ANÁLISIS DE LAS CARACTERÍSTICAS DEL SECTOR MICROEMPRESARIAL EN LATINOAMÉRICA Y SUS LIMITANTES EN LA ADOPCIÓN DE TECNOLOGÍAS PARA LA SEGURIDAD DE LA INFORMACIÓN

ANALYSIS OF THE CHARACTERISTICS OF THE MICROENTERPRISE SECTOR IN LATIN AMERICA AND ITS LIMITATIONS IN THE ADOPTION OF TECHNOLOGIES FOR INFORMATION SECURITY

Francisco Xavier Jurado Pruna, Mgs.
Magíster en Redes de Comunicaciones Pontificia Universidad Católica del Ecuador (Ecuador).
Docente de la Facultad de Ingenierías de la Universidad Tecnológica Israel, Ecuador.
https://orcid.org/0000-0001-8689-0398
fjurado@uisrael.edu.ec

Pamela Valeria Yarad Jeada, Ph.D.
Doctora en Sociología y Antropología (España).
Docente investigadora.
https://orcid.org/0000-0002-5040-4324
vale.yarad@gmail.com

Joe Luis Carrión Jumbo, Ph.D.
Doctor en Informática por la Universidad Autónoma de Barcelona (España).
Docente de la Facultad de Ingenierías de la Universidad Tecnológica Israel, Ecuador.
https://orcid.org/0000-0003-3632-5352
jcarrion@uisrael.edu.ec

ARTÍCULO DE REFLEXIÓN
Recibido: 7 de enero de 2020.
Aceptado: 29 de enero de 2020.

RESUMEN

El artículo presenta un análisis de la situación actual de las tecnologías relacionadas con la seguridad de la información en las microempresas de Latinoamérica, las mismas que representan a un amplio sector en la economía de los países de la región y como toda empresa producen información valiosa relacionada a sus actividades, por ejemplo, informes técnicos, diseños, datos contables, bancarios, lista de clientes, entre otros. debido a la capacidad de empleo que generan y a su productividad comercial. Para realizar el análisis planteado se emplea la revisión sistemática de varias fuentes confiables para la recolección de información relevante relacionada con las características de este sector empresarial y las soluciones tecnológicas para el manejo de la información, de esta forma definir las limitantes que este tipo de empresas tienen al tratar de adoptar este tipo de tecnologías, dificultades relacionadas a las características propias de las microempresas y del no disponer de soluciones que se ajusten a sus necesidades como las existentes para las medianas y grandes compañías.

Palabras clave: seguridad de la información, tecnología, normas, MiPymes.

ABSTRACT

The article presents an analysis of the current situation of technologies related to information security in the microenterprises of Latin America, which represent a large sector in the economy of the countries of the region and how every company produces valuable related information to its activities, for example, technical reports, designs, accounting data, banking, customer list, among others. Due to the employment capacity they generate and their commercial productivity. To carry out the proposed analysis, a systematic review of several reliable sources is used for the collection of relevant information related to the characteristics of this business sector and the technological solutions for information management, in this way defining the limitations that this type of companies when trying to adopt this type of technologies, difficulties related to the characteristics of microenterprises and the lack of solutions that meet their needs such as those existing for medium and large companies.

Keywords: information security, technology, standards. MiPyme

INTRODUCCIÓN

Desde hace décadas se habla de Latinoamérica como aquella región inviable, ingobernable (De Sousa Santos, 2004) y donde las desigualdades sociales y la pobreza han llevado a sus ciudadanos a buscar nuevas formas de subsistir ante el desempleo y la falta de oportunidades, estos problemas han dado paso al denominado emprendimiento (Kantis, Federico, & Menéndez, 2012).

La Organización Internacional del Trabajo (OIT), a partir de los años noventa empezó a visibilizar un nuevo modelo de empleo desarrollado en el ámbito informal al que se lo denominó microempresa, esta nueva forma de empleo como lo menciona Infante (1999), se relaciona a los trabajadores independientes, quienes se agrupan para desarrollar emprendimientos basados en la prestación de servicios o ventas, alcanzando a generar importantes fuentes de empleo. Esto se evidencia en especial cuando los países se encuentran en periodos de crisis donde la baja productividad hace que las microempresas se conviertan en una alternativa al empleo formal y una herramienta para enfrentar la desigualdad y pobreza, contrario a lo que sucede en los periodos de crecimiento donde el empleo es absorbido por las empresas formales con mejores remuneraciones debido a la mayor producción existente, lo que hace que en muchas de las ocasiones el empleo informal sea absorbido por éstas (Mac-Clure, 2001).

Este modelo empresarial al que por sus características se lo ha englobado dentro del término MiPymes reúne las micro, pequeñas y medianas empresas, cada una dentro de su desarrollo es influida de forma directa por las Tecnologías de la Información y Comunicación (TIC), las cuales forman parte de casi todas las actividades de los seres humanos, alcanzando gran importancia dentro del sector empresarial donde es primordial no solo disponer de tecnología para la producción sino también mantener buenos sistemas para proteger la información privada de cada empresa como lo indica Bertolín (2008), se debe incluir el nivel de conocimiento y la capacidad de manejo de las TIC de cada persona

involucrada en los diferentes procesos productivos para alcanzar un desarrollo adecuado en las organizaciones.

Estos nuevos cambios generados como el resultado del desarrollo de la tecnología ha llevado a la simplificación de las actividades, entre las cuales se encuentra el comercio electrónico o *e-commerce* que se realiza a través de Internet y en el que los flujos de información las transacciones financieras y las compras de productos por medio de una página web generan un mayor volumen de datos, los cuales pueden derivar en vulnerabilidades que algunas empresas todavía no están listas para enfrentar y que hace necesario que todos los involucrados conozcan cuales son los riesgos en cuanto al manejo de información y como mitigarlos.

La importancia que la tecnología adquiere día a día en todos los sectores hace que se deba tener en cuenta dos factores inherentes al desarrollo de las TIC, el primer factor es la seguridad de la información especialmente en el sector empresarial, este concepto como lo define Andress “es la protección de la información y los sistemas de información de accesos no autorizados, que tengan como objetivo de divulgar, interrumpir, modificar o destruir dicha información” (2014, 3).

