UNIVERSIDAD DEL AZUAY

DEPARTAMENTO DE POSGRADOS

MAESTRIA EN AUDITORÍA INTEGRAL Y GESTIÓN DE RIESGOS FINANCIEROS
VERSION III

"Evaluación de la Metodología Ecu@Risk en la gestión de riesgos de Información de empresas MIPYMES de comercio exterior de la ciudad de Cuenca."

Trabajo de graduación previo la obtención del título de:
Magister en Auditoría Integral y Gestión de Riesgos Financieros

Autor:
Ing. Erika Lucero Q.

Director:
MBA, MSc. Esteban Crespo Martínez

Cuenca – Ecuador
Enero 2021

DEDICATORIA

El presente trabajo va dedicado a mis padres Sonia y Pablo, a mi hermana Michelle, a mi hija Emily y a mi abuelita Laura; quienes son el pilar fundamental en mi vida y sin duda con su paciencia y apoyo incondicional me han motivado a seguir adelante cada dia, con los valores y principios inculcados para conseguir mis objetivos.

Erika Johanna Lucero Quintuña.

AGRADECIMIENTO

Agradezco A Dios, por la fortaleza y bendición para alcanzar este objetivo en mi vida profesional.

Al Magister Esteban Crespo, por su apoyo incondiconal para llevar a cabo con éxito este proyecto al transmitirme sus valiosos conocimientos.

Erika Johanna Lucero Quintuña.

Resumen

En la actualidad el mundo digital forma parte diaria de la sociedad, incluyendo en pequeñas, medianas y grandes empresas. Los avances tecnológicos hacen que la información constituya un recurso primordial en cualquier tipo de organización sin importar su tamaño o actividad, y a su vez, da una ventaja competitiva ante las demás empresas. No obstante, la falta de organización y desconocimiento de las MIPYMES seguridad de la información constituye una debilidad, dificultando el cumplimiento de los objetivos planteados como organización. En el presente trabajo se aplica la metodología ECU@risk para la gestión del riesgo informático del sector MIPYMES, lo que permitió identificar y analizar la información de una empresa que brinda servicios de comercio exterior dentro de la ciudad de Cuenca. Como resultado, se generó y valoró el inventario de activos de información, las amenazas de entorno, y se determinó su nivel de exposición al riesgo.

Palabras Clave: *Activos de Información, ECU@risk, Seguridad de la Información, Riesgo informático, Ciberseguridad.*

Abstract

Currently, the digital world is a large part of society, including in small, medium, and large companies. Technological advances make information a fundamental resource in any type of organization regardless its size or activity. Additionally, it gives a competitive advantage to other companies. Nevertheless, the lack of organization and lack of awareness of MIPYMES in its information security demonstrates a weakness, which complicates the completion of the objectives in an organization. In the current work, the ECU@risk methodology was applied for the process of computer risk in the MIPYMES sector which allowed me to identify and analyze the information of one enterprise that provides services of external business within Cuenca. As a result, I was able to generate and value the inventory of information assets, the risks of surroundings, and determine the level of exhibition at risk.

Key Words: *Information assets; ECU@risk, Information Security, Information risk, Cybersecurity*

Translated by

Erika Lucero

Evaluación de la Metodología Ecu@Risk en la Gestión de Riesgos de Información de Empresas MIPYMES de Comercio Exterior de la Ciudad de Cuenca.

Erika Johanna Lucero Quintuña[1], Esteban Crespo-Martínez[1,2]
[1] Departamento de Posgrados, Universidad del Azuay, [2] LIDI
Cuenca, Ecuador
eriluceroq@es.uazuay.edu.ec; ecrespo@uazuay.edu.ec

***Resumen*— En la actualidad el mundo digital forma parte diaria de la sociedad, incluyendo en pequeñas, medianas y grandes empresas. Los avances tecnológicos hacen que la información constituya un recurso primordial en cualquier tipo de organización sin importar su tamaño o actividad, y a su vez, da una ventaja competitiva ante las demás empresas. No obstante, la falta de organización y desconocimiento de las MIPYMES en seguridad de la información constituye una debilidad, dificultando el cumplimiento de los objetivos planteados como organización. En el presente trabajo se aplica la metodología ECU@risk para la gestión del riesgo informático del sector MIPYMES, lo que permitió identificar y analizar la información de una empresa que brinda servicios de comercio exterior dentro de la ciudad de Cuenca. Como resultado, se generó y valoró el inventario de activos de información, las amenazas de entorno, y se determinó su nivel de exposición al riesgo.**

Palabras Clave— Activos de Información, ECU@risk, Seguridad de la Información, Riesgo informático, Ciberseguridad.

***Abstract*—Currently, the digital world is a large part of society, including in small, medium, and large companies. Technological advances make information a fundamental resource in any type of organization regardless its size or activity. Additionally, it gives a competitive advantage to other companies. Nevertheless, the lack of organization and lack of awareness of MIPYMES in its information security demonstrates a weakness, which complicates the completion of the objectives in an organization. In the current work, the ECU@risk methodology was applied for the process of computer risk in the MIPYMES sector which allowed me to identify and analyze the information of one enterprise that provides services of external business within Cuenca. As a result, I was able to generate and value the inventory of information assets, the risks of surroundings, and determine the level of exhibition at risk.**

Keywords— Information assets; ECU@risk, Information Security, Information risk, Cybersecurity

I. INTRODUCCIÓN

La información se considera uno de los activos más importantes de las organizaciones [1], ya que de ello depende el proceso que se realiza para el correcto funcionamiento. Por ello, el uso y difusión es muy importante ya que contribuye al cumplimiento de los objetivos organizacionales, además de ser una herramienta fundamental para la toma de decisiones, [2].

Según el texto citado por [3], las características de las pequeñas empresas se pueden considerar como: i) componente familiar, ii) falta de formalidad, iii) falta de liquidez, iv) problemas de solvencia, y v) fuente de financiamiento propio; y los rasgos que comparten son que operan con escalas bajas de producción y utilizan tecnologías adaptadas. En las MIPYMES, una de ellas, es el uso de tecnología en un mínimo nivel, los cuales son acondicionados únicamente para satisfacer una necesidad básica sin proyección a futuro. Así mismo, las actividades no están definidas específicamente en un manual de funciones y el acceso a la información está al alcance de todos.

Todas las organizaciones, independientemente del tamaño, actividad o capital, están expuestas al riesgo, y las MIPYMES no son una excepción, ya que tienen amenazas por diferentes factores tanto internos como externos; además [4]consideran que la informática es un área de soporte, y que la inversión en elementos y mecanismos de seguridad convergen solamente en soluciones antivirus. Es importante considerar la seguridad de la información en una MIPYMES como una estrategia organizacional, ya que existen procesos que involucra información sensible, y al ser divulgada a terceras personas sin autorización, podría encaminar en consecuencias graves para la organización.

Un sistema de gestión de seguridad de la información contempla elementos principales para una adecuada gestión de seguridad tales como: i) la confidencialidad de la información, no se pone a disposición ni se revela a

individuos, entidades no autorizados; ii) la Integridad hace referencia a la exactitud de la información; y, finalmente, iii) la Disponibilidad que permite el acceso y uso de la información cuando sea requerida [5].

Para [6], la seguridad de la información está relacionada con las medidas preventivas aplicadas con el fin de salvaguardar y proteger la información bajo la confidencialidad, disponibilidad e integridad. Por otro lado, y siguiendo los lineamientos de la norma, el principal objetivo de la ISO 27001, es proteger la confidencialidad, integridad y disponibilidad de la información que posee la empresa [7].

La seguridad de los activos de información está en función de una correcta gestión para el análisis de riesgos que involucre a todo el personal de la empresa. Así, los autores [8] mencionan que la implementación de un sistema de seguridad de información es un factor importante en las organizaciones, ya que la omisión de este sistema puede comprometer los activos de la empresa.

ECU@Risk es una metodología para la gestión del riesgo informático aplicable a MIPYMES, partiendo de la identificación de los activos financieros, la valoración en términos de disponibilidad, integridad y confidencialidad, identificación de amenazas, concluyendo con el análisis de los riesgos a los que se ve afectado la organización por la falta de una adecuada gestión de riesgos [1].

En este trabajo se evalúa el porcentaje de exposición de las MIPYMES frente al riesgo de información aplicando la metodología ECU@Risk en una empresa de prestación de servicios de comercio exterior de la Ciudad de Cuenca.

Para el desarrollo se establecen 5 secciones que lo componen y que están divididas de la siguiente manera: i) Estado del arte, en el que se indica la teoría referente a: comercio exterior, MIPYMES, gestión de riesgos, activos de información; ii) la metodología aplicada que explica el procedimiento para selección de las herramientas que fueron utilizadas; iii) los resultados iniciando con los datos obtenidos de las encuestas aplicadas y valores obtenidos en el que se detalla los datos numéricos ya aplicando la metodología con el uso de la herramienta propuesta por la metodología ECU@Risk; iv) discusión entre varios autores con trabajos relacionados y finalmente v) las conclusiones y trabajos futuros.

II. ESTADO DEL ARTE

El comercio exterior constantemente va tomando mayor espacio a nivel nacional e internacional; es por ello que, en muchos casos forma parte de la cotidianidad de algunas empresas, ya que de cierta manera resulta una respuesta al riesgo de la producción nacional [9]. Para [10], en su informe analizan las políticas de comercio exterior en el periodo 2014-2018, definiendo como políticas de comercio exterior a un instrumento de negociación que facilita las transacciones entre países.

Esta rama comercial surge con la necesidad del intercambio de productos, no solo nacional, sino internacionalmente, considerando los más estrictos estándares de calidad para ser aceptados en los mercados internacionales [11]. Como consecuencia de una constante expansión, nacen las empresas intermediarias de comercio exterior, con el fin de solventar las necesidades y manejar toda la logística integral y el proceso aduanero de las diferentes empresas exportadoras e importadoras.

En el proceso de las importaciones, las mercancías que ingresan al país, deben ser nacionalizadas bajo ciertos regímenes, ya sean especiales o comunes, capitulo VII del Código Orgánico de la producción, comercio e inversión [12]; de igual manera, deben ingresar a las diferentes bodegas de almacenamiento temporal autorizadas por la Aduana hasta que se realice el proceso de nacionalización en el cual intervendrán el importador, intermediario o agente de aduana (Art. 231 del COPCI) [12], para la recolección de la documentación respectiva a ingresar en el sistema aduanero.

La sección II del Capítulo VII del COPCI estable todas las directrices para las exportaciones, iniciando con el registro del operador económico autorizado (Art. 231 COPCI), el proceso de la salida de mercaderías es igual al de ingreso; en consecuencia, está sujeto a una revisión aduanera para la autorización de salida [12].

