Universidad de Buenos Aires – Facultad de Ciencias Económicas
Instituto de Investigaciones en Administración, Contabilidad y Métodos Cuantitativos para la Gestión
Sección de Investigaciones Contables

Contabilidad y Auditoría

ISSN 1515-2340 (Impreso) ISSN 1852-446X (En Línea) ISSN 1851-9202 (Vía Mail)
Nº 53 – año 27

LA CIBERSEGURIDAD Y SU CONCEPCIÓN EN LAS PYMES DE CUENCA, ECUADOR

Autores
MARCO LEONARDO PERALTA ZUÑIGA
marco.peralta2901@ucuenca.edu.ec

DANIELA NICOLE AGUILAR VALAREZO

Universidad de Cuenca

CPA. Marco Leonardo Peralta Zúñiga
- Contador Público Auditor.
- Técnico Docente de la Universidad de Cuenca
- Contador del Fondo Previsional Cerrado de los Servidores de la Universidad de Cuenca.
- Maestría en Contabilidad y Auditoría (II Cohorte)

Srta. Daniela Nicole Aguilar Valarezo
- Contadora Bachiller.
- Estudiante de Pregrado de la Universidad de Cuenca de la Carrera de Contabilidad y Auditoría.
- Tutora de las asignaturas: Contabilidad, Finanzas y Economía
- Condecorada por Excelencia Académica en el año 2019 y 2020 en la Universidad de Cuenca

Publicación:
- Presentada el 22/02/2021
- Aprobada el 04/06/ 2021
- Publicada en Junio del 2021

ISSN 1515-2340 (Impreso) ISSN 1852-446X (En Línea) ISSN 1851-9202 (Vía Mail).

LA CIBERSEGURIDAD Y SU CONCEPCIÓN EN LAS PYMES DE CUENCA, ECUADOR

CYBERSECURITY AND ITS CONCEPTION IN SMES IN CUENCA, ECUADOR

SUMARIO

Palabras clave:
Política de Inversión - Tecnología de la Información - Cultura Corporativa

Keywords:
Investment Policy - Information Technology - Corporate Culture

Resumen
El presente artículo tiene como finalidad determinar la concepción de las PYMES cuencanas (Ecuador) respecto a la inversión en ciberseguridad, para ello se han establecido las siguientes variables de análisis: Costo-Beneficio, empleados, filosofía empresarial, capacitación-mantenimiento y capacidad de reacción.
Los resultados señalan que existe una significativa relación entre la variable filosofía empresarial con el resto de las variables de forma inversa, es decir, cuando un gerente adopta medidas menos tradicionales esto involucraría considerar invertir mayores recursos en ciberseguridad, contando con empleados capacitados y de esta manera las empresas podrían tener mayor capacidad de reacción frente a cambios.

Abstract
The purpose of this article is to determine the conception of the Cuenca SMEs (Ecuador) regarding investment in cybersecurity, for these the following analysis variables have been established: Cost-Benefit, employees, business philosophy, training-maintenance and reaction capacity.
The results indicate that there is a significant relationship between the business philosophy variable and the rest of the variables inversely, that is, when a manager adopts less

traditional measures, this would involve considering investing more resources in cybersecurity, counting on trained employees and in this way, companies could be more responsive to changes.

1. Introducción

En los últimos años se han dado constantes cambios en el ámbito tecnológico, originándose innovaciones en: comunicaciones, redes y sistemas de información creándose así el ciberespacio; en él se puede encontrar algunos beneficios que ayudan a las empresas en los procesos de negocio y el procesamiento de información; fomentando eficiencia, eficacia y rapidez en las respuestas a los cambios que se producen en el entorno, es decir se pretende utilizar de mejor manera los activos para incrementar los niveles de producción y minimizar los costos.

Pero a medida que los sistemas de información se han desarrollado también la delincuencia lo ha hecho, en la actualidad se cuentan con sofisticados métodos para delinquir como los ataques cibernéticos que crecen a ritmos exponenciales, estos consisten en aprovechar las vulnerabilidades de los sistemas de cualquier tipo de organización sea pública o privada para robar información y venderla en el mercado negro o como medio de extorsión para conseguir sumas de dinero elevadas, convirtiéndose así en la nueva modalidad de atraco y en el negocio más rentable de la última década.

La Gerencia al momento de gestionar sus riesgos, también tiene que enfocarse en el tema informático, pues debe ser consciente del riesgo tecnológico, amenazas cibernéticas y deficiencias de los sistemas, ya que estos elementos también ponen en peligro el cumplimiento de los objetivos organizacionales y, por ende, la continuidad del negocio.

