LA SEGURIDAD DE LA INFORMACIÓN DE LAS MICROEMPRESAS EN EL ECUADOR

INFORMATION SECURITY FOR MICRO-ENTERPRISES IN ECUADOR

Francisco Jurado Pruna, Mgtr.
https://orcid.org/0000-0001-8689-0398
Universidad Tecnológica Israel, Quito, Ecuador.
fjurado@uisrael.edu.ec

Erika Escobar Redín, Ph.D.
https://orcid.org/0000-0002-4955-4886
Universidad Tecnológica Israel, Quito, Ecuador.
eescobar@uisrael.edu.ec

Joe Carrión Jumbo, Ph.D.
https://orcid.org/0000-0003-3632-5352
Universidad Internacional SEK, Quito, Ecuador.
joe.carrión@uisek.edu.ec

ARTÍCULO DE INVESTIGACIÓN
Recibido: 15 de septiembre de 2021
Aceptado: 18 de octubre de 2021

RESUMEN

La información y su gestión son de gran importancia dentro de las diversas actividades que se desarrollan en las organizaciones empresariales, esto se ha evidenciado en gran parte por el crecimiento de estas en lo referente a la presencia en el mercado, pero también por el crecimiento en los ataques y amenazas a la información en todo tipo de organizaciones, dentro de las cuales se encuentran las microempresas. El presente trabajo presenta los resultados de la encuesta realizada que abarca al sector microempresarial del Ecuador, con el objetivo de evidenciar la brecha que existe en este tipo de organizaciones en lo referente a la gestión y protección de la información, lo que permite a una empresa tener bases sólidas para dar continuación futura a su negocio asegurando el éxito a corto y largo plazo, con el empleo de buenas prácticas establecidas por las normas existentes, para ello se empleó la metodología de investigación del tipo descriptiva, utilizando como técnica para recolectar datos la encuesta, esta se realizó a un número determinado de esta clase de organizaciones empresariales buscando representatividad de las microempresas cuyas características y campo de acción incluyen el manejo y empleo de tecnología.

Palabras claves**:** Mipymes, encuesta, microempresas, seguridad de la información

https://doi.org/10.21855/ecociencia.80.600

ABSTRACT

Information and its management are of great importance within the various activities carried out in business organizations, this has been evidenced largely by their growth in terms of market presence, but also by growth in attacks and threats to information in all types of organizations, including micro-enterprises. This paper presents the results of the survey carried out in the Ecuadorian microenterprise sector, with the aim of showing the gap that exists in this type of organization with regard to the management and protection of the information, which allows a company to have solid foundations to continue its business in the future, ensuring success in the short and long term, with the use of good practices established by existing standards, for this the descriptive research methodology was used, using the survey as a technique to collect data, this was carried out to a certain number of this class of business organizations looking for representativeness of the microenterprises whose characteristics and field of action include the management and use of technology.

Keywords: MSMEs, survey, micro-enterprises, information security

INTRODUCCIÓN

El avance tecnológico relacionado al manejo de la información ha fomentado el desarrollo de estándares, metodologías y herramientas que permitan la gestión eficiente y adecuada de la información, es así como en el sector empresarial se ha evidenciado que la información relaciona a cada una independiente de su tipo, ha permitido que mediante el análisis adecuado de esta emplearla como herramienta para generar ventajas competitivas, optimización de procesos que fomentan el crecimiento, desarrollo y continuidad en el mercado (Bejarano & Siu, 2017), como parte de este manejo, resalta el hecho de que tener conciencia de los problemas que se pueden generar en una organización, por las diferentes clases y niveles de amenazas relacionadas al robo o pérdida de información, también deben ser consideradas.

Es así que el campo asociado al manejo de la información se han desarrollado estándares, metodologías y herramientas que permiten la gestión eficiente y adecuada de la información, en este sentido resalta la normativa ISO 27000, la cual suele ser guía para el planteamiento de diversas propuestas para la gestión de la seguridad de la información que se han plasmado en varios trabajos, como el presentado por Andrés & Gómez (2009), en el que desarrolla una guía con diversos conceptos y recomendaciones generales para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en una Pyme, de igual forma, está el trabajo de Ladino & López (2011), que presenta una descripción general de la normativa ISO 27001 y cómo implementarla empleando las denominadas buenas prácticas, en este sentido, Valencia & Orozco (2017), proponen una metodología para implementar un sistema de

gestión de la Información en base a cuatro normativas relacionadas a la ISO/IEC 27000 como lo son la ISO/IEC 27001 de actividades a cumplir para la implementación de un sistema de gestión de información, la ISO/IEC 27002 relacionada a los controles de seguridad, la ISO/IEC 27005 relacionada al esquema de riesgos y los pasos descritos en la ISO/IEC 27003 con el objetivo de alcanzar una implementación exitosa del sistema.

La importancia de los sistemas de gestión de la información, analizada desde diferentes perspectivas, permite brindar soporte y generar nuevos servicios relacionadas a la gestión de los negocios actuales, basados en la capacidad de integración y escalado lo que permite crear un ambiente adecuado que favorece y sustenta la transformación digital que las empresas están alcanzado en la actualidad, partiendo desde el proceso más básico, hasta alcanzar un nivel estratégico. (Proaño et al., 2018).