En forma general la seguridad de información hace referencia a la protección del activo más importante que produce una empresa como lo es la información relacionada a su actividad, esta debe ser protegida de cualquier situación ya sea por eventos naturales o provocados, que produzcan falla en la infraestructura de red, incluye también los ataques por el uso de virus informáticos, vandalismo entre otros, por último está el factor asociado al conocimiento de las personas pertenecientes a cada organización, porque un alto nivel de conocimiento teórico y práctico de las TIC aporta sustantivamente al desarrollo de la empresa.

1. REVISIÓN TEÓRICA

1.1. Las microempresas caracterización e importancia

Este modelo empresarial como lo indica González (2005), posee criterios de clasificación que se basan en el número de empleados asociados a cada una, junto con el volumen de ventas e ingresos al año, el número de las microempresas a nivel de Latinoamérica alcanza una representación del 88,4% de empresas formales según los datos proporcionados por la Comisión Económica para América Latina y el Caribe (CEPAL) (Dini & Stumpo, 2018), la relevancia de las microempresas resalta por el número existente, la cantidad de empleo que pueden generar y la capacidad de desenvolverse en casi todos los sectores productivos relacionados a la economía de cada país.

Ahora bien, para poder definir a las microempresas se debe realizar un análisis de las características de este tipo de empresas, empezando por el número de personas que se asocian a cada una, es decir el número de empleados que las pueden conformar, como se puede observar en la Tabla 1 no existe un criterio común para esta característica, ya que dependiendo de cada país el criterio varía.

Tabla 1. Clasificación de las microempresas

País	**Microempresa No. De personas**
Argentina	Máximo 5
Bolivia	Máximo 4
Brasil	Máximo 19
Chile	Máximo 9
Colombia	Máximo 9
Costa Rica	Máximo 30
Ecuador	Máximo 9
El Salvador	Máximo 20
México	Máximo 15
Nicaragua	Máximo 3
Paraguay	Máximo 5
Perú	Máximo 10
Trinidad y Tobago	Máximo 5

Uruguay	Máximo 4
Venezuela	Máximo 4

Fuente: Elaboración propia con base en datos proporcionados por la CEPAL (2012)

Esta característica muestra el número de personas asalariadas con las que puede contar una microempresa, generalmente la mayoría de éstas suelen ser familiares o personas muy cercanas al propietario, esta nueva forma de empresa coincide con el criterio presentado por Roblés & Alcérreca (2000), quienes afirman que las microempresas además de atender necesidades especializadas son flexibles en cuanto a su operabilidad, debido a que no gozan de jerarquías complejas como las compañías más grandes. Asimismo, otra característica propia es la centralización de funciones en el representante legal ante que en la mayoría de los casos es la persona encargada de realizar todas las actividades que se requieren para llevar a cabo su normal funcionamiento; es decir, realiza actividades financieras, administrativas, de ventas, instalaciones, entre otras, que a diferencia de una empresa de mayor tamaño las actividades son divididas en departamentos con sus responsables respectivos (De Asís, Labie, & Mataix, 2000).

Las microempresas también se caracterizan por no dedicarse a un sector productivo exclusivo, lo que les permite desarrollarse en cualquier ámbito dentro de la economía de un país (Benito, 2009), son heterogéneas, también se requieren de una baja capitalización para realizar sus actividades productivas lo que les permite definir el tipo de producto o servicio que proveerán de acuerdo a las aptitudes de quienes las conforman, de esta forma responden a las necesidades de autoempleo para la cual fueron concebidas, por último se destaca que muchas se desenvuelven en el campo de la informalidad cuya característica puede ser contraproducente, ya que al no estar formalmente constituidas no gozan de las garantías legales que otras empresas tienen.

La relevancia de este sector empresarial radica en la capacidad de generar empleo en cualquier país, así lo evidencian varios estudios que presentan la relación entre el crecimiento económico y el desarrollo empresarial, uno de estos estudios es el presentado por Davison, Lindmark & Olofsson (1994), en el que destacan la importancia de las pequeñas empresas en la generación de nuevos empleos y que la formación de nuevas

empresas tiene gran influencia en el desarrollo económico de Suecia, cuyo país es uno de los referentes en materia de bienestar ciudadano y calidad de vida. En Latinoamérica también se han realizado este tipo de investigaciones, destaca el trabajo de Saavedra & Hernández (2008) quienes presentan la importancia de las MiPymes a nivel social debido a que permiten combatir el desempleo en personas mayores de 55 años que por su edad les resulta difícil incorporarse a un mercado laboral competitivo, también está el presentado por Alemán (2006) para quien el desarrollo a nivel local puede estar basado en las empresas MiPyme de Colombia, por último se encuentra la investigación realizada por Reynolds (1997) quien demuestra la importancia de crear empresas para satisfacer la necesidad de empleo debido al aumento en el número de habitantes, este factor favorece a la conformación de las microempresas.

1.2. Relación de las microempresas con la tecnología

En la actualidad el desarrollo social y económico alcanzado por el desarrollo de la denominada sociedad del conocimiento/red (Stehr, 1994; Castells, 1997) se evidencia en casi todos los campos donde intervienen las personas, a nivel empresarial este desarrollo se refleja cuando se alcanza una producción adecuada basada en el incremento de la producción de bienes junto con la inclusión de la aplicación de conocimientos tecnológicos para gestionar de forma óptima todos los procesos que intervienen en la producción y distribución de bienes o servicios a los consumidores finales (Borja, Castells, Belil, & Benner, 1998), así también lo resalta Van Stel (2005) quien indica que asociar las TIC de forma adecuada en las empresas reduce significativamente los costos del capital y la información, por ello la importancia de las microempresas no solo se relaciona con la capacidad de empleo que generan, sino también como lo argumentan Durán, Guadaño & García (2005), las microempresas apoyan al desarrollo del territorio en el que se desempeñan ya que favorecen a la llegada de las TIC.

La importancia que las TIC han alcanzado dentro de una empresa para que ésta logre sus objetivos de permanencia y éxito en el mercado, aparece cuando la tecnología aporta de forma directa en la calidad y costos de los productos o servicios presentados a los consumidores (Castells & Pasola, 2004), lo que hace que una empresa sea exitosa cuando

esta incluye dentro de sus procesos de negocio la tecnología (Saavedra & Tapia, 2013), las TIC ofrecen grandes oportunidades para facilitar a las empresas su expansión al poder desarrollar nuevos productos, mejorar el servicio de atención al cliente (Castel & Sanz, 2009), es así como la optimización de los procesos ha generado que proveedores de software desarrollen varios recursos como los ERP (Enterprise Resource Planning) y los BMP (Business Process Management) enfocados a la administración y gestión en los negocios que se impactan en la competitividad de la organización.

Estos aspectos han creado nuevos flujos de información, que al analizarlos correctamente permiten optimizar las diferentes actividades que se desarrollan tanto dentro como fuera de una empresa (Porter & Millar, 1985), el éxito del uso de tecnología como ya lo demostraron Jeon, Han y Lee (2006) donde los factores de éxito que se pueden obtener en las pequeñas empresas se dan al adoptar el *e-business* o negocios en línea en Corea.

Las TIC aportan de manera significativa al mejoramiento en el desempeño de las empresas (Peirano & Suárez, 2006), el alcanzar mejoras depende de seguir cuatro pasos: automatizar los diferentes procesos productivos, la accesibilidad a la información importante para la toma de decisiones, los costos de transacción que se manejan dentro de la empresa para que los procesos productivos fluyan, por último están los procesos de aprendizaje basados en modelos virtuales que empleando simulaciones facilitan la producción y reducen costos.

El impacto que la tecnología produce en una empresa le permite evolucionar y adaptarse a los nuevos requerimientos del mercado, por ello el sector microempresarial no se encuentra exento de incorporar las TIC para alcanzar un adecuado desarrollo, es así como los productos alcanzan éxito ya sea por su costo, calidad, diseño, estrategias de publicidad o por disponer de una red comercial amplia, la globalización obliga a todo tipo de empresas a ser innovadoras adaptándose a los cambios requeridos para desarrollar productos nuevos y mejores procesos de fabricación, ya que de no hacerlo corre el riesgo de ser superada por sus competidores (Escorsa & Valls, 2003).

Dentro de los procesos de innovación es posible diferenciar a la tecnología en dos clases, la primera clase es la tecnología relacionada al equipamiento productivo, entre los que se

encuentran equipos de computación, maquinarias, dispositivos de medición, software para diseño como planos, programas que las empresas adquieren para mejorar los productos o servicios que ofrecen a los consumidores (Cadenilla, 2005). Esta tecnología ligada a la automatización de procesos de producción y a la sustitución de materiales permite reducir los ritmos productivos y mejorar la competitividad, pero para poder alcanzar los beneficios de la automatización es necesario que los involucrados en los diferentes procesos tengan la capacidad de aplicar las TIC ya que la evolución de la tecnología solo facilita el acceso, pero por sí sola no garantiza que los conocimientos sean transmitidos (Luna & Pezo, 2005).

La evolución de las TIC basada en la aplicación de tecnologías permite obtener varias ventajas, las cuales no se reflejan en todos los sectores ya que el desarrollo tecnológico también crea la conocida Brecha Digital debido al limitante de acceso y uso de las TIC, la Unión Internacional de Telecomunicaciones (UIT) indica que la mitad de la población mundial sigue sin estar en línea, es decir alrededor de 3900 millones de personas (ITC Facts & Figures, 2017), no tienen acceso a estas tecnologías. Estos datos son corroborados por el Banco Mundial que resalta que el 60% de la población mundial sigue aún sin poder participar de los beneficios que proporciona la tecnología ("World Bank Group - International Development, Poverty, & Sustainability," 2018).

Asimismo, ambos organismos hablan de la tecnología como un ente transformador dentro de las sociedades promoviendo mejora en una calidad de vida, en la comunicación y en los sistemas políticos-organizacionales. La penetración masiva del teléfono móvil y la Internet pueden llegar a transformar las economías, sociedades e instituciones (Goggin & Hjorth, 2014). Sin embargo, para estas transformaciones exigen que los Estados deben estar dispuestos a invertir y promover una cultura de innovación en donde las tecnologías se convierten en herramientas aliadas al desarrollo de los ciudadanos.

En lo referente al mundo empresarial, el aparecimiento de las TIC genera un impacto positivo debido a la mejora de los procesos que manejan lo que permitirá alcanzar cierto éxito, al implementar como primer paso la digitalización de los flujos de información y comunicación en los procesos productivos, asimismo, estas implementaciones ayudan a

validar el desempeño actual y generando redes que contribuyan a la competitividad de la empresa (Casalet & González, 2004).

Otro aspecto que destacar es la tecnología utilizada para la seguridad y manejo de la información, esta última adquiere importancia, ya que es la base para que una empresa se mantenga innovando en comparación a sus competidores, en la actualidad la información interna de cada empresa permite desarrollar estrategias de negocio que ayudan a incrementar la productividad e innovación de productos. Una buena estrategia de seguridad de la información representa una ventaja competitiva, si es que esta información se pierde o es vulnerada podría ocasionar pérdidas económicas e incluso la desaparición de empresas (Prieto & Martínez, 2004), por lo que dentro del mundo de las microempresas este tipo de tecnología debe ser tomada a consideración.

1.3. Tecnologías para la seguridad de la información en las microempresas

Al hablar de seguridad de la información en forma general se hace referencia a los recursos necesarios para proteger los sistemas informáticos y mantener su normal funcionamiento, esta protección debe ser tanto en lo tangible (hardware) como el intangible (software). La primera que hace alusión a la protección de los equipos informáticos ante cualquier eventualidad, por ejemplo desastres naturales, incendios, inundaciones, problemas eléctricos robos entre otras, la segunda relacionada con los programas informáticos que sirven para proteger la información ante ataques a la red como por ejemplo robo de datos de usuarios, pérdida de datos debido a la infección de virus en equipos informáticos, modificaciones en datos no autorizadas entre otros, ambas son complementarias y al implementarlas de forma adecuada protegen la información (Portantier, 2012).

Al realizar el análisis de la tecnología en las microempresas, la infraestructura tecnológica presenta un rezago comparado con los demás tipos de empresas así lo presenta Durán (2015), en el que se realiza una investigación sobre las tecnologías para las microempresas que funcionan como talleres mecánicos en la comuna de Chillán en Chile en los cuales las TIC empleadas son internet, correo electrónico, redes sociales, en este estudio se presentan resultados interesantes como que el 77% de las microempresas poseen un

computador y que el 73% tiene acceso a Internet, el uso del correo electrónico se relaciona directamente con el nivel de educación que poseen los propietarios es así como el 36% de estos que utilizan el correo poseen educación media, mientras que la cifra aumenta al 80% cuando los propietarios alcanzan un nivel educativo superior (Técnico Profesional o Universitaria).

Asimismo, Medina (2017) presenta la incidencia que los cambios tecnológicos tienen en las microempresas de la construcción en la ciudad de Durán ubicada a pocos kilómetros de la ciudad de Guayaquil, aquí se destaca que existe una brecha tecnológica entre las empresas MiPymes y las grandes empresas debido a que el uso de las TIC es limitado y no permite que estas se desarrollen, en este sentido García Pereyra & Cantó (2018) plantean que las microempresas deben implementar cuatro variables para promover su crecimiento y rentabilidad. A) mejorar el perfil profesional del propietario en temas gerenciales, B) definir una estructura organizacional para mejorar los procesos productivos, C) implementar las TIC para mejorar la gestión, la interacción con los clientes, proveedores entre otros; y D) desarrollar una planificación estratégica de sus competencias con relación a las demás.

Cuando se habla de seguridad de la información a nivel de las microempresas, hay que pensar que dichas estrategias engloban aspectos que van más allá de una buena conexión a Internet o de la adquisición de buenos equipos, es necesario poner a consideración otros factores de seguridad que son relevantes y se relacionan con mantener la integridad de la información producida durante el desarrollo de los diferentes procesos de producción, uno de esos conceptos ligados a la confidencialidad de la información tanto de los públicos internos (empleados, directivos, proveedores), así como de los externos (clientes) (Gómez, Pérez, Donoso, & Herrera, 2010), estos datos son reservados y no suelen ser públicos (cuentas bancarias, números de identificación, etc.), cuya información en caso de ser pública puede generar un daño en el individuo o en la organización.

El acceso a información privilegiada ocasiona daños no solo a personas sino también a empresas donde a más de los productos o servicios que comercializan, la información relacionada a sus estrategias de ventas, patentes, base de datos de clientes, etc., a; llegar a ser pública o compartida con sus competidores puede ocasionar pérdidas económicas y

de competitividad, el uso de la tecnología en todos sus procesos de negocio ayuda a desarrollar directrices para que las estrategias que utilicen les permitan competir con las demás empresas (Scheel, 2005).

La importancia que estas tecnologías y su implementación en el sector empresarial es evidente al analizar cifras relacionadas con la seguridad de la información, a nivel de Latinoamérica cabe mencionar la investigación desarrollada por la empresa ESET que en su documento "Report 2018" (Laboratorio de Investigación ESET Latinoamérica, 2018), muestra información obtenida de más de 4.500 personas relacionadas a la parte ejecutiva, técnica y gerencial de las empresas a las que clasificó en pequeñas con menos de 50 empleados, medianas de entre 50 y 250 empleados, grandes de entre 250 y 1000 empleados y las Enterprise de más de 1000 empleados, en base a los datos presentados se elaboró la Tabla 2 donde se muestran los resultados considerados relevantes.

Tabla 2. Principales resultados Ciberseguridad en Latinoamérica

Parámetro	Resultado
Políticas y planes para gestión de la seguridad de la información	Al menos el 25 % de empresas no posee políticas para asegurar su protección
Infecciones por "ransomware"	57% Siendo el Ecuador el país con mayor índice de infecciones de *ransomware*
Infecciones por "malware"	53%
Ataques por Vulnerabilidades	55% En el año 2017 se reportaron más de 14700 vulnerabilidades en comparación a las 5447 del 2016
Incidente de seguridad	Al menos 3 de cada 5 empresas sufrieron al menos un incidente de seguridad
Robo de Información	51%

Fuente: Elaboración propia con base en datos proporcionados por el Reporte de ESET (2018)

En este mismo campo están las cifras presentadas por Fortinet para el año 2018 de ataques relacionados al robo de información, se observa que estos eventos van en crecimiento, al revisar los resultados presentados se muestran que las cifras por intentos por intrusión a las redes de datos que alcanzan más de 545.000 casos cada minuto, neutralización de más de 140.000 programas tipo malware cada minuto (Juniper Research, 2018), estos datos muestran la demanda creciente por conseguir información cada momento no solo de empresas sino también de personas.

Como información adicional obtenida de la encuesta global realizada por Ernst & Young Global Limited (2019), a más de 1.400 ejecutivos a nivel mundial, destaca que a nivel industrial existe una interconexión masiva de diversos dispositivos electrónicos que permiten interactuar a personas y sistemas en cualquier lugar y a cualquier hora, pero todo este avance requiere que se preste una especial atención a la ciberseguridad ya que los ataques están en crecimiento y el Foro Económico Mundial se calcula que para el año 2021 el costo de los ataques superarían los 6'000.000 de dólares. La consultora señala que, únicamente el 13% de las empresas encuestadas dedican un presupuesto para ciberseguridad acorde a sus necesidades, lo que aún es una inversión baja considerando los riesgos existentes.

Asimismo, la empresa CheckPoint (2018) en su reporte de ciberseguridad indica que los ataques cibernéticos se han desarrollado de forma progresiva alcanzando en la actualidad la quinta generación, contrario a los dispositivos y sistemas de seguridad que poseen las empresas que únicamente llegan a proteger contra ataques de segunda o tercera generación.

Con el objetivo de cubrir la creciente demanda de seguridad existen normas aplicables a nivel mundial además de leyes que algunos países han desarrollado, entre las normas están la ISO 27001, ISO 27002, los controles del CIS (Center for Internet Security), la UNE7150, el Reglamento General de Protección de Datos (RGDP), que las empresas deben cumplir, en lo relacionado a leyes existentes. En algunos de Latinoamérica destacan Uruguay y Argentina que como lo mencionan Mayorga, García, Duret, Carrión & Yarad (2019) que poseen una normativa desarrollada en comparación a los demás países de la

región en lo referente a la protección de datos a nivel personal, el objetivo principal de estas normas y leyes es proveer métodos de protección de la información en una entidad ya sea pública o privada, por ello en la actualidad existen empresas dedicadas a distribuir productos para proteger la infraestructura de red, ya sean estos programas o equipos, entre algunas de estas se puede mencionar a IBM, Veracoide, AVG, Symantec, CISCO, Hewlett Packard entre otras.

1.4. Limitantes en implementación de las tecnologías para la seguridad de la información y estándares existentes en las microempresas.

Entre los factores limitantes en la implementación de tecnologías de protección de datos en empresas es el relacionado al acceso, una parte de los colaboradores o la mayoría no utilizan herramientas TIC o incluso todos los miembros de la organización no cuentan con esos insumos. La segunda limitante se asocia a la falta de conocimientos en la aplicabilidad y uso de las TIC, ya que no todos los empleados están debidamente capacitados para la correcta utilización de éstos. Por último, existen colaboradores que saben manejar este tipo de equipos/software, no obstante, el uso que hacen de ellos no es el adecuado (Camacho, 2005). Este mal uso puede conllevar a deterioros leves o severos tanto en tangibles como en intangibles.

Es así que la sociedad la base para avanzar es el conocimiento (Stehr, 1994) es necesario estar preparados para la solución de problemas para Cornella (2001) la capacidad de manejo de la tecnología depende también de las características generacionales de las personas llegando a ser de gran impacto porque muchas no logran adaptarse a las nuevas características que exige la sociedad, por ende son desplazadas haciendo que la disponibilidad de información que existe en la red de Internet no sea suficiente para reducir la falta de conocimiento, a esta brecha generacional Marc Prensky (2001) lo denominó nativos-inmigrantes digitales.

Además, de los factores mencionados (acceso, falta de uso, uso indebido), las microempresas por las dificultades de inversión sufren en ocasiones retrocesos en materia de innovación, debido a que se mantienen empresas con equipamiento sencillo suficiente

para mantener conectividad; es decir, infraestructura de red física básica compuesta por equipos empleados para uso en casa, disponen de un programa antivirus gratuito con las limitantes que esto con lleva, este software es la única protección ante ataques cibernéticos por los denominados hackers, dejando a una microempresa lejos de poder seguir la tendencia general y creciente de proteger la información.

Las empresas de cualquier tipo involucradas en cualquier sector productivo están expuestas a riesgos en sus sistemas de información, planteando la necesidad de implementar un Sistema de Gestión de Seguridad de la Información (SGSI), una estrategia a aplicar puede ser la norma UNE-ISO/IEC 27001 y el modelo de Esquema Nacional de Seguridad (ENS), siendo este último de aplicación obligatoria en algunos países como España (Gómez & Andrés, 2012).

Devia & Pardo (2014), muestran un análisis comparativo entre las características más comunes y representativas de los diferentes modelos para análisis de riesgos de TI, entre ellos se encuentran el modelo de CRAMM, COBIT, ITIL además de los estándares de riesgos de TI como la ISO/IEC 27000, UNE7150 4:2008, presentando una posible integración entre éstos y las diferentes normas en los modelos de riesgos que las MiPymes dedicadas al desarrollo de software deberían tomar en cuenta. Otro trabajo para resaltar es el de Ampuero (2011), que presenta el diseño de un Sistema de Gestión de Seguridad de Información SGSI que podría ser implementado por cualquier compañía de seguros en base a los requerimientos de la Superintendencia de Banca y AFP del Perú basados en la normativa internacional ISO/IEC 27001.

La aplicación del estándar ISO 27001se aplica más al ámbito de las pymes dejando fuera de este grupo al sector microempresarial, así lo evidencia también Ana Andrés y Luis Gómez (2009) en cuyo documento se proporcionan diversos conceptos y presenta recomendaciones generales para implementar un SGSI en una pyme basándose en la norma UNE-ISO/IEC27001, en este mismo sentido está el trabajo de investigación de Ladino & López (2011) que presentan una descripción de los fundamentos del estándar ISO27001 y su aplicación en organizaciones pymes.

A nivel general una de las normas más importantes es la ISO/IEC 27001 Garzá, Fernández & Piattini (2009), describen procesos e implementación de tecnología para minimizar los inconvenientes que pueden ocasionar en una empresa por no disponer de Sistemas de Gestión de la Seguridad de la Información. Esta normativa creada en el año 2005 se refiere a los procesos necesarios para la gestión adecuada de la información, lo que se logra cuando una empresa sigue rigurosamente el conjunto de reglas establecidas, este estándar es de aplicabilidad para cualquier tipo empresa para ello esta debe cumplir con cinco etapas obligatorias para alcanzar la certificación internacional como lo muestran Valencia & Orozco (2017), de forma general las descripciones de éstas son:

Etapa 1: Obtener la aprobación de la gerencia o altos directivos para iniciar la implementación de un SGSI debido a que los sistemas deben incluir a toda la organización.

Etapa 2: Definir alcance, límites y políticas del sistema que deberá tener y cumplir el sistema a implementar.

Etapa 3: Análisis de los requisitos de seguridad, es establecer los requisitos de seguridad de la información contemplando cinco elementos: A) identificar activos de información importantes, B) visión de la entidad en cuanto a los requisitos a futuro sobre procesamiento de información, C) forma actual de procesar la información, D) requerimientos legales, pólizas de seguros, reglamentos, obligaciones contractuales, normas del sector productivo al que pertenecen, acuerdos con clientes internos, externos y proveedores, entre otros; y E) nivel de conciencia sobre seguridad y capacitación del personal en lo referente a seguridad de la información.

Etapa 4: Valorar y planificar riesgos: esta etapa constituye la principal dentro del SGSI y el referente lo constituye la normativa ISO 27001, en esta etapa también es factible utilizar otras metodologías como por ejemplo la de OCTAVE, CRAMM, NIST SP 800-300, MAGARIT, FAIR, RISK FOR COBIT.

Etapa 5: Diseñar el SGSI: el diseño debe contemplar tres componentes como lo son la documentación, la implementación de controles definidos y el monitoreo constante de la seguridad de la información.

Dentro de las normativas es importante hacer hincapié en la guía desarrollada por el Centro de Seguridad en Internet (CIS) para pequeñas y medianas empresas, la cual presenta un conjunto de buenas prácticas de seguridad para tratar con las amenazas y vulnerabilidades, esta guía presenta tres fases, la primera que se enfoca en saber qué activos importantes están en la red, es decir conocer su entorno, la segunda fase se basa en la protección de los activos definidos en la fase anterior y la tercera fase consiste en preparar la organización ante cualquier evento ("CIS Controls SME Companion Guide," n.d.), todos los trabajos mencionados resaltan la falta de desarrollo de herramientas SGSI enfocadas al sector de las microempresas con relación a la seguridad de la información.

Es por ello que al analizar los requerimientos de los estándares para ser implementados, especialmente el estándar ISO 27001 considerado como referente de la seguridad de información, junto a las características que definen las microempresas se evidencia las dificultades que éstas tendrían para cumplirlos tanto por la inversión económica como por el nivel de conocimiento requerido, es así que es posible asegurar que los estándares son enfocados para empresas que disponen de una infraestructura de red con características mínimas para implementar cualquier sistema tecnológico, además de disponer de recursos económicos para la reinversión de nuevas tecnologías y estrategias de seguridad de la información.

Además de los estándares ya mencionados, también se han desarrollado herramientas de software que permiten enfrentar algunas de las amenazas actuales en una red, entre estas herramientas es factible encontrar una gran variedad como las presentadas por la revista especializada COMPUTERWOLD en un artículo publicado en su versión digital ("El mejor software de seguridad de 2018," 2018) donde se presentan algunas herramientas de ciberseguridad que no disponen de versiones gratuitas según se puede validar al revisar sus páginas de Internet entre las que se encuentran: Balbix dentro de la categoría de gestión de vulnerabilidades de las redes, presenta datos y predice la probabilidad de que

se produzca algún acontecimiento debido a éstas, también esta BluVector dentro de la categoría de seguridad de la red que puede detectar y responder ante la detección de una amenaza, dentro de la categoría de control de tráfico está la herramienta denominada Vectra Cognito que incluye inteligencia artificial para el monitoreo del tráfico de una red y detectar amenazas que se encuentren dentro de una red protegida.

Estos programas que cumplen una función determinada de acuerdo a las características presentadas por el fabricante pueden aportar a la protección de la información, pudiendo afirmar que no es suficiente para decidir cuál(es) implementar en una microempresa ya que estos programas al igual que las normativas y guías sobre seguridad de la información están enfocadas en empresas pequeñas y medianas que poseen características diferentes a las microempresas.

2. MATERIALES Y MÉTODOS

Diseño: Se realizó la revisión sistemática de documentación relevante como la presentada por las entidades gubernamentales de varios países, en entidades como la CEPAL, Banco Mundial para obtener información sobre las microempresas sus características e importancia, adicional se buscó información sobre seguridad de la Información y la normativa existente en artículos científicos, libros y empresas de renombre como ESET, CheckPoint entre otras.

Estrategia de búsqueda: para caracterizar a las microempresas se buscó la definición en las entidades gubernamentales de rentas de cada país, adicional de información proporcionada por organismos internacionales como la CEPAL y el Banco Mundial para determinar la importancia que este tipo de empresas alcanzan dentro de la economía de los países, la búsqueda de los artículos se la realizo tanto en el idioma inglés como en el español empleando bases de datos en línea como "*scienceDirect*", "*scielo*" y Google Académico de artículos disponibles.

Criterios de inclusión y exclusión: en la revisión sistemática de todo tipo de documentos publicados por diferentes organismos internacionales, entidades gubernamentales y

artículos científicos, se aplicó como criterio de inclusión se empleó la revisión de todos los artículos relacionados a la seguridad de la información y las tecnologías en las pymes y MiPymes, mientras que el principal criterio de exclusión fue el que los documentos no incluyeran información relacionada al tema de la seguridad y la información en las microempresas.

3. ANÁLISIS DE RESULTADOS

Se ha puesto en evidencia la importancia de la seguridad de información en todas las organizaciones, ahora bien, como se ha presentado tanto las normativas como las herramientas desarrolladas para alcanzar este objetivo están enfocadas a empresas pequeñas, medianas y grandes, lo que deja al sector microempresarial rezagado, pese a que gran parte de las sociedades maneja información por medio de dispositivos electrónicos como computadoras, Smartphone, tabletas, memorias USB entre otras. Además de información que se produce en papel como informes, facturas, contratos, todo esto debe ser protegido, es aquí donde las tecnologías para proteger la información adquieren un papel relevante ya que reducir los riesgos que los avances tecnológicos traen consigo relacionados a la información requiere de una planificación e implementación de controles que permitan mantener los riesgos en niveles aceptables.

Los ataques a la seguridad de la información son cada día más sofisticados y para demostrar que es así sus blancos preferidos son las grandes empresas, un ejemplo de esto es el ocurrido en el 2017, cuando un virus informático denominado Wanna Cry afectó a más de 180 países, entre ellos China, España, Reino Unido, Italia, Estados Unidos, Rusia, Taiwan por mencionar a algunos, en la lista de afectados se encontraban hospitales, bancos, redes de transporte, las telecomunicaciones, empresas de toda clase (Herrero, 2017), este pese a que muchas de las compañías atacadas manejan estándares e inversiones relacionadas con la seguridad de la información fueron víctimas de estos ataques. Por ello, es necesario generar una conciencia en el sector microempresarial sobre la importancia en la implementación de protocolos que ayuden a proteger la información interna y externa.

En lo referente a las herramientas para proteger la información en el sector microempresarial debido a la creciente demanda y variedad de ataques por obtener información, es necesario desarrollar metodologías y herramientas que se ajusten a las características de éstas, con foco en el nivel de conocimiento de las personas asociadas a cada microempresa y a su capacidad económica, que representan uno de los principales limitantes para adoptar herramientas existentes, esto se puede evidenciar con el análisis de los requerimientos de la norma ISO/IEC y buscar aplicarlos en una microempresa, ya que muchas de las etapas resultan ser inaplicables a este tipo de empresas.

Los microempresarios además deben conocer qué herramientas son las que mejor se adaptan a sus necesidades y al sector, puesto que en ocasiones las limitantes se dan por la falta de conocimiento de quien lidera la empresa. Una alternativa a esta problemática puede ser la dotación de formación por parte del Estado, de los organismos seccionales y de las universidades tanto a los propietarios de estas empresas como a los mismos empleados, esto con el objetivo de proteger la información confidencial y de hacer buen uso de las tecnologías existentes, lo que repercute en mejoras de la productividad, más competitividad y claro está un manejo responsable de sus datos.

La aplicabilidad de las tecnologías para la seguridad de la información en el sector microempresarial presenta grandes retos asociados directamente a las características de este sector, las normas mencionadas los programas existentes requieren de un análisis previo del tipo de estrategia de seguridad a ser implementada debido al campo de acción de las empresas, es decir que depende de los productos o servicios que maneja, lo que implícitamente requiere involucrar terceras personas especialistas en el tema para que realicen este análisis y hacer una inversión tanto en hardware como en software para cubrir los resultados presentados

CONCLUSIONES

En la actualidad y debido a los flujos masivos de información tanto las personas como las empresas deben implementar técnicas y sistemas para proteger su información confidencial

de terceros, quienes al obtenerla pueden comercializarla y causar daños leves o graves tanto a los trabajadores de la organización como a sus clientes.

A pesar de existir modelos para análisis de riesgos, normativas programas enfocados a mantener la información protegida, todos estos elementos no son aplicables a las microempresas en Latinoamérica, debido especialmente a la capacidad económica de estas en lo referente a la adquisición de tecnología y las características propias de este tipo de empresas limitando sus posibilidades de conseguir y mantener clientes para mantenerse a flote en el mercado que es cada vez más competitivo.

Los datos de reportes de empresas dedicadas a la seguridad de la información muestran vulnerabilidad no solo del sector microempresarial poniendo en evidencia que las metodologías, técnicas, normativas, equipos y demás elementos desarrollados en la actualidad para proteger la información no están disponibles y al alcance de todos.

Las capacidades en manejo de tecnología que las personas asociadas no solo a las microempresas sino a las empresas en general aportan al desarrollo de cada una en todos los ámbitos de acción de estas, pero para el caso de las microempresas se convierte en una debilidad impidiendo que estas mantengan un desarrollo adecuado en especial en el campo de la seguridad de la información ya que son vulnerables ante cualquier tipo de ataque.

La adaptación de la tecnología va de la mano de la innovación, las microempresas al acceder a TIC especializadas a su entorno apoyarían al crecimiento sostenible de los países lo que se reflejaría directamente en el aporte que hacen a la economía.

REFERENCIAS BIBLIOGRÁFICAS

Alemán, F. (2006). Importancia de las MiPymes en las Aglomeraciones Empresariales. Una estrategia para el Desarrollo regional en Colombia. **Revista Facultad de Ciencias Económicas: Investigación y Reflexión***,* 14(1),173-186*.*

Ampuero, C. (2011**). Diseño de un Sistema de Gestión de Seguridad de Información para una compañía de Seguros.** (Tesis Doctoral), Pontificia Universidad Católica del Perú, Perú.

Andrés, A., Gómez, L. (2009*).* **Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes I Edición.** España: AENOR.

Andress, J. (2014). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Syngress.*

Benito, S. (2009). El papel de las microempresas en el desarrollo económico regional: las redes de cooperación empresarial en España. **REVESCO. Revista de Estudios Cooperativos,** (99), 31–59.

Bertolín, J.A. (2008). **Seguridad de la Información. Redes, informática y sistemas de información.** Madrid, Editorial Paraninfo.

Borja, J., Castells, M., Belil, M., & Benner, C. (1998). **Local y global: la gestión de las ciudades en la era de la información.** Taurus Madrid.

Cadenilla, J. F. (2005). **Tecnologías Empresariales procesos y paquetes tecnológicos.** Colombia, Convenio Andrés Bello.

Camacho, K. (2005). La brecha digital", en Ambrosi, A., Peugeot. V. & Pimienta, D. (coord.) **Palabras en Juego: Enfoques Multiculturales sobre las Sociedades de la Información**. C & F Éditions, pp. 66-71.

Casalet, M., & González, M.L. (2004). Las tecnologías de la información en las pequeñas y medianas empresas mexicanas. *Scripta Nova:* **Revista Electrónica de Geografía y Ciencias Sociales***.* 8, 21.

Castel, A., & Sanz, F. (2009). El papel de las tecnologías de la información y la comunicación en las empresas de economía social. **REVESCO: Revista de Estudios Cooperativos.** (97), 90-116.

Castells, M. (1997). **La era de la información. Volumen 1: La sociedad red**. Madrid, Alianza Editorial.

Castells, E. & Pasola, J.V. (2004). **Tecnología e innovación en la empresa**. Barcelona, Universitat Politécnica de Catalunya

CHECKPOINT. (2018). **Security Report Welcome to The Future of Cyber Security.** Retrived from: https://www.checkpoint.com/downloads/product-related/report/2018-security-report.pdf

CIS (s.f.). **Controls SME Companion Guide.** Retrieved from: https://www.cisecurity.org/white-papers/cis-controls-sme-guide/

Cornella, A. (2001). **Infonomía.com: la gestión inteligente de la información en las organizaciones.** Grupo Planeta (GBS).

CSO Computerworld (2018). **El mejor software de seguridad de 2018.** Retrieved from: https://cso.computerworld.es/tendencias/el-mejor-software-de-seguridad-de-2018

Davidsson, P., Lindmark, L., & Olofsson, C. (1994). **New firm formation and regional development in Sweden.** *Regional Studies*. 28(4), 395–410.

De Asís, A., Labie, M., & Mataix, C. (2000). **Las microempresas como agentes de desarrollo en el sur.** Madrid, CIDEAL.

De Sousa Santos, B. (2004). **Nuestra América: reinventando un paradigma.** En CECEÑA, A.E (dir). Chiapas 12, México: Universidad Nacional Autónoma de México, pp.31-70.

Devia, G.A.V., & Pardo, C.J. (2014). Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT. **Sistemas & Telemática**, 12(30), 35–48.

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

Durán, M. (2015). **Factores críticos en la adopción de las tecnologías de la información en microempresas del rubro talleres mecánicos de la comuna de Chillán.** (Tesis de pregrado), Chile, Universidad del Bío Bío.

Durán, P. B., Guadaño, J.F., & García, M. (2005). La creación de puestos de trabajo en el ámbito rural para su desarrollo: las organizaciones de participación agrarias. **Revista de Economía Pública, Social y Cooperativa,** (52), 335–360.