Además, los auditores deberán especializarse en técnicas forenses que les permita identificar de mejor manera el riesgo de auditoría, documentar oportunamente la evidencia y dictaminar con mayor seguridad.

2. Estado del Arte

Todo negocio con la finalidad de mejorar continuamente y con la visión de desarrollar un mejor control interno para su organización, que se encaminen a lograr los objetivos organizacionales, se apoyan en sistemas informáticos que integren las diferentes áreas que conforman la empresa. Su aplicación supone una erogación monetaria considerable de acuerdo a las necesidades empresariales, existen algunos sistemas que arrojan información relevante sobre gestión de riesgos, tales como: puntos críticos, niveles de tolerancia, establecimiento del riesgo operativo; y, con ello prevenir, detectar y dar respuesta a puntos susceptibles de fraude dentro de la organización. (Alzamora, 2013).

Según (Acosta *et al*., 2020), los actos ilícitos informáticos cada día van incrementándose, atentando contra la privacidad de la información de las personas o entidades, muchas veces se debe al descuido en cuanto a la protección de los datos, por lo que es muy importante instaurar un sistema de seguridad que permitan el resguardo de la información, finalmente con el análisis realizado en la legislación de los diferentes países concluyen que a pesar de las leyes que tienen, existen vacíos legales, que no permiten atribuirles responsabilidades judiciales directas a los infractores cibernéticos.

Una de las herramientas para precautelar la información de la organización es la inversión en ciberseguridad y con ello evitar los fraudes usando la tecnología; es así que, (Baez *et al.*, 2017), han analizado la interrelación de la Ciencia, Tecnología, Sociedad, con la inversión en ciberseguridad en aspectos claves, como: la

aplicación de sistemas contables, el papel del internet y las redes sociales con los fraudes que pueden ocasionarse usando como herramienta la tecnología dentro de las empresas; enfocando a la ciberseguridad como una herramienta factual y formal, en la que factual se centra en la investigación del hecho económico y la formal en el análisis de estructura lógica del pensamiento al fraude. De igual manera, los riesgos de ciberseguridad se pueden prevenir desde la auditoría forense relacionada íntimamente con la gestión del conocimiento o talento humano, según (Caamaño y Gil, 2020), estos pueden ser el fraude financiero, delitos informáticos, actos de corrupción y de seguridad a los que están expuestos las organizaciones en la actualidad. Este análisis empieza con la identificación del riesgo y de los responsables de la información, sigue con la medición de las causas y posibles consecuencias, evaluar la probabilidad e impacto de ocurrencia, definir los controles al riesgo inherente identificado, establecer medidas de prevención y control y por último el seguimiento con la evaluación de las medidas adoptadas, esto permitirá una efectiva gestión integral de la seguridad informática con el uso de las TIC. Anchundia (2017), señala que la tecnología es de suma importancia para las empresas y sus beneficios son grandes, pero también conlleva a problemas de seguridad y de privacidad de datos.

Según (Gavilanes y Proaño, 2018), establecen que la seguridad informática implica también conocer cómo actuar frente a un evento donde se ha vulnerado dicha seguridad y cómo tratar la evidencia identificada, por lo cual los autores entregan una solución, basada en normas internacionales y respetando la legalidad ecuatoriana vigente. Cualquier ataque informático será analizado por los peritos autorizados y siguiendo todos los procedimientos del caso. Durante todo el proceso se debe garantizar la integridad, confiabilidad de los datos. Finalmente, la guía propuesta puede ayudar al intercambio de evidencia digital entre distintas

jurisdicciones permitiendo procesar evidencia digital válida en casos de litigio o controversia.

También se manifiesta la importancia de un sistema de seguridad informática para proteger sus recursos financieros, sistemas, bienes entre otros (Gil y Gil, 2017); por ello, sería ideal desarrollar un modelo de simulación que permita evaluar el nivel óptimo de seguridad que deben tener las organizaciones. Una técnica para analizar el comportamiento de los sistemas en el corto, mediano y largo plazo. Concluyendo que, si las empresas no cuentan con un plan efectivo, no se alcanzaran los niveles de seguridad óptimos.