La transformación digital, permite mejorar diversos procesos como la atención al cliente, la productividad y desarrollar nuevos modelos de negocios, lo que ha hecho que cada vez más empresas se incluyan en la transformación digital, esta es imposible alcanzarla sin tener en cuenta una metodología, ya que no se consigue únicamente con la adquisición de tecnología sofisticada, sino que se debe tener presente la capacidad de poder rediseñar el modelo de negocio, con la definición de procesos eficientes basados en la tecnológica.

Como lo mencionan varios autores (Legner et al., 2017; Schwertner, 2017; Verina & Titko, 2019) la transformación digital llega a ser una reinvención de la organización basada en el uso de la tecnología para mejorar la forma en que la organización se desempeña. El componente digital hace referencia al uso de la tecnología que genera, almacena y procesa los datos con el objetivo de mejorar los resultados empresariales los que se alcanzan cuando se mejora la eficiencia, permite una toma de decisiones rápida y efectiva, amplia la accesibilidad, permite incrementar la satisfacción del cliente, por último, se mejoran los beneficios y el retorno de la inversión, todo esto se refleja en su tasa de éxito a corto y largo plazo.

REVISIÓN TEÓRICA

Análisis situación actual

Los sistemas de gestión y seguridad de la información

Los sistemas de información parten del estudio de la organización de la empresa, para entender el contexto y las implicaciones del ambiente en el que se desenvuelve la entidad, para lo cual incluyen un conjunto de componentes, que buscan recolectar, almacenar, procesar datos para proporcionar información de los productos o procesos que se desarrollan. En lo relacionado a los componentes principales de un sistema de información se puede

encontrar a los componentes físicos, los programas, la infraestructura de comunicaciones, las bases de datos y sus servidores, por último están los recursos humanos y procesos (de Pablos Heredero et al., 2019), en base a estos componentes los sistemas de información permiten definir el nivel administrativo, donde se desarrollan las funciones de seguimiento, control, toma de decisiones y administración de todos los recursos existentes, para lo cual se emplean herramientas de planificación y toma de decisiones todas encaminadas a mejorar de la productividad, a este nivel los sistemas tienen como objetivo proporcionar informes periódicos relacionados a las operaciones y procesos que se ejecutan en la organización.

La existencia de información inevitablemente debe incluir sistemas para proteger la misma, dada la importancia que esta representa en el crecimiento de las organizaciones en los últimos años, por ello se han desarrollado diversos estándares enfocados a la protección de este activo que en la actualidad es vital para una empresa, entre estos estándares, uno de los más empleados y conocidos es la norma ISO/IEC 27000, que de forma general presenta un conjunto de estándares desarrollados por la Organización Internacional de Estandarización y la Comisión Internacional Electrotécnica, por medio de los cuales se define el marco de gestión de la seguridad de la información en una organización de cualquier clase que puede ser del tipo grande o pequeña.

También está el modelo COBIT (Control Objetives for Information and related Technology), este define un marco de buenas prácticas para el control de la información, es aceptado internacionalmente, se lo emplea para implementar el denominado gobierno de Tecnologías de Información (TI) y mejorar el control de los procesos, este modelo proporciona información a los gerentes de las empresas para cubrir las brechas de control en los aspectos técnicos y riesgos de negocio, haciendo viable la elaboración de políticas claras y buenas prácticas dentro de la organización, hace énfasis en la conformación de las regulaciones que permiten incrementar el valor de una organización desde las TI.

En este campo, también se encuentra la biblioteca de Infraestructura de Tecnologías de la Información ITIL desarrollada por la Oficina Gubernamental de Comercio del Reino Unido, que presenta un conjunto de las mejores prácticas para gestionar los servicios de las tecnologías de información en lo referente a personas, procesos y tecnología en cada departamento que puede existir en una empresa, los objetivos que persigue es la reducción de costos, mejorar la calidad de servicio a los clientes ya sean internos y externos, todo esto mediante la optimización de las habilidades y destrezas del personal (Orrego, 2013).

Por último cabe mencionar el modelo de OCTAVE de sus siglas en inglés “Operationally Critical Threat, Asset and Vulnerability Evaluation”, esta metodología desarrollada en el año 2001 por el CERT/CC la cual permite analizar la tecnología relacionada a las prácticas de seguridad y toma de decisiones para proteger la información teniendo en cuenta los riesgos de confidencialidad, integridad y disponibilidad que pueden afectar la información crítica de la empresa (García & Moreta, 2019).

De entre las normativas y modelos existentes es importante mencionar que ninguno de ellos es mejor que otro, debido a que la decisión de cual se empleará en una organización empresarial está relacionado a la decisión de quienes la dirigen en base a la necesidad de la empresa y sus características, partiendo de esta premisa, se presenta en este documento el resultado obtenido del análisis de la encuesta realizada teniendo como enfoque el sector microempresarial del Ecuador, para analizar la posibilidad de incorporar un Sistema de Gestión de la Seguridad de la Información que tome en cuenta las características de este sector empresarial.