Ernst, & Young Global Limited. (2019). **¿La ciberseguridad es algo más que protección? Encuesta Global de Seguridad de la Información 2018-19** (Encuesta Global de Seguridad de la Información No. 21; p. 73). Retrieved from: https://americas.ey-vx.com/916/14087/landing-pages/ey-ec-giss-2019-26mar19-secured.pdf

Escorsa, P., Valls, J. (2003). **Tecnología e innovación en la empresa**. Barcelona, Universitat Politècnica de Catalunya.

García, C., Pereyra, A., & Cantó, A. (2018). **La profesionalización en la microempresa familiar: primeros pasos para alcanzarla.** *Revista del Centro de Graduados e Investigación*. Instituto Tecnológico de Mérida, 33, 67–73.

Garzás, J., Fernández, C., & Piattini, M. (2009). Una aplicación de la Norma ISO/IEC 15504 para la Evaluación por Niveles de Madurez de Pymes y Pequeños Equipos de Desarrollo. **REICIS. Revista Española de Innovación, Calidad e Ingeniería Del Software**, 5(2). pp. 88-98.

Goggin, G., & Hjorth, L. (2014). **The Routledge Companion to Mobile Media.** Abingdon, Rouledge.

Gómez, L., & Andrés, A. (2012). **Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes II Edición.** España, AENOR.

Gómez, R., Pérez, D. H., Donoso, Y., & Herrera, A. (2010). Metodología y gobierno de la gestión de riesgos de tecnologías de la información. **Revista de Ingeniería**, (31), 109–118.

González, T. (2005). Problemas en la definición de microempresa. **Revista Venezolana de Gerencia**, 10(31), 408–423.

Herrero, E. (2017). WannaCry pone en alerta al mundo: El ataque evidencia nuevamente la importancia de la seguridad TIC y la concienciación. **Red Seguridad: Revista Especializada En Seguridad Informática, Protección de Datos y Comunicaciones**, 77, 18–20.

Infante, R. (1999). **La calidad del empleo: la experiencia de los países latinoamericanos y de los Estados Unidos.** Oficina Internacional del Trabajo.

International Telecommunications Union (2017). ITC Facts & Figures 2017. Retrieved from: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf

Jeon, B. N., Han, K. S., & Lee, M. J. (2006). Determining factors for the adoption of e-business: the case of SMEs in Korea. **Applied Economics**, 38(16), 1905–1916.

Juniper Research. (2018). **Soluciones contra la vulnerabilidad empresarial latente.** 28. Retrieved from: http://revista.computerworld.com.ec/publication/db5b382a/mobile/

Kantis, H., Federico, J., & Menéndez, C. (2012). **Políticas de fomento al emprendimiento dinámico en América Latina: tendencias y desafíos.** CAF Documento de trabajo,

2012/09, Caracas: CAF. Retrieved from: http://scioteca.caf.com/handle/123456789/239

Laboratorio de Investigación ESET LATINOAMÉRICA. (2018). *ESET Security Report 2018*. Retrieved from: https://www.welivesecurity.com/wp-content/uploads/2018/06/ESET_security_report_LATAM2018.pdf

Ladino, M. I., Villa, P. A., & López, A. (2011). Fundamentos de iso 27001 y su aplicación en las empresas. **Scientia et Technica**, 17(47), pp. 334-339.

Luna, V. R., & Pezo, A. (2005). **Cultura de la innovación y la gestión tecnológica para el desarrollo de los pueblos.** Convenio Andrés Bello.

Mac-Clure, O. (2001). **Las microempresas: ¿una solución a los problemas de empleo?** Santiago, Chile: Ediciones Sur.

Mayorga T., García M., Duret J., Carrión J., & Yarad V. (2019). Historia de la normativa reguladora de la Protección de Datos de carácter personal en distintos países Latinoamericanos. **Dominio de Las Ciencias**, 5, 518–537.

Medina, M. A. (2017). **Incidencia de los cambios tecnológicos en el desempeño de microempresas de materiales de construcción de Durán, provincia del Guayas**. (Tesis de pregrado), Universidad Politécnica Salesiana.

Peirano, F., & Suárez, D. (2006). Las economías por informatización como una forma de captar el impacto de las TICs en el desempeño de las empresas. **Congreso Internacional de Información**, 9a. Ed. La Habana, 17–21.

Portantier, F. (2012). *Seguridad informática*, Usershop.

Porter, M. E., & Millar, V. E. (1985). **How information gives you competitive advantage.** Harvard Business Review Cambridge, MA.

Prensky, M. (2001). Digital natives, digital immigrants' part 1. **On the Horizon**, 9(5), pp.1–6.

Prieto, A., & Martínez, M. (2004). Sistemas de información en las organizaciones: Una alternativa para mejorar la productividad gerencial en las pequeñas y medianas empresas. **Revista de Ciencias Sociales (Ve),** 10(2), pp. 322-337.

Reynolds, P. D. (1997). New and Small Firms in Expanding Markets. **Small Business Economics,** 9(1), 79–84.

Robles, G. R., & Alcerreca, J. (2000). **Administración: un enfoque interdisciplinario**, México, Pearson Educación.

Saavedra, G., & Hernández. (2008). Caracterización e importancia de las MIPYMES en Latinoamérica: Un estudio comparativo. **Actualidad Contable Faces**, 11(17), 122–134.

Saavedra, M., & Tapia, B. (2013). El uso de las tecnologías de información y comunicación TIC en las micro, pequeñas y medianas empresas (MIPyME) industriales mexicanas. **Enl@ce**, 10(1), pp. 85-104.

Scheel, C. (2005). Creating economic value added through enabling technologies. **Journal of Integrated Design and Process Science,** 9(4), 41–59.

Stehr, N. (1994). **Sociedad del Conocimiento**. Reino Unido: British University.

Valencia, F. J., & 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. *RISTI* - **Revista Ibérica de Sistemas e Tecnologias de Informação**, (22), 73–88.

Van Stel, A. (2005). **Entrepreneurship and Economic Growth. Some empirical studies.** Netherlands: Tinbergen Institute.

WORLD BANK GROUP (2018). **International Development, Poverty, & Sustainability.** Retrieved from: http://www.worldbank.org/