Toda la información es ingresada a la página del Servicio Nacional de Aduana del Ecuador SENAE para el manejo de procesos aduaneros, para lo que se requiere aplicaciones basadas en JAVA para su correcto funcionamiento y una actualización constante de este aplicativo. Los requisitos solicitados en el proceso de ingreso de la información para la revisión por parte de la aduana, así como las observaciones al trámite, estado del trámite, valores de aranceles y tasas, se reflejan en el sistema ECUAPASS, al ingresar con un código único asignado por la SENAE a cada usuario de comercio exterior.

Las empresas intermediarias de comercio exterior se establecen con el fin de prestar servicios de asesoría logística en trámites de importación y exportación, y brindar un servicio integral a sus clientes, iniciando con la coordinación del embarque de la mercadería, nacionalización y entrega en destino al cliente. Esto es, un servicio integral tanto para el importador como para el exportador, adaptándose a las necesidades de los clientes. Estas organizaciones son pequeñas y de carácter familiar, cumplen con todos los requisitos establecidos por el ente controlador y con sus obligaciones a la Superintendencia de Compañías.

Según [13], el término MIPYMES hace referencia a las micro, pequeñas y medianas empresas del entorno. Las microempresas tienen un número de empleados igual o menor a 9 personas y sus ingresos anuales no superan los 100 mil dólares, para las pequeñas empresas el número de empleados no supera los 49 empleados y sus ventas anuales son inferiores a 1 millón de dólares, las medianas empresas cuentan hasta con 199 empleados y sus ingresos anuales no sobrepasan los 5 millones dólares y finalmente las grandes

empresas que superan los 200 colaborados y sus ingresos anuales son superiores a los 5 millones de dólares. En todos los casos prevalece el criterio del valor anual de los ingresos sobre las demás características. [14]

Para [15], el Ecuador cuenta con una gran cantidad de MIPYMES en diferentes áreas tales como comerciales, de servicios o industriales. El informe [16] indica que a nivel nacional, del total de las empresas censadas, el 58.3% son microempresas, el 28% son pequeñas empresas, 9.6% medianas empresas y tan solo el 4.1% son grandes empresas, por lo cual, las MIPYMES ocupan un espacio estratégico en el mercado comercial y laboral del país, y a su vez es un generador de fuentes de empleo en este sector, alcanzando el 60.5% al 2018 según los Indicadores Nacionales de la plaza de empleos generados [17], aportando también a la sostenibilidad del país y a la disminución de la tasa de desempleo nacional.

Yance et al [18], resaltan la importancia de MIPYMES para el buen desarrollo en un ambiente de mejora continuo, que les permita un crecimiento sostenible en el tiempo, con el objetivo de posicionarse y mantenerse en el mercado, con adecuadas fuentes de financiamiento. Por otro lado, la necesidad de incrementar su desempeño e implementar estrategias que beneficien las operaciones con el fin de reducir los costos de operación, mejorar la eficiencia de los procesos, los niveles de inventario, la calidad de los productos y por supuesto incrementar la productividad. Estas organizaciones han ido evolucionando a nivel nacional con el pasar de los años, pero sin duda se enfrentan a la competencia de grandes empresas con poderes económicos, por lo que la subsistencia les resulta algo completo, sin embargo, por su tamaño pueden ajustarse con mayor facilidad a los nuevos requerimientos del mercado y de los clientes, lo cual genera una ventaja competitiva frente a las grandes empresas que se ven más comprometidas.

Dentro de las características de las MIPYMES, se menciona que son de componente familiar, carecen de formalidad y liquidez lo que conlleva a tener problemas de solvencia [3]. Así mismo, cuentan con una estructura organizacional sencilla que básicamente ayuda a la toma de decisiones y a su vez afrontan el problema, ya que se exige un mayor grado de responsabilidad sobre el socio principal o dueño de la empresa en el manejo de la organización, forzados a tomar la orientación, la sostenibilidad y subsistencia. De la misma manera, al ser de carácter familiar no se da la importación adecuada a las capacitaciones del personal, y a medida que la organización crece se dificultan las funciones asignadas por la magnitud de la empresa [19]. Dentro de los rasgos que comparten se resumen: i) operación con escalas bajas de producción, ii) utilización de tecnologías adaptadas, y iii) autofinanciamiento [3].

En los últimos 25 años, la economía mundial se ha caracterizado por numerosos avances científicos y tecnológicos, lo cual ha modificado los patrones de producción en todo el mundo [20]. Para [15], a causa de la globalización, las MIPYMES se ven afectadas por la prolongación de la competitividad mundial, ya que muchas de éstas no cuentan con apoyo financiero, economías de escala, o no son lo suficientemente competentes para mantenerse en los mercados competitivos, a causa de la falta de digitalización. Por otra parte, [21] menciona que las empresas necesitan una infraestructura informática segura, que minimice los riesgos asociados con la seguridad y los costos de administración y operaciones, ya que, de no contar con las seguridades necesarias, se ven expuestas a riesgos que amenazan de manera directa los activos de la empresa, siendo los activos de información uno de los más importantes para las empresas.

Las TIC son recursos esenciales para la productividad y competitividad de las organizaciones, por ello, están sujetas a diferentes amenazas que se pueden materializar en riesgos, con múltiples consecuencias [22]. Su participación en el desarrollo de actividades de MIPYMES, permiten procesar, administrar, compartir datos, información y conocimientos a través de soportes tecnológicos [23]. Su uso es esencial para mejorar la productividad de las empresas, la calidad, el control y facilitar la comunicación [24]. Considerando los criterios antes citados, es importante mencionar que la tecnología obliga a una actualización constante en los sistemas tecnológicos de las diferentes empresas sin importar su tamaño o actividad económica. Según [21], la globalización económica exige que las organizaciones cuenten con plataformas tecnológicas para sus negocios, con este fin se desarrollan proyectos que garanticen la seguridad de la información.

La seguridad de la información es fundamental para la supervivencia de las organizaciones en la era de la información, lo cual, incluye la protección de información, sistemas, recursos y demás activos contra desastres, errores (intencionales o no) y manipulación no autorizada, para reducir la probabilidad y el impacto de los incidentes de seguridad [25]. Por otra parte, se enfatiza sobre el principal objetivo de la ISO 27001 [7], que es proteger la confidencialidad, integridad y disponibilidad de la información que posee la empresa, ya que aporta al sistema de seguridad de la información mediante medidas para la protección contra cualquier amenaza, basada en la gestión de riesgos.

La metodología ECU@risk provee de manera detallada los principios y procesos que son necesarios para identificar y valorar los activos de información, las amenazas, cálculo del riesgo, identificar las contramedidas y establecer políticas de seguridad; así mismo, propone utilizar en los procesos elementos que todas las MIPYMES cuentan para el inventario de activos de información; considerando como: edificaciones o instalaciones, el hardware, el software, la información electrónica, la información en papel, la infraestructura de comunicaciones, los medios de almacenamiento extraíbles y los recursos humanos [1].

III. METODOLOGIA

Mediante la aplicación de la metodología ECU@RISK, se evaluó la eficiencia de la gestión de riesgo en una empresa de

comercio exterior. Para ello se consideraron las etapas de análisis que se exponen a continuación.

El proceso de recolección de información se realizó mediante la aplicación de una encuesta a tres empresas del sector de comercio exterior dentro de la ciudad, las mismas fueron realizadas a los principales directivos de las empresas selectas para el estudio, aplicando el muestreo por conveniencia. Las preguntas fueron establecidas para determinar el nivel de exposición de la información, las seguridades con las que cuenta la empresa para el resguardo y el motivo de la falta de implementación de un sistema de gestión de seguridad de la información. Las preguntas para considerar fueron seleccionadas, referentes al conocimiento de las empresas respecto a los activos de información, frecuencia de los respaldos de la información, sistemas antivirus, mantenimiento de los equipos y seguridad de la información. De igual manera para la aplicación de la metodología se realizó una visita a una de las empresas encuestadas considerando su nivel de trabajo, colaboradores, infraestructura, activos, ingresos y gastos; para determinar información sobre el manejo tecnológico y analizar el nivel de seguridad que poseen respecto a la información.

Para el análisis del contexto externo se utilizó la herramienta PESTEL, la cual permite el análisis descriptivo del entorno de una empresa, para describir el contexto de la empresa, considerando seis factores: Políticos, Económicos, Sociales, Tecnológicos, Ecológicos o Ambientales y Legales [26].

Para la etapa de identificación de los activos de información se consideró la clasificación sugerida por la metodología ECU@RISK: Edificaciones o instalaciones (ED), hardware (HW), software (SW), información electrónica (IE), información en papel (IP), infraestructura de comunicaciones (IC), medios de almacenamiento extraíbles (Extraíble) y los recursos humanos (RRHH); elementos con que toda organización del sector MIPYMES cuenta [1], al igual que para la valoración se consideró las dimensiones de seguridad de valoración: Disponibilidad (D), integridad (I) y confidencialidad (C).

Se inventariaron y valoraron los activos de información y las amenazas de contexto según lo sugerido por ECU@RISK. Este último aspecto fue agrupado mediante: i) Riesgos naturales, ii) Riesgos provocados (deliberados), iii) Riesgos provocados (por error), iv) Riesgos informáticos y v) Riesgos de comunicaciones.

Consecuentemente, se calculó el riesgo absoluto mediante la ecuación riesgo = probabilidad * impacto, y los resultados fueron registrados en la matriz de riesgo. Esto permitió formular las contramedidas para hacer frente a las amenazas, y con su evaluación y control, hacer el cálculo residual en un futuro.

Al ser una empresa MIPYME, las probabilidades de sufrir incidentes no deseados son muy altas. En el siguiente apartado se muestran los resultados obtenidos, así como el nivel de impacto que se llegaría a tener en caso de la materialización de una amenaza.

IV. Resultados

Una vez analizados los resultados obtenidos de las encuestas realizadas a tres empresas que pertenecen al sector de comercio exterior dentro de la ciudad de Cuenca, en primera instancia, se aprecia que el 100% de las empresas encuestadas no tienen identificados los activos de información que disponen.

Para hacer frente a los respaldos de información que realizan las empresas, se determinó que el 100% los realiza. Así mismo, se logró obtener que en ningún caso bajo procedimientos formales.

Con respecto a la frecuencia de los respaldos realizados de la información, se identificó que el 33% lo realiza semestralmente, mientras que el 67% lo hace mensualmente.

Se identificó también, que, el 100% de las empresas encuestadas cuentan con un sistema antivirus, de estos, el 33% cuenta con el sistema antivirus Eset Nod32 y el 67% restante cuenta con el sistema antivirus Norton.

Por otro lado, respecto al mantenimiento de los equipos, se evidenció que el 67% de las empresas encuestadas realiza mantenimiento de los equipos por personal calificado, mientras que, el 33% no lo hace con personal calificado. Por otro lado, se determinó que los mantenimientos los realizan semestralmente en un 67% y el restante lo hace mensualmente.