La ciberseguridad afecta al bienestar digital de la sociedad, de las organizaciones y de los países accediendo a datos privados a nivel personal como organizacional. Los sistemas informáticos están sometidos a potenciales amenazas de seguridad de diversa índole, originadas tanto dentro de la propia organización, como desde fuera, procedentes de una amplia variedad de fuentes. Los autores identificaron tres fases para el diseño de la guía, siendo estos: auditoría interna en los procesos de las áreas de Redes, Desarrollo de Software y Documentación; Análisis de Vulnerabilidades e Identificación de Riesgos. Esta guía permitiría a las organizaciones llevar un mejor análisis y estudio de vulnerabilidades de forma ordenada estipulando que hacer y cómo hacer ayudando a proteger sus activos digitales y plantear políticas para actuar y estar preparados ante los posibles ciberataques (Morales Carrillo *et al.*, 2020).

2.1 La ciberseguridad en un Contexto Internacional

En España, según (Ribagorda Garnacho, 2018) a mediados del 2017 las PYMES presentaban datos alarmantes con respecto a ciberseguridad, pues el 25% de ellas no disponían de programas

antivirus, el 50% no actualizaban sus sistemas operativos, el 47% no utilizaban contraseñas de acceso para los diferentes módulos de los sistemas informáticos y solamente la tercera parte de estas empresas respaldaban su información mediante copias de seguridad. Adicionalmente, (Ribagorda Garnacho, 2018) encontró evidencia que las PYMES españolas conceptualizan a la ciberseguridad en un gasto antes que una inversión, en este sentido estas compañías no hacen un adecuado análisis del costo beneficio lo que aumenta la confianza de los ciberdelicuentes para cometer sus actos ilícitos. En el trabajo también se obtuvo una estimación del 12.8% en el crecimiento de las inversiones por ciberseguridad.

Además, (Ruiz y Hurtado, 2020) aporta en el sentido literario de la ciberseguridad e indica que de nada sirven los modelos sofisticados si no aportan valor, ya que el modelo de gestión de la seguridad debe enfocarse en una gestión efectiva y eficiente de la información, para que los efectos de cada uno de los dominios de seguridad no solo suman sino que multiplican la operatividad de la empresa, constituyéndose las inversiones en ciberseguridad, en una vía alterna para salir de una crisis que tiene un tinte recesivo con un escenario de economías en contracción.

Por el contrario, (Hernández y Marino Medina, 2020) recalcan que el entorno actual, posiblemente se extienda más allá de las cuarentenas y es necesario replantearse los planes de continuidad de las empresas, que a su vez van de la mano con las inversiones en ciberseguridad, en su investigación aplicada a empresas financieras de España se llegó a la conclusión que es importante incrementar los servicios externalizados y controlar mediante gestión de riesgos tecnológicos end to end.

Adicionalmente, (Lerma Gangoiti, 2020) establece que la certificación ISO/IEC 27001:2013 (Sistemas de Gestión), no es un

mecanismo apropiado para establecer una relación de eficiencia entre el valor de lo protegido y los elementos de salvaguarda implementados por la empresa, se afirma que la certificación solo se basa en documentos que no justifican la aplicación de controles sin un análisis de la situación real, para implementar un sistema de gestión se debe partir del estudio exhaustivo de las empresas con la finalidad de identificar debilidades y aplicar correctivos necesarios.

La virtualización debe trascender límites y alcanzar entornos industriales, pues se reducirán considerablemente costos de producción como: energía, utilización de espacio físico, entre otros (Sucunza, 2020). De esta manera, se pasa de costos fijos a costos variables haciendo que se reduzcan considerablemente costos de corto plazo, alcanzando eficiencia de recursos, esto será eficiente siempre y cuando se apliquen controles oportunos sobre todo en inversiones en ciberseguridad.

Por otra parte, (Martínez, 2020) indica que el factor humano no debe temer el desarrollo de la tecnología y la automatización de procesos, por el contrario, se debería considerar como la herramienta y medio que permitirá perfeccionar el trabajo sin estresarse. La automatización jamás podrá sustituir la experiencia y la intuición humana.

En este sentido, (SIC, 2020) afirma en su publicación que el 84% de los CEOs españoles consideran complejo gestionar adecuadamente un entorno de seguridad compuesto por múltiples proveedores. No obstante, el 80% de ellos, han visto como alternativas viables para solucionar parcialmente estos problemas, apostar por automatización de procesos y por soluciones de protección en la nube, además de establecer políticas de colaboración entre equipos de red y seguridad. En definitiva, es indispensable invertir en ciberseguridad.

Para combatir el cibercrimen los países de habla hispana tipifican los delitos informáticos dentro de sus normativas con penas de privación de la libertad de máximo 360 meses teniendo como marco de referencia el convenio de la ciberdelincuencia de Budapest. En algunos países como Uruguay y Bolivia el cometimiento de estos delitos no implica privación de la libertar, Republica Dominicana se caracteriza por ser una nación con mayor severidad penal contra el cibercrimen gracias a la gran cantidad de delitos informáticos tipificados y las más altas penas de prisión. (Rojas Parra, 2016)

Según Riascos *et al.*, (2015) la estrategia de utilizar los sistemas de información para mejorar oportunidades para las PYMES es muy conocida y las organizaciones deberán implementar mecanismos de seguridad que permitan proteger la información. El objetivo principal es analizar el nivel de seguridad de los sistemas de información en las PYMES de la ciudad de Santiago de Cali (Colombia). Por lo cual se consideraron tres variables: Confiabilidad, Disponibilidad e Integridad, dando como resultados un nivel medio de seguridad en los sistemas de información.

Asimismo, Zuña *et al.*, (2019) indican que la seguridad informática es de suma importancia para las PYMES ya que podría brindar protección de los ciberataques, debido a que las pérdidas económicas son muy altas, ya sea por phishing o malware, ya que no se implementa métodos de detección temprana, además por la nula importancia y porque se cree que sería un gasto innecesario, las PYMES deben capacitar al personal en estos temas además de resguardar la información ya que se debe proteger los intereses de las PYMES, Por los cual, surgen los Sistemas de Seguridad y la Ciberseguridad que brindan la estabilidad de los sistemas de la información empresarial.

2.2 La ciberseguridad en el Ecuador

Para que exista una estrategia nacional de ciberseguridad, es indispensable elaborar una Política de Estado; considerándola como una Estrategia de Seguridad Nacional en donde se establezcan propósitos, principios rectores, políticas, objetivos, leyes y normativa, instituciones coordinadas y con capacidades, infraestructura, presupuesto, etc., en la que estén involucrados el Estado, la empresa privada, la sociedad, la academia y las relaciones internacionales. El Ecuador tiene un acceso al internet del 43 % de la población permitiendo estar conectados a la información que está en el ciberespacio lo cual es una puerta de entrada para los delincuentes aumentando el riesgo a la seguridad, por lo cual se debe adaptar su política y estrategias de Ciberdefensa considerando los modelos implementados en países de la región y en las recomendaciones que entrega la OEA y Chile especialmente respecto a esta nueva amenaza. Es fundamental que el estado cuente un marco legal contra los delitos informáticos, que puede afectar la infraestructura crítica y proteja la información, este marco jurídico debe estar basado en precedentes tomados de acuerdos internacionales y de la legislación de otros países. (Tates Almeida y Recalde Herrera, 2019)

También (Caraguay, 2020), menciona que la auditoría forense es una técnica que permite localizar, recopilar y organizar información relevante almacenada de forma electrónica incluso, con el uso de programas informáticos especializados, si esta fuera eliminada con ello se garantiza el custodio de la evidencia electrónica para sancionar el cometimiento de hechos ilegales. Sin embargo, en el Ecuador no existe una normativa expresa en lo referente a informática forense, lo que ocasiona que la auditoría gubernamental no garantice en su totalidad el control de los recursos públicos gestionados mediante TIC y más aún en un medio en la que los funcionarios públicos miran el bienestar propio

y dejan de lado el bienestar colectivo. Es así, que la informática forense debe complementarse con la evidencia digital en los procesos de auditoría gubernamental efectuada por la Contraloría General del Estado.

Un estudio realizado por la empresa Deloitte sobre como las empresas en Ecuador manejan el tema de la seguridad de la información arroja los siguientes resultados en torno a tres principales componentes que son: asegurar, detectar y responder. Para el componente de asegurar el estudio indica que 8 de cada 10 empresas en Ecuador tiene un responsable de seguridad de la información dentro de su organización, la detección lo realizan mediante el monitoreo de riesgos de seguridad y aunque las empresas cuentan con un sistema para este efecto aún existen debilidades en este ambiente sobre todo en lo que se trata de respaldar la información de terceros, el 50% de las empresas participantes aseguran haber sufrido ataques cibernéticos pero sólo una cuarta parte de estas han medido el impacto de este ataque y han destinado recursos tanto económicos como humanos y tecnológicos para aumentar su seguridad. (Oswaldo Bravo, 2017)

En torno a las leyes y siguiendo un enfoque cuantitativo y cualitativo se ha realizado un estudio de la evolución legal que ha tenido el tema de delitos informáticos en el Ecuador, aunque se ha visto la necesidad de regular este campo por el impacto que estos delitos ha tenido en el país aún existen debilidades en el tