PERCEPCIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LAS PEQUEÑAS Y MEDIANAS EMPRESAS EN SANTO DOMINGO

Carlos Roberto Sampedro Guamán[1]*, Silvio Amable Machuca Vivar[2]*, Diego Paúl Palma Rivera[3]*, Frankz Alberto Carrera Calderón[4]**,
*Universidad regional Autónoma de los Andes, Santo Domingo, Ecuador
**Universidad regional Autónoma de los Andes, Ambato, Ecuador

ABSTRACT
The applications of a computer and the way to program them have evolved in a very fast way in the world and consequently in Ecuador, advances that impact in the educational field. The teaching of algorithms is a basic subject of engineering careers in Systems and Software, requires students to develop logical reasoning, so that the initial dropout in this area is high. Students think that programming a computer is a trial-and-error process in a programming language. To avoid this, we must have specific elements and an appropriate methodology that motivate the students to visualize in a concrete way the results of the programs written by them. A diagnosis is presented on the development of the programming logic of the students of the systems and software careers of the face-to-face and blended modalities of the extension of the Autonomous Regional University of the Andes (UNIANDES) in Santo Domingo, the learning habits of the students, teaching methods and techniques of the teacher. To this end, a survey was applied to all students of Systems and Software careers, teachers were interviewed, a pilot survey of students from the Catholic University in Santo Domingo and participatory observation. Obtaining results that demonstrate the need to improve the teaching-learning strategy of algorithms to achieve a better development of programming logic, as a basis for a student of systems engineering and software.

KEYWORDS: Teaching programming, programming logic, programming language. Systems engineering, algorithms.

RESUMEN
Todas las Empresas e Instituciones públicas y privadas tienen un gran volumen de información confidencial sobre su estado financiero, productos, proveedores, clientes, y otros datos. Con el uso de sistema informático, esta información es reunida, tratada, almacenada y puesta a disposición de las personas que deseen revisarla de forma local o remota. De darse el caso de que la información caiga en manos no autorizadas, se pierda por daños en el computador o se contamine por malware, supone graves consecuencias, ya que la empresa perderá credibilidad de los clientes, perderá posibles negocios, se puede enfrentar a demandas e incluso puede causar la quiebra de la empresa. Ante este problema la respuesta es la Seguridad Informática, este campo ofrece muchas áreas de especialización una de ellas la seguridad de la información, que implica una inversión cuyos valores no son considerados en el presupuesto de las Pequeñas y Medianas Empresas (PyMES) en Santo Domingo de los Tsáchilas, ya sea por desconocimiento o por los altos costos, deciden entonces correr el riesgo con las consecuencias ya mencionadas. Fue necesario generar datos estadísticos en materia de seguridad de la información para que los empresarios hagan conciencia de los problemas a los que están expuestos y las medidas que deben implementar en medidas proactivas y reactivas para proteger uno de los activos más valiosos con los que cuenta las PyMES, la información tanto física como digital.

PALABRAS CLAVE: Seguridad, PyMES, Información, Seguridad de la Información, Seguridad informática.

1. INTRODUCCIÓN

El término seguridad informática, seguridad de tecnología de la información o ciberseguridad hace referencia a la protección de la infraestructura computacional o medio informático, mientras que la seguridad de la información es el conjunto de medidas preventivas y reactivas que las organizaciones deben generar y aplicar: políticas, normas, procedimientos, evaluar el riesgo, planes de contingencia, entre otras medidas, con el objetivo de mantener y asegurar la confidencialidad, integridad y disponibilidad de la información.
Para identificar el conjunto de acciones preventivas y correctivas aplicadas en las pequeñas y medianas empresas (PyMES) del Ecuador, provincia de Santo Domingo de los Tsáchilas, se obtuvo la base datos de las PYMES

[1] us.carlossampedro@uniandes.edu.ec
[2] us.silviomachuca@uniandes.edu.ec
[3] us.diegopalma@uniandes.edu.ec
[4] ua.frankzcarrera@uniandes.edu.ec

proporcionado por el Servicio de Rentas Internas (SRI) y el Ministerio de Industrias y productividad (MIPRO) en el 2018, de estas dos fuentes se determinó una población de 106 PyMES, realizando entrevistas a 99 gerentes que dieron la apertura para realizar el trabajo de investigación de campo y encuestas a los responsables del área informática o su equivalente.

Con el análisis e interpretación de los resultados, se identificó un alto porcentaje de PyMES que tiene establecidas acciones preventivas y correctivas, pero no las aplican, exponiendo su vulnerabilidad ante cualquier intento de alteración, pérdida o robo de información. Con ello se está emprendiendo acciones para concientizar a los directivos de las PyMES sobre la necesidad de invertir en seguridad de la información y las acciones necesarias en función del tipo de empresa y actividad.

2. SEGURIDAD DE LA INFORMACIÓN EN LAS PYMES

Las tendencias de la seguridad de la información se han convertido en la parte esencial de las empresas, convirtiéndose la información en el activo más relevante, el cual requiere la atención de todos los que tienen acceso a la misma.

El componente humano continúa siendo una pieza crítica en la gestión de seguridad de la información en las empresas, la gran mayoría de iniciativas recae en el ámbito estratégico y táctico (Deloitte, 2017).

"Una empresa es una unidad institucional considerada como productora de bienes y servicios." (SCN, 2008). Como agente económico con autonomía, puede adoptar decisiones financieras y de inversión con autoridad y responsabilidad para asignar recursos a la producción de bienes y servicios y puede realizar una o varias actividades productivas.

Las pequeñas y medianas empresas (PyMES) se caracterizan por ser administradas por una persona natural o jurídica y que realizan algún tipo de actividad dentro del sistema productivo del país, que comercialización bienes o servicios. Según: "La ley de Compañías mediante el artículo 428, en Ecuador, se establece que las PyMES pueden ser asociaciones de formalidades. A su vez exige que todas estas unidades de negocio deben cumplir con lo establecido en la Ley de Régimen Tributario Interno y RUC". (Superintendencia de Compañías, 2012):

Según el Instituto Nacional de Estadística y Censos (INEC), en su función de proveedor oficial de las estadísticas para Ecuador, pone a disposición de la ciudadanía los resultados de la Encuesta Estructural Empresarial (ENESEM) periodo de referencia 2016, la investigación es de tipo cuantitativo inferencial, los datos presentados corresponden a un marco censal aplicado para las empresas consideradas como grandes y un muestreo probabilístico para las empresas medianas, temática que se amplía en la metodología adjunta de la publicación, de esta manera clasificando a las PyMES.

Todo proceso mediante el cual se obtiene bienes y servicios que cubren las necesidades se denomina actividad económica y pueden describirse y clasificarse de acuerdo a sus características tales como: tipo de bienes o servicios producidos y de insumos utilizados o consumidos. (INEC, 2012).

Para la determinación del tamaño de empresa se consideró empresas: mediana (tipo A y tipo B) y grandes. Tomando como referencia la estratificación de la Comunidad Andina de Naciones (CAN) de la Decisión 702, establecida de la siguiente manera:

Tabla 1 Clasificación de las pymes

Clasificación de la empresa	Personal Ocupado	Ventas anuales (USD$)
Microempresa	1 – 9	Hasta 100.000
Pequeña empresa	10 – 49	100.001 – 1.000.000
Mediana empresa	50 – 199	1.000.001 - 5.000.000
Mediana empresa Tipo A	50 – 99	1.000.001 - 2.000.000
Mediana empresa Tipo B	100 – 199	2.000.001 - 5.000.000
Grande empresa	200 y más	5.000.001 y más

Fuente: INEC (2012): Instituto Nacional de Estadísticas y Censos

Seleccionar la forma de organización de una empresa es una de las decisiones más importantes que el propietario debe tomar. Las opciones disponibles dependen de las leyes y los impuestos establecidos por el país en el cual la empresa se encuentra operando. La forma de organización que la empresa elige influye directamente en las operaciones de la empresa, tales como impuestos, pasivos (deudas), sucesión (dentro del organigrama de la empresa) y en otras posibilidades financieras, de esta manera la selección de la forma organizacional de una empresa es de vital importancia para el funcionamiento efectivo de las PyMES. (Brown, 2009).

La forma de organización de las empresas debe estar cubierta por un sistema de seguridad informática, de esta manera se salvaguarda el acceso a la información o modificación de la misma, permitiendo que solo personas autorizadas puedan plegarse. (Costas Santos, 2011).
Los principales objetivos de la seguridad informática en las empresas por tanto son:

- ✓ Detectar los posibles problemas y amenazas a la seguridad, minimizando y gestionando los riesgos.
- ✓ Garantizar la adecuada utilización de los recursos y de las aplicaciones de los sistemas.
- ✓ Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
- ✓ Cumplir con el marco legal y con los requisitos a nivel organizativo.

Es menester además la fiabilidad en el comportamiento del sistema de seguridad, lo cual conlleva a tener en cuenta tres aspectos: la confidencialidad, que no es más que la privacidad de la información del sistema, así, solo puede ser leída por quien se encuentre acreditado a hacerlo; la integridad, que permite corroborar que no ha existido alteración en la documentación empresarial; finalmente, la disponibilidad, es decir, la facultad de hacer que la información sea accesible a los usuarios en el momento que sea notoria su necesidad, restando impedimentos por bloqueos o pérdidas. (Costas Santos, 2011).
Se puede asegurar, que la información es un activo con valor para el curso de las actividades empresariales, en este caso, estaríamos hablando de seguridad de la información, es decir, la protección de la integridad, disponibilidad y confidencialidad de la información, dependiendo de lo demandado para cumplir las metas de la empresa. (Miguel Pérez, 2015).
Para la ISO 27001, la seguridad de la información es la conservación de la confidencialidad, la integridad y la disponibilidad, al igual que de los sistemas necesarios para su tratamiento dentro de la empresa. La forma de avalar la seguridad de la información se realiza mediante un procedimiento sistemático registrado e identificado por la organización desde una perspectiva de contingencia empresarial, proceso que constituye un SGSI. (Portal ISO 27001, 2012).
Las definiciones de seguridad informática y seguridad de la información pueden confundirse como similares, sin embargo, no lo son. La seguridad de la información promete un proyecto de valoración de amenazas con el fin de reducir riesgos en base a normas correctas, en tanto, la seguridad informática es un conjunto de técnicas que permiten proteger la información, estas pueden ser antivirus o firewalls. Hablamos de un continente y su contenido. Por esto, David Jaramillo, gerente de Icontec, empresa dedicada a las capacitaciones, propone que lo correcto es hablar de la seguridad de la información, siendo este, un bosquejo que incluye todos los sistemas de seguridad y estrategias de solución para proteger los datos (seguridad informática): (Computerworld Powered by Ekos, 2015).
Ahora, al remarcar la gestión de la seguridad de la información (ISO 27001), la intención es detectar los puntos débiles que puedan acarrear pérdidas de información, sean estos por problemas de los sistemas informáticos, eliminación de archivos o desfases cibernéticos. Añadiendo, además, figuraciones de ataques informáticos verificando la seguridad del sistema. Se provee una completa metodología de labor que permite identificar, analizar y administrar los riesgos, valorar los posibles tratos de riesgos y encaminar planes de tratamientos de estos, determinar medidas e indicadores de la eficacia de los controles, y demás. (Tundidor Días, 2016).
El componente humano es un pilar crítico en la determinación de la seguridad de la información, esto es medido casi por el 50% de las empresas, cuya principal idea para el 2018 es la capacitación y la sensibilización en seguridad de la información, lo que recae en el campo de estrategias y tácticas nuevas como principales tendencias.
Por ende, es menester en las iniciativas de la seguridad de la información, es el factor humano. Aunque, se presentan otros ámbitos que tienen gran afluencia para el próximo año. Las organizaciones reconocen la importancia de indicadores que permitan verificar el cumplimiento de las metas planteadas, tal como sostener un enfoque proactivo ante ataques por medio del seguimiento de indicios de amenazas tanto internas como externas. (Deloitte, 2017).
Los sistemas de información son conjuntos de recursos interrelacionados (pueden ser medios técnicos, el factor humano y los procesos) que promueve la captura de datos, almacenarlos y convertirlos para luego expender lo obtenido. (Riascos Erazo, 2008).
Es responsabilidad de los actores de una empresa, mantener la confidencialidad, integridad y disponibilidad de la información, ya que estos procesos son importantes para la organización de la entidad.
La seguridad de la información es una prioridad en esta era digital. Así mismo, es relevante concienciar a los involucrados en el uso correcto de este sistema integral, para lo cual se debe afianzar el conocimiento en los siguientes aspectos:

- ✓ Entender los tipos de riesgos de seguridad de los recursos informáticos y su implicación en el desempeño del centro.
- ✓ Lineamientos para realizar los respaldos de información.
- ✓ Buenas prácticas en el manejo y conservación de los soportes informáticos (dispositivos USB, discos compactos, DVD, documentación física, archivos, etc.)
- ✓ Buen manejo del correo electrónico.
- ✓ Normas para el intercambio de información.
- ✓ Principios de comportamiento ético profesional que guíen a los empleados en sus decisiones en el manejo y utilización de los recursos informáticos. (Policia del Ecuador, 2018).

La seguridad de la información en una empresa debe confrontar cualquier fallo de la seguridad, sin división alguna de los departamentos, de esta manera se evita que existan áreas desprotegidas. Así, un Sistema de gestión de Seguridad de la Información es una estructura organizativa, técnica y de procedimientos cuyo fin es conseguir seguridad de la información mediante:

- ✓ Análisis de la situación y planificación.
- ✓ Aplicación de controles.
- ✓ Revisión de su funcionamiento.
- ✓ Aplicación de mejoras y correcciones. (Miguel Pérez, 2015).

En Congreso Iberoamericano se pronunció la importancia de la seguridad de la información, en el mismo se destacó una de las políticas que consiste en que los representantes de empresas públicas y privadas tomen conciencia de lo importante que es la seguridad de la información para potenciar tales.
Con el avance de las TICs, los gobiernos prestan mayor atención a la protección de sus activos de información, para que exista mayor confianza en la ciudadanía minimizando riesgos informáticos. De esta manera, importante es que existan políticas de seguridad generales que provean control y eficacia en la administración pública, áreas de negocio y comercio electrónico. (Ministerio de Telecomunicaciones, 2017).
La información se debe proteger contra algunas amenazas, las mismas pueden ser: alteraciones eléctricas (picos o cortes de suministro), catástrofes (fuego, inundaciones, terremotos), virus informáticos (spywares, troyanos), vandalismo, robo, error humano (usuarios, operadores, programadores), actos intencionados de daños, espionaje, filtraciones de información los cuales puedes ser internos (personal propio o subcontratados) o externos (piratas informáticos, hackers): (Miguel Pérez, 2015).
Explicando de mejor manera, los delitos informáticos son conductas antijurídicas, antiéticas o no autorizadas en contra del proceso de la trasmisión de la información. La informática y las redes tienen características idóneas para participación de delitos. Es más, se puede asegurar que son utilizados por parte de organizaciones de crimen organizado internacional para concurrir en estafas electrónicas intercambiando información a través de Internet. (Gómez Vieites, 2013).
Entre los tipos de ataques informáticos podemos mencionar a los ataques activos, que provocan modificaciones en la información; y los ataques pasivos limitan el uso o acceso de la información guardada o trasmitida. (Álvaro Gómez, 2011)**.**
Con el objetivo de crear buenas prácticas de seguridad de la información además de salvaguardarla, cualquier organización con o sin fines de lucro, públicos o privados, grande o pequeña, puede incluir la norma ISO/IEC 27001, recalcando nuevamente que de esta manera se garantiza la confidencialidad, integridad y disponibilidad de la información. (Servicio de Acreditación Ecuatoriano, 2018).
Según el Instituto Nacional de Ciberseguridad de España, hay cuatro tipos de ataques cibernéticos que perjudican a las empresas, gobiernos y ciudadanos, estos son: el robo de dinero y extorsión a través del internet, filtraciones o fuga de datos y espionaje, ataques a servicios importantes (sensibles y/o masivos) y explotación de la vulnerabilidad de plataformas, sistemas y protocolos ampliamente utilizados.
La norma ISO 17799 es un conjunto de controles para mejorar la práctica de la seguridad de la información y cumple con todos los aspectos sobre la misma. (Diario El Universo, 2018).
Además, esta, es una norma internacional que provee sugerencias a los responsables de iniciar y mantener la seguridad de la organización. Asimismo., conceptualiza a la información como un activo importante para la empresa, por ende, requiere una protección adecuada para mermar daños en la organización y mejorar las inversiones y las oportunidades de comercio.

Mediante la presente investigación se pueden examinar los resultados del nivel de seguridad de la información de las pequeñas y medianas empresas de la Provincia de Santo Domingo de los Tsáchilas, específicamente en los cantones Santo Domingo y la Concordia.
Entonces, el objetivo general es valorar el nivel cultural de las pequeñas y medianas empresas en la Provincia de Santo Domingo de los Tsáchilas con respecto a la materia de seguridad de la información, para plantear estrategias basadas en normas internacionales.

3. METODOLOGÍA

MÉTODOS

Los métodos de trabajo contemplan la revisión bibliográfica en los temas referentes a la seguridad de la información en las pequeñas y medianas empresas en la Provincia de Santo Domingo de los Tsáchilas.
La investigación de campo con las personas encargadas de las pequeñas y medianas empresas permitió conocer en forma directa la problemática que existe en la seguridad de la información y la documentación existente en cada empresa.
Las características de esta investigación son las siguientes:

- ✓ Alcance exploratorio: presenta informe estadístico del nivel cultural en materia de seguridad de la información.
- ✓ Alcance descriptivo: describe la realidad de las medidas proactivas y reactivas para la seguridad de la información en las PyMES.
- ✓ Con una modalidad cuali-cuantitativa se presentan valores cualitativos y cuantitativos que resumen los principios de la calidad de la información en las PyMES.

Los métodos y técnicas del nivel empírico de los conocimientos empleados fueron los siguientes:

- ✓ Observación científica: Indica cuales son los procedimientos empleados con respecto a la seguridad de la información en las PyMES.
- ✓ Para desarrollar esta investigación se encuestó a una muestra de las pequeñas y medianas empresas ubicadas en Santo Domingo y La Concordia, según los datos proporcionados por el Servicio de Rentas Internas.

POBLACIÓN

Siendo el conjunto de todos los elementos a los cuales se refiere la investigación, existiendo 106 empresas entre pequeñas y medianas cuyos datos fueron proporcionados por el Servicio de Rentas Internas y el Ministerio de Industrias y productividad (MIPRO) en su base de datos del 2018.

Tabla 2. Población de PyMES en Santo Domingo

Empresas	Nº
Pequeña empresa	73
Mediana empresa	33
Total	**106**

Fuente: Servicio de Rentas Internas (SRI) y el Ministerio de Industrias y productividad (MIPRO)

Muestra
Nivel de confianza: 98%

Tamaño de la muestra: $\frac{N*(a_c*0{,}5)^2}{1+\left(e^2*(N-1)\right)}$ = 99 empresas.

Muestreo

Muestreo no probabilístico por conveniencia

Permite seleccionar aquellos empresarios que permiten el acceso a la información y que acepten ser incluidos. Esto, fundamentado en la conveniente accesibilidad y proximidad de los sujetos para el investigador. (Gómez Armijos, y otros, 2017):

4. ANÁLISIS DE RESULTADOS

Análisis de instrumentos escritos, Alfa de Cronbach.
Para el cálculo de Alfa de Cronbach se utilizaron las siguientes variantes:

Tabla 3. Cálculo de Alfa de Cronbach por items

	Items										
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**suma**
Si	66	55	22	33	33	33	33	0	88	88	451
No	0	33	11	0	11	11	*66*	0	0	0	132
Parcialmente	22	11	66	66	44	55	0	55	0	0	319
Desconoce	11	0	0	0	11	0	0	44	11	11	88
Varianza	**627.7**	**446.2**	**627.7**	**748.7**	**204.2**	**446.2**	**748.7**	**627.7**	**1353.7**	**1353.7**	
$\sum S\,i^2$	**7184.5**									S_{T^2}	**21326.25**

Elaborado por: Autores

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\sum S\,i^2}{S_{T^2}}\right]$$

Dónde:
K = El número de ítems: (10)
$\sum S\,i^2$ = Sumatoria de las Varianzas de los Items: (7184.5)
S_{T^2} = La Varianza de la suma de los Items: (21326.25)
α = Coeficiente de Alfa de Cronbach: (0.74)

El 0,74 es un valor aceptable en el análisis de confiabilidad de las respuestas obtenidas en los 10 ítems de opción múltiple. Este valor se lo obtuvo utilizando el MS Excel 2013 a partir de la fórmula equivalente del coeficiente α de Lord y Novick y los datos de la tabla en la cual, las filas representan las opciones de respuesta y las columnas las preguntas con el total de respuestas para cada opción.

Encuesta realizada a las pequeñas y medianas empresas de Santo Domingo.

Los diez ítems evalúan las políticas en materia de seguridad de la información (ítems 1 y 2), confidencialidad de la información (ítems 3, 4, 5 y 6), integridad de la información (ítem 7 y 9) y disponibilidad de la información (ítems 8 y 10): Para su análisis se utilizó una matriz de correlación en entre ítems utilizando la herramientas de análisis del MS Excel 2013.
Para lo cual se partió de la matriz de datos, tabla Nro 4.

Tabla 4. Tabla de datos de la encuestas a los responsables del área informática de las PyMES.

	CRITERIOS / VARIABLES									
	POLÍTICAS		**CONFIDENCIALIDAD**				**INTEGRIDAD**		**DISPONIBILIDAD**	
Respuestas	**M_SI**	**Ev_R**	**P_Di**	***Re_A***	***A_cl***	***Cap***	***Pr_M***	***C-Mi***	***Fa_A***	***ResP***
Si	66	55	22	33	33	33	33	88	0	88
No	0	33	11	0	11	11	66	0	0	0
Parcialmente	22	11	66	66	44	55	0	0	55	0
Desconoce	11	0	0	0	11	0	0	11	44	11

Ítems	1	2	3	4	5	6	7	9	8	10

Fuente: Encuesta a responsables del área informática de las PyMES.

Obteniendo la matriz de correlación mostrada en la tabla 5.

Tabla 5. Matriz de correlación por criterios de seguridad de la información

	POLÍTICAS		**CONFIDENCIALIDAD**				**INTEGRIDAD**		**DISPONIBILIDAD**	
	M_SI	**Ev_R**	**P_Di**	***Re_A***	***A_cl***	***Cap***	***Pr_M***	***C-Mi***	***Fa_A***	***ResP***
M_SI - Manual de Seguridad	1									
Ev_R - Evaluación de riesgo	0,67	1								
P_Di - Prevenir Divulgación	0,18	-0,1	1							
Re_A - Restricción de acceso	0,43	0,04	0,96	1						
A_cl - Asignar Claves	0,57	0,18	0,91	0,99	1					
Cap - Capacitación	0,44	0,19	0,96	0,98	0,98	1				
Pr_M - Prevenir modificaciones	-0,1	0,67	-0,4	-0,5	-0,4	-0,3	1			
C-Mi - Control de modificaciones	0,94	0,77	-0,1	0,11	0,27	0,15	0,1127	1		
Fa_A - Fallas de acceso	-0,3	-0,9	0,47	0,43	0,32	0,27	-0,894	-0,533	1	
ResP _ Respaldos	0,94	0,77	-0,1	0,11	0,27	0,15	0,1127	1	-0,5333	1

Elaborado por: Autores.

De acuerdo al criterio de que cuando la correlación es positiva, esto indica que su proyección de la regresión lineal va a tender a crecer conjuntamente con la contra variable. Cuando la correlación es negativa, indica que su proyección de la regresión lineal va a tender a decrecer conjuntamente con la contra variable, se puede concluir que:

1. Las variables que corresponden a las políticas, manual de seguridad y evaluación de riesgo están relacionadas, en porcentaje más del 50% cuenta con un manual de seguridad de la información y ha hecho una evaluación de riesgo.
2. En cuanto la confidencialidad las variables de prevención de divulgación, restricción de acceso, asignación de contraseñas y capacitación tienen correlación positiva, en términos de porcentaje, más de la mitas de las PyMES cumple parcialmente con estas variables.
3. Para el control de la integridad de la información es necesaria la prevención y control de los cambios o modificaciones que se haga, la correlación sigue siendo positiva, pero las respuestas indican que las PyMES no realización acciones encaminadas a la prevención y si realizan el control de cambios en la información.
4. Para garantizar la disponibilidad de la información se consideró las fallas presentadas durante el acceso a la información y la existencia de respaldo de la información, dando como resultado una correlación negativa, debido a que no han registrado fallas en la disponibilidad de la información y aunque realizan copias de respaldo no las han necesitado.

Los porcentajes obtenidos en la encuesta a los responsables del área informática coinciden con las respuestas obtenidas en las entrevistas a los gerentes de las PyMES.

5. DISCUSIÓN.

- La mayoría de las PyMES cuentan con documentos que determinan las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales para precautelar la seguridad de la información, lo han socializado superficialmente pero se requiere de un seguimiento al cumplimiento de las políticas establecidas.

- Los empresarios están conscientes de los riesgos a los que está expuesta la información de su empresa, pero prefieren asumir el riesgo en el afán de minimizar costos y muchas veces toman medidas luego de ocurrido un incidente y cuyo costo es mucho más alto que la inversión inicial.
- La confidencialidad, integridad y disponibilidad no son medidas que se toman en cuenta para la protección de la información sea esta de forma total o parcial.
- Las PyMES plantean acciones preventivas pero un buen porcentaje requiere mejorar sus medidas reactivas y que sean basadas a un estándar como ISO o similar.
- A medida que las PyMES denotan un crecimiento o implementan Sistemas Informáticos como estrategia competitiva quedan más expuestas a los ciberataques.

RECEIVED: OCTOBER, 2018.
REVISED: FEBRUARY, 2019.

REFERENCIAS

[1] ÁLVARO GÓMEZ, V. (2011): **Gestión de Incidentesde Seguridad Informática**. StarBook Madrid.
[2] BROWN, C. J. (2009): **Administración de las Pequeñas y Medianas Empresas**. Trillas, México.
[3] COMPUTERWORLD POWERED BY EKOS. (2015): **Computerworld Powered by Ekos**. Obtenido de http://computerworld.com.ec.
[4] COSTAS SANTOS, J. (2011): **Seguridad y Alta Disponibilidad**. Ra-Ma, Madrid.
[5] DELOITTE. (2017): **Seguridad de la Información**. Obtenido de https://www2.deloitte.com/ec/es/pages/deloitte-analytics/articles/seguridad-de-la-informacion.html
[6] DIARIO EL UNIVERSO. (08 de 05 de 2018): **La seguridad de la tecnología de la información es clave para un negocio exitoso**. Obtenido de https://www.eluniverso.com/tendencias/2018/05/08/nota/6749997/seguridad-tecnologia-informacion-es-clave-negocio-exitoso
[7] GÓMEZ VIEITES, Ä. (2013): **Auditoría de Seguridad Informática. Bogotá: Ediciones de la U.**
[8] **INEC. (2012): Instituto Nacional de Estadísticas y Censos.** Obtenido de http://www.ecuadorencifras.gob.ec
[9] MIGUEL PÉREZ, J. C. (2015): **Protección de Datos y Seguridad de la Información**. Ra-Ma, Madrid:.
[10] MINISTERIO DE TELECOMUNICACIONES. (14 de 01 de 2017): **Ministeriode Telecomunicaciones y de la Sociedad de la Información**. Obtenido de www.telecomunicaciones.gob.ec/la-importancia-de-la-seguridad-de-la-informacion-se-destaco-en-congreso-iberoamericano/
[11] POLICIA DEL ECUADOR. (18 de 01 de 2018): **Policia Nacional del Ecuador**. Obtenido de http://www.policiaecuador.gob.ec/la-responsabilidad-en-la-seguridad-de-la-informacion/
[12] PORTAL ISO 27001. (2012): **El Portal de ISO 27001**. Obtenido de http://www.iso27000.es
[13] RIASCOS ERAZO, S. C. (2008): Modelo para la evaluación de la efectividad de la tecnología informática. En **Ingeniería E Investigación**, 159.
[14] SCN. (2008): **Sistema de Cuentas Nacionales 2008**. Obtenido de https://unstats.un.org/unsd/nationalaccount/docs/SNA2008Spanish.pdf
[15] SERVICIO DE ACREDITACIÓN ECUATORIANO. (2018): **Servicio de Acreditación Ecuatoriano**. Obtenido de http://www.acreditacion.gob.ec/seguridad-de-la-informacion/
[16] TUNDIDOR DÍAS, A. (2016): **Cómo Innovar en las Pymes**. Alfaomega Grupo Editor, México:.
[17] VILLALÓN HUERTA, A. (2004): **El Sistema de Gestión de Seguridad de la Información**. Nau Llibres, Valencia.