El 100% de los encuestados entrega claves de seguridad a todos sus colaboradores para el acceso a la información confidencial, únicamente en el proceso de entrega del cargo. Respecto a la manipulación de la información confidencial dentro de la empresa, se determinó que el 33% considera que la información no es manipulada correctamente por su personal, mientras que el 67% coincide que la información confidencial es tratada de forma acertada.

Con relación a las amenazas, el 33% argumenta que, si ha identificado aquellas que afectan a los activos de información, mientras que el 67% no las ha identificado. De las empresas encuestadas el 100% no ha identificado sus amenazas bajo procedimientos formales ni normas internacionales.

Las razones por las que las empresas no ha implementado un sistema de gestión de seguridad de la información son, el 67% coincide que no ha realizado por la complejidad de la norma a implementar, mientras que el 33% por desconocimiento de los procesos y normas que se deben establecer para obtener una gestión adecuada de la información.

Identificación del tipo y tamaño de la organización

La empresa analizada brinda servicios de comercio exterior y servicios de asesoría logística para trámites de importación y exportación. Se clasifica como empresa privada y está bajo control de la Superintendencia de Compañías y Seguros, ubicada dentro de la ciudad con varios años en el mercado.

Por su trayectoria en el mercado y considerando aspectos antes mencionadas referente a las características de las MIPYMES, la empresa está dentro de las medianas empresas. Por su cobertura económica, el ámbito de la empresa es de nivel nacional.

ANÁLISIS DE CONTEXTO EXTERNO

Para el estudio se han identificado los factores presentados a continuación:

FACTORES POLÍTICOS

La Organización Mundial del Comercio (OMC) es una organización internacional conformada por 164 países miembros, tiene como objetivo velar por que las corrientes comerciales circulen con la mayor fluidez, previsibilidad y libertad posible mediante acuerdos negociados y firmados por la gran mayoría de las economías que participan en el comercio mundial y ratificados por sus respectivos Parlamentos; para instaurar un marco estable y transparente para ayudar a los productores de bienes y de servicios, los exportadores y los importadores a llevar adelante sus actividades con el objetivo es mejorar el nivel de bienestar de la población de los Miembros de la OMC [27].

Ecuador actualmente mantiene 11 acuerdos Comerciales vigentes, que son: Acuerdo De Cartagena, Acuerdo Ce De Cuba, AAPR México, AAPCE Mercosur, Acuerdo Con Chile, AAP 25tm 42 Guatemala, ACM Unión Europea, AAP 25tm 45 Nicaragua, AAP 25tm 46 El Salvador, AAEI EDTA, Acuerdo Con Reino Unido [28].

Las empresas que operan en los mercados desarrollados como en los emergentes enfrentan un panorama de riesgo político complejo y volátil en 2020, con desafíos para el multilateralismo y el libre comercio; los niveles de deuda global siguen siendo motivo de preocupación, y la deuda en los mercados emergentes alcanzó el 170% del PIB a fines de 2018; por otro lado, el informe indica la posibilidad de que reduzca la capacidad de recuperación a los impactos económicos en 2020, [29].

El Comité de Comercio Exterior es el organismo que aprueba las políticas públicas nacionales, en materia de política comercial; implementadas para el manejo correcto del comercio internacional; estas políticas existen para el área de competencia y son: -Política Arancelaria, Negociaciones internacionales, Políticas para el desarrollo de los regímenes especiales, Medidas para contrarrestar el comercio desleal, Definir políticas y Aprobar plan de promoción de exportaciones

FACTORES ECONÓMICOS

Dentro de los factores económicos, la rápida propagación del COVID-19 y las medidas adoptadas por los gobiernos han tenido graves consecuencias en las principales economías mundiales, interrumpiendo la producción a nivel mundial, y el cierre de fronteras; es así que en mayo de 2020 el volumen del comercio mundial de bienes cayó en un 17,7% con respecto al mismo mes de 2019 y afecto principalmente a Estados Unidos, Japón y la Unión Europea. Por otra parte, China experimentó una contracción menor, ya que controló el brote y reabrió su economía relativamente rápido. América Latina y el Caribe es la región en desarrollo más afectada. El valor de las exportaciones e importaciones de bienes se redujo en un 17% entre enero y mayo de 2020 en comparación con el mismo período de 2019 [30].

Por otro lado, el informe presentado por el INEC al 2014, para el sector de servicios, del 54,51% de las empresas innovadoras el 26,44% corresponden al sector servicios [33].

El COVID-19 ha impactado la economía ecuatoriana, el sector exportador se ve afectado ya que el comercio internacional representa un factor primordial en la economía; los ingresos percibidos de la nación dependen de la exportación de productos [31].

Con el fin de fomentar las importaciones de bienes de capital y materias primas necesarias para el desarrollo de un proyecto, b) Dividendos distribuidos por sociedades nacionales o extranjeras domiciliadas en el Ecuador, en el Art.- 27 de la ley orgánica para el fomento productivo, atracción de inversiones, generación de empleo, y estabilidad y equilibrio fiscal se establece la exoneración del Impuesto a la salida de divisas (ISD) [32]. Por otra parte, el Art. 68., establece los criterios a los que pueden acogerse las empresas privadas que requieran financiamiento para desarrollar nuevas inversiones, y que a su vez quisieran ejecutar un programa de apertura de capital; entre los beneficios figura, el uso de un crédito flexible con tasas de interés preferenciales y créditos a largo plazo.

FACTORES SOCIO-CULTURALES

Los resultados de la Encuesta de Estratificación del Nivel Socioeconómico presentados por el INEC al 2011, realizado a 9.744 viviendas del área urbana de Quito, Guayaquil, Cuenca, Machala y Ambato, indica que los hogares de Ecuador se dividen en cinco segmentos, siendo el segmento A el que involucra el mayor puntaje sobre 1000 y, posee las características acordes de vivienda tecnología, educación, servicios básicos, bienes y economía; mientras que, el segmento D es el segmento que menor puntaje obtuvo por la carencia o deficiencia en las características antes mencionadas. Siendo así, el 1,9% pertenece al nivel A, el 11,2% al nivel B, el 22,8% al nivel C+, el 49,3% está en estrato C- y el 14,9% en el nivel D; con estos resultados se conoce los grupos socioeconómicos relevantes y las características de cada uno [34].

La población Cuencana es conocida como emprendedora y muchos empresarios azuayos tienen la visión para desarrollar sus negocios y convertirlos de micro o pequeñas fábricas a grandes industrias. En las últimas tres décadas, no solo invirtieron en la producción, tecnología y calidad sino también en mano de obra y nuevas estrategias comerciales y servicios. La industria cuencana se consolida en el Ecuador y sus productos llegan a más de 30 países [35].

FACTORES TECNOLÓGICOS

La opinión de interés N°390 publicada por el Observatorio PYME, con su autora [36] acota que, actualmente las MIPYMES invierten en tecnología para adaptarse a la nueva normalidad. En este contexto se puede mencionar que el Ministerio de Trabajo reporta que el 91,4% de las MIPYMES están en teletrabajo, las cuales se vieron obligadas para continuar con su actividad y sin contar con una planificación establecida para hacer frente a la inversión en esta nueva forma de trabajo.

FACTORES ECOLÓGICOS O AMBIENTALES

La Organización Mundial de la Salud [27] informa del actual brote de enfermedad por coronavirus (COVID-19) que fue notificado por primera vez en Wuhan (China) el 31 de diciembre de 2019; así mismo, está colaborando estrechamente con expertos mundiales, gobiernos y asociados para ampliar rápidamente los conocimientos científicos sobre este nuevo virus, rastrear su propagación y virulencia y asesorar a los países y las personas sobre la medidas para proteger la salud y prevenir la propagación del brote.

Actualmente se vive ante una situación de salud compleja que ha puesto en jaque al mundo entero y que, además, sorprende con inesperadas consecuencias medioambientales.

El aislamiento en casi todo el mundo y la paralización de la actividad industrial, así como la reducción de desplazamientos, han devuelto a las principales ciudades del mundo sus cielos azules y reducido los niveles de contaminación. Eso sí, el coronavirus además de ser una amenaza para la salud pública se está convirtiendo en una amenaza real para el medioambiente si no se actúa a tiempo y con responsabilidad. El uso de mascarillas, guantes y geles desinfectantes se han convertido en esenciales para la humanidad, pero son nocivos si no actuamos con responsabilidad a la hora de desecharlos; mientras, se pueden ver cielos despejados y sin contaminación, el consumo de plásticos sigue aumentando considerablemente [37].

En este contexto, en Ecuador el Ministerio del Ambiente es el ente encargado de emitir las políticas generales para promover las buenas prácticas ambientales en las entidades del sector público y privado con el objetivo de reducir la contaminación ambiental [38].

El Art. 72 del COPCI atribuye las Competencias como deberes y atribuciones del organismo rector en materia de política comercial al literal S: Promover exportaciones e importaciones ambientalmente responsables [12].

La normativa está comprometida y enfocados en la ayuda al medio ambiente y concientizar el cuidado y la protección, ya que al prestar servicios de comercios exterior tanto importadores como exportadores deben concientizar y priorizar el uso de material biodegradable para su embalaje.

FACTORES LEGALES

El Art. 124.- del COPCI indica que toda persona podrá presentar reclamo administrativo en contra de los actos administrativos que afectaren directamente sus derechos, dentro del plazo de veinte días contados desde la fecha en que hubiere sido notificado con dicho acto [12].

Tomando como referencia el artículo mencionado anteriormente, existe normativa vigente para acceder a reclamos aduaneros en caso de que afecten al importador o exportador, lo que genera una ventaja y un beneficio en el cumplimiento de los derechos de los usuarios de comercio Exterior.

ANÁLISIS DE CONTEXTO INTERNO

El análisis FODA para [3], es una herramienta que puede ser aplicada para obtener un diagnóstico preciso que permite tomar decisiones estratégicas para mejorar la situación actual en el futuro. Los elementos que conforman el análisis como las fortalezas y debilidades, son de origen interno; mientras que de origen externo tenemos las oportunidades y amenazas. Para el estudio se han identificado los aspectos presentados en la siguiente tabla.

TABLA 1: FODA

FODA PARA LA EMPRESA DE COMERCIO EXTERIOR	
FORTALEZAS	**DEBILIDADES**
Personal con conocimiento en comercio exterior.	Infraestructura inadecuada.
Personal comprometido.	Falta de automatización.
Posibilidad de inversión.	Falta de capacitación.
Diferenciación de las empresas del medio.	Falta de manuales para la ejecución de procesos.
Experiencia en el servicio de logística.	Uso de equipos obsoletos.
OPORTUNIDADES	**AMENAZAS**
Alta demanda de clientes para importaciones y exportaciones.	Cambios constantes en la normativa.
Automatización de procesos en aduana para agilitar documentación.	Retrasos en la logística internacional.
Reducción de tasas arancelarias.	Retrasos en la aduana.
Crecimientos a nivel nacional de exportadores e importadores.	Incremento de tarifas de fletes internacionales por la competitividad.
Creciente Apertura de financiación para importaciones.	Ingreso de nuevos competidores.

