ESCUELA DE NEGOCIOS

MAESTRIA EN ADMINISTRACIÓN DE EMPRESAS MBA

TEMA: Plan de Negocio para la creación de una Empresa Consultora en Prevención de Riesgos de Ciberseguridad para entidades financieras.

Profesor

Gabriel Fernando Gonzalez Castro

Autor

Abata Bautista William Javier

2023

Contenido

Contenido de Figuras

Contenido de Tablas

TITULO DEL PROYECTO

Plan de Negocio para la creación de una Empresa Consultora en Prevención de Riesgos de Ciberseguridad para entidades financieras.

Capítulo 1

Resumen

Wilds Security Consulting es una empresa de seguridad cibernética que brinda soluciones integrales para proteger a las empresas y organizaciones de las amenazas cibernéticas. Con el rápido crecimiento del delito cibernético y la creciente sofisticación de los ataques cibernéticos, nuestros servicios son esenciales para cualquier organización que valore sus datos, privacidad y reputación. Nuestro equipo de profesionales está comprometido con la prestación de servicios y cuenta con años de experiencia en el negocio de la ciberseguridad el más alto nivel de protección a nuestros clientes. Ofrecemos una gama de servicios que incluyen evaluaciones de riesgos, pruebas de vulnerabilidad, detección de amenazas y respuesta a incidentes, así como capacitación de empleados sobre las mejores prácticas de seguridad cibernética.

Análisis de mercado: la industria de la ciberseguridad está creciendo a un ritmo exponencial, con una creciente demanda de servicios y soluciones de ciberseguridad debido al aumento de las amenazas y ataques cibernéticos. Según Cybersecurity Ventures, se espera que el gasto mundial en ciberseguridad supere el billón de dólares para 2025. La pandemia de COVID-19 ha acelerado aún más esta tendencia, ya que el trabajo remoto ha hecho que las organizaciones sean más vulnerables a los ciberataques. Nuestro mercado objetivo incluye pequeñas y medianas empresas en diversas industrias, como finanzas, atención médica y

tecnología. Estas empresas son particularmente vulnerables a las amenazas cibernéticas debido a sus recursos limitados y falta de experiencia en ciberseguridad.

Estrategia de Marketing y Ventas: nuestra estrategia de marketing y ventas se centrará en crear alianzas y colaboraciones sólidas con otras empresas y expertos en ciberseguridad para mantenerse al día con las últimas amenazas y soluciones. También aprovecharemos los canales de marketing digital como las redes sociales, la optimización de motores de búsqueda y el marketing de contenido para llegar a nuestro público objetivo. Nuestra estrategia de ventas consistirá en ofrecer soluciones flexibles y escalables que se puedan adaptar para satisfacer las necesidades de diferentes tipos y tamaños de empresas.

Proyecciones financieras: proyectamos que nuestros ingresos aumentarán constantemente durante los próximos cinco años a medida que adquirimos nuevos clientes y ampliamos nuestros servicios. Esperamos generar $ 5500 en ingresos en nuestro primer año de operación, y se proyecta que nuestros ingresos alcancen $ 27500 para el quinto año. Nuestro margen de utilidad bruta se estima en 42%, y los gastos operativos consisten principalmente en salarios, gastos de tecnología y costos de marketing. Planeamos reinvertir una parte de nuestras ganancias en investigación y desarrollo para mantenernos por delante de la competencia y ofrecer soluciones innovadoras a nuestros clientes.

Wilds Security Consulting está preparada para convertirse en líder en la industria de la seguridad cibernética al ofrecer soluciones integrales y experiencia inigualable a nuestros clientes. Con la creciente demanda de servicios y soluciones de ciberseguridad, estamos seguros de que nuestro negocio experimentará un crecimiento y un éxito significativos en los próximos años.

Abstract

Wilds Security Consulting is a cybersecurity firm that provides comprehensive solutions to protect businesses and organizations from cyber threats. With the rapid growth of cybercrime and the increasing sophistication of cyber-attacks, our services are essential for any organization that values their data, privacy, and reputation.

Market Analysis: the cybersecurity industry is growing at an exponential rate, with increasing demand for cybersecurity services and solutions due to the rise in cyber threats and attacks. The COVID-19 pandemic has further accelerated this trend, as remote work has made organizations more vulnerable to cyber-attacks. Our target market includes small to medium-sized businesses in various industries such as finance, healthcare, and technology.

Marketing and Sales Strategy: our marketing and sales strategy will focus on building strong partnerships and collaborations with other cybersecurity companies and experts to stay up to date with the latest threats and solutions. We will also leverage digital marketing channels such as social media, search engine optimization, and content marketing to reach our target audience. Our sales strategy will involve offering flexible and scalable solutions that can be tailored. We will also emphasize the importance of employee training and compliance with applicable regulations and laws to minimize the risk of cyber-attacks.

Financial Projections: we project that our revenue will increase steadily over the next five years as we acquire new clients and expand our services. We expect to generate $ 5500 in revenue in our first year of operation, and our revenue is projected to reach $ 27500 by year five. Our gross profit margin is estimated to be 42%, with operating expenses primarily consisting of salaries, technology expenses, and marketing costs. We plan to reinvest a portion of our profits into research and development to stay ahead of the competition and offer innovative solutions to our clients.

Wilds Security Consulting is poised to become a leader in the cybersecurity industry by offering comprehensive solutions and unmatched expertise to our clients. With the increasing demand for cybersecurity services and solutions, we are confident that our business will experience significant growth and success in the years to come.

Introducción

El vivir en una era digital ha creado la necesidad que cooperativas y financieras busquen adaptarse a nuevas tecnologías. En este sentido, una consultoría en ciberseguridad se ha convertido en una inversión indispensable para todas las organizaciones conectadas a la red e internet. La importancia de la ciberseguridad no se limita solo a preservar la información sensible de las empresas, sino también a establecer garantías de cumplimiento de normativa establecida en el país donde se desenvuelve las compañías. Las consultorías de esta clase exigen contar con conocimientos específicos, y cuente con el personal capacitado en la materia.

Estos expertos deben estar cualificados para implementar técnicas capaces de mejorar el rendimiento de los flujos de información, a la vez que se incrementa la seguridad del sistema. Además, que los expertos en ciberseguridad deben ser capaces de localizar todas las posibles falencias presentes. La consultoría de ciberseguridad tiene por objetivo la implementación de técnicas específicas que permitan prevenir, proteger y mejorar el rendimiento de los flujos de información dentro de las compañías. El proceso es igual al de una auditoria en el cual se pondría a prueba la capacidad de respuesta que tienen los sistemas, el personal, y protocolos de actuación asociados ante la detección de cualquier falla de seguridad.

¿Qué beneficios tiene una consultoría de ciberseguridad?

- Confidencialidad y uso restringido de la información: Definiendo los protocolos y roles de acceso pertinente.

- Mejora de la reputación: Adquiriendo una imagen corporativa más segura y fiable.
- Reducción de riesgos: La preparación e incremento de la conciencia colectiva de todo el personal mejorará la eficiencia operativa y de la infraestructura IT
- Reducción de costes y mayor resiliencia: El uso de las herramientas adecuadas en materia de seguridad informática reducirá las opciones de sufrir un ciberataque que vulnere la capacidad operativa de la empresa.

Descripción de la empresa

La consultora brinda soluciones de ciberseguridad a nivel nacional usando metodología de alta efectividad que proporciona valor agregado con una mínima inversión por parte de nuestros clientes. Además, que nuestra habilidad para observar el negocio busca considerar escenarios de ataques reales y concretos, de esta manera crear software preventivo y libre para entregar un servicio de calidad con personal de seguimiento en cada una de las empresas con las que trabajamos lo cual nos ayuda a fidelizar a cada uno de nuestros clientes. Su objetivo es frenar los robos de identidad, los ciberataques y la divulgación de información sensible, implementando una efectiva herramienta para evitar hackeos de los sistemas informáticos y violaciones de datos que llevarían a la organización a la quiebra. Debido a la constante aparición de nuevos virus en todo el mundo, el personal de ciberseguridad se encargará de mantener completamente actualizados los sistemas anti ataque de la organización.

Objetivo General

Reducir los costos operativos al tiempo que ofrece una protección óptima e inteligente para evitar accesos no deseados.

Objetivos Específicos

- Establecer procedimientos de seguridad para salvaguardar los datos de nuevos incidentes.

- Crear una matriz de riesgos que especifique el tipo de peligro y la respuesta a los incidentes de ciberseguridad.
- Elaborar informes de acuerdo con su valor, sensibilidad y cualquier legislación aplicable.

Interrogantes	Elementos
1. ¿Qué cambiar?	Prevenir el robo de identidad, los ciberataques y la divulgación de información privada.
2. ¿Para quién?	Entidades financieras de Ecuador segmento 2 al 4.
3. ¿Cómo?	Asesorando y tratando de mitigar los riesgos de los ciberataques
4. ¿Dónde?	En la red perimetral de los clientes que deseen, pertenecer al SOC.
5. ¿Cuándo?	En un periodo de dos años.

Necesidad que satisface

Reduzca los gastos operativos e impulse la productividad mitigando el acceso no autorizado a los sistemas lógicos al tiempo que ofrece una protección óptima e inteligente.

Misión

Ser un aliado estratégico para nuestros clientes mediante nuestro apoyo experto en concientización del elemento humano en Ciberseguridad y Vulnerabilidades.

Visión

Ser en el 2025, para ser reconocidos como líderes del sector que brinda experiencia y asesoría en la presentación de servicios y soluciones de Ciberseguridad.

Modelo de negocio

La consultora usa una estrategia empresarial basada en los servicios. A continuación, se describen con más detalle las dos partes principales de este concepto:

Propuesta de Valor

Mantener la seguridad al tanto del entorno digital reforzando el control con un servicio gestionado desde nuestro servicio administrativo Cloud Operation Center los 365 días.

Análisis de Ciberseguridad + Análisis de Vulnerabilidades+ ISO27001		
Alcance	**Actividades:** Reuniones y revisión de controles. Recomendación de proyectos a implementar. Análisis de riesgos de Ciberseguridad. **Entregables:** Reportes semanales y mensuales. Reporte técnico.	$20.000
Cronograma	3 meses de ejecución a partir de la fecha de inicio.	

Estructura de utilidad

La consultora se sustenta a partir de los ingresos recibidos a cambio de los servicios prestados a las empresas generando estabilidad y confianza a cada uno de nuestros clientes adaptándonos a sus necesidades.

Ubicación de la consultora

Las reuniones tendrán lugar en los lugares de trabajo de los clientes de esta manera se optimizaría el uso del presupuesto y de ser necesario se utilizaría Coworking.

Organigrama

Al ser una consultora que está ingresando en el mercado de ciberseguridad contamos con un organigrama lineal establecido con puntos principales que nos ayudan a llevar un mejor control de cada proceso.

Figura 1

Organigrama

Aliados Clave	Actividades Clave	Propuesta de Valor	Relación con el Cliente	Segmentos de Clientes
• Empresas del sector financiero como son cooperativas y financieras del segmento 2 y 3. • Empresas de servicios en la nube. Microsoft Azure & Google Cloud.	• Desarrollo de metodologías y políticas. • Apoyarse con la inteligencia artificial.	• Productos que reducen el acceso no autorizado a los sistemas lógicos, ofrecen una seguridad óptima e inteligente, reducen los gastos operativos y aumentan la productividad del personal.	• El sistema de seguridad de la información o SGSI (Información Security Management System) tiene como objetivo evaluar todos los riesgos asociados con los datos e información que se manejan en una empresa.	• Empresas con sistemas lógicos. • Organizaciones dedicadas a los servicios financieros de intermediación de dinero en el Ecuador. • 299 cooperativas y financieras que actualmente podrían ser nuestros futuros clientes.