Análisis de la situación actual

De forma general el planteamiento de cualquier sistema de gestión y seguridad de la información requiere como primer paso el análisis inicial, donde se puedan identificar y valorar los diferentes activos que posee la organización junto con las amenazas y evaluación de las mismas, para ello en el presente trabajo de investigación se inicia con un análisis DAFO (Debilidades, Amenazas, Fortalezas y Oportunidades), este tipo de metodología permite plantear de forma general la situación actual de las microempresas, en base las características que definen a este tipo de organizaciones y algunos requerimientos de los sistemas de seguridad de la información basadas en algunas normativas existentes, este análisis se lo presenta en la Tabla 1.

Tabla 1

Análisis DAFO

	POSITIVO	**NEGATIVO**
Interno	**Fortalezas:** - Se desarrollan en cualquier ámbito dentro de la economía de un país. - Requerimientos tecnológicos mínimos.	**Debilidades:** - Imposibilidad en proyectos grandes debido a la falta de asesoría, deficiente administración, talento no calificado, desconocimiento del mercado, entre otros. - Elevado costo en el análisis de los sistemas SGSI

Externo	**Oportunidades:** - Un SGSI permite brindar soporte y generar nuevos servicios relacionadas a la gestión de los negocios actuales. - Un SGSI permite a una empresa cumplir con estándares legales.	**Amenazas:** - No existen SGSI que se adapten a las características de estas organizaciones. - Se requiere la actualización constante de los panes de seguridad de la información

Fuente: Elaboración propia.

Como complemento al análisis DAFO se planteó el análisis de brecha, debido a la importancia que la información que se obtiene del mismo aporta a la investigación, este análisis como lo define Catoira (2013), permite identificar las posibles deficiencias que posee una organización, en el ámbito de la protección de la información más aún si se desea alcanzar una certificación internacional, como por ejemplo esta la ISO 27001 referente a la seguridad de la información una de las más renombradas a nivel mundial, en este sentido es factible encontrar diversas herramientas informáticas que permiten evaluar la gestión de la seguridad de la información en una organización, entre las que se encuentran por ejemplo la desarrollada por ESET Intelligence Labs (ESET, 2019), el programa ISOLUTION desarrollado por la empresa del mismo nombre (ISOLOCION, s. f.), también existe el programa NovaSec de la empresa NewNet (2021), entre otras, estas herramientas tienen como objetivo identificar los activos de información que se deberán proteger, este resultado toma importancia ya que permite definir las características que el sistema de seguridad de información deberá poseer.

Este de análisis de brecha como lo indica Gallegos (2006), también puede ser del tipo cualitativo o cuantitativo, de esta forma debe permitir realizar una estimación de la incertidumbre y el impacto que tendría en la empresa, mientras que para Sikdar (2011), se compone de dos aspectos el que permite identificar las diferentes amenazas a las que una organización puede estar expuesta y la valoración de estas amenazas para cuando se pudieran materializar.

En lo referente al análisis de riesgos para Alemán & Rodríguez (2015),destacan metodologías como OCTAVE, MAGERIT, MEHARI, NIST SP 800:300, Coras, Cram y Ebios que poseen características muy similares, pero diferenciándose entre ellas en dos aspectos principales, el primero, la forma en que estiman la probabilidad de ocurrencia de un evento relacionado a la violación a la seguridad de la información y el segundo el cómo determinan el impacto que este evento puede llegar a tener en la organización.

Como se presenta en el trabajo de Jurado et al.(2020), las metodologías y herramientas existentes se caracterizan por ser desarrolladas para implementarse en empresas e instituciones que poseen una organización, personal capacitado, tecnología y recursos para invertir en el crecimiento de la misma, a diferencia de las microempresas denominadas así por sus características, donde resalta algunos elementos que las hacen incompatibles con estas herramientas, como por ejemplo el no emplear tecnología que no se relacione directamente a generación de ingresos económicos, en este sentido resalta el hecho de que el invertir en tecnologías relacionadas a la seguridad de la información no es primordial.

También es importante mencionar que este tipo de organizaciones manejan un número reducido de empleados que puede ir desde uno hasta veinte dependiendo del país en donde se encuentren, esto lo indica a nivel de Latinoamérica la Comisión Económica para América Latina y el Caribe (CEPAL) (Dini & Stumpo, 2018), estas personas suelen ser en la mayoría familiares o amigos del representante legal y en muy pocos casos son personas con altos conocimientos técnicos o capacitadas en un área específica, dado que este modelo empresarial nació con el objetivo de satisfacer las necesidades de empleo que las PYMES no son capaces de cubrir, el número de las microempresas a nivel de Latinoamérica alcanza una representación del 88,4% de empresas formales según los datos proporcionados CEPAL, esta información junto a las características de los diferentes recursos tecnológicos existentes para implementar los sistemas de gestión y seguridad de la información son los insumos tomados para realizar el análisis de brecha de este sector, debido a la importancia que estas empresas a nivel de un país representan por su número y cantidad de empleo que son capaces de generar.

MATERIALES Y MÉTODOS

La metodología de investigación empleada en el presenta trabajo es la científica que como lo define Tamayo "… procura obtener información relevante y fidedigna, para entender, verificar, corregir o aplicar el conocimiento." (2004, p. 37), para la elaboración del análisis de brecha en las microempresas se utilizó el enfoque cualitativo, partiendo de la teoría relacionada a las herramientas, normativas y metodologías existentes que son reconocidas y empleadas para un adecuado manejo y gestión de la seguridad de la información como base para poder analizar los resultados obtenidos de este análisis, también existe el enfoque descriptivo debido a que se realiza un análisis de la situación actual de las tecnologías relacionadas a la seguridad y gestión de la información de este sector empresarial, para la obtención de los datos se emplea como técnica de recolección de información la encuesta.

Para la aplicación de la encuesta y obtener los datos, esta se la realizó de forma presencial, el trabajo de campo realizado para la obtención de estos corresponde al segundo semestre del año 2019, en base a los datos estadísticos proporcionados por el Instituto Nacional Ecuatoriano de Estadísticas y Censos INEC en su informe denominado como directorio de empresas 2019, en cual se expone la existencia de un total de 882.766 empresas las cuales se clasifican de acuerdo a su tamaño en Microempresas cuyo número es de 802.353 lo que representa el 90.89% de las empresas en el país (INEC, 2019).

Partiendo de esta información y empleando la ecuación matemática (1) para el cálculo de la muestra para poblaciones finitas cuyos datos que permiten determinar este valor son N que representa el número total de microempresas del país que es de 802.353, Z que se relaciona con el valor para alcanzar una seguridad del 95%, la proporción esperada es del 5%, por último, con el objetivo de maximizar el tamaño de la muestra y manejar un error máximo en términos de proporción se emplea el valor de 3%.

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

En base a estos datos se determinó que el número de encuestas que se requieren para obtener datos es de 202,7; en base a este número se las aplico la encuesta a los propietarios de microempresas buscando representatividad de aquellas que se encuentran dentro de los sectores económicos definido por el INEC como servicios y comercio, que según la información presentada por esta entidad representa el 44,55% y el 33,9% del total de empresas siendo los sectores más representativos ya que incluye actividades como información y comunicación; actividades financieras y de seguros; actividades inmobiliarias; actividades profesionales, científicas y técnicas; servicios administrativos y de apoyo; enseñanza; intercambio de materiales; compra y venta de bienes, servicios entre otras, en este sentido evidencia que su campo de acción incluye el uso de tecnología.

Por último, se decidió aplicar la encuesta a las empresas que se encuentran en las provincias de Pichincha y Guayas debido a que concentran el 30,85% y 26,7% de empresas respectivamente según información del INEC.

Análisis de la encuesta

El análisis de los datos obtenidos para determinar la situación actual de las microempresas, se basa en tomar como ejes de análisis la tecnología que disponen; el conocimiento relacionado al uso de la tecnologías; las herramientas que utilizan para proteger su información en caso de tenerla, para lo cual se elaboró un cuestionario de 27 preguntas

divididas en cinco secciones, la primera para obtener información general de cada empresa como lo es el nombre, tipo de empresa en base a la cantidad de personas asociada a esta y actividad económica, la segunda sección enfocada en la forma de organización interna que posee la empresa, la tercera sección se orienta en obtener datos sobre la infraestructura tecnológica que poseen, la cuarta sección para identificar el tipo de información que manejan y que es considerada importante junto con la forma en que se la gestiona, por último, está la sección para evaluar el nivel de conocimiento de la persona o personas encargadas de la parte tecnológica incluyendo el manejo y gestión de la información, bajo estos parámetros se aplicaron 538 encuestas cuyos resultados se presentan a continuación.

RESULTADOS

Los resultados obtenidos de las encuestas realizadas en base a las secciones definidas se obtuvo, para la primera sección relacionada a la información general de cada microempresa, se evidencia una de las características propias de este tipo de organizaciones que es la de poder desenvolverse en casi todos los sectores productivos que aportan al desarrollo económico de un país, desde la comercialización de bienes hasta como mano de obra en diversas actividades como por ejemplo transporte, alimentación, educación, instalaciones, consultorías entre otras, esto se evidencia con las respuestas obtenidas a la pregunta planteada: A qué tipo de sector productivo pertenece la entidad? donde los resultados obtenidos mencionan que 437 microempresas se dedican al sector productivo de servicios en general y 101 microempresas indican que prestan servicios relacionados con la tecnología.

De la segunda sección, los datos obtenidos permiten evaluar el nivel de organización de estas organizaciones, el resultado presentó que de las 538 organizaciones 355 mencionaron que no disponen de un organigrama es decir el 66% de las microempresas encuestadas, resultado a la pregunta planteada de si ¿Existe un organigrama en la entidad?, la importancia de este indicativo se da porque permite evaluar si el personal tiene o no definidas funciones y responsabilidades, por la importancia que dentro de una organización empresarial tiene el definir los roles y responsabilidades de cada colaborador, porque permite que las actividades se desarrollen de forma adecuada, evita la duplicidad de tareas o esfuerzos durante todo el proceso productivo, lo que resalta otra característica de este tipo de empresas en las que todos hacen de todo.

Dentro de esta sección también se evidencia la poca presencia que las microempresas tienen en la red de Internet, este resultado se lo puede considerar como un indicativo de una brecha entre estas organizaciones con las demás, ya que como lo mencionan Gutiérrez & Martín (2005), toda empresa debe considerar la expansión de su negocio empleando el

Internet como medio adicional para poder adaptarse a los nuevos condicionamientos de mercado, bajo esta afirmación de los datos obtenidos se determinó que 374 microempresas del total de encuestadas es decir el 70% no disponen de una página web para ofrecer sus servicios, lo que evidencia la poca importancia que en la mayoría de estas organizaciones tiene el asignar tareas y responsabilidades a sus colaboradores recayendo todas estas en el propietario o representante legal de la microempresa, además de existir gran limitación al momento de buscar visibilidad ante posibles nuevos clientes, por ello a pesar de que representan en cantidad la mayor parte de empresas existentes no crecen al ritmo de las demás.

Del análisis de los datos obtenidos a la tercera sección defina en esta encuesta que permite evaluar la tecnología disponible en estas organizaciones para lo cual se realizó un clasificación de la infraestructura tecnológica en base a características generales sobre los tipos de dispositivos y funcionabilidad de la red que disponen, esta clasificación se la dividió en tres clases que se las denominó Simple, Básica y Completa, en la primera clase hace referencia a disponer de un equipo que provee acceso a internet y al cual se conectan los demás dispositivos electrónicos como computadores y celulares, para la segunda se debe disponer de una la infraestructura de red LAN que incluya cableado y equipamiento para conmutación y ruteadores que permitan la conectividad a los usuarios internos pero no dispone de mecanismos o equipamiento para la gestión y seguridad de la información, por último la tercera clase hace referencia a una infraestructura de red acorde a normativas y estándares internacionales enfocados a mecanismos o equipamiento para la gestión y seguridad de la información.

El resultado de esta clasificación se lo puede observar en el Figura 1, donde resalta el hecho que 359 propietarios de las microempresas entrevistadas consideran que su infraestructura es del tipo simple lo que equivale al 66,73 % del total de encuestas, 116 que corresponden al 21.56 % la consideran como básica y 63 empresas que corresponden al 11,71% la consideran como completa de acuerdo a la clasificación planteada.

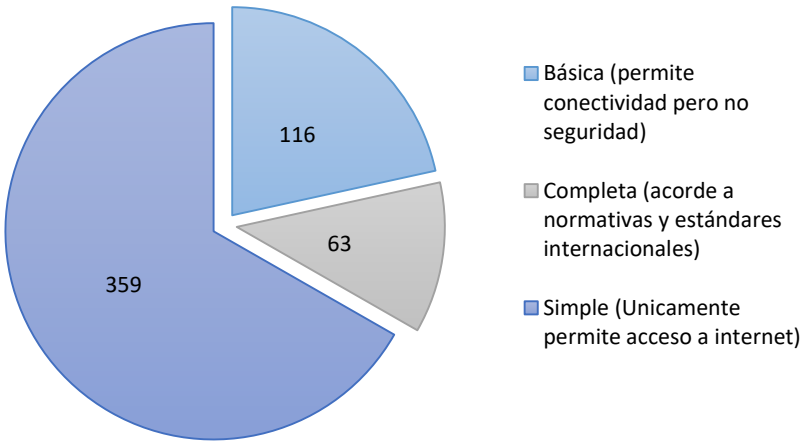

Figura 1. Tipo de infraestructura tecnológica disponible. Fuente Elaboración Propia

Como complemento a la pregunta anterior también se buscó información referente al equipamiento tecnológico que se emplea, en este sentido se obtuvo que el 87,2% de los encuestados indicó que disponen de ordenadores en sus instalaciones, el 72% disponen de equipos para tener conectividad de red del tipo LAN como lo son conmutadores y ruteadores, el 49,8% menciono tener equipamiento para tener una red inalámbrica como los son los ruteadores inalámbricos mientras que tan solo el 0.1% de los entrevistados mencionó que no dispone de ningún tipo de estos dispositivos electrónicos para que los colaboradores realicen actividades relacionadas con el funcionamiento de su organización.

En lo relacionado al uso de la red de Internet en sus actividades diarias se presentaron los siguientes resultados; 508 de la personas entrevistadas indicaron que en su organización emplean esta red lo que equivale al 94%, mientras que tan solo 30 mencionaron que no emplean este recurso tecnológico lo que corresponde al 6%, en este sentido también se consultó sobre los programas de mayor uso y que se encuentren instalados en dispositivos electrónicos dentro de la empresa como ordenadores, en este sentido se destaca el empleo de programas antivirus donde el 90,2% de las entrevistados poseen uno de cualquier fabricante en su versión gratuita, también se mencionaron programas de ofimática donde el 68.8% indico que los emplea y un 60.8% indico que también utiliza programas especializados para la contabilidad, facturación y gestión de inventarios.

Los datos obtenidos en relación al tipo de información que se genera y que se considera importante dentro de la microempresa correspondiente a la cuarta sección planteada resalta que el 70,4% considera importante la Información personal de los empleados y la de sus clientes, también está que el 74,9% considera que la información de la contabilidad, contratos e informes de sus actividades son importantes mientras que el 40,2% considera importante la información que se maneja en cualquiera de las redes sociales que disponen, en este

sentido también se consultó sobre la forma en que se gestiona y protege la información considera importante, el resultado de la encuesta indica que 452 entrevistados indicaron que en su microempresa no se dispone de documentación ni políticas relacionadas a la seguridad de la información que producen este dato equivale al 84% del total, mientras que el 16% de los entrevistados que en número representan a 86 encuestados mencionaron que disponen ya sea documentación o alguna política para proteger su información.

En esta sección de la encuesta también se averiguo de forma general cómo se gestiona la información dentro de cada organización, para ello se preguntó si se realizaba algún tipo de inducción sobre buenas prácticas o hábitos que deben conocer y aplicar sus colaboradores para proteger la información producida, a esta interrogante respondieron 458 de los encuestados indicaron que no, lo que corresponde al 85%, mientras que el 14% que equivale a 74 encuestados indicaron que si se realizaba este tipo de capacitación, mientras que 6 encuestados indicaron que desconocían totalmente sobre el tema lo que equivale al 1%.

Como parte de la gestión también se buscó conocer si para el manejo de esta información existía algún responsable que no fuera el propietario de la microempresa, a lo que 454 encuestados que corresponde al 84% indicaron que no existe una persona encargada de esta tarea, mientras que 84 encuestados que equivale al 16% indicaron que sí, que la persona responsable de esto era aquella que demostraba algún conocimiento sobre informática, lo cual no es un indicador que permita evidenciar que sea una persona especializada en temas seguridad informática.

Para complementar los datos de la existencia de políticas sobre seguridad de la información se consultó si dentro de la microempresa cuentan con algún tipo documentación sobre políticas, reportes de incidentes o manuales referentes a la seguridad de información utilizados por los colaboradores ya sea en forma física o en formato digital, a esta interrogante el 83% de los encuestados mencionaron que no tienen este tipo de documentación, el 7% indicaron que poseen documentación en forma física dentro de la empresa, el 9% indico que poseen esta documentación en formato digital, mientras que tan solo el 1% que corresponde a 7 encuestas indicaron que poseen este tipo de documentación tanto en forma física como digital.

En base a estos datos se evidencia que la inversión en tecnología es mínima y se enfoca únicamente en equipamiento y programas sencillos que les permiten desarrollar su actividad, sin tomar en cuenta la gestión y seguridad de la información que generan y es importante para cada una, lo que se refleja en la poca importancia que esta clase de empresas le dan al manejo de su información, tomando en cuenta que en la actualidad la información se ha

convertido en un bien que permite a todo tipo de organización realizar un análisis de esta para tomar decisiones que directamente se relacionan al crecimiento de la organización.

Por último, no solo el disponer de políticas, tecnología para la gestión y protección de la información asegura que esta se encuentre protegida, también se requiere que el personal encardo de esta gestión tenga determinados conocimientos para aprovechar los recursos disponibles, es por ello que en la quinta sección se enfoca en el análisis del nivel de conocimiento sobre seguridad de información que tienen los encargados en caso de existir dentro de estas organizaciones y de los responsables legales o propietarios de la microempresa, en este sentido se consultó de forma general terminología básica relaciona a los sistemas de gestión de la seguridad de la información, partiendo de la interrogante de que si se conoce sobre seguridad de la información, a lo que respondieron que si 271 encuestados que equivale al 50% mientras que 267 indicaron que no que en porcentaje también corresponde al 50%.

Como parte de este grupo de preguntas sobre seguridad de información se consultó la definición y diferencia entre los términos de ataque, amenaza, vulnerabilidad y riesgo, de las definiciones que proporciono cada persona encuestada, 458 mencionaron no tienen claro estas definiciones número que en porcentaje equivale al 85%, mientras que tan solo el 14% de los encuestados que corresponde en número a 80 encuestados demostraron que si tenían clara las definiciones y diferencias de estos términos.

Otra pregunta de esta sección averiguó si ha escuchado y conoce la definición de términos como Trashing, ataque de denegación de servicios, Ingeniería social, entre otros a lo que se obtuvo como resultado que el 80% que equivale a 432 encuestados no conocen sobre esta terminología ni su definición, mientras que 106 encuestados que corresponde al 20% tienen conocimiento general de estos términos, por último, se preguntó si se tenía conocimiento de que dentro de la organización se ha suscitado algún problema relacionado a la seguridad de la información.