Así mismo, se obtuvo información de los valores compartidos de la organización. Dicha información reposa en los archivos de la organización.

Considerando los cuestionarios de aplicación de la Metodología ECU@Risk para la identificación del estilo organizacional, las dos siguientes tablas presentan los resultados de la encuesta realizada al máximo representante de la empresa y al encargado del departamento de talento humano para evaluar tal como lo sugiere la metodología.

La ponderación está basada como 1 es “Muy Bajo” y 5 es “Muy Alto”. [1].

TABLA 2: MATRIZ DE IDENTIFICACIÓN DEL ESTILO ORGANIZACIONAL: TALENTO HUMANO

Matriz de identificación del estilo organizacional					
Cuestionamientos	**1**	**2**	**3**	**4**	**5**
¿La rotación del personal en la empresa es?		X			
¿La empresa tiene empleados con exceso de trabajo?				X	
¿Existen situaciones de controversia entre los empleados?	X				
¿El índice de reclamos por parte de los clientes es?	X				
¿El número de empleados que trabaja horas adicionales es?					X

Para la siguiente tabla se considera un intervalo de: 1: “nunca” 2: “Casi nunca” 3: “A veces” 4: “Con frecuencia” 5: “Siempre”.

TABLA 3: : MATRIZ DE IDENTIFICACIÓN DEL ESTILO ORGANIZACIONAL: GERENTE

Matriz de identificación del estilo organizacional					
Cuestionamientos	**1**	**2**	**3**	**4**	**5**
¿La gerencia general tiene reclamos por parte de sus empleados?			X		
¿Los clientes han reclamado por mala atención del personal?	X				
¿Los clientes han reclamado por servicios incumplidos?		X			
¿Los clientes han reclamado por negligencia?	X				
¿Se han producido robos internos?	X				
¿La empresa ha sido víctima de actos fraudulentos?	X				
¿La empresa ha sido víctima de sabotajes de información?	X				
Los valores compartidos organizacionales son transmitidos (durante el año):			X		
Ha realizado evaluaciones a sus empleados a fin de determinar el nivel de conocimiento sobre los valores compartidos		X			

IDENTIFICACIÓN DE ROLES Y ACTIVIDADES

La siguiente tabla muestra los procesos principales de la empresa analizada y sus respectivas actividades, en este contexto se determinó que la empresa no cuenta con manuales para el correcto desempeño y cumplimiento de las actividades del personal que labora dentro de la organización.

TABLA 4: PROCESOS Y ACTIVIDADES

PROCESO	ACTIVIDADES
Operación y Logística de importaciones.	Apertura de los tramites de Importación, coordinación y manejo de documentos, gestión logística.
Operación y Logística de Exportaciones.	Apertura de los tramites de Exportación, coordinación de embarques y manejo de documentos, gestión logística interna.
Registro Contable.	Ingresos y egresos relacionados a contabilidad.

IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN

Para la identificación de los activos de información se consideró los procesos y actividades de la organización detallados en la tabla 4, obteniendo el inventario de los activos con los que cuenta la empresa, considerando la clasificación y la codificación sugerida por la metodología.

Mediante la aplicación de la metodología, para la clasificación de ECU@Risk se realizó el inventario de los activos para: a) Edificaciones, la empresa tiene sus instalaciones ubicadas dentro del sector urbano de la Ciudad, mismo que es arrendado; b) Hardware, en el que se desglosa 5 computadoras portátiles a cargo del personal de la empresa de las diferentes áreas y 1 computadora de escritorio, además de 4 impresoras de marca Epson; c) Software, se determinó que la empresa cuenta con la licencia del sistema antivirus Norton que es renovado anualmente para todos los equipos de la empresa. Por otro lado, se determinó un dominio de la cuenta de correo electrónico de la empresa que es renovado en la misma frecuencia que el sistema antivirus, sin embargo, la instalación es defectuosa en dos de los equipos inventariados; d) Información electrónica, se consideró los archivos más importantes para la organización entre los que se disponen de Plantilla de Importaciones y exportaciones, Matriz gestión embarques, Matriz Contabilidad Anexos y los archivos de respaldo, mismos que no están actualizados a la fecha de inventario, manteniendo un retraso de 8 meses; e) Información en papel, se registra en las oficinas de la empresa y una sola persona es la encargada de mantener el archivo actualizado; f) infraestructura de comunicaciones; g) extraíble y h) recursos humanos; son elementos con los que cuenta la organización como parte de su inventario de activos de información. (Anexo 2: Identificación de Activos)

VALORACIÓN DE ACTIVOS DE INFORMACIÓN

Para la identificación de los activos de información y su respectiva valoración, se obtuvo la aprobación de los directivos; se estableció un comité integrado por el gerente general, jefe de operaciones y el jefe de contabilidad, quienes formaron parte de todo el proceso y brindaron información oportuna y veraz para el desarrollo del presente estudio.

Por otro lado, se establecieron parámetros para la valoración de activos, considerando el número de veces ocurrido durante el último año, en donde 1 significa un daño mínimo y 5 un daño extremo, para ello su calificación depende de la importancia de cada activo considerando los 3 elementos mencionados: confidencialidad, integridad y disponibilidad.

TABLA 5: CRITERIOS DE VALORACIÓN

VALOR	CRITERIO	
5	Extremo	Daño extremadamente grave
4	Alto	Daño muy grave
3	Moderado	Daño grave
2	Menor	Daño importante
1	Leve	Daño menor
0	Despreciable	Irrelevante

FUENTE: [1]

A partir de obtener información de los activos, clasificación y valoración; mediante un diálogo con el personal de la

empresa se diagnosticó que la organización no dispone de un proceso para la gestión de riesgo informático, falta de mantenimiento a los equipos, inadecuado cableado de red, deficiencia de personal con experiencia en el área informática, la información no es respaldada en unidades extraíbles externas a excepción del departamento contable que lo hace en diferentes periodos no delimitados y cuando la persona encargada lo considera conveniente, las contraseñas son manipuladas por diferentes usuarios. Cuentan con un sistema contable desde hace aproximadamente 10 años el cual presenta dificultades y únicamente se adapta a las necesidades básicas del giro del negocio.

IDENTIFICACIÓN DE AMENAZAS

La identificación de las posibles amenazas que afecten a la organización es fundamental para la determinación del riesgo, previo a la identificación, codificación y valoración de las amenazas se identifica los problemas con los que cuenta la organización detallados en un registro para su fácil identificación.

La siguiente tabla representa la escala usada para el análisis.

TABLA 6: ESCALA

Evento	Frecuencia de ocurrencias en el año	Escala
Extremo	Más de 7	5
Alto	7	4
Moderado	5-6	3
Menor	3-4	2
Leve	1-2	1
Despreciable	0	0

En la siguiente tabla se procede con la identificación de amenazas para cada activo, en donde se verificó la frecuencia con la que se has suscitado los problemas medida en ocurrencias anuales durante el último año, cada amenaza fue codificada para identificarlas fácilmente, tal como lo indica la metodología ECU@risk.

TABLA 7: CÓDIGO DE AMENAZA

CODIGO DE AMENAZA
[NO_INTENCIONADO.1]
[NO_INTENCIONADO.2]
[NO_INTENCIONADO.6]
[NO_INTENCIONADO.7]
[PROVOCADO. *]
[EC.1]
[EL.1]

TABLA 8: AMENAZAS

AMENAZAS	FRECUENCIA
Errores del personal.	3
Errores en los registros.	3
Alteración de información en el proceso de respaldo.	2
Perdida de información accidentalmente	2
Alteración de información, corte de energía.	3
Error en él envió de información por red - correo electrónico.	5
Propagación de virus por falta de control.	4

De igual manera, se estableció los activos de información amenazados y las dimensiones afectadas ya sea por confidencialidad (C), disponibilidad (D) e integridad (I), reflejados en la tabla presentada a continuación:

TABLA 9: IDENTIFICACIÓN DE AMENAZAS

CÓDIGO DE AMENZA	ACTIVO AMENAZADO	C	D	I
[NO_INTENCIONADO.1]	HARDWARE (HW)	X	X	X
	SOFTWARE (SW)			
	MEDIO DE ALMACENAMIENTO EXTRAÍBLE (EXTRAÍBLE)			
	INFORMACIÓN ELECTRÓNICA (IE)			
[NO_INTENCIONADO.2]	INFRAESTRUCTURA DE COMUNICACIONES (IC)	X	X	X
[PROVOCADO. *]	HARDWARE (HW)		X	
	INFRAESTRUCTURA DE COMUNICACIONES (IC)			
	INFORMACIÓN ELECTRÓNICA (IE)			
[EL.1]	INFORMACIÓN ELECTRÓNICA (IE)	X	X	X
	SOFTWARE (SW)			
[NO_INTENCIONADO.6]	SOFTWARE (SW)			X
	MEDIO DE ALMACENAMIENTO EXTRAÍBLE (EXTRAÍBLE)			
[NO_INTENCIONADO.7]	SOFTWARE (SW)		X	
	INFORMACIÓN ELECTRÓNICA (IE)			
	MEDIO DE ALMACENAMIENTO EXTRAÍBLE (IE)			
[EC.1]	INFRAESTRUCTURA DE COMUNICACIONES (IC)	X		

Una vez determinada las dimensiones a las que afectada cada amenaza se establece el nivel de ocurrencia para cada una, y a su vez la matriz permite encontrar los resultados del riesgo absoluto e identificar con sus respectivos criterios respecto al impacto y probabilidad que se obtuvieron de la valoración de los activos de información. Al igual que, para la valoración del nivel de riesgo se considera la Matriz de Riesgos, para determinar la calificación del riesgo considerando 5 niveles: leve, menor, moderado, alto y extremo. Para el análisis, se calcula el nivel de riesgo que es el producto de la multiplicación del impacto por la probabilidad; de la matriz de valoración de activos se multiplica por la frecuencia por cada una de las dimensiones afectadas que fueron previamente valoradas.

TABLA 10: VALORACIÓN DE RIESGO

Clasificación	Valoración	Calificación
E – Casi certero (frecuente)	20-25	5
A – Probable	10-16	4
M – Posible	5-9	3
B – Baja o no muy común	3-4	2
L – Raro	1-2	1

Fuente: [1]

Como resultado de la valoración se obtuvo como calificación mínima del riesgo absoluto un valor de 6 para los Archivos de respaldo, Disco Duro Extraíble, y como calificación máxima un valor 20 para el Servidor de Correo; situando los valores en la tabla 10 y tabla 11, los activos de la organización tienen un riesgo moderado, alto y extremo.

TRATAMIENTO DEL RIESGO.

De los resultados obtenidos del cálculo del riesgo, se consideran los siguientes niveles para la aceptación del riesgo

TABLA 11: NIVELES DE RIESGO – VALORACIÓN

NIVELES DE RIESGO	
Riesgo extremo - E	Requiere una acción y respuesta inmediata
Riesgo alto - A	Atención prioritaria
Riesgo moderado - M	Determinar si existe controles y si son aplicados correctamente
Riesgo menor - B	Requiere de supervisión
Riesgo leve - L	Monitoreos constantes

A partir de la identificación y valoración de los riesgos, se determina el tipo de tratamiento para cada riesgo identificado según el nivel de riesgo expuesto, así mismo se busca que este sea adecuado para lograr su implementación y reducir el nivel de exposición o minimizar el riesgo.

Para el nivel de riesgo extremo se requiere una acción y respuesta inmediata a la amenaza que afecta él envió de información por una red incorrecta, el tratamiento a establecer es contratar personal experto en el área para la revisión constante de las redes.

Para el nivel de riesgo alto, se requiere una atención prioritaria. En este nivel se determinaron las siguientes amenazas y tratamiento para cada una de ellas.

TABLA 12: NIVEL DE RIESGO ALTO

AMENAZAS	TRATAMIENTO
Errores de manipulación por parte de los usuarios.	Capacitación al personal de la organización.
Corte de energía eléctrica.	Adquisición de un generador eléctrico.
Falta de mantenimiento.	Establecer un cronograma de mantenimiento a los equipos.
Propagación de virus.	Mantener actualizados los programas para evitar la propagación.
Errores de los usuarios.	Capacitación al personal de la organización.
Falta de conocimiento en el manejo de los programas.	Programa de capacitación al personal para el manejo de los programas informáticos.
Envió de información por una red incorrecta.	Contratar personal experto en el área para la revisión constante de las redes.
Fallas en el proceso de manipulación de información.	Capacitación al personal en temas informáticos, mantener la licencia actualizadas.
Alteración de la información.	Poseer contraseñas por usuarios para el acceso a la información y dar permisos de autorización.

Para el nivel de riesgo moderado, se requiere determinar si existe controles y si estos son aplicados correctamente. En este nivel se determinaron las siguientes amenazas y tratamiento para cada una de ellas:

TABLA 13: NIVEL DE RIESGO MODERADO

AMENAZAS	TRATAMIENTO
Errores en el mantenimiento de los equipos	Identificar un proveedor único para el mantenimiento de los equipos y su instalación
Error de Instalación	
Corte de energía eléctrica	Adquisición de un generador eléctrico
Error en el respaldo de la información	Establecer un cronograma de respaldo de información y dar seguimiento su cumplimiento, al igual que disponer de varios medios para el respaldo
Falta de respaldo permanente	Establecer una política, un cronograma y dar seguimiento al respaldo de información
Perdida accidental de información	Mantenimiento constante de los dispositivos extraíbles de respaldo y poseer varios medios de respaldo de información

Para el análisis del riesgo se comprobó la situación actual de la organización, y que no cuentan con ningún control que se aplique actualmente, dando como resultado los problemas detallados a continuación. Al no contar con controles actuales para los problemas identificados se establecen posibles controles que para prevenir la materialización del riesgo. A continuación, se detallan los problemas, controles en caso de existir y sus posibles controles para disminuir el nivel de riesgo.

TABLA 14: ANALISIS DE RIESGO, PROBLEMAS Y POSIBLES CONTROLES

PROBLEMA	POSIBLE CONTROL
1. Falla de la ventilación de los equipos portátiles	Control y monitoreo de los equipos portátiles Implementación de un sistema de monitoreo de alerta temprana ante posibles desconexiones.
2. Falla en la red	Monitoreo de la red. Implementación de programas de gestión y monitoreo de red basadas en los 5 principios de gestión: Configuración, Rendimiento, Fallos,
3. Propagación de virus	Contratación de licencias de un antivirus corporativo
4. Falla del correo electrónico	Contratar un servicio de alojamiento con un nivel alto en cuanto a disponibilidad y seguridad informática
5. Actualizaciones javas	Llevar una bitácora de actualizaciones para programar ajustes, instalaciones y mantenimientos
6. Falta de mantenimiento en los equipos contables	Implementación de un programa de gestión de redes y el despliegue de una política de seguridad para mantenimiento, control y seguimiento permanente
7. Personal sin conocimiento	Implementar una política de evaluaciones del nivel de desempeño al personal y aplicar estrategias de capacitación a los usuarios.
8. Sistema contable	Desarrollar un proyecto para evaluación, adquisición e Implementación de un software contable actualizado

9. Error en el ingreso de trámites	Desarrollar y desplegar una política para registrar el ingreso de trámites en un sistema informático. Aplicar controles de validación en el sistema de trámites. Seguimiento y revisión previa de la documentación
10. Facturación de ventas con retraso	Recepción electrónica de los documentos

Siguiendo la secuencia de problemas que acarrean a la empresa se constató que, uno de los equipos en red es obsoleto y está depreciado en su totalidad, al igual que presentan dificultades, ya que no tienen el mantenimiento adecuado por personal técnico, sin embargo, existe una planificación para la adquisición de equipos nuevos y reponer a los actuales como se mencionó en líneas anteriores.

POLÍTICAS Y CONTRAMEDIDAS DE LOS RIESGOS IDENTIFICADOS.

A continuación, se muestra el detalle de las contramedidas necesarias para que se apliquen a los riesgos identificados que afectan a los activos de información, para evitar la materialización del riesgo que puede conllevar a la perdida de información y a pérdidas económicas; así mismo, la implementación garantiza la disponibilidad, integridad y confidencialidad de los activos de información a cada uno de los problemas detectados.

Los problemas se vinculan con la secuencia de la tabla 14, y para cada uno se considera la política y las actividades a realizar para asegurar la validación de la contramedida. (Anexo 7: Políticas y Contramedidas)

Problema 1
Política: Gestión de mantenimiento de los equipos para adquirir equipos nuevos para reemplazar los actuales
Actividades:

- Evaluación de proveedores, mínimo de tres cotizaciones.
- Adquisición de equipos con capacidad suficiente de acuerdo con las aplicaciones necesarias para la labor diaria.
- Desplegar una política de mantenimiento preventivo de equipos de computación.

Problema 2
Política: Mantenimiento de los equipos para establecer un plan de contingencia.
Actividades:

- Establecer un cronograma para el mantenimiento de la red.
- Solicitar reportes de los mantenimientos realizados por el técnico encargado.
- Implementar mecanismos de monitoreo y reporte de clientes mediante tickets.

Problema 3
Política: Gestión de Sistemas Antivirus, adquisición de un sistema de antivirus que permita proteger la información.
Actividades:

- Evaluar las soluciones antivirus apoyándose en el reporte de av-comparatives.org
- Evaluar a los proveedores, mínimo de tres cotizaciones.
- Revisar el correcto funcionamiento del sistema de antivirus.
- Realizar la gestión de la licencia del antivirus.
- Instalar el antivirus en todas las maquinas en perfecto estado para su correcto funcionamiento.

Para la instalación de un sistema antivirus, se detallan las siguientes actividades:

La instalación se la debe hacer con credenciales de usuario administrador, considerando:

- Limpiar el equipo con un software para detección de troyanos y malware. Puede apoyarse con CCleaner, Superantispyware o Hitman pro.
- Desconectar el equipo de la red.
- Desinstalar el sistema antivirus actual.
- Instalar el nuevo software antivirus.
- Conectar el equipo a la red.
- Aplicar las actualizaciones.
- Gestionar la instalación desde la consola.

Otra forma:

- Desplegar la solución antivirus mediante las herramientas de consola.
- Desinstalar las soluciones antivirus existentes.
- Reiniciar el equipo.
- Aplicar las actualizaciones.

Problema 4
Política: Evaluar al proveedor del dominio para lograr una Adquisición de un dominio seguro y que evite la deficiencia o caída de la red principal.
Actividades:

- Definir el acuerdo de nivel de servicio (SLA) y comunicarlo a los proveedores.
- Evaluación de proveedores, mínimo de tres cotizaciones.
- Seguimiento constante y actualización del dominio
- Monitorear el servicio entregado vs. el servicio solicitado.

Problema 5
Política: Establecer un cronograma de mantenimiento de los equipos y actualizaciones constantes.
Actividades:

- Identificar y contratar un proveedor para el soporte técnico.

- Establecer un cronograma para la verificación de actualización de todos los programas de los equipos.
- Registrar la asistencia del técnico y las actividades realizadas.

Problema 6
Política: Gestión de mantenimiento de los equipos para realizar un mantenimiento periódico de todos los equipos
Actividades:

- Identificar un proveedor adecuado para el mantenimiento de los equipos.
- Establecer un cronograma para el mantenimiento de los equipos.
- Verificar el cumplimiento del cronograma establecido.

Problema 7
Política: Evaluación de desempeño. Establecer evaluaciones constantes al personal para calificar su desempeño e incluir capacitaciones trimestrales.
Actividades:

- Establecer un cronograma de capacitaciones anuales para todos los empleados.
- Evaluar las capacitaciones y el aprendizaje generado en ellas.
- Realizar una evaluación de desempeño.

Problema 8
Política: Gestión de Software, para la adquisición o Actualización del sistema contable.
Actividades:

- Evaluación de proveedores, mínimo de tres cotizaciones.
- Evaluar a la cotización y experiencia de los proveedores.
- Implementación del sistema adquirido por parte de los técnicos de proveedor.
- Establecer una capacitación y seguimiento en el uso del sistema.

Problema 9
Política: Evaluación de desempeño. Establecer si existe exceso de carga laboral y gestionar contratación de personal calificado.
Actividades:

- Establecer un cronograma de capacitaciones anuales para todos los empleados.
- Realizar una evaluación de desempeño.
- Identificaciones del proceso que genera retraso.
- Reuniones constantes con los jefes departamentales para la verificación del cumplimiento de funciones.

Problema 10
Política: Evaluación de desempeño. Definir el tiempo de retraso entre el ingreso del trámite y facturas emitida.
Actividades:

- Verificar el cumplimiento de las funciones del personal.
- Establecer si existe sobre carga de trabajo.
- Automatizar la facturación e integrarla con los sistemas.

V. DISCUSIÓN

Los resultados obtenidos de las empresas encuestadas permitieron identificar aspectos relevantes para el inventario de los activos de información, y su posterior identificación y valoración tanto de los activos como de las amenazas detectadas; de los resultados se pudo determinar el nivel de riesgo al que están expuestos como organización y establecer contramedidas para mitigar el riesgo.

De esta manera, las particularidades de los intercambios de información en las empresas MIPYMES son simples y carecen de procesos formales, así mismo requiere promover los procesos y actividades de negocio que generan las ventajas competitivas de las empresas ante sus más fuertes competidores [39]; las grandes empresas cuentan con procesos formales establecidos, manuales específicos, técnicos en el área tecnológica para que al intercambiar la información se la realice de forma segura y sin exponer la información confidencial en redes no deseadas, evitando también que las cuentas empresariales sean vulneradas.;

Como menciona [3], las características de las MIPYMES como ser consideradas de componente familiar limitan la liquidez y no poseen de un óptimo nivel tecnológico, limitando las actividades y en su mayoría los procesos se realizan de manualmente, lo cual conlleva a que se cometan errores involuntarios afectando el correcto proceso y el logro de los objetivos organizacionales.

Coincidiendo con [22] , las TIC son un recurso necesario y no un privilegio en la actualidad, ya que la tecnología debe estar presente en todas las organizaciones incluyendo al sector del comercio exterior, su evolución facilita el acceso a la información mediante la interacción por medio del correo, la web, chat, etc.; y, concordando con [24], la aplicación ayuda a mejorar la productividad, calidad, control y facilitar la comunicación organizacional. La información de estas empresas es fundamental ya que ayuda al mejor funcionamiento y guía a la toma correcta de decisiones; deben proteger su información para evitar consecuencias por la falta de seguridad y que posiblemente se vean materializadas de manera económica. La carencia de inversión en tecnología en las empresas de servicios de comercio exterior genera deficiencias ya que dispone del mínimo de recursos tecnológicos para el desempeño de sus funciones.

Considerando el criterio de [21], las empresas necesitan tener una infraestructura informática segura que ayude a minimizar los riesgos asociados con la seguridad y los costos de administración y operaciones independientemente del tamaño o actividad que realice cada empresa; esto involucra a las pequeñas y medianas empresas de nuestro entorno, ya que los avances tecnológicos generan una ventaja competitiva para los negocios.

Sin embargo, la seguridad informática es deficiente, ya sea por la falta de organización o desconocimiento de las MPYMES, lo cual crea una debilidad frente al cumplimiento de objetivos y conlleva a que la información confidencial sea manipulada por terceras personas sin autorización. La seguridad informática involucra todos los procesos de la organización para mantener resguardada la información y que los datos confidenciales no sean divulgados sin control a personas no deseadas; con el análisis actual de la organización y con la evaluación de riesgos, se establece el estado actual de la organización, identificando las causas de vulnerabilidades y soluciones de control que permitan la mitigación o reducción del nivel de riesgo detectado [6].
La empresa de estudio, al ser pequeña, las probabilidades de sufrir incidentes no deseados son muy altas; sin embargo, la implementación de herramientas y prácticas asociadas a las TIC influye de manera positiva en sus diferentes formas de innovación, a pesar de que, en Ecuador las MIPYMES tienen todavía un grado de uso de TIC apenas aceptable [40].

Con la aplicación de la metodología ECU@risk, se consideraron procesos y elementos que todas las MIPYMES cuentan para el inventario de activos de información; entre estas: edificaciones o instalaciones, el hardware, el software, la información electrónica, la información en papel, la infraestructura de comunicaciones, los medios de almacenamiento extraíbles y los recursos humanos [1].

La identificación de las amenazas que afectan a la organización es fundamental para la determinación del riesgo, ya que su correcta y eficiente identificación y valoración será esencial para la toma de decisiones y poder mitigar la amenaza para no incurrir en riesgos por la materialización de estas. Es por ello, que las amenazas deben ser identificadas oportunamente y que la organización puede anticiparse a dar soluciones a eventos no deseados a futuro por la falta de control. Para la correcta clasificación de la identificación de las amenazas es necesario llevar una matriz en la que se presente el respectivo código y la amenaza encontrada y su respectiva frecuencia.

Dentro de las amenazas detectadas, el uso del dominio del correo electrónico presenta dificultades de instalación en los equipos, lo que genera problema en el manejo por el personal de la organización; en ciertos casos, el uso del correo se lo hace directamente desde la web del proveedor de correo electrónico. El sistema contable fue adquirido hace más de una década y únicamente se actualiza a las necesidades del ente controlador; existen módulos manuales, los reportes en su mayoría no son eficientes y se deben procesar manualmente en plantillas de Office, no existen claves de acceso para los diferentes usuarios y genera que la responsabilidad de la información se vea dividida entre sus usuarios. Adicional, el sistema presenta errores frecuentemente, lo cual ocasionó por 2 instancias en años anteriores se vea afectada la información ya procesada.

Los resultados de la aplicación de la metodología ECU@risk determinaron que los problemas encontrados afectan directamente a la confidencialidad, integridad y disponibilidad de los activos de información, ya que la información está expuesta y es vulnerable a las amenazas detectadas. Dentro de los problemas detectados, se evidencia la inexistencia de controles para proteger los activos de información, siendo el más expuesto el Software con una amenaza en el Servidor de correo electrónico en él envió de la información por una red incorrecta, con la metodología aplicada obtuvo un nivel de riesgo extremo, lo que conlleva a que esta amenaza es frecuente. Por otro lado, los activos menos amenazados son: i) Información electrónica, ii) extraíble con las amenazas como Alteración de información y Perdida accidental de información, y iii) Infraestructura de comunicaciones amenazado por el Corte de energía eléctrica con un nivel de riesgo moderado.

Con estos resultados podemos observar el nivel de riesgo al que está expuesto la empresa, existiendo amenazas que ocasionan un nivel de riesgo extremo, alto y moderado. Los controles serán expuestos con los resultados obtenidos del riesgo acumulado. La determinación de políticas, procedimientos que ayuden a salvaguardar la información de la organización.

VI. Conclusiones

La aplicación de la metodología ECU@risk permitió identificar y valorar los activos de información y a las amenazas a las que se somete la organización. También permitió calcular el riesgo para proponer contramedidas de mitigación de las posibles y actuales amenazas.

Con la metodología ECU@risk se conoció a mayor profundidad el contexto empresarial, considerando la actividad económica de la organización, la cual se dedica a la prestación de servicios de comercio exterior y su clasificación dentro de las MIPYMES. Esta evaluación permitió identificar los activos de información que posee la empresa considerando los grupos de activos a los que pertenece en los que se tiene (ED) Edificaciones, (HW) Hardware, (SW) Software, (IE) Información electrónica, (IP) Información en papel, (Extraíble) Medios de almacenamiento extraíble, (IC) Infraestructura de comunicaciones y (RRHH) Recursos humanos.

Mediante el resultado del riesgo absoluto, se detectaron las amenazas más representativas que afecta de manera directa a la organización, entre los resultados más destacados se tienen: i) los errores de los usuarios o personal a cargo, ya que al no contar con un manual de procedimientos, no se procesa de una manera correcta la información ni la gestión de claves, ii) la falta de conocimiento por parte del personal nuevo, ya que no existe un plan de capacitación a los empleados que ingresan a la empresa, iii) el envío de información por red, uno de los problemas que prevalece es la transmisión de información por correo electrónico no existe una configuración adecuada y constantemente tiene fallas y no permite el correcto envió o recepción de mensaje, iv) la falta de mantenimiento de los equipos; y v) la propagación de virus.

Considerando la información proporcionada por parte del representante legal de la empresa y con el análisis realizado,

se determinó que la falta de soporte técnico para el mantenimiento de los equipos, la carencia de instalación, la deficiencia de licencias y la actualización de programas, se convierten en los principales problemas de la empresa, ya que se malgasta mucho tiempo tratando de que el usuario lo haga de manera autónoma.

La implementación de las contramedidas, sin duda, involucra un compromiso de todo el personal de la organización mediante la gestión y mantenimiento de los equipos, evaluación de desempeño al personal para el correcto funcionamiento de los procesos, con el objetivo de que a la postre se implementen manuales específicos dentro de la organización; y para un trabajo futuro, determinar el nivel de riesgo residual con las contramedidas aplicadas.

VII. BIBLIOGRAFÍA

[1] E. Crespo Martínez, «Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMEs,» *Enfoque UTE,* 2017.

[2] F. M. Arévalo, I. P. Cedillo y y. S. A. Moscoso, «Metodología Ágil para la Gestión de Riesgos Informáticos,» *Revista Killkana Técnica,* 2017.

[3] Arriaga-López, Fabiola Guadalupe, & Ávalos-Cueva, David, & Martinez-Orozco, Edgardo, «PROPUESTA DE ESTRATEGIAS DE MEJORA BASADAS EN ANALISIS FODA EN LAS PEQUEÑAS EMPRESAS DE ARANDAS, JALISCO, MÉXICO,» *Ra Ximhai,* 2017.

[4] J. Rubio y C. Burgos, «Metodología de selección de procesos para la gestion de servicios en laa pymes,» *TCyE,* 2017.

[5] R. L. Peña, «Diseño de un Sistema de Gestión de Seguridad de la Información basado en las Normas ISO/IEC 27001 e ISO/IEC 27002 para proteger los activos de información en el proceso de suministros de medicamentos de la Red de Salud de Lambayeque 2015",» 2016.

[6] Francisco Nicolás Javier Solarte Solarte, Edgar Rodrigo ENRIQUEZ ROSERO, Mirian del Carmen Benavides Ruano, «Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001,» *Revista Tecnológica ESPOL – RTE,* 2015.

[7] ISO27001, «GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN,» 2013.

[8] Ana Abril ,Jarol Pulido, John A. Bohada, «ANÁLISIS DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN,» 2013.

[9] A. R. Gómez, «Globalización, competitividad y comercio exterior,» *Análisis Económico,* 2006.

[10] M. Quiñónez y L. Quiñónez, «Política de comercio exterior en Ecuador: Un análisis comparativo,» Centro Sur. Social Science Journal, 2020.

[11] F. Quinde, L. Carvajal, O. Realpe y J. Bolaños, «Los Servicios de logística y los procedimientos comerciales en la Direccion Distrital de Aduna Tulcan,» *Sathiri No 5* , 2013.

[12] COPCI, «CÓDIGO ORGÁNICO DE LA PRODUCCIÓN, COMERCIO E INVERSIONES,» 2013.

[13] Vásquez y López, «Estudio comparativo entre las metodologías Microsoft Secure Risk Management y Octave.,» 2016.

[14] SUPERCIAS, «CLASIFICACION DE PEQUEÑAS Y MEDIANAS EMPRESAS».

[15] A. R. E. RON y C. V. A. SACOTO, «Las PYMES ecuatorianas: su impacto en el empleo como contribución del PIB PYMES al PIB total,» *REVISTA ESPACIOS,* 2017.

[16] SUPERCIAS, «Ranking de empresas,» 2019.

[17] INEC, «Indicadores Nacionales, Porcion de plazas de empleoregistrados por tamaño de empresas,» 2018.

[18] C. Yance, L. Solis, I. Burgos, Hermida y Lia, «"La importancia de las PYMES en el Ecuador",» *Revista Observatorio de la Economía Latinoamericana, Ecuador,* 2017.

[19] L. Carrion, J. Zula y L. Castillo, «Analisis del model de gestion en pequeñas y medianas empresas y su aplicacion en la industria del catering en Ecuador,» 2016.

[20] A. R. Gómez, «Globalización, competitividad y comercio exterior,» *Análisis Económico,* 2006.

[21] C. A. Dussan Clavijo, «Políticas de seguridad informática.,» *Entramado,* 2006.

[22] F. J. Valencia y D. M. O. Alzate, «Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000,» *RISTI,* 2017.

[23] D. ESPÍN, « INCIDENCIA DE LAS TIC EN LAS PYMES DE LA CIUDAD DE SANTO,» 2019.

[24] G. Cano, «Las TICs en las empresas: evolución de la tecnología y cambio,» *DOMINIO DE LAS CIENCIAS,* 5 Enero 2018.

[25] REDCEDIA, «Gestión de la Seguridad de la Informacion,» [En línea]. Available: https://www.cedia.edu.ec/dmdocuments/publicaciones/Libros/GTI8.pdf.

[26] D. BETANCOURT, «INGENIO EMPRESA,» 2018. [En línea]. Available: www.ingenioempresa.com/analisis-pestel..

[27] OMS, «Brote de enfermedad por coronavirus (COVID-19),» 06 10 2020. [En línea]. Available: https://www.who.int/es/emergencies/diseases/novel-coronavirus-2019?gclid=CjwKCAjwq_D7BRADEiwAVMDdHhb3gB_sDYBZixlbVOtz2ba9KCUgJz3gIu-w1KaP9bd220c9MR_5YxoChQUQAvD_BwE.

[28] MIPRO, «Acuerdos Comerciales».

[29] MARSH, «Mapa de Riesgo Político 2020:,» 2020.

[30] CEPAL, «Los efectos del COVID-19,» 2020.

[31] B. Quevedo, L. Vásquez, V. Quevedo y P. Pinzon, «COVID-19 y sus efectos en el comercio internacional. Caso Ecuador COVID-19,» *Dominio de las Ciencias*, 2020.

[32] A. NACIONAL, «LEY ORGÁNICA PARA EL FOMENTO PRODUCTIVO, ATRACCIÓN DE INVERSIONES, GENERACIÓN DE EMPLEO, Y ESTABILIDAD Y EQUILIBRIO FISCAL,» 2019.

[33] INEC, «Principales Indicadores de Actividades de Ciencia, Tecnología e Innovacion,» 2014 .

[34] INEC, «Encuesta de Estratificación del Nivel Socioeconómico NSE 2011,» 2011.

[35] J. Mora, «Todo Comercio Exterior,» 2018. [En línea]. Available: http://comunidad.todocomercioexterior.com.ec/profiles/blogs/exportaciones-de-cuenca. [Último acceso: 29 09 2020].

[36] P. GONZALEZ, «PYMES INVIERTEN EN TECNOLOGIA Y SE ADAPTAN A LA NUEVA NORMALIDAD,» 2020.

[37] A. Gutiérrez, «COVID-19 y su impacto en el medioambiente,» 2020.

[38] MAE, «Politicas generales para promover las buenas practicas ambientales en entidades del sector publico y privado,» 2014.

[39] A. L. &. P.-M. M. P. &. T.-G. J. A. &. N.-R. D. Quispe-Otacoma, «Tecnologías de información y comunicación en la gestión empresarial de pymes comerciales.,» *Ingenieria Industrial* .

[40] Morán-Quiñonez y Cañarte-Rodríguez, «Las PYMEs y su incorporación en las TICs, Manta, Ecuador,» *REVISTA CIENTIFICA*, 2017.

[41] OMC, «LA OMC EN POCAS PALABRAS,» 2018.

ANEXOS

Anexo 1: Valores Compartidos Organizacionales

Valores Compartidos Organizacionales	
MISIÓN	Nos comprometemos a brindar servicios con asesoría técnica especializada, eficiente en el seguimiento de operaciones, con un excelente tiempo de respuesta el cual supera las expectativas de nuestros clientes, respaldados con personal técnicamente capacitado y con vocación de servicio al cliente, así con una sólida estructura organizacional y tecnología de punta
VISIÓN	Ser reconocidos en el mercado ecuatoriano como una de las empresas líderes en brindar soluciones para sus operaciones de Comercio Exterior otorgándoles claridad y certeza de que las mismas serán realizadas correctamente, cumpliendo con las leyes que la rigen.
VALORES	• Servicio de calidad • Honestidad • Confianza • Compromiso • Discreción • Respeto • Responsabilidad
OBJETIVOS INSTITUCIONALES	• Brindar aseria logística de comercio exterior • Proveer de servicios y soluciones integrales en el ramo aduanal y logístico en el mejor tiempo a través de un proceso de calidad que optimice el servicio y el costo para nuestros clientes siempre bajo nuestros valores

Anexo 2: Identificación de Activos

CLASIFICACIÓN		**ACTIVO**	**DESCRIPCIÓN**
HARDWARE	**(HW)**	(PC)	Computadoras de Escritorio
		(LAPTOP)	Computadoras Portátil
		(PRINT)	Impresoras
SOFTWARE	**(SW)**	(AV)	Antivirus
		(SUB)	Desarrollo sub contratado
		(STD) (EMAIL)	Servidor de Correo
INFRAESTRUCTURA DE COMUNICACIONES	**(IC)**	(WIFI)	Red Wifi Inalámbrica
		(ROUTER)	Router
		(LAN)	Red de Cableado
		(MODEM)	Módem
		(PBX)	Central Telefónica
MEDIO DE ALMACENAMIENTO EXTRAÍBLE	**(EXTRAIBLE)**	(MECANICO)	Disco Duro Extraíble
	(IE)	(ARCHIVO)	Matriz de Excel Dpto. Operaciones

INFORMACIÓN ELECTRÓNICA		(ARCHIVO)	Matriz de Excel Dpto. Contable
		(ARCHIVO)	Matriz de Excel Dpto. Logístico
		(COPIA)	Archivos de respaldo
Información en papel	**(IP)**	(DOCS)	Documentos

Anexo 3: Valoración de Activos de Información

CLASIFICACIÓN		ACTIVO	DESCRIPCIÓN	C	D	I	VALORACIÓN	VALOR
Hardware	**(HW)**	(PC)	COMPUTADORAS DE ESCRITORIO	1	4	3	4	ALTO
	(HW)	(LAPTOP)	COMPUTADORAS PORTÁTILES	1	3	3	3	MODERADO
	(HW)	(PRINT)	IMPRESORAS	1	4	3	4	ALTO
Software	**(SW)**	(AV)	ANTIVIRUS	3	4	4	4	ALTO
	(SW)	(SUB)	DESARROLLO SUB CONTRATADO	2	4	4	4	ALTO
	(SW)	(STD) (CLIEMAIL)	SERVIDOR DE CORREO	3	4	4	4	ALTO
Infraestructura de comunicaciones	**(IC)**	(WIFI)	RED WIFI INALÁMBRICA	2	3	1	3	MODERADO
	(IC)	(ROUTER)	ROUTER	2	3	1	3	MODERADO
	(IC)	(LAN)	RED DE CABLEADO	2	3	1	3	MODERADO
	(IC)	(MODEM)	MÓDEM	1	2	1	2	MENOR
	(IC)	(PBX)	CENTRAL TELEFÓNICA	1	2	2	2	MENOR
Medio de almacenamiento extraíble	**(EXTRAIBLE)**	(MECANICO)	DISCO DURO EXTRAÍBLE	3	1	2	3	MODERADO
Información electrónica	**(IE)**	(ARCHIVO)	MATRIZ DE EXCEL DPTO. OPERACIONES	3	4	3	4	ALTO
	(IE)	(ARCHIVO)	MATRIZ DE EXCEL DPTO. CONTABLE	3	4	3	4	ALTO
	(IE)	(ARCHIVO)	MATRIZ DE EXCEL DPTO. LOGÍSTICO	3	4	3	4	ALTO
	(IE)	(COPIA)	ARCHIVOS DE RESPALDO	1	3	3	3	MODERADO
Información en papel	**(IP)**	(DOCS)	DOCUMENTOS	1	3	2	3	MODERADO

Anexo 4: Identificación de Amenazas

CÓDIGO DE AMENZA	ACTIVO AMENAZADO	DESCRIPCIÓN DE LA AMENAZA	C	D	I
[NO_INTENCIONADO.1]	HARDWARE (HW)	Errores de los usuarios, falta de conocimiento en el manejo de los programas informáticos	X	X	X
	SOFTWARE (SW)				
	MEDIO DE ALMACENAMIENTO EXTRAÍBLE (EXTRAÍBLE)				
	INFORMACIÓN ELECTRÓNICA (IE)				
[NO_INTENCIONADO.2]	INFRAESTRUCTURA DE COMUNICACIONES (IC)	Errores de administrador - error en la instalación	X	X	X
[PROVOCADO. *]	HARDWARE (HW)	Corte de energía eléctrica, errores en la actividad humana, alteración de la información		X	
	INFRAESTRUCTURA DE COMUNICACIONES (IC)				
	INFORMACIÓN ELECTRÓNICA (IE)				
[EL.1]	INFORMACIÓN ELECTRÓNICA (IE)	Propagación de virus	X	X	X
	SOFTWARE (SW)				
[NO_INTENCIONADO.6]	SOFTWARE (SW)	Alteración de información			X
	MEDIO DE ALMACENAMIENTO EXTRAÍBLE (EXTRAÍBLE)				
[NO_INTENCIONADO.7]	SOFTWARE (SW)	Perdida accidental de información		X	
	INFORMACIÓN ELECTRÓNICA (IE)				
	MEDIO DE ALMACENAMIENTO EXTRAÍBLE (IE)				
[EC.1]	INFRAESTRUCTURA DE COMUNICACIONES (IC)	Errores de comunicación, envió de información por una red incorrecta	X		
	SOFTWARE (SW)				
	MEDIO DE ALMACENAMIENTO EXTRAÍBLE (IE)				

Anexo 5: Cálculo del riesgo

ACTIVO	DESCRIPCIÓN	C	D	I	VALORACIÓN	FRECUENCIA	IMPACTO			RIESGO ACUMULADO			RIESGO ABSOLUTO
							C	D	I	C	D	I	
(HW)(PC) (001)	**PC de Escritorio Contabilidad**	**1**	**4**	**3**	**4**								
[NO_INTENCIONADO.1]	Errores de manipulación por parte de los usuarios	X	X	X		**3**	1	4	3	3	12	9	**12**
[PROVOCADO. *]	Corte de energía eléctrica		X			**3**		4			12		**12**
(HW)(LAPTOP) (001)	**Laptop Portátil LENOVO**	**1**	**3**	**3**	**3**								
(HW) (LAPTOP (004)	**Laptop Portátil HP**	**1**	**3**	**3**									
(HW)(LAPTOP) (005)	**Laptop Portátil Sony Vaio**	**1**	**3**	**3**									
[NO_INTENCIONADO.1]	Errores en el mantenimiento de los equipos	X	X	X		**3**	1	3	3	3	9	9	**9**
(HW)(PRINT)(001)	**Impresora Matricial Epson LX300**	**1**	**4**	**3**	**4**								
(HW)(PRINT)(002)	**Impresora Matricial Epson LX350**	**1**	**4**	**3**									
(HW)(PRINT)(003)	**Impresoras EPSON L210**	**1**	**4**	**3**									
(HW)(PRINT)(004)	**Impresoras EPSON L555**	**1**	**4**	**3**									
[NO_INTENCIONADO.1]	Falta de mantenimiento	X	X	X		**3**	1	4	3	3	12	9	**12**
[PROVOCADO. *]	Corte de energía eléctrica		X			**3**		4			12		**12**
(SW)(AV)	**Antivirus**	**3**	**4**	**4**	**4**								
(SW)(STD) (CLIEMAIL)	**Servidor de Correo**	**3**	**4**	**4**									
[NO_INTENCIONADO.1]	Falta de conocimiento en el manejo de los programas	X	X	X		**3**	3	4	4	9	12	12	**12**
[EL.1]	Propagación de virus	X	X	X		**4**	3	4	4	12	16	16	**16**
[EC.1]	Envió de información por una red incorrecta	X				**5**	3			15			**20**
(SW)(SUB)	**Desarrollo sub CONTRATADO**	**2**	**4**	**4**	**4**								
[NO_INTENCIONADO.1]	Errores de los usuarios	X	X	X		**3**	2	4	4	6	12	12	**12**
[NO_INTENCIONADO.1]	Falta de conocimiento en el manejo de los programas	X	X	X		**3**	2	4	4	6	12	12	**12**
[NO_INTENCIONADO.7]	Perdida accidental de información		X			**2**		4			8		**8**
(IC)(WIFI)	**Red Wifi Inalámbrica**	**2**	**3**	**1**	**3**								
(IC)(ROUTER)	**Router**	**2**	**3**	**1**									
(IC)(LAN)	**Red de Cableado**	**2**	**3**	**1**									
[NO_INTENCIONADO.2	Error de Instalación	X	X	X		**3**	2	3	1	6	9	3	**9**
[PROVOCADO. *]	Corte de energía eléctrica		X			**3**		3			9		**9**
(IC)(MODEM)	**Módem**	**1**	**2**	**1**	**2**								

[EC.1]	Envió de información por una red incorrecta	X				**5**	1			5			**10**
[PROVOCADO. *]	Corte de energía eléctrica		X			**3**		2			6		**6**
(EXTRAIBLE) (MECANICO)	**Disco Duro Extraíble**	**3**	**1**	**2**	**3**								
[NO_INTENCIONADO.1]	Error en el respaldo de la información	X	X	X		**3**	3	1	2	9	3	6	**9**
[NO_INTENCIONADO.6]	Alteración de información			X		**2**			2			4	**6**
[NO_INTENCIONADO.7]	Perdida accidental de información		X			**2**		1			2		**6**
(IE)(ARCHIVO)	**Matriz de Excel Dpto. Operaciones**	**3**	**4**	**3**	**4**								
	Matriz de Excel Dpto. Contable	**3**	**4**	**3**									
	Matriz de Excel Dpto. Logístico	**3**	**4**	**3**									
[NO_INTENCIONADO.1]	Fallas en el proceso de manipulación de información	X	X	X		**3**	3	4	3	9	12	9	**12**
[PROVOCADO. *]	Alteración de la información		X			**3**		4			12		**12**
[EL.1]	Propagación de virus	X	X	X		**4**	3	4	3	12	16	12	**16**
[NO_INTENCIONADO.7]	Perdida accidental de información		X			**2**		4			8		**8**
(IE)(COPIA)	**Archivos de respaldo**	**1**	**3**	**3**	**3**								
[NO_INTENCIONADO.6]	Falta de respaldo permanente			X		**2**			3			**6**	**6**
[NO_INTENCIONADO.7]	Perdida accidental de información		X			**2**		3			**6**		**6**

Anexo 6: Niveles de Riesgo – Tratamiento

NIVEL DE RIESGO	ACCIÓN	RIESGO IDENTIFICADO	TRATAMIENTO
Extremo - E	**Requiere una acción y respuesta inmediata**	Envió de información por una red incorrecta	Contratar personal experto en el aérea para la revisión constante de las redes
Alto - A	**Atención prioritaria**	Errores de manipulación por parte de los usuarios	Capacitación al personal de la organización
		Corte de energía eléctrica	Adquisición de un generador eléctrico
		Falta de mantenimiento	Establecer un cronograma de mantenimiento a los equipos
		Propagación de virus	Mantener actualizados los programas para evitar la propagación
		Errores de los usuarios	Capacitación al personal de la organización
		Falta de conocimiento en el manejo de los programas	Programa de capacitación al personal para el manejo de los programas informáticos
		Envió de información por una red incorrecta	Contratar personal experto en el área para la revisión constante de las redes
		Fallas en el proceso de manipulación de información	Capacitación al personal en temas informáticos, mantener la licencia actualizadas
		Alteración de la información	Poseer contraseñas por usuarios para el acceso a la información y dar permisos de autorización
Moderado - M	**Determinar si existe controles y si son aplicados correctamente**	Errores en el mantenimiento de los equipos	Identificar un proveedor único para el mantenimiento de los equipos y su instalación
		Error de Instalación	
		Corte de energía eléctrica	Adquisición de un generador eléctrico
		Error en el respaldo de la información	Establecer un cronograma de respaldo de información y dar seguimiento su cumplimiento, al igual que disponer de varios medios para el respaldo
		Falta de respaldo permanente	Establecer una política, un cronograma y dar seguimiento al respaldo de información
		Perdida accidental de información	Mantenimiento constante de los dispositivos extraíbles de respaldo y poseer varios medios de respaldo de información

Anexo 7: Políticas y Contramedidas

PROBLEMA IDENTIFICADO	POLÍTICA	DESCRIPCIÓN	ACTIVIDADES
Falla de la ventilación de los equipos portátiles	Gestión de mantenimiento de los equipos	Adquirir equipos nuevos para reemplazar los actuales	• Evaluación de proveedores, mínimo de tres cotizaciones • Adquisición de equipos con capacidad suficiente de acuerdo con las aplicaciones necesarias para la labor diaria • Desplegar una política de mantenimiento preventivo de equipos de computación.
Falla en la red	Mantenimiento de los equipos	Establecer un plan de contingencia	• Establecer un cronograma para el mantenimiento de la red • Solicitar reportes de los mantenimientos realizados por el técnico encargado.

			• Implementar mecanismos de monitoreo y reporte de clientes mediante tickets.
Propagación de virus	Gestión de Sistemas Antivirus	Adquisición de un sistema de antivirus que permita proteger la información.	• Evaluar las soluciones antivirus apoyándose en el reporte de av-comparatives.org • Evaluar a los proveedores, mínimo de tres cotizaciones • Revisar el correcto funcionamiento del sistema de antivirus • Realizar la gestión de la licencia del antivirus • Instalar el antivirus en todas las maquinas en perfecto estado para su correcto funcionamiento.
		Instalación de un sistema antivirus	La instalación se la debe hacer con credenciales de usuario administrador, considerando: - Limpiar el equipo con un software para detección de troyanos y malware. Puede apoyarse con ccleaner, superantispyware o hitman pro. - Desconectar el equipo de la red - Desinstalar el sistema antivirus actual - Instalar el nuevo software antivirus - Conectar el equipo a la red - Aplicar las actualizaciones. - Gestionar la instalación desde la consola. Otra forma: - Desplegar la solución antivirus mediante las herramientas de consola - Desinstalar las soluciones antivirus existentes - Reiniciar el equipo - Aplicar las actualizaciones.
Falla del correo electrónico	Evaluar al proveedor del dominio	Adquisición de un dominio seguro y que evite la deficiencia o caída de la red principal	• Definir el acuerdo de nivel de servicio (SLA) y comunicarlo a los proveedores. • Evaluación de proveedores, mínimo de tres cotizaciones • Seguimiento constante y actualización del dominio • Monitorear el servicio entregado vs. el servicio solicitado.
Actualizaciones de Java	Mantenimiento de los equipos	Establecer un cronograma de actualizaciones constantes	• Identificar y contratar un proveedor para el soporte técnico. • Establecer un cronograma para la verificación de actualización de todos los programas de los equipos. • Registrar la asistencia del técnico y las actividades realizadas.

Falta de mantenimiento en los equipos contables	Gestión de mantenimiento de los equipos	Mantenimiento periódico de todos los equipos	• Estableces un proveedor adecuado para el mantenimiento de los equipos • Establecer un cronograma para el mantenimiento de los equipos • Verificar el cumplimiento del cronograma establecido
Personal sin conocimiento en comercio exterior	Evaluación de desempeño	Establecer evaluaciones constantes al personal para calificar su desempeño e incluir capacitaciones trimestrales	• Establecer un cronograma de capacitaciones anuales para todos los empleados • Evaluar las capacitaciones y el aprendizaje generado en ellas • Realizar una evaluación de desempeño
Sistema contable obsoleto	Gestión de Software	Adquisición o Actualización del sistema contable	• Evaluación de proveedores, mínimo de tres cotizaciones • Evaluar a la cotización y experiencia de los proveedores • Implementación del sistema adquirido por parte de los técnicos de proveedor • Establecer una capacitación y seguimiento en el uso del sistema
Error en el ingreso de trámites	Evaluación de desempeño	Establecer si existe exceso de carga laboral y gestionar contratación de personal calificado	• Establecer un cronograma de capacitaciones anuales para todos los empleados • Realizar una evaluación de desempeño • Identificaciones del proceso que genera retraso • Reuniones constantes con los jefes departamentales para la verificación del cumplimiento de funciones
Facturación de ventas con retraso	Evaluación de desempeño	Definir el tiempo de retraso entre el ingreso del trámite y facturas emitida	• Verificar el cumplimiento de las funciones del personal • Establecer si existe sobre carga de trabajo • Automatizar la facturación e integrarla con los sistemas