<table>
<tr>
<td></td>
<td>Recursos Clave
Especialista consultor de ciberseguridad y riesgos.
Infraestructura tecnológica en la nube.</td>
<td></td>
<td>Canales
Portal web
Redes sociales
Correo electrónico
Comunicados internos.</td>
<td></td>
</tr>
<tr>
<td colspan="3">Estructura de Costes
Servicios en la nube Microsoft y Google.
Sueldos colaboradores.
Publicidad en los diferentes canales.</td>
<td colspan="2">Estructura de Ingresos
Cuota por renta mensual del servicio.
Cuota por actualizaciones del software.
Cuota anual de soporte.
Buscar inversionistas</td>
</tr>
</table>

Tipos de investigación

Estudio descriptivo: se usará este tipo de investigación debido a que mediante la recolección de información se puede describir la realidad que los colaboradores están atravesando en la empresa, de esta manera tenemos un enfoque más real y una solución a plantear. La investigación de mercados desarrolla los métodos de recopilación de datos, aplica el proceso de recogida de datos, analiza los resultados y transmite las conclusiones y sus implicaciones. (Malhotra, 2008, p. 82).

Tipos de métodos

En esta investigación se usará el método inductivo que empezará con la observación para poder evidenciar las falencias de la empresa para de esta manera poder entregar una posible solución con una perspectiva más real.

Investigación Cualitativa

En la investigación cualitativa, la información se obtiene mediante diversos métodos, como la entrevista y la observación. El objetivo de la investigación cualitativa es descubrir el carácter fundamental de las realidades, su red de conexiones y su estructura dinámica. (Fernández, 2002, p. 370).

Método de análisis: se logrará un diagnóstico más preciso para detallar las fortalezas y debilidades de la empresa. Y también se usará el método sintético que lo usaremos posterior al diagnóstico para tener en claro la fuente del problema y una posible solución.

Análisis situacional

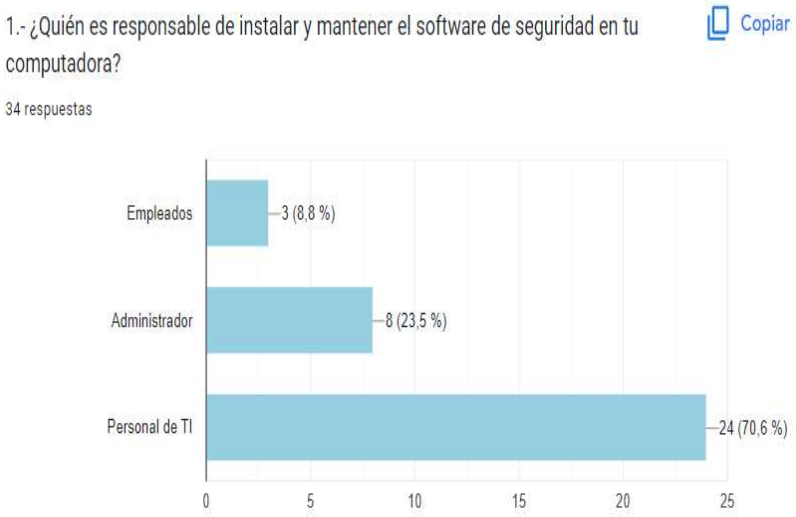
Población y muestra

Se realizará a 100 personas elegidas aleatoriamente de varias entidades financieras mediante la técnica de la observación y encuesta se realizará preguntas concretas y claras para que puedan ser contestadas con sinceridad y así obtener un panorama más claro de los problemas a solucionarse.

Encuesta
Procesamiento y Análisis de Datos

Figura 2

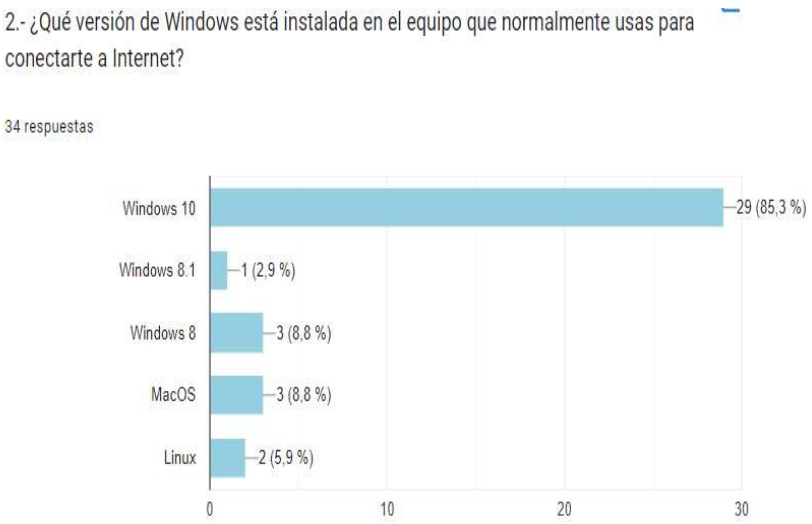
Pregunta 1 Encuesta



Se puede evidenciar que el 70,6 % afirma que el personal de TI son los responsables de instalar y mantener el software de seguridad en sus computadoras.

Figura 3

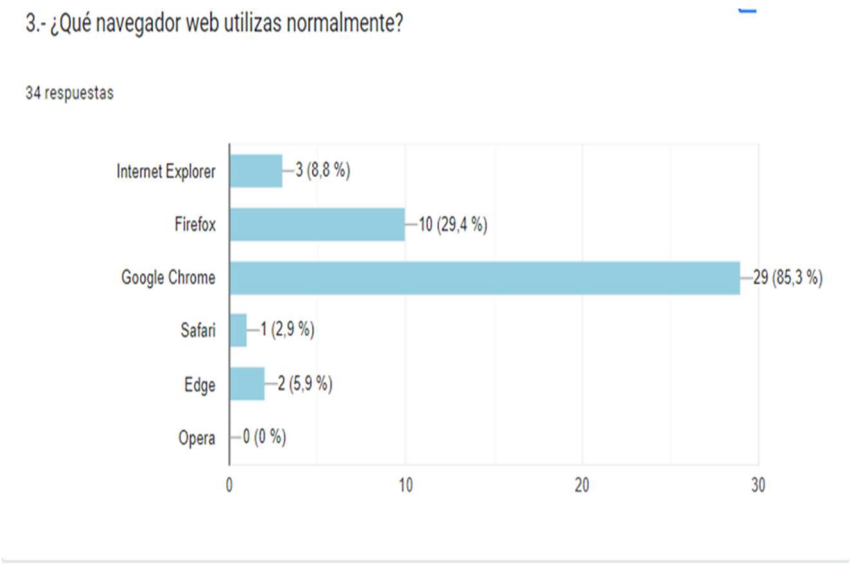
Pregunta 2 Encuesta



Como resultado de la pregunta se evidencia que la mayoría el 85,3% tiene instalado Windows 10 en sus equipos de uso habitual.

Figura 4

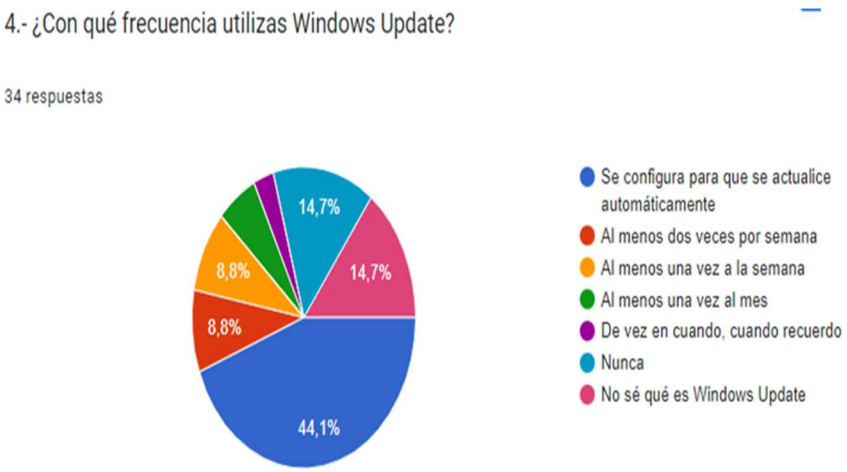
Pregunta 3 Encuesta



La mayoría de las personas afirma con un 85,3% que el navegador más usado es Google Chrome, seguido por Firefox con 29,4%.

Figura 5

Pregunta 4 Encuesta



En esta pregunta se puede evidenciar que el uso de Windows Update no es de notable importancia por esta razón se configura para que se actualice automáticamente.

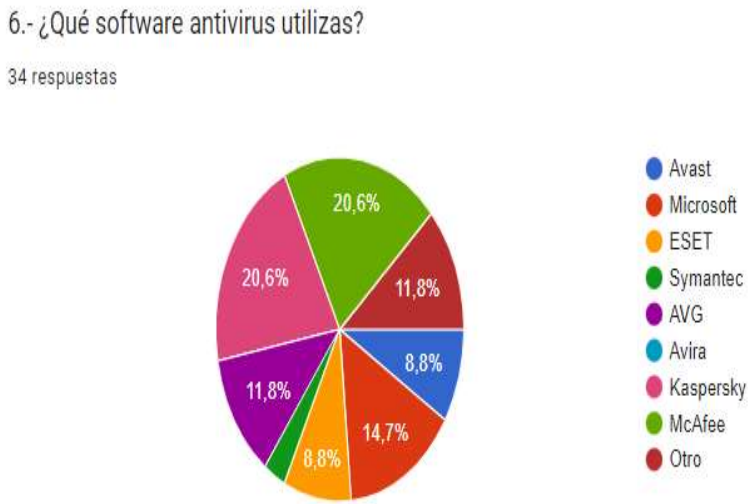
Figura 6

Pregunta 5 Encuesta

Se evidencia con un 88,2% que mantienen un software antivirus instalado en sus computadoras por lo que si hay una cultura de seguridad en las empresas.

Figura 7

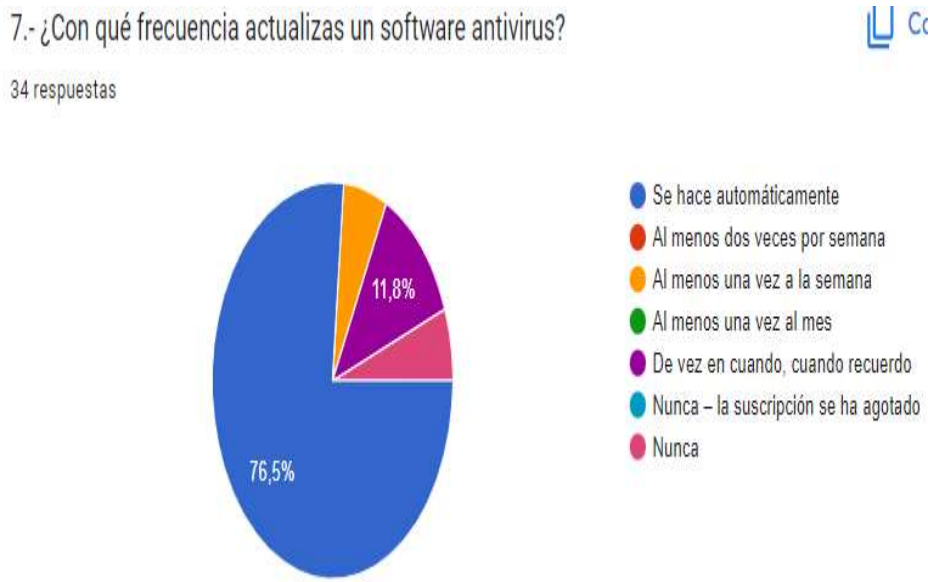
Pregunta 6 Encuesta



Mediante la encuesta se puede evidenciar que los antivirus más usados son Symantec y Kaspersky con un 20,6% seguido por Microsoft con un 14,7%.