Esto incluye la perdida de datos por cualquier motivo ya sea por robo o falla en los equipos, robo de claves entre otros, a esta interrogante el 64% que corresponde a 345 de los encuestados menciono que no tiene conocimiento sobre estos incidentes, el 6% que corresponde a 33 encuestados indicaron que si conocían y sufrieron de alguno de estos incidentes, mientas que 160 encuestados que corresponden al 30% no estaban seguros o desconocían si la en la organización existió esta clase de incidentes, estos datos, permiten evidenciar que son organizaciones vulnerables ante cualquier tipo de ataque o incidente que afecte a la información importante de estas, ya sea por los denominados hackers, programas maliciosos o simplemente la perdida de información por alguna falla técnica en sus equipos.

Como resultado del análisis de brecha en este tipo de organizaciones en lo referente a tecnologías para la gestión y seguridad de la información se demuestra que no se le da la importancia que esta tiene, ya que más del 80% de estas empresas no implementan algún sistema de gestión, esto va asociado a varios factores inherentes a estas organizaciones, el principal es la limitante económica que impide implementar cualquiera de los sistemas o normativas existentes, esto se evidencia por la inversión que se requiere realizar para cumplir con los requerimientos mínimos que se necesitan para implementar normas como a ISO 27000 o metodologías como OCTAVE MAGERIT entre otros, lo que incluye adquirir equipos y contratar personal especializado, la información obtenida sobre la organización interna de las microempresas junto a su infraestructura tecnológica evidencia lo difícil que resultaría implementar un SGSI basado en normas como la ISO 27001 o metodologías como OCTAVE.

El empleo de tecnología lo que va de la mano con sistemas de seguridad para proteger la información resulta muy importante, con los resultados obtenidos de la encuesta que evidencian que las tecnologías para información y comunicación en estas organizaciones no son las adecuadas, esto se pudo evidenciar por la situación extraordinaria asociada a la pandemia ocasionada por el COVID-19 que afecto a todo tipo de empresas y en gran parte a las microempresas que no disponían de los medios tecnológicos adecuados para adaptarse al comercio electrónico que tubo y está en auge en esta época, lo que permitió que muchas empresas continúen laborando mientras otras debieron cerrar por no poder adaptarse a los cambios que el mercado requería.

CONCLUSIONES

La información que generan las microempresas se encuentra dispersa, es decir información como por ejemplo los datos del personal que labora en ella, informes, cotizaciones, documentos de contabilidad entre otros, se encuentran almacenados en diferentes computadores sin seguridad y a los cuales tienen acceso cualquier persona, ciertos caso la contabilidad se la maneja por personas externas, los informes de los trabajos realizados pasan a ser responsabilidad de la persona que los realizó por lo que se encuentran en los computadores personales o en muchas ocasiones se almacenan en memorias USB que se pueden extraviar con facilidad, lo que se mostró con los datos obtenidos en la encuesta, de esta forma se evidencia la falta de organización que se maneja en estas organizaciones.

La forma en que se gestiona la información en las microempresas ya sea que esta se encuentre en organización o fuera de ella, la hace vulnerable a cualquier tipo de posible eventualidad que puede ir desde la perdida de información por una falla eléctrica en los equipos, hasta el robo de la misma por terceros, evidenciando que a este bien no se lo

considera como un posible generador de recursos económicos, por tal motivo no tiene el trato ni la importancia debida, ya sea por no tener la voluntad de implementar algún recurso tecnológico sino también por la falta de conocimiento sobre que recurso se pude implementar.

La tecnología empleada en las microempresas como se evidencio es muy limitada, la mayoría de estas para su funcionamiento únicamente consideran adecuado el disponer de un computador portátil o de escritorio, acceso a la red de Internet y un dispositivo móvil para que desarrollen sus actividades lo que resulta una limitante para la implementación de sistemas o estándares enfocados en la gestión y seguridad de la información como los descritos en este documento.

El análisis de brecha presentado en este trabajo evidencia que las normativas y metodologías que mayormente se implementan por sus buenos resultados no toman en cuenta las características de este tipo de organizaciones, el personal asociado a esta clase de empresas no es especializado en temas de tecnología asociada a la gestión de la información y los recursos tecnológicos son muy limitados, adicional el costo de implementación de cualquier sistema no está al alcance de estas organizaciones ya que generalmente incluye dispositivos electrónicos, programas y personal especializado, todos necesarios para que el sistema de gestión y seguridad de la información funcione adecuadamente.

REFERENCIAS BIBLIOGRÁFICAS

Alemán, H., & Rodríguez, C. (2015). Metodologías para el análisis de riesgos en los sgsi. Universidad Nacional Abierta y a Distancia, UNAD. https://repository.unad.edu.co/handle/10596/29673

Andrés, A., & Gómez, L. (2009). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. AENOR. http://www.varios.cen7dias.es/documentos/documentos/90/iso.pdf

Bejarano, M. A. G., & Siu, D. R. S. (2017). La Gestión del Conocimiento y los Sistemas de Información como fuentes de Ventaja Competitiva para las Empresas. INNOVA Research Journal, 2(4), 73-76. https://doi.org/10.33890/innova.v2.n4.2017.242

Catoira, F. (2013, noviembre 13). ESET Intelligence Labs: GAP Analysis para empresas | WeLiveSecurity. welivesecurity. https://www.welivesecurity.com/la-es/2013/11/13/eset-security-services-gap-analysis/

de Pablos Heredero, C., Agius, J. J. L. H., Romero, S. M.-R., & Salgado, S. M. (2019). Organización y transformación de los sistemas de información en la empresa. Esic. https://books.google.com.ec/books?hl=es&lr=&id=hnCLDwAAQBAJ&oi=fnd&pg=PT6&dq=los+sistemas+de+informaci%C3%B3n&ots=V46sKwKnz9&sig=oBjfQ07HM1zG7yc4u0eEAPjzkj0&redir_esc=y#v=onepage&q=los%20sistemas%20de%20informaci%C3%B3n&f=false

Dini, M., & Stumpo, G. (2018). Mipymes en América Latina: Un frágil desempeño y nuevos desafíos para las políticas de fomento. CEPAL. https://repositorio.cepal.org/handle/11362/44148

ESET. (2019). Servicios de seguridad informática para empresas [Sitio Web mundial]. ESET Intelligence Labs. https://www.eset.com/ec/empresas/servicios-de-seguridad-informatica-para-empresas/

Gallegos, J. D. C. (2006). Análisis del riesgo en la administración de proyectos de tecnología de información. Industrial Data, 9(1), 104-107.

García, F. Y., & Moreta, L. M. (2019). Modelo para Medir la Madurez del Análisis de Riesgo de los Activos de Información en el contexto de las Empresas Navieras. RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação, 31, 1-17. http://dx.doi.org/10.17013/risti.31.1-17

Gutiérrez, M. D. C., & Martín, F. (2005). La importancia del intangible en la empresa de internet: Una propuesta de medición contable. Universidad Politécnica de Cartegena.

INEC. (2019). Directorio de Empresas [Gubernamental]. Instituto Nacional de Estadística y Censos. https://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Economicas/DirectorioEmpresas/Directorio_Empresas_2019/Principales_Resultados_DIEE_2019.pdf

ISOLOCION. (s. f.). ISOLUCIÓN® Seguridad de la Información. Recuperado 1 de enero de 2020, de https://web.isolucion.com.co/isolucion-seguridad-de-la-informacion/

Jurado, F., Yarad, V., & Carrión, J. (2020). Análisis de las características del sector microempresarial en latinoamérica y sus limitantes en la adopción de tecnologías para la seguridad de la información. REVISTA CIENTÍFICA ECOCIENCIA, 7(1), 1-26. https://doi.org/10.21855/ecociencia.71.303

Ladino, M., & López, A. (2011). Fundamentos de iso 27001 y su aplicación en las empresas. Scientia et technica. Scientia et technica, 17(47), 334-339.

Legner, C., Eymann, T., Hess, T., Matt, C., Böhmann, T., Drews, P., Mädche, A., Urbach, N., & Ahlemann, F. (2017). Digitalization: Opportunity and challenge for the business and information systems engineering community. Business & information systems engineering, 59(4), 301-308.

NewNet S.A. (2021). Software GRC | Gestión Integral de Riesgos | Ciberseguridad | SGSI. NewNet S.A. https://www.newnetsa.com/software-grc/

Orrego, V. M. (2013). La gestión en la seguridad de la información según Cobit, Itil e Iso 27000. Revista Pensamiento Americano, 4(6), 21-23.

Proaño, M. F., Orellana, S. Y., & Martillo, I. O. (2018). Los sistemas de información y su importancia en la transformación digital de la empresa actual. Revista Espacios, 39(45). http://es.revistaespacios.com/a18v39n45/18394503.html

Schwertner, K. (2017). Digital transformation of business. Trakia Journal of Sciences, 15(1), 388-393.

Sikdar, P. (2011). Alternate approaches to business impact analysis. Information Security Journal: A Global Perspective, 20(3), 128-134.

Tamayo, M. (2004). El proceso de la investigación científica: Incluye evaluación y administración de proyectos de investigación (4ta ed.). Editorial Limusa. https://books.google.com.ua/books?hl=es&lr=&id=BhymmEqkkJwC&oi=fnd&pg=PA11&dq=investigacion+descriptiva&ots=TrbJdiW8hM&sig=SeqGLkh0tEM8ooklYPTHcX-pR_U&redir_esc=y#v=onepage&q=investigacion%20descriptiva&f=false

Valencia, F., & Orozco, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. Revista Ibérica de Sistemas e Tecnologias de Informação, 22, 73-88. https://dx.doi.org/10.17013/risti.22.73-88

Verina, N., & Titko, J. (2019). Digital transformation: Conceptual framework. Proc. of the Int. Scientific Conference “Contemporary Issues in Business, Management and Economics Engineering’2019”, Vilnius, Lithuania, 9-10.