2000 mensuales por 12 meses
Pago de sueldo a un contador	$ 7,200.00		$ 600 mensuales por 12 meses
Pago de sueldo a una secretaria recepcionista	$ 4,800.00		$ 400 mensuales por 12 meses
Pago de sueldo a los 3 trabajadores técnicos	$ 14,400.00		$ 700 mensuales por 12 meses por 3 trabajadores

Beneficios de ley		**$ 12,219.60**	Rubro que se debe calcular en base a lo dispuesto por la ley vigente en el Ecuador; sale de la sumatoria de décimo tercer sueldo, décimo cuarto sueldo, aporte patronal y fondos de reserva
Décimo tercer sueldo	$ 4,200.00		Es un sueldo adicional que los trabajadores reciben en el mes de diciembre (máximo hasta el 24), su cálculo es igual a los ingresos percibidos por cada trabajador en el año dividido para doce (ya que el año tiene 12 meses). En este caso como los ingresos de los trabajadores en total es de $50400, dividimos este monto para doce y nos arroja $4200, que es lo que la empresa debe pagar a la totalidad de empleados del área administrativa por este concepto. Su periodo de cálculo es del 1 de diciembre del año anterior al 30 de noviembre del año en curso.
Décimo cuarto sueldo	$ 2,400.00		Es igual a un sueldo básico unificado por cada trabajador, se calcula desde el primero de agosto del año anterior, hasta el 31 de julio del año en curso en la sierra y el orienta cancelándose hasta el 15 de agosto de cada año y en la costa y región insular el cálculo es del 1 de marzo del año anterior hasta el 28 o 29 de febrero del año en curso y debe ser pagado hasta el 15 de marzo; actualmente el sueldo básico unificado en el país es de $400, por lo tanto, en el ejemplo, como son seis trabajadores, multiplicamos $400 por los seis trabajadores lo que nos da $2.400,00

Sueldo básico unificado para el 2021= 400 **USD**

Aporte patronal	$ 5,619.60		De acuerdo con lo que establece el IESS a la fecha, el aporte patronal mínimo es igual al 11,15% de los ingresos que perciba el trabajador en un mes. En nuestro caso como el cálculo se quiere hacer anual lo hacemos en base a los sueldos y salarios para el año 1 ya calculados (50400 X 11,15%).	El porcentaje de aportación para trabajadores en relación de dependencia es: Aporte Patronal: 11,15% Aporte Personal: 9,45% Total de aportación al IESS: 20,60%
Fondos de reserva	$ -		Tiene derecho todos los trabajadores que han cumplido un año de trabajo para el mismo patrono y se calcula del 1 de julio del año anterior al 30 de junio del año en curso, la forma de cálculo es la doceava parte de lo recibido en el período que se calcula o su proporcional, la base de cálculo se da en relación a todos los ingresos percibidos por un trabajador en el año y puede ser cancelado mensualmente junto con el sueldo o de manera acumulada cada año hasta el 30 de septiembre, en el formato que para el efecto otorga el IESS. En este caso como se trata de una empresa nueva y ninguno	Aporte Patronal: 11,15%

			de los empleados a cumplido el año, no se debe pagar fondos de reserva.	
Vacaciones	$ -		Tienen derecho todos los trabajadores que han cumplido un año de trabajo para el mismo patrono, caso contrario, se debe pagar el proporcional, el período de cálculo es en relación con el año de servicios y equivale a la veinticuatroava parte lo recibido en el período que se calcula. El trabajador puede acumular sus vacaciones hasta tres años y gozarlas en el cuarto año, de no hacerlo pierde el primer año de vacaciones. En el ejemplo, si partimos del supuesto que los trabajadores tomarán sus vacaciones, no es necesario hacer ningún cálculo, pues estos harán uso de este beneficio, siendo recomendable que los trabajadores tomen sus vacaciones en todos los casos.	Aporte Personal: 9,45%
Suministros de oficina		**$ 400.00**	$ 400 por cuatro trimestres que tienen el año, puesto que la compra se hará cada tres meses.	Total, de aportación al IESS: 20,60%
Activos menores		**$ 400.00**	$ 100 por cuatro trimestres que tiene el año, puesto que la compra se hará cada tres meses.	
TOTAL GASTOS DE ADMINISTRACIÓN		**$ 70,979.60**	Sumatoria de los diferentes gastos del área administrativa	

GASTOS DE VENTA			
CONCEPTO	**PARCIAL**	**PRESUPUESTO ANUAL**	**CÁLCULO**
Sueldos y salarios personal de ventas		**$ 36,000.00**	Sumatoria de los sueldos anuales del personal del área
Pago sueldo jefe de ventas	$ 24,000.00		$2.000 mensuales por 12 meses
Pago sueldo vendedores	$ 12,000.00	**son 2 vendedores**	$ 500 mensuales por 12 meses lo que nos da $6.000; pero como son dos vendedores, los $6.000 multiplicamos por 2 vendedores y nos da $12.000
Beneficios de ley		**$ 8,214.00**	Rubro que se debe calcular en base a lo dispuesto por la ley vigente en el Ecuador; sale de la sumatoria de décimo tercer sueldo, décimo cuarto sueldo, aporte patronal y fondos de reserva
Décimo tercer sueldo	$ 3,000.00		Es un sueldo adicional que los trabajadores reciben en el mes de diciembre (máximo hasta el 24), su cálculo es igual a los ingresos percibidos por cada trabajador en el año dividido para doce (ya que el año tiene 12 meses). En este caso como los ingresos de los trabajadores en total es de $36.000, dividimos este monto para doce y nos arroja $3.000, que es lo que la empresa debe pagar a la totalidad de empleados del área administrativa por este concepto. Su periodo de cálculo es del 1 de diciembre del año anterior al 30 de noviembre del año en curso.

Décimo cuarto sueldo	$ 1,200.00		Es igual a un sueldo básico unificado por cada trabajador, se calcula desde el primero de agosto del año anterior, hasta el 31 de julio del año en curso en la sierra y el orienta cancelándose hasta el 15 de agosto de cada año y en la costa y región insular el cálculo es del 1 de marzo del año anterior hasta el 28 y 29 de febrero del año en curso y debe ser pagado hasta el 15 de marzo; actualmente el sueldo básico unificado en el país es de $400, por lo tanto, en el ejemplo, como son tres trabajadores, multiplicamos $400 por los tres trabajadores lo que nos da $1.200
Aporte patronal	$ 4,014.00		De acuerdo con lo que establece el IESS a la fecha, el aporte patronal mínimo es igual al 11,15% de los ingresos que perciba el trabajador en un mes. En nuestro caso como el cálculo se quiere hacer anual lo hacemos en base a los sueldos y salarios para el año 1 ya calculados (28.200 X 11,15%).
Fondos de reserva	$ -		Tiene derecho todos los trabajadores que han cumplido un año de trabajo para el mismo patrono y se calcula del 1 de julio del año anterior al 30 de junio del año en curso, la forma de cálculo es la doceava parte de lo recibido en el período que se calcula o su proporcional, la base de cálculo se da en relación a todos los ingresos percibidos por un trabajador en el año y puede ser cancelado mensualmente junto con el sueldo o de manera acumulada cada año hasta el 30 de septiembre, en el formato que para el efecto otorga el IESS. En este caso como se trata de una empresa nueva y ninguno de los empleados a cumplido el año, no se debe pagar fondos de reserva.
Vacaciones	$ -		Tienen derecho todos los trabajadores que han cumplido un año de trabajo para el mismo patrono, caso contrario, se debe pagar el proporcional, el período de cálculo es en relación con el año de servicios y equivale a la veinticuatroava parte lo recibido en el período que se calcula. El trabajador puede acumular sus vacaciones hasta tres años y gozarlas en el cuarto año, de no hacerlo pierde el primer año de vacaciones. En el ejemplo, si partimos del supuesto que los trabajadores tomarán sus vacaciones, no es necesario hacer ningún cálculo, pues estos harán uso de este beneficio, siendo recomendable que los trabajadores tomen sus vacaciones en todos los casos.

Publicidad y promociones		**$ 2,000.00**	$1000 por 2 semestres que tiene el año, porque se presupuesta gastar $1000 cada seis meses.
Viáticos		**$ 18,000.00**	$1.500 que se presupuesta gastar mensualmente por doce meses que tiene el año
Suministros de limpieza		**$ 180.00**	$ 15 por doce meses que tiene el año
TOTAL GASTOS DE VENTA		**$ 64,394.00**	Sumatoria de los diferentes gastos del área comercial

TOTAL, GASTOS OPERACIONALES AL AÑO	
GASTOS ADMINISTRATIVOS	$ 70,979.60
GASTOS DE VENTA	$ 64,394.00
TOTAL	**$ 135,373.60**

GASTOS NO OPERACIONALES			
CONCEPTO	**PARCIAL**	**PRESUPUESTO ANUAL**	**CÁLCULO**
GASTOS FINANCIEROS		**$ 240.00**	Sumatoria de gastos financieros, en este caso solo hay un rubro, por lo tanto, se repite el valor
Servicios y comisiones bancarias	$ 240.00		$20 mensuales por 12 meses que tiene el año
OTROS GASTOS NO OPERACIONALES		**$ 6,768.68**	Sumatoria de otros gastos no operacionales, en este caso solo hay un rubro, por lo tanto, se repite el valor
Imprevistos	$ 6,768.68		Cinco por ciento de los gastos operacionales ($135.375,60 por 5% = $6.768,68)
TOTAL GASTOS NO OPERACIONALES		**$ 7,008.68**	Sumatoria de los diferentes gastos no operacionales

RESUMEN DE CAPITAL DE TRABAJO			
RUBRO	**EGRESO**		**ANÁLISIS DE CÁLCULOS**
	ANUAL	**MENSUAL**	
GASTOS OPERACIONALES	$ 135,373.60	$ 11,281.13	El egreso presupuestado anual dividimos para doce con el propósito de conocer el rubro mensual.
GASTOS NO OPERACIONALES	$ 7,008.68	$ 584.06	El egreso presupuestado anual dividimos para doce con el propósito de conocer el rubro mensual.
TOTAL	**$ 142,382.28**	**$ 11,865.19**	Sumatoria del inventario más gastos operacionales y no operacionales
CÁLCULO DEL CAPITAL DE TRABAJO PARA TRES MESES		**$ 35,595.57**	Egreso presupuestado mensualmente por tres meses de requerimiento para el capital de trabajo.

RESUMEN DE INVERSIONES	
CONCEPTO	**RUBRO**
Inversión de activos fijos	$ 79,850.00
Inversión de activos diferidos e intangibles	$ 21,500.00
Inversión en capital de trabajo	$ 35,595.57
INVERSIÓN TOTAL	**$ 136,945.57**