Figura 8

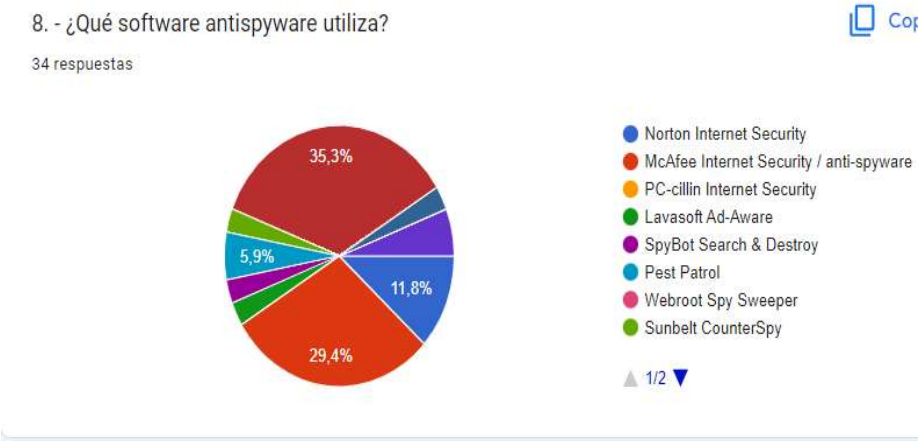
Pregunta 7 Encuesta



El 76,5% de las personas encuestadas indica que la actualización de su antivirus se realiza automáticamente.

Figura 9

Pregunta 8 Encuesta



McAfee Internet Security con el 35,3% es software antispyware más utilizado por los usuarios.

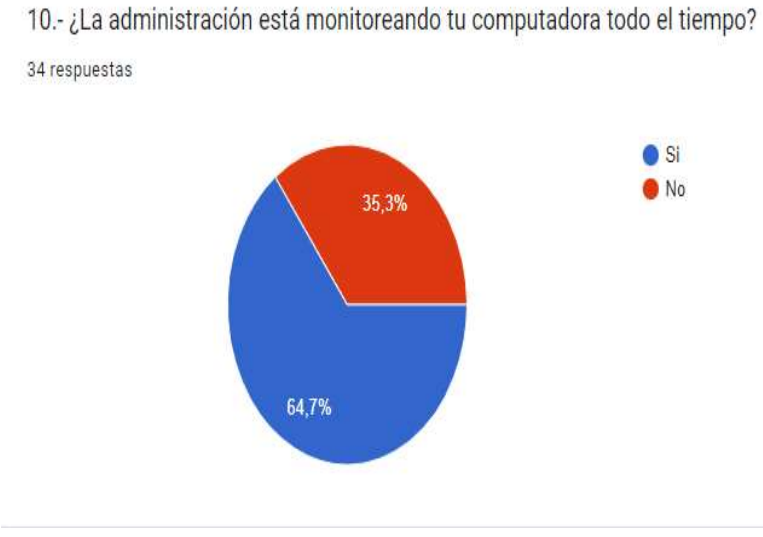
Figura 10

Pregunta 9 Encuesta

Con el 44,1 % de usuarios afirman que usan un software de firewall en su ordenador seguido por un 32,4% de usuarios que desconocen.

Figura 11

Pregunta 10 Encuesta



El 64,7% menciona que su computadora se encuentra monitoreada todo el tiempo, por lo que se puede considerar que las empresas si cuentan con ciertos conocimientos de ciberseguridad.

Capítulo 2

Entorno macroeconómico y político

Hace diez años, nos enteramos de un incidente de seguridad especial en una empresa conocida en el sur. Este es probablemente uno de los primeros ejemplos de un ciberataque efectivo contra una empresa ecuatoriana importadora de equipos de fábricas chinas. Las comunicaciones por correo electrónico entre los propietarios de negocios locales y los exportadores asiáticos se han visto comprometidas por piratas informáticos que utilizan técnicas de ataque man-in-the-middle (correo electrónico). En un correo electrónico similar al original, los piratas informáticos engañaron a un empresario ecuatoriano para que pagara aproximadamente $ 40,000 a través de una transferencia bancaria internacional a una cuenta fraudulenta en Hong Kong. Los contratistas y proveedores identificaron el ataque semanas después. La primera vez fue por no recibir la confirmación de la compra y la segunda vez por no recibir el pago.

Desde ese incidente, en los últimos cinco años, los ataques cibernéticos en todo el mundo han crecido exponencialmente, volviéndose más efectivos y peligrosos a medida que explotan las variaciones, las fuentes geográficas, el crimen organizado y diversas complejidades tecnológicas. Las más comunes son una combinación de técnicas llamadas falsificación de correo electrónico (phishing), ingeniería social de SMS (smishing), phishing telefónico (vishing) y secuestro de información. Como infraestructura, programa maligno o malware móvil.

Marco Legal

Mediante Acuerdo Nro. 052, de 10 de mayo de 2021. La Política Ecuador Digital está compuesto por tres programas: Ecuador conectado, Ecuador eficiente y ciberseguro; y, Ecuador innovador y competitivo. El programa Ecuador eficiente y ciberseguro tiene como objetivo proteger a la sociedad frente a las amenazas cibernéticas, generar confianza en el uso del internet y fomentar el desarrollo económico y social basado en el uso de las Tecnologías de la Información y de la Comunicación (TIC). La Vigésima Sesión Ordinaria del Gabinete Sectorial de Seguridad tuvo lugar en la ciudad de El Coca el 1 de abril de 2021. En ella se aprobó la Política Nacional de Ciberseguridad y se designó al Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) como el encargado de publicarla mediante Acuerdo Ministerial.

Análisis del sector

La consultora está dentro del sector de servicios, debido a que no ofrece un producto como tal sino un software de ciberseguridad a distintas entidades financieras con el fin de proteger su información de todo tipo de daños virtuales.

Análisis del Mercado Nacional

En este sentido, las empresas ecuatorianas han enfrentado muchos incidentes de seguridad y sufrido pérdidas importantes por no estar preparadas para enfrentar posibles amenazas digitales. En Ecuador, muchas organizaciones invierten en recursos humanos y tecnología para mejorar la seguridad, prevenir ciberataques y proteger la información financiera y sensible de sus empresas y clientes. La prevención es más que comprar e instalar tecnología de seguridad. Utilizando un arma muy antigua y eficaz, la ingeniería social, los ataques de los hackers triunfan porque golpean el punto más estratégico de una empresa: las personas. La pandemia ha exacerbado todo lo anterior y ha aumentado inimaginablemente los riesgos cibernéticos que enfrentan las empresas. El teletrabajo, el

mayor uso de Internet y el consumo de servicios a través de medios digitales requieren una atención urgente para prevenir actividades ilegales por parte de las autoridades o la alta dirección de las organizaciones.

Desarrollo tecnológico

En Ecuador uno de los mayores problemas a los que se encuentra expuesto es a la falta de un plan de acción ante una amenaza cibernética ya que normalmente recae la responsabilidad en un administrador de sitio web, por esta razón es importante plantear lineamientos que permitan a Ecuador coordinar sus estrategias con los diferentes sectores que se pueden ver afectados, es indispensable recalcar que la poca inversión que se asigna a la contratación de estos servicios ha expuesto potencialmente a nuestro país.

Tendencia del Mercado

En 2020 se consolidó el proceso de digitalización con la pandemia del coronavirus. Sin embargo, los temas relacionados con la ciberseguridad también se han incrementado significativamente. Desde ESET señalan que existen formas de evadir los ciberataques y son más las empresas que las implementan. “El 30 % de las organizaciones ha implementado la gestión ‘Zero Trust’ y el 72 % planea implementarla pronto”, dijo la compañía.

Fortalezas

- Uso de los recursos informáticos.
- Reducción de riesgos que afectan la disponibilidad, integridad y confidencialidad de la información.
- Uso consecuente de la información.
- Enfoque hacia la automatización.

Oportunidades

- Obtener certificaciones de la industria en ciberseguridad (ISO 27001, Magerit).

- Acceso a varios sistemas
- Mejorar la calidad de la información dentro de la organización.

Debilidades

- Resultados a medio y largo plazo.
- Falta asignación presupuestaria para nuevos procesos.
- Costos elevados al aplicar los controles de seguridad apropiados.
- Bajo posicionamiento de la nueva marca.

Amenazas

- No, contar con el apoyo de los Stakeholders.
- Mecanismos no apropiados en la implementación.

Análisis PESTEL para el diseño de un SGSI

Se ha desarrollado un análisis PESTEL con el objetivo de captar con precisión las implicaciones que tiene el diseño de un SGSI en las organizaciones del sector financiero aplicando en diversos ambientes como político, económico, social, tecnológico, legislativo y ecológico, por lo tanto, a lo indicado anteriormente se exponen los siguientes puntos.

Tabla 1

Análisis PESTEL del diseño SGSI

Político - **Cambios y aplicación de nuevas disposiciones o procesos regulatorios relacionados con el modelo de negocio de la compañía, pueden llegar a dificultar la implementación del SGSI**	**Económico** - **Acciones y cambios de nuevos impuestos pueden afectar en la concesión de controles de seguridad, lo cual puede llegar a retrasar la implementación del SGSI.**	**Social** - **Imagen corporativa, da confianza a los clientes, proveedores y colaboradores.**
Tecnología - **La implementación de un SGSI proporciona a la empresa una**	**Ecológico** - **Revela una tendencia a utilizar correctamente la información, es decir,**	**Legislación** - **Los colaboradores son conscientes que existe una política interna de la**

estrategia competitiva que crea una diferenciación significativa en el mercado frente a otros competidores.	**no divulgar información digitalmente para hacerla más segura utilizando procedimientos mejores y más seguros, reduciendo el uso de papel e impresoras.**	**organización la cual por su incumplimiento pueden llegar a ser sancionados dependiendo de la gravedad de la contravención.**

Capítulo 3

Objeto de Estudio

Las pérdidas financieras más relevantes que pueden conllevan un ciberataque Un ciberataque genera son:

- Pérdida de productividad.
- Costo de recuperación de casos.
- Implementar nuevos sistemas de información.
- Pérdida de reputación.

Según la revista Cibercrimen indica que en el año 2021 los ataques cibernéticos causaron perdidas que ascienden a los $16.4 billones que es un valor realmente alto el cual denota la vulnerabilidad que actualmente tenemos.

Análisis externo

Las 5 fuerzas de Porter están compuestas por: los competidores potenciales, amenaza de productos sustitutos, competencia en los mercados y el poder de los compradores y proveedores. (Porter, 2009, p. 101).

Estrategias de marketing

"La estrategia de marketing de una empresa describe la forma en que la empresa cubrirá las necesidades y deseos de sus clientes, según los resultados obtenidos en la investigación de mercados, como son las encuestas y entrevistas realizadas tanto a

personal interno de la empresa, como a clientes y personas externas a la misma. En otras palabras, la estrategia de marketing es un método para la forma en que la empresa usará sus fortalezas y habilidades para juntarlas con las necesidades y requerimientos del mercado.” (Ferrell O, 2012, p. 180).

Segmentación

Se refiere a diferenciar el total de mercado de un producto o servicio en grupos diferentes de consumidores, iguales entre sí y diferentes a los demás, en cuanto a hábitos, necesidades y gustos, que podrían precisar producto o combinaciones de marketing diferentes. (Monferrer, 2013, p. 80).

La segmentación del mercado es transcendental para definir una buena estrategia comercial y proponer un servicio eficaz. Las estrategias de segmentación de mercado nos permiten conocer las necesidades de nuestros clientes potenciales para llegar a ellos de la manera más eficaz. Después de realizar una investigación de mercado e identificar y evaluar los segmentos existentes, se implementa una estrategia de segmento que determine a qué clientes vamos a comercializar nuestro producto de acuerdo con cada una de sus necesidades.

Patrones

La información que se genera desde la extracción y análisis forman un dominio de conocimientos que se genera de varias condiciones.

Uso de patrones

El análisis de datos nos permite resolver algunos criterios de la seguridad de la información que nos proporcionará un esquema más amplio de los patrones que son usados para los ataques cibernéticos.

Capítulo 4

Tabla 2

Glosario de Términos

TÉRMINO	DEFINICIÓN
Proceso de administración de riesgos	Método lógico y sistemático de establecer el contexto e identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados a las actividades de una organización.
Amenaza	Potencial ocurrencia de un hecho que pueda manifestarse en un lugar específico, con duración e intensidad determinadas.
Evento	Ocurrencia o cambio de un conjunto particular de circunstancias.
Vulnerabilidad	Debilidad o grado de exposición de un sujeto, objeto o sistema a una determinada amenaza.
Impacto	Consecuencia efectiva, de carácter positivo o negativo, de la ocurrencia de un evento.
Probabilidad	Posibilidad de que algo suceda, es el factor que determina la velocidad de materialización de un riesgo.
Fórmula de cálculo del Riesgo	Se expresa en Riesgo es igual al producto de Impacto y Probabilidad (R=IxP).
Riesgo	Efecto de la incertidumbre sobre los objetivos.
Riesgo inherente	Riesgo natural que se encuentra en el ambiente en el que se desarrollan las actividades organizacionales.
Riesgo residual	Riesgo que subsiste incluso después de haber implementado controles y planes de acción, considera el Impacto y la Probabilidad residuales
Riesgo emergente	Riesgo que aparece en un momento determinado, como consecuencia de un nuevo peligro o amenaza identificada, generalmente porque no ha sido identificado o por un cambio en el contexto de la organización.
Plan de acción	Marco o estructura que incluye las actividades más importantes para cumplir con determinados objetivos y metas.
Plan de tratamiento	Instrumento de gestión que contiene medidas técnicas, humanas y organizativas necesarias para la continuidad de las operaciones de una organización.
Evitar	Opción del plan de tratamiento que decide eliminar la causa raíz del problema.
Mitigar	Opción del plan de tratamiento que implementa controles efectivos con la finalidad de disminuir la probabilidad y el impacto.
Aceptar	Opción del plan de tratamiento que le permite a la organización vivir con el riesgo.
Transferir	Opción del plan de tratamiento que le permite a la organización distribuir o compartir entre algunas dependencias externas el riesgo. (Aseguradoras, Entidades de Control, etc.)
Riesgo aceptable	Nivel de riesgo que es aceptado por la Máxima Autoridad, expresado en mapa de calor (Niveles: Bajo, Medio, Alto y Crítico).
Global Suite	Herramienta que permite Gestionar los Riesgos de manera automatizada.
CEO Estratégico	Comité conformado por todos los directores, Coordinadores, Asesores de Gerencia, Máxima Autoridad y presidente del Directorio.
SW	Software
HW	Hardware

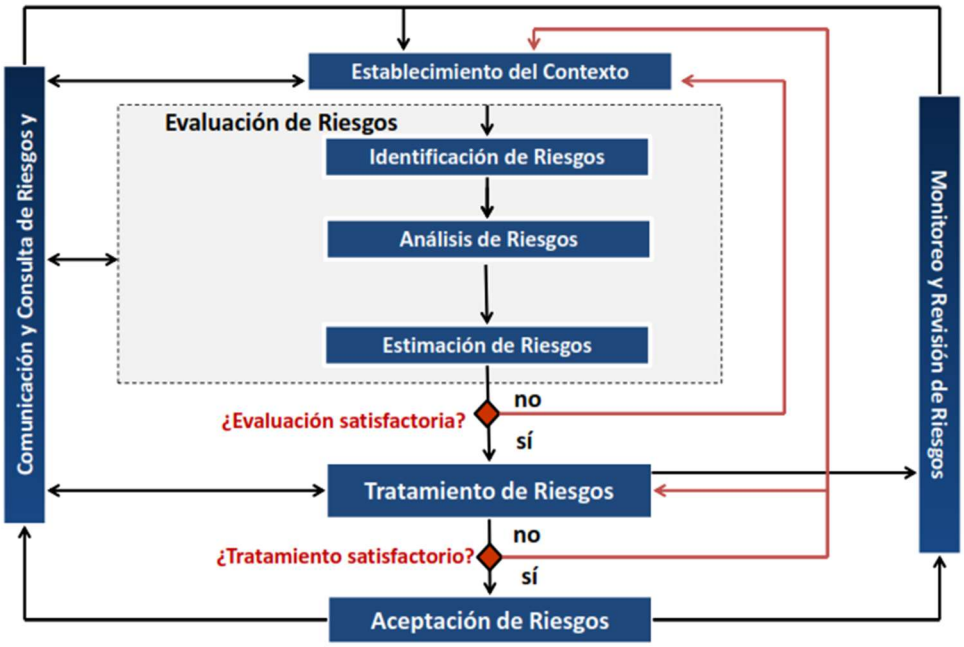
Metodología de gestión de riesgos de seguridad de la información

Administración de riesgos

Considerando que la gestión de riesgos conforme al proceso de la ISO31000:2018 se establece el tratamiento holístico contextualizado en el siguiente gráfico:

Figura 12

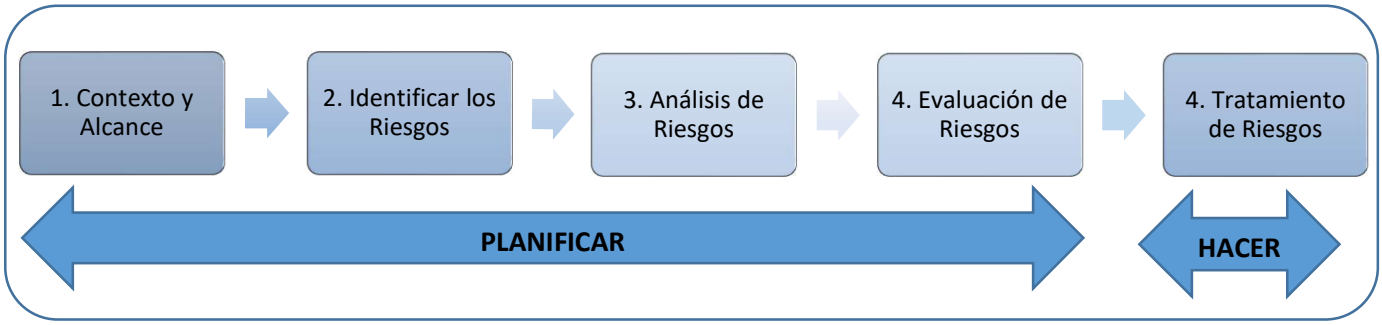
Proceso Gestión de Riesgos de Seguridad de la Información ISO27005



En esta metodología los conflictos, considerando el ciclo de Deming PHVA (Planificar, Hacer, Verificar y Actuar), estos serán administrados a lo largo del ciclo de vida de un plan, proyecto o proceso, con base en el siguiente alcance que contempla las fases de Planificación y Hacer.

Figura 13

Fases de la Administración de Riesgos en la Metodología



Para llevar a cabo la Administración de Riesgos, se utilizará la Herramienta Global Suite, con esta herramienta nos ayudará en la prevención de riesgos de seguridad, con el propósito de determinar aquellos que, por su impacto potencial y alta probabilidad de ocurrencia, se constituyen un peligro crítico para el logro de los objetivos organizacionales.

Sintaxis

Amenaza y vulnerabilidad: Las siglas a utilizar para la codificación de las amenazas y vulnerabilidades se contextualizan en la siguiente tabla:

Tabla 3

Amenazas y Vulnerabilidades

Ítem	Codificación
Amenaza	AME-0000
Vulnerabilidad	VUL-0000

Responsables

El responsable del riesgo será designado según la siguiente tabla:

Tabla 4

Designación de responsables

Ítem	Responsable del riesgo	Área	Código
Institucional (Global)	Máxima Autoridad	Gerencia General	GG
Planes Estratégicos, Operativos, Procesos y Proyectos.	Coordinador/director del área responsable.	Coordinador Técnico de Mecanismos de Seguridad Financiera.	CMSF
		Coordinar Gestión y Control de Fideicomisos.	CGCF
		Coordinador Técnico de Riesgos y Estudios.	CTRE
		Coordinador Técnico de Protección a Seguro y Fondos.	CPSF
		Coordinador General Administrativo Financiero.	CGAF
		Director de Recuperación y Juicio de Coactivas.	DRJC
		Director de Planificación y Gestión Estratégica.	DPGE

Tabla 5

Stakeholders – Partes Interesadas

Stakeholder / Interesados
Presidencia de la República
Banco Central del Ecuador
Superintendencia de Economía Popular y Solidaria
Superintendencia de Bancos
Junta de Política de Regulación Monetaria y Financiera
Superintendencia de Compañías, Valores y Seguros
Secretaría Nacional de la Presidencia
Bolsa de Valores de Quito
Bolsa de Valores de Guayaquil
Red Financiera de Desarrollo
Aso Banca
Red de Integración Ecuatoriana de Cooperativas de Ahorro y Crédito (ICORED)
Asociación de Compañías de Seguros del Ecuador (ACOSE)
Asociación de Casas de Valores del Ecuador
Unión de Cooperativas de Ahorro y Crédito del Norte (UCACNOR)
Unión de Cooperativas de Ahorro y Crédito del Sur (UCACSUR)
Red Nacional de Finanzas Populares y Solidarias (RENAFIPSE)
Asociación de Organismos de Integración del Sector Financiero Popular y Solidario (ASOFIPSE)
Asociación de Instituciones de Microfinanzas (ASOMIF)
Casas de Valores
Depositantes
Asegurados de 31compañías de seguros privados
Ex administradores de entidades financieras
Empresas de Seguros Privados
Agentes de Pago
Ministerio de Gobierno
Servicio Nacional de Contratación Pública
Contraloría General del Estado
Asamblea Nacional
Consejo de la Judicatura
Fiscalía General del Estado
Registro Oficial
Procuraduría General del Estado
Defensoría del Pueblo
Consejo Nacional de Participación Ciudadana y Control Social
Municipio de Quito
Agencia Nacional de Tránsito
Consejo Nacional para la Igualdad de Discapacidades
Medios de Comunicación
Policía Nacional del Ecuador

Armada Nacional
Dinardap
Universidades
Personal de Código de Trabajo

Objetivo y alcance

Objetivo

Proveer una Metodología de Gestión de Riesgos de Seguridad de la Información, que establezca los lineamientos necesarios para que ésta identifique, evalúe y trate eficazmente los riegos Inherente y Residuales, que pudiesen afectar.

Riesgos de seguridad de la información "AAV".

Siendo que la definición matemática de un riesgo es igual a la velocidad de materialización de un impacto potencial que causa efecto en la organización sobre un activo (R=IxP), en esta sección como el principal componente de la gestión de riesgos se abordará la fase de identificación de activos de información que deben ser protegidos en la organización, así como la contextualización de estos por tipo.

Identificación de activos y propietarios del riesgo por activo.

Considerando el alcance establecido para la presente Metodología de Gestión de Riesgos de Seguridad de la Información, el cual corresponde al Proceso Agregador de Valor del Pago del Seguro de Depósitos y de Seguros Privados, se establece que los activos deben ser identificados con base en el inventario institucional y los componentes que conforman el proceso formalmente levantado y autorizado en la organización, considere que los activos son todo aquel bien tangible o intangible que posee la organización y que mantienen o generan valor, adicionalmente deberá hacer uso de la Tabla 6 a fin de establecer su codificación y mantener un orden adecuado.

Contextualización de activos por tipo.

Considerando como referencia la clasificación macro de activos que proporciona Magerit versión 3. Libro II – Catálogo de Elementos, la clasificación de activos se dará haciendo uso de la siguiente tabla:

Tabla 6

Siglas Utilizadas para Activos

TIPO	CLASE	SIGLAS	DESCRIPCIÓN
Servicios	Esencial	ACT-SRV-000	Todo aquel servicio institucional que la organización presta, tanto al usuario interno como al Ciudadano Objetivo, con el fin de satisfacer una necesidad.
Datos	Esencial	ACT-DAT-000	Cualquier información digital y física de la cual depende la organización y que cuya carencia la afectarían directamente.
Telecomunicaciones	Soporte	ACT-TEL-000	Cualquier activo que permita la comunicación de datos, internet y seguridad en la organización.
Software	Soporte	ACT-SFW-000	Corresponde al Sistema Operativo, programas, aplicaciones y desarrollos que transformen los datos en información a ser empleada en los Servicios Institucionales. (No aplica al código fuente)
Hardware	Soporte	ACT-HRW-000	Se aplica a equipos tales como computador de escritorio, laptop, servidores, impresoras, etiquetadoras, escáneres, etc.
Personas	Soporte	ACT-PER-000	Compuesta por los cargos organizacionales.
Instalaciones	Soporte	ACT-INS-000	Todas aquellas ubicaciones que usa la institución para su normal funcionamiento, data centers, bodegas, salas de reuniones, áreas de seguridad, etc.

Amenaza – vulnerabilidad – afectación "CID" por tipo de activo

Con la finalidad de mantener un alineamiento con las mejores prácticas en Seguridad de la Información, para la identificación de amenazas y vulnerabilidades se hará uso de Magerit versión 3 Libro II Catálogo de Elementos y la Norma ISO/IEC 27005:2012, adicionalmente se empleará el juicio de expertos y dueños de los riesgos (Coordinadores/Máxima Autoridad); por lo tanto a continuación se detalla el modelo a seguir para la contextualización de las amenazas y vulnerabilidades a las cuales se expone un activo de información (A+A+V), así como el impacto que este sufre producto de la

materialización de un riesgo, esto considerando la afectación sobre la Confidencialidad, Integridad y Disponibilidad (**CID**), observadas desde dos ámbitos

- Universo de Amenazas y Vulnerabilidades: empleando para la codificación.
- Impacto CID y Responsable.

Análisis de riesgos de seguridad de la información "IP-F"

En esta sección se abordará la estimación del riesgo a partir de los criterios contextualizados anteriormente para impacto, probabilidad, amenaza y vulnerabilidad, esto considerando los tres factores establecidos como el ADN institucional tales como Eficiencia, Liquidez e Inversiones.

Estimación del impacto

Con la finalidad de contar con un panorama global sobre el impacto que se produce a nivel organizacional sobre los factores de Eficiencia, Liquidez e Inversiones, producto de la materialización de uno o varios riesgos, por la inobservancia de amenazas y vulnerabilidades, a continuación, se expone la ponderación del impacto con un criterio aplicado a los tres factores:

Tabla 7

Estimación del Impacto - Contextualización

Nivel Impacto	Valor	Eficiencia	Liquidez	Inversiones	Ponderación
Bajo	1	Sin daños o con daños menores en los activos de Hardware, Software, Datos e Infraestructurales; para Sistemas o Servicios Institucionales que usan Tecnologías de la Información para su funcionamiento hasta 60 minutos fuera de línea; Para el Recurso Humano no hay lesiones y/o muertes.			1 – 1.75
Medio	2	Daños leves en los activos de Hardware, Software, Datos e Infraestructurales; para Sistemas o Servicios Institucionales que usan Tecnologías de la Información para su funcionamiento mayores a 60 minutos y menores a 180 minutos fuera de línea; Para el Recurso Humano hay lesiones leves.			1.76 – 2.5
Alto	3	Daños de gravedad en los activos de Hardware, Software, Datos e Infraestructurales; para Sistemas o Servicios Institucionales que usan Tecnologías de la Información para su funcionamiento mayores a 180 minutos y menores a 8 horas fuera de línea; Para el Recurso Humano hay lesiones leves.			2.6 – 3.25

Crítico	4	Daños de gravedad en los activos de Hardware, Software, Datos e Infraestructurales; para Sistemas o Servicios Institucionales que usan Tecnologías de la Información para su funcionamiento mayores a 8 horas fuera de línea; Para el Recurso Humano hay lesiones graves y/o muertes.	3.26 - 4

La ponderación ha sido establecida con la siguiente fórmula:

Valor Máximo (4) – Valor Mínimo (1) = Resultado (3) / Valor Máximo (4)

4 – 1 = 3/4

Valor para incremento en ponderación = 0.75

El valor de 0.75 será sumado a de manera secuencial desde el valor mínimo hasta alcanzar el valor máximo. (**Ponderación**)

Una vez contextualizada la interpretación que se dará al impacto que ocurra, debido a la ejecución de un riesgo, sobre un activo de información; es importante considerar su afectación sobre la Confidencialidad, Integridad y Disponibilidad (**CID**), para esto será fundamental que tanto los propietarios de los riesgos, Oficial de seguridad de la Información y la Máxima Autoridad, realicen una votación sobre la mencionada afectación en donde se buscará un consenso o alineamiento, a continuación la guía que se deberá seguir:

Tabla 8

Estimación del Impacto - Contextualización

CÓDIGO ACTIVO	NOMBRE ACTIVO	EVALUADOR	FACTORES									PROMEDIO	CALIFICACIÓN IMPACTO
			EFICIENCIA			LIQUIDEZ			INVERSIONES				
			C	I	D	C	I	D	C	I	D		
ACT-HRW-001	Computador portátil del CMSF	Propietario de Riesgo	2	3	1	4	2	3	1	4	2	2,44	
		Oficial de Seguridad	2	3	2	3	1	3	1	4	1	2,22	
		Máxima Autoridad	2	3	2	3	1	3	1	4	2	2,33	
											PROMEDIO CID - FACTORES	2,33	Medio

CALIFICACIÓN CID	BAJO = 1
	MEDIO = 2
	ALTO = 3
	CRÍTICO = 4

CALIFICACIÓN IMPACTO	BAJO	1 : 1.75
	MEDIO	1.76 : 2.50
	ALTO	2.56 : 3.25
	CRÍTICO	3.26 : 4

Evaluación de controles para vulnerabilidad

En esta fase de la metodología abordaremos los criterios que permitan evaluar los controles respecto de las vulnerabilidades presentes en los activos de información que pudieran estar siendo amenazados, recordando que un activo de información es todo

aquello tangible o intangible para la organización que de una manera u otra mantiene o genera valor.

Para este propósito es necesario considerar un modelo de evaluación de madurez, el mismo que será adaptado a las necesidades de la organización, en este caso se empleará el Modelo de Madurez de Capacidades o por sus siglas en inglés CMMI (Capability Maturity Model Integration).

Tabla 9

Niveles de evaluación de Controles - Contextualización

NIVEL	MODELO	DESCRIPCIÓN
MALO	NIVEL 1 – NO CONFIABLE	Ambiente impredecible, sin documentación de soporte, no se dispone de personas, procesos o tecnologías para el debido control.
REGULAR	NIVEL 2 - INFORMAL	Las actividades, procesos, personas y tecnologías para el debido control existen, pero no se ponen en práctica. Los controles dependen básicamente de las personas, por lo que los controles son propensos a no ser utilizados o mal utilizados. No hay un entrenamiento formal del recurso humano ni comunicacional.
ACEPTABLE	NIVEL 3 - ESTANDARIZADO	Las actividades, procesos, personas y tecnologías para el debido control existen y están diseñados para atender las necesidades debidas, han sido documentados y comunicados a los funcionarios, las desviaciones de las actividades, procesos, personas y tecnologías dedicadas al control probablemente no se detecten.
BUENO	NIVEL 4 - MONITOREADO	Las actividades, procesos, personas y tecnologías para el debido control existen y están diseñados para atender las necesidades debidas, han sido documentados y comunicados a los funcionarios, las desviaciones de las actividades, procesos, personas y tecnologías dedicadas al control son monitoreadas debidamente.
MUY BUENO	NIVEL 5 - OPTIMIZADO	Esta estructura la maneja control interno en el cual se realiza un monitoreo continuo con esto se realizan cambio más preciso y a tiempo al momento de detectar errores en los procesos que se ejecutan en tiempo real.

De acuerdo con el nivel de madurez CMMI con el cual se podrá clasificar a los controles, es fundamental que cada uno pueda ser asociado con un valor que permita

disminuir un posible ataque y que en el caso de darse su impacto no se vea reflejado en los activos de información de la organización, para esto se deberá emplear la siguiente guía que será de mutuo acuerdo entre el Propietario del Riesgo, y la persona encargada de Seguridad de la Información.

Tabla 10

Ponderación de la reducción del Activo

NIVEL	CONDICIÓN	DESCRIPCIÓN	VALOR REDUCCIÓN	
			IMPAC.	PROBA.
MALO (1)	NO EXISTE	Ambiente impredecible, sin documentación de soporte, no se dispone de personas, procesos o tecnologías para el debido control.	-0	-0
REGULAR (2)	EXISTE, PERO FUNCIONA DEFICIENTEMENTE, O NO SE LO USA.	Las actividades, procesos, personas y tecnologías para el debido control existen, pero no se ponen en práctica. Los controles dependen básicamente de las personas, por lo que los controles son propensos a no ser utilizados o mal utilizados. No hay un entrenamiento formal del recurso humano ni comunicacional.	-1	-0
ACEPTABLE (3)	EXISTE Y FUNCIONA PARA LO PREVISTO.	Las actividades, procesos, personas y tecnologías para el debido control existen y están diseñados para atender las necesidades debidas, han sido documentados y comunicados a los funcionarios, las desviaciones de las actividades, procesos, personas y tecnologías dedicadas al control probablemente no se detecten.	-2	-1
BUENO (4)	EXISTE Y FUNCIONA PARA LO PREVISTO Y SON MONITOREADOS.	Las actividades, procesos, personas y tecnologías para el debido control existen y están diseñados para atender las necesidades debidas, han sido documentados y comunicados a los funcionarios, las desviaciones de las actividades, procesos, personas y tecnologías dedicadas al control son monitoreadas debidamente.	-3	-2
MUY BUENO (5)	EXISTE Y FUNCIONA PARA LO PREVISTO, SON MONITOREADOS Y MEJORADOS CONSTANTEMENTE.	Con esta metodología en tiempo real vamos a tener una respuesta más rápida a un posible evento.	-3	-3

Identificación de controles y niveles de probabilidad (AV)

Adaptando como referencia las normas ISO 27001:2015/27002:2015, a continuación, se procede a presentar la guía como deberá ser presentada la matriz de controles asociados al universo de amenazas y vulnerabilidades.

A continuación, se expresa la ponderación para los niveles de probabilidad a ser empleados en la presente metodología de gestión para el cálculo del riesgo, esto considerando que la Probabilidad de ocurrencia es el factor que corresponde a la velocidad con la que una Amenaza se puede llegar a materializar en función de los controles que la organización cuente, se detalla:

Tabla 11

Ponderación de la Probabilidad (AV)

PROBABILIDAD (AMENAZA VULNERABILIDAD)	PONDERACIÓN
Baja	1
Media	2
Alta	3
Muy Frecuente	4

Una vez que tenemos definidos los criterios para la que establecen el cálculo del Riesgo Inherente, siendo que este es igual al producto del Impacto por la Probabilidad, siendo este último expresado en términos de Amenaza y Vulnerabilidad, por lo que la formula a emplear se expresaría de la siguiente manera:

$$R_{(Inherente)} = I_{(Inherente)} * P\ (AV)_{(Inherente)}$$

Riego Inherente = Impacto Inherente por Probabilidad (Amenaza Vulnerabilidad) Inherente

Así también se desprende, considerando los controles y su nivel de reducción, la fórmula que se empleará para el cálculo del Riesgo Residual:

$$R_{(Residual)} = I_{(Reducido)} * P\ (AV)_{(Reducido)}$$

Riego Residual = Impacto Reducido por Probabilidad (Amenaza Vulnerabilidad) Reducido

Considerando lo expuesto y con base en el criterio de aceptación del riesgo (se tolera hasta nivel Alto, Crítico no es aceptable), los niveles del riesgo que se observarán para su adecuada gestión corresponden al siguiente plano cartesiano:

Figura 14

Niveles del Riesgo para Gestionar (Crítico)

Crítico	Crítico	Crítico	Crítico	Crítico
Alto	Medio	Alto	Crítico	Crítico
Medio	Bajo	Medio	Alto	Crítico
Bajo	Bajo	Bajo	Medio	Alto
Producto Cartesiano	*Baja*	*Media*	*Alta*	*Muy Frecuente*

Evaluación del riesgo

Los eventos de riesgo identificados deben ser asociados a un activo, considerando que el inicio de un evento de riesgo es:

- Servicios
- Datos
- Telecomunicaciones
- Software
- Hardware
- Personas
- Instalaciones

Sin embargo, los activos mencionados también están expuestos a factores externos que pueden comprometer la Confidencialidad, Integridad y Disponibilidad, considerados como la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos al control de la institución, tales como: fallas en los servicios públicos, ocurrencia de desastres naturales, atentados y actos delictivos entre otros, los cuales pudieran alterar el desarrollo normal de las actividades.

A continuación, en el ejemplo, se detalla el cálculo del Riesgo (Impacto x Probabilidad) según el tipo de activo identificado dentro de las amenazas para cada vulnerabilidad y obteniendo la valoración de la siguiente:

Impacto Confidencialidad = (C - Eficiencia + C - Liquidez + C - Inversiones) / n

Impacto Integridad = (I - Eficiencia + I - Liquidez + I - Inversiones) / n

Impacto Disponibilidad = (D - Eficiencia + D - Liquidez + D - Inversiones) / n

Impacto Promedio = (Confidencialidad + Integridad + Disponibilidad) / n

Riesgo = Impacto Promedio x Probabilidad

Tabla 12

Evaluación del Riesgo

Activo	Amenaza	Vulnerabilidad	Impacto			Impacto Promedio	Probabilidad	Riesgo	Nivel Riesgo
			C	I	D				
Servicios	AME-0001	VUL-0001	4	4		4	1	1,00	Bajo
		VUL-0002	4			4	2	2,00	Medio
		VUL-0003	4			4	3	3,00	Alto
		VUL-0004	4	4		4	4	4,00	Crítico
	AME-0002	VUL-0005							
		VUL-0006	4		4	4	2	2,00	Medio
		VUL-0007			4	4	3	3,00	Alto
		VUL-0008	4	4		4	4	4,00	Crítico
	AME-0003	VUL-0009			4	4	1	1,00	Bajo
		VUL-0010			4	4	2	2,00	Medio
		VUL-0011			4	4	3	3,00	Alto
		VUL-0012			4	4	4	4,00	Crítico
	AME-0004	VUL-0013	4	4	4	4	1	1,00	Bajo
		VUL-0014	4	4	4	4	2	2,00	Medio
		VUL-0015	4	4	4	4	3	3,00	Alto
		VUL-0016	4	4	4	4	4	4,00	Crítico
	AME-0005	VUL-0017		4	4	4	1	1,00	Bajo
		VUL-0018		4	4	4	2	2,00	Medio
		VUL-0019	4	4	4	4	3	3,00	Alto
		VUL-0020	4	4	4	4	4	4,00	Crítico

Tabla 13

Calificación del Riesgo

RIESGO	DESCRIPCIÓN	CALIFICACIÓN
Crítico	El valor del riesgo es menor o igual a 4	**4**
Alto	El valor del riesgo es menor o igual a 3	**3**
Medio	El valor del riesgo es menor o igual a 2	**2**
Bajo	El valor del riesgo es menor o igual a 1	**1**

Las evaluaciones del evento de riesgo son realizadas por el propietario del activo, donde se encuentra el riesgo de la siguiente manera:

Se determina el Riesgo Inherente sin considerar los posibles controles existentes, es decir, el peor escenario posible. Cada propietario del activo emitirá una elección individual y consistente de la probabilidad e impacto en base a sus conocimientos sobre el evento de riesgo y el proceso de acuerdo con los Niveles de Evaluación del Riesgo.

Se determina el Riesgo Residual considerando los controles existentes dentro del proceso, estos controles son evaluados basándose en la sección Identificación de Controles de esta metodología.

Los controles actuales están enfocados a reducir la probabilidad o el impacto, por lo que el nivel de Riesgo Inherente llegará a un nivel de Riesgo Residual de acuerdo con la efectividad de estos.

Es muy importante considerar que, si no existen controles para modificar, evitar o trasferir el riesgo, se aceptaría que el Riesgo Residual corresponde al Riesgo Inherente.

Con el fin de simular el nivel de riesgo al que se espera llegar en relación con el Riesgo Inherente, se determina el riesgo deseado que es definido de igual forma que el Riesgo Inherente determinando un impacto y una probabilidad, pero en un escenario ideal mediante la implementación de controles.

Tratamiento del riesgo

Una vez evaluado el riesgo, los propietarios de activos deben definir la respuesta al riesgo, de acuerdo con las siguientes categorías: evitar, aceptar, modificar o transferir.

Evitar el Riesgo

Consiste en identificar riesgos extremadamente altos y que los costos para la implementación de controles son mayores que los beneficios propios del servicio o producto para evitar por completo la materialización del riesgo. Por esta razón se debe eliminar el evento, proceso o actividad capaz de producir el riesgo y después de los cambios aplicados se debe realizar una nueva iteración de análisis del riesgo.

Aceptar el Riesgo

Consiste en asumir el riesgo, es decir "convivir el riesgo", incluyendo los posibles riesgos que aún no han sido identificados. Esta definición es acuerdo con los criterios de aceptación del riesgo definidos por la institución y sin la implementación de controles. Esta es una medida consiente de la Gerencia General que debe estar bien sustentada y registrada. Es importante que se cree una bitácora de los riesgos asumidos, soportados en los criterios de aceptación y en los responsables de su aprobación.

Modificar el Riesgo

Consiste en la implementación de controles para reducir los riesgos considerablemente. Los controles deben tener en cuenta criterios y condiciones de aceptación, tales como: requisitos legales, reglamentarios, contractuales, culturales y ambientales, además de considerar aspectos técnicos, normativos, costos y plazos para la implementación de controles.

Transferir el Riesgo

Reubicar los riesgos a una entidad externa, una forma de transferir el riesgo es el uso de seguros que cubran los efectos por la ocurrencia de un evento que atenta a la seguridad de la información. Sin embargo, hay que considerar la responsabilidad legal entre las partes por la ocurrencia de riesgos que no puede ser transferida.

Niveles de Evaluación del Riesgo

Los riesgos ubicados en un nivel de riesgo "**Bajo**", resultado de las combinaciones de impacto y probabilidad, y cuya ocurrencia no afecta significativamente a las operaciones y continuidad de la institución se considerarán dentro del apetito al riesgo.

Los riesgos ubicados en un nivel de riesgo "**Medio**" o "**Alto**", resultado de las combinaciones de impacto y probabilidad, se considerarán dentro de la tolerancia al riesgo, y deberán contar con planes de mitigación que permitan: evitar, aceptar, modificar o transferir el riesgo, hasta alcanzar el apetito de riesgo definido.

Los riesgos que se ubiquen en un nivel de riesgo "**Crítico**", corresponden a eventos que no están dentro de la tolerancia al riesgo de la institución, y deberán ser tratados con procesos y planes de continuidad del negocio, considerando que su impacto implica afectaciones críticas en las operaciones de la institución.

Actividades de Control

Una vez que se ha evaluado el nivel de riesgo inherente, los propietarios de activos deben identificar controles implementados actualmente como respuesta a los riesgos identificados. Luego de identificar los controles deben determinar hacía donde están orientados, si es a reducir la probabilidad o el impacto. Como parte fundamental del control y seguimiento es necesario definir el personal o área responsable en cada etapa

del proceso y se evaluará periódicamente por parte de los propietarios de activos asignando responsabilidades en la ejecución de estos.

A continuación, en el ejemplo, se muestra el Nivel de Riesgo después de la implementación de Controles sobre el Impacto (C, I o D) y el Riesgo es recalculado.

Tabla 14

Riesgo Residual

Activo	Amenaza	Vulnerabilidad	Nivel Riesgo	Impacto			Impacto Promedio	Probabilidad	Riesgo	Después de Controles
				C	I	D				
Servicios	AME-0001	VUL-0001	Bajo	4	4		4	1	1,00	Bajo
		VUL-0002	Medio	2			2	2	1,00	Bajo
		VUL-0003	Alto	2			2	3	1,50	Medio
		VUL-0004	Crítico	3	2		3	4	2,50	Alto
	AME-0002	VUL-0005								
		VUL-0006	Medio	2		2	2	2	1,00	Bajo
		VUL-0007	Alto			3	3	3	2,25	Alto
		VUL-0008	Crítico	3	1		2	4	2,00	Medio
	AME-0003	VUL-0009	Bajo			4	4	1	1,00	Bajo
		VUL-0010	Medio			2	2	2	1,00	Bajo
		VUL-0011	Alto			2	2	3	1,50	Medio
		VUL-0012	Crítico			3	3	4	3,00	Alto
	AME-0004	VUL-0013	Bajo	4	4	4	4	1	1,00	Bajo
		VUL-0014	Medio	2	2	2	2	2	1,00	Bajo
		VUL-0015	Alto	2	3	3	3	3	2,00	Medio
		VUL-0016	Crítico	2	2	2	2	4	2,00	Medio
	AME-0005	VUL-0017	Bajo		4	4	4	1	1,00	Bajo
		VUL-0018	Medio		2	2	2	2	1,00	Bajo
		VUL-0019	Alto	2	3	3	3	3	2,00	Medio
		VUL-0020	Crítico	3	3	3	3	4	3,00	Alto

Aceptación del riesgo

En esta fase, la máxima autoridad de la institución analizará cuidadosamente el tratamiento de los riesgos aceptados por los propietarios de los activos, estableciendo la responsabilidad de manera formal en un documento que formará parte de SGSI en el cual se identificará la aceptación del riesgo residual, así también en este documento constarán los controles que no son aplicables o no tienden a la reducción la probabilidad o el

impacto inherentes en los riesgos; a continuación se contextualiza la aceptación del riesgo residual en la organización:

Tabla 15

Tolerancia al Riesgo

RIESGO	NIVEL DE ACEPTACIÓN	DESCRIPCIÓN
Crítico	No Aceptable	La organización no acepta el riesgo crítico, debe ser notificado al CEO Estratégico y debe ser monitoreado con una frecuencia por hora o las que sean necesarias para mitigarlo, es decir que el riesgo debe ser tratado inmediatamente.
Alto	Aceptable	La organización acepta el riesgo alto, debe ser notificado al Comité de Seguridad de la Información y monitoreado con frecuencia diaria.
Medio		La organización acepta el riesgo medio, debe ser notificado al Dueño del Riesgo y monitoreado con una frecuencia semanal.
Bajo		La Organización acepta el riesgo, no requiere tratamiento.

Capítulo 5

Factibilidad económica y financiera del modelo de negocios

Esta sección examina los costos que la empresa deben asumir para implementar negocios en ciberseguridad y seguridad de la información. Se enumeran las inversiones en recursos requeridos, activos tangibles e intangibles, costos de construcción, tarifas de licencia de software, tarifas de sitio, gastos generales, materiales directos e indirectos requeridos, costos de mano de obra y todo el capital importante. Desde su inicio, el valor de mantener el negocio hasta que obtenga una ganancia de los servicios prestados.

Activos Fijos tangibles

Los siguientes bienes físicos son la inversión requerida para iniciar las operaciones, además como parte de la propuesta de coworking y una oficina.

Tabla 16

Activos Fijos tangibles

Equipos de cómputo	Cantidad	Costo Unitario	Costo Total	Vida Útil	Depreciación
Laptops	10	$ 500.00	$5.000,00	5	20%
Servidores en la nube	2	$ 5,500.00	$11.000,00	5	20%
Router	1	$ 200.00	$200,00	5	20%
Switch capa 3	1	$ 720.00	$720,00	5	20%
Proyector	1	$ 600.00	$600,00	5	20%
Teléfonos móviles	5	$ 200.00	$1.000,00	5	20%
Teléfonos fijos	2	$ 25.00	$50,00	5	20%
Impresoras Láser	2	$ 120.00	$240,00	5	20%
Total, Equipos de cómputo	**24**		**$18.810,00**		

Flujo de egresos	
Año	**Egresos**
0	$65.000,00
1	$67.000,00
2	$68.700,00
3	$70.400,00
4	$72.100,00

Flujo de ingresos	
Año	**Ingresos**
0	$80.500,00
1	$86.000,00
2	$91.500,00
3	$97.000,00
4	$102.500,00

Flujo de efectivo	
Año	**Efectivo Neto**
0	$15.500,00
1	$19.000,00
2	$22.800,00
3	$26.600,00
4	$30.400,00

Año	0	1	2	3	4
Ingresos	$80.500,00	$86.000,00	$91.500,00	$97.000,00	$102.500,00
Egresos	$65.000,00	$67.000,00	$68.700,00	$70.400,00	$72.100,00
Efectivo Neto	$15.500,00	$19.000,00	$22.800,00	$26.600,00	$30.400,00

Negocio	
Año	**Flujo Caja**
0	-$65.000,00
1	$15.500,00
2	$19.000,00
3	$22.800,00
4	$26.600,00
5	$30.400,00

EVALUACIÓN FINANCIERA DEL PROYECTO

Tasa de Interés Libre de Riesgo [1]	6.64%
Rendimiento de Mercado de Acciones [2]	10.58%
Beta desapalancado [3]	0.90
Beta Apalancada	1.07
Tasa de Impuestos	0.00%
Participación de Trabajadores	15.00%
Escudo Fiscal	15.00%
Riesgo País [4]	12.61%
Razón deuda/Capital	1
Costo de la Deuda Actual [5]	15.00%

(1) Estimación basada en el rendimiento de los Bonos del Tesoro norteamericano a 5 años
(2) Riesgo de mercado del a partir del rendimiento del índice S&P 500 en 5 años
(3) Promedio de la industria en base a información de Damodaran de la industria de muebles
(4) Riesgo País de Ecuador tomado de Ambito.com
(5) Tasa de Interés Productivo PYMES tomado del Banco Central
(6) En base a AMBITO.com

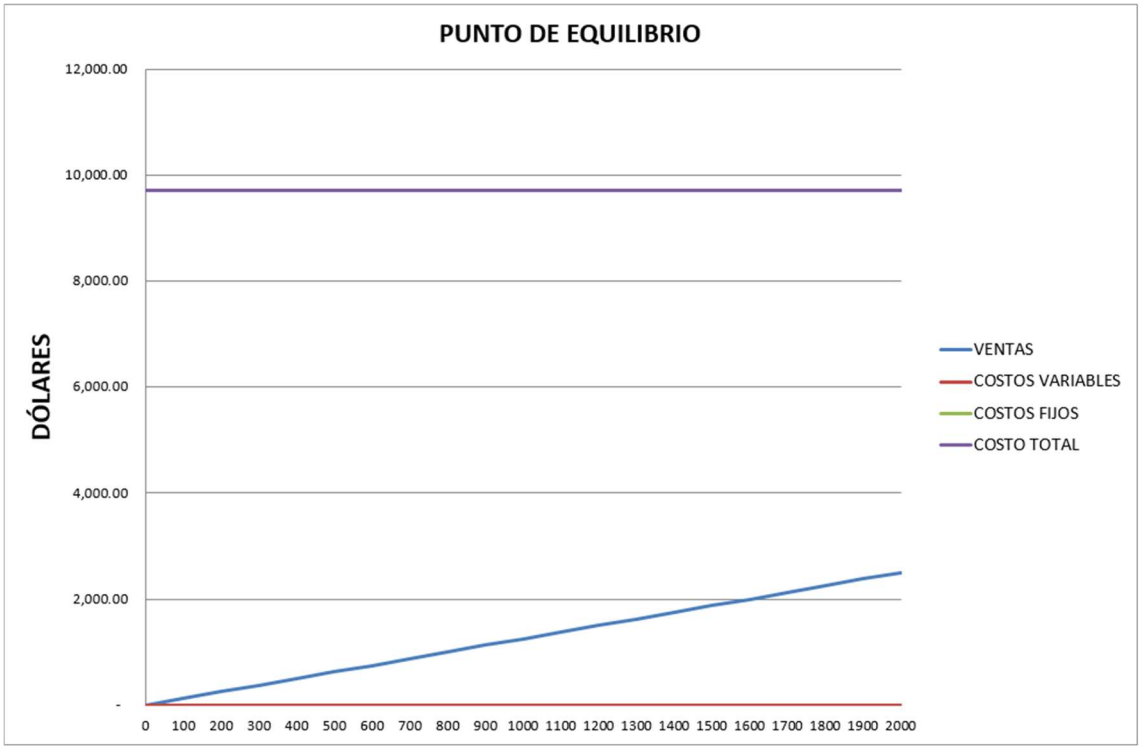
S&P 500			
Hoy	$ 2,787.00	*Hace 5 años*	$ 1,685.70

TASAS DE DESCUENTO	
CAPM	23.44%
WACCC	18.10%

Flujo de Caja del Proyecto Anual					
0	1	2	3	4	5
$ (39,074.00)	$ 138,260.01	$ 319,318.85	$ 344,736.19	$ 365,825.73	$ 350,793.80
	$ 138,260.01	$ 457,578.85	$ 802,315.04	$ 1,168,140.77	$ 1,518,934.57

Flujo de Caja del Inversionista Anual					
0	1	2	3	4	5
$ (15,933.30)	$ 132,747.83	$ 313,624.65	$ 338,830.72	$ 359,675.02	$ 344,358.42
	$ 132,747.83	$ 446,372.49	$ 785,203.21	$ 1,144,878.22	$ 1,489,236.65

Criterios de Inversión Proyecto		Criterios de Inversión Inversionista	
VAN	$857,021.43	VAN	$752,552.43
IR	$22.93	IR	$48.23
TIR	441.70%	TIR	943.48%
Periodo Rec.	0.78	Periodo Rec.	0.72


PUNTO DE EQUILIBRIO
DÓLARES
12,000.00
10,000.00
8,000.00
6,000.00
4,000.00
2,000.00
-
0 100 200 300 400 500 600 700 800 900 1000 1100 1200 1300 1400 1500 1600 1700 1800 1900 2000
VENTAS
COSTOS VARIABLES
COSTOS FIJOS
COSTO TOTAL

Conclusiones

Para crear un plan de negocios de seguridad cibernética exitoso, es importante sacar conclusiones y recomendaciones basadas en el estado actual de la industria de la seguridad cibernética y las tendencias del mercado. Aquí hay algunas conclusiones clave y recomendaciones a considerar:

La ciberseguridad es una industria en rápido crecimiento con una demanda creciente de servicios y soluciones de ciberseguridad debido al aumento de las amenazas y ataques cibernéticos.

Debido a la pandemia que hemos atravesado en estos últimos años ha llevado a una mayor dependencia del trabajo remoto, lo que ha hecho que las organizaciones sean más vulnerables a los ataques cibernéticos.

Las amenazas de ciberseguridad son cada vez más sofisticadas, lo que requiere que las empresas implementen medidas y soluciones de seguridad avanzadas.

Las regulaciones de cumplimiento y las leyes de privacidad de datos son cada vez más estrictas, lo que significa que las empresas deben asegurarse de cumplirlas para evitar multas y daños a la reputación.

Recomendaciones

Desarrollar una solución integral de ciberseguridad que incluya una variedad de servicios, como evaluaciones de riesgos, pruebas de vulnerabilidad, detección de amenazas y respuesta a incidentes.

Enfatizar la importancia de capacitar a los empleados en las mejores prácticas de ciberseguridad para minimizar el riesgo de error humano.

Ofrecer soluciones flexibles y escalables que se puedan adaptar para satisfacer las necesidades de diferentes tipos y tamaños de empresas.

Crear alianzas y colaboraciones sólidas con otras empresas y expertos en ciberseguridad para mantenerse al día con las últimas amenazas y soluciones.

Cumplir con todos los reglamentos y leyes aplicables, y trabaje con expertos legales para mantenerse informado de cualquier cambio o actualización.

Renovarse con las tecnologías y tendencias emergentes, como la seguridad en la nube, la inteligencia artificial y la cadena de bloques, para adelantarse a la competencia y ofrecer soluciones innovadoras a los clientes.

No es posible crear un entorno totalmente seguro por lo que es necesario se realicen auditorias frecuentes que muestren el nivel de seguridad y prevenga posibles ataques.

Es importante que el país cuente con un marco legal contra los delitos informáticos que pueden afectar infraestructura crítica y proteger la información, apoyándose en acuerdos internacionales y legislación de otros países que ya cuenten con una política vigente.

Es fundamental mejorar la comunicación, coordinación y colaboración entre instituciones, organizaciones y empresas, tanto públicas como privadas, de esta manera mejorar la respuesta a los riesgos que se puedan suscitar.

Se debe considerar el desarrollo procesos de análisis y gestión de riesgos que permitan la identificación de vulnerabilidades **y** amenazas relacionados con el uso, procesamiento, almacenamiento y transmisión de datos.

Referencias

Almeida, C. A. (2018). *LA CIBERSEGURIDAD EN EL ECUADOR, UNA PROPUESTA DE ORGANIZACION.* Sangolquí, Ecuador: Revista de Ciencias de Seguridad y Defensa (Vol. IV, No. 7, 2019) pp. 156-169.

Enríquez, L. (31 de agosto de 2022). *Universidad Andina Simón Bolívar*. Obtenido de https://www.uasb.edu.ec/ciberderechos/2022/08/31/hacia-una-cultura-de-valor-al-riesgo-en-la-ciberseguridad-del-ecuador/#:~:text=En%20este%20contexto%2C%20el%20sector,2022)%2C%20y%20muchos%20otros.https://revistas.flacsoandes.edu.ec/urvio/article/download/

Navarrete, J. (14 de septiembre de 2020). *Digital Transformation Lead Partner*. Obtenido de https://www.bdo.ec/es-ec/noticias/2020/ecuador-en-riesgo-ciberataques

Vaca, A. (2017). *Incidencia de la inteligencia de negocios en la ciberseguridad, con aplicación en las políticas nacionals, caso Ecuador.* Quito.

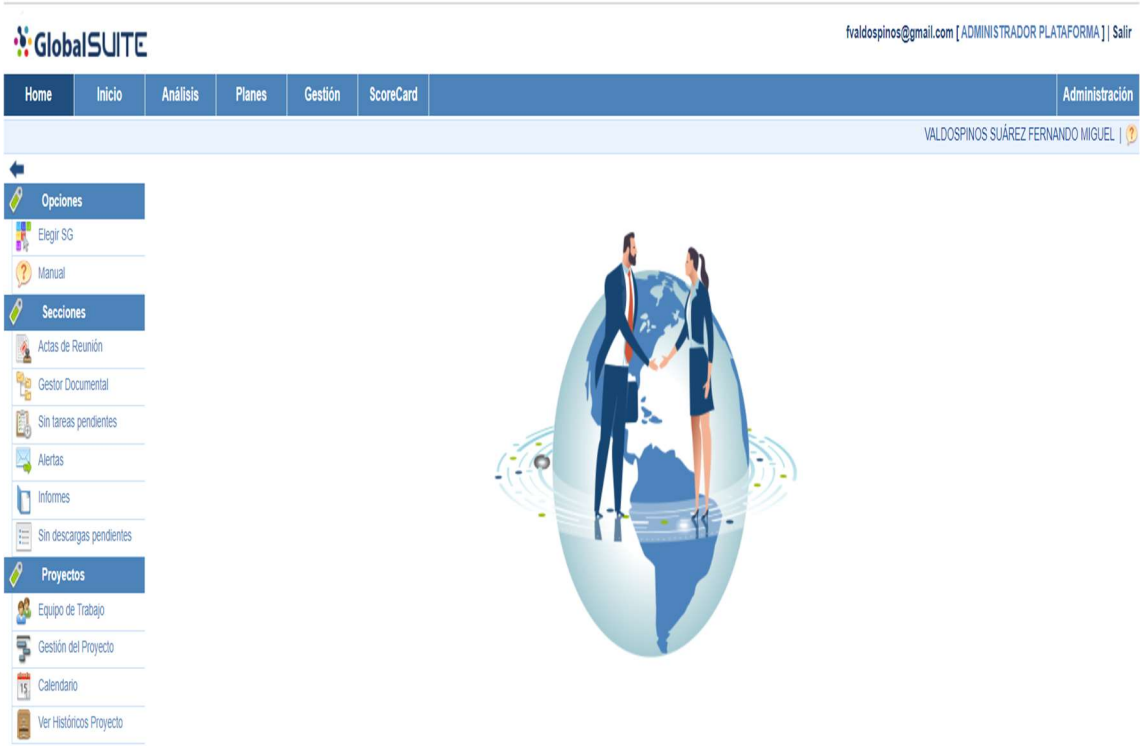
Vargas, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa. *Revista Latinoamericana de Estudios de Seguridad*, pp. 31-45.

Hernández, S. R; Fernández, C. C y Baptista, L. P. (2010). *Metodología de la Investigación. Quinta edición. Mc Graw Hill. México. 613 p.*

Apéndice

Apéndice A

https://sg.globalsuite.es/GS/form_Index.php



Apéndice B

TIPO	CLASE	CÓDIGO SGSI	CÓDIGO INVENTARIO	DESCRIPCIÓN	PROPIETARIO
Servicios	Esencial	ACT-SRV-00X			
Datos	Esencial	ACT-DAT-00X			
Telecomunicaciones	Soporte	ACT-TEL-00X			
Software (SW)	Soporte	ACT-SFW-00X			

Hardware (HW)	Soporte	ACT-HRW-00X			
Personas	Soporte	ACT-PER-00X			
Instalaciones	Soporte	ACT-INS-00X			

Apéndice C

UNIVERSO DE AMENAZAS Y VULNERABILIDADES									
Amenaza	**COD Amenaza**	**Vulnerabilidad**	**COD Vulnerabilidad**	**TIPOS DE ACTIVOS**					
				Servicios	**Datos**	**Telecom.**	**Software**	**Hardware**	**Personas**	**Instalaciones**
Uso no autorizado de Sistemas Informáticos	AME-0001	Ausencia de definición de Roles y Perfiles de Acceso	VUL-0001	CI	I	X	I	X	X	X
		Falta de Política de Bloqueo de equipos y sistemas	VUL-0002	C	CI	X	CI	X	X	X
		Debilidad en los parámetros de seguridad de los sistemas.	VUL-0003	C	I	X	I	X	X	X
		Ausencia de un proceso de pruebas de los Sistemas Informáticos	VUL-0004	CI	I	I	I	X	X	X
Robo de Información	AME-0002	Infraestructura física sin control de acceso	VUL-0005	X	CD	CD	X	CD	X	CD

		Inadecuada gestión y protección de contraseñas	VUL-0006	**CD**	**CD**	**X**	**C**	**X**	**X**	**X**
		Falta de Capacitación a Usuarios	VUL-0007	**D**	**CD**	**D**	**D**	**D**	**X**	**X**
		Ausencia o mala ejecución de Auditorías Internas	VUL-0008	**CI**	**CI**	**I**	**CI**	**X**	**X**	**X**
Denegación de Servicios	AME-0003	Ausencia de un proceso de Análisis de Vulnerabilidades	VUL-0009	**D**	**D**	**D**	**D**	**D**	**X**	**X**
		Falta de reglas FW	VUL-0010	**D**	**D**	**D**	**D**	**D**	**X**	**X**
		Falta de HA	VUL-0011	**D**	**D**	**D**	**D**	**D**	**X**	**X**
		Falta de respaldos o copia controlada de datos	VUL-0012	**D**	**D**	**D**	**D**	**D**	**X**	**X**

Abuso de privilegios de acceso	AME-0004	Falta de control sobre las acciones de ejecución con roles de administrador	VUL-0013	**CID**	**CID**	**D**	**CID**	**CID**	**X**	**X**
		Ausencia de usuarios nombrados para servidores de aplicación y base de datos	VUL-0014	**CID**	**CID**	**X**	**CID**	**CID**	**X**	**X**
		Inadecuada administración de usuarios que se incorporan cambia de área o se desvinculan de la institución	VUL-0015	**CID**	**CID**	**D**	**CID**	**CID**	**X**	**X**

		Falta de un sistema de administración de identidades	VUL-0016	**CID**	**CID**	**X**	**CID**	**CID**	**X**	**X**
Uso no previsto	AME-0005	Falta de control sobre instalación de aplicaciones (por uso de interés personal)	VUL-0017	**ID**	**ID**	**D**	**ID**	**D**	**X**	**D**
		Falta de control sobre perfiles de navegación en internet (por uso de interés personal)	VUL-0018	**ID**	**ID**	**D**	**D**	**D**	**X**	**X**
		Falta de control en uso de servicios de mensajería (por uso de interés personal)	VUL-0019	**CID**	**CID**	**D**	**CID**	**D**	**X**	**X**
		Falta de control por almacenamiento de datos personales (por uso de interés personal)	VUL-0020	**CID**	**CID**	**D**	**CD**	**D**	**X**	**X**

Apéndice D

UNIVERSO DE AMENAZAS Y VULNERABILIDADES										
Amenaza	**COD Amenaza**	**Vulnerabilidad**	**COD Vulnerabilidad**	**Control**	**TIPOS DE ACTIVOS**						
					Servicios	**Datos**	**Telecom.**	**Software**	**Hardware**	**Personas**	**Instalaciones**
Uso no autorizado de Sistemas Informáticos	AME-0001	Ausencia de definición de Roles y Perfiles de Acceso	VUL-0001	A.9.1.1	CI	I	X	I	X	X	X
		Falta de Política de Bloqueo de equipos y sistemas	VUL-0002	A.9.2.2 A.11.2.8	C	CI	X	CI	X	X	X
		Debilidad en los parámetros de seguridad de los sistemas.	VUL-0003	A.9.4.1 A.9.4.4	C	I	X	I	X	X	X
		Ausencia de un proceso de pruebas de los Sistemas Informáticos	VUL-0004	A.12.1.4 A.14.2.8 A.14.2.9	CI	I	I	I	X	X	X
Robo de Información	AME-0002	Infraestructura física sin control de acceso	VUL-0005	A.8.3.3 A.9.2.6 A.11.1.1 A.11.1.2 A.11.1.6 A.11.2.1	X	CD	CD	X	CD	X	CD

		Inadecuada gestión y protección de contraseñas	VUL-0006	A.9.4.3 A.9.2.5 A.9.2.4 A.9.2.6	**CD**	**CD**	**X**	**C**	**X**	**X**	**X**
		Falta de Capacitación a Usuarios	VUL-0007	A.7.2.1 A.7.2.2 A.8.1.3 A.12.2.1	**D**	**CD**	**D**	**D**	**D**	**X**	**X**
		Ausencia o mala ejecución de Auditorías Internas	VUL-0008	A.12.7.1 A.18.1.3	**CI**	**CI**	**I**	**CI**	**X**	**X**	**X**
Denegación de Servicios	AME-0003	Ausencia de un proceso de Análisis de Vulnerabilidades	VUL-0009	A.5.1.1 A.6.1.4 A.12.2.1 A.12.6.1	**D**	**D**	**D**	**D**	**D**	**X**	**X**
		Falta de reglas FW	VUL-0010	A.9.1.1 A.9.1.2 A.13.1.1 A.13.1.2 A.13.1.3	**D**	**D**	**D**	**D**	**D**	**X**	**X**
		Falta de HA	VUL-0011	A.6.1.3 A.11.2.4 A.12.1.3 A.12.7.1 A.13.1.1	**D**	**D**	**D**	**D**	**D**	**X**	**X**
		Falta de respaldos o copia	VUL-0012	A.12.3.1 A.12.2.1	**D**	**D**	**D**	**D**	**D**	**X**	**X**

		controlada de datos									
Abuso de privilegios de acceso	AME-0004	Falta de control sobre las acciones de ejecución con roles de administrador	VUL-0013	A.6.1.2 A.7.2.1 A.8.1.3 A.9.1.2 A.9.2.1 A.9.2.2 A.9.2.5 A.9.4.4 A.12.4.1 A.12.4.2 A.12.4.3	**CID**	**CID**	**D**	**CID**	**CID**	**X**	**X**
		Ausencia de usuarios nombrados para servidores de aplicación y base de datos	VUL-0014	A.7.2.3 A.8.2.3 A.9.1.2 A.9.2.3 A.9.4.1 A.9.4.2 A.9.4.4 A.9.4.5	**CID**	**CID**	**X**	**CID**	**CID**	**X**	**X**

		Inadecuada administración de usuarios que se incorporan cambia de área o se desvinculan de la institución	VUL-0015	A.6.1.1 A.6.1.2 A.7.2.1 A.7.3.1 A.9.1.2 A.9.2.1 A.9.2.2 A.9.2.6 A.9.3.1	**CID**	**CID**	**D**	**CID**	**CID**	**X**	**X**
		Falta de un sistema de administración de identidades	VUL-0016	A.6.1.2 A.7.2.3 A.8.2.3 A.9.1.2 A.9.2.4 A.9.4.1 A.9.4.2	**CID**	**CID**	**X**	**CID**	**CID**	**X**	**X**
Uso no previsto	AME-0005	Falta de control sobre instalación de aplicaciones (por uso de interés personal)	VUL-0017	A.12.5.1 A.12.6.2	**ID**	**ID**	**D**	**ID**	**D**	**X**	**D**
		Falta de control sobre perfiles de navegación en internet (por uso de interés personal)	VUL-0018	A.9.1.1 A.12.7.1 A.13.1.1 A.13.1.2 A.13.1.3	**ID**	**ID**	**D**	**D**	**D**	**X**	**X**

		Falta de control en uso de servicios de mensajería (por uso de interés personal)	VUL-0019	A.10.1.1 A.13.2.1 A.13.2.2 A.13.2.3 A.13.2.4	**CID**	**CID**	**D**	**CID**	**D**	**X**	**X**
		Falta de control por almacenamiento de datos personales (por uso de interés personal)	VUL-0020	A.6.2.2 A.7.2.1 A.7.2.2 A.8.2.1 A.8.2.3	**CID**	**CID**	**D**	**CD**	**D**	**X**	**X**

Apéndice E
Detalle de Controles y calificación

DETALLE DE CONTROLES									
Amenaza	**COD Amenaza**	**Vulnerabilidad**	**COD Vul.**	**Control**	**DETALLE DEL CONTROL ISO 27001/27002:2015**	**EXISTE**	**NIVEL**	**VALOR**	
								IMAC	**PROBA**
Uso no previsto	AME-0005	Falta de control sobre instalación de aplicaciones (por uso de interés personal)	VUL-0017	A.12.5.1	Instalación del software en los sistemas operativos: Los procedimientos deben ser implementados para controlar la instalación de software en los sistemas operativos.	**SI**	**4**	**-3**	**-2**
				A.12.6.2	Restricciones en la instalación del software: Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.	**SI**	**5**	**-3**	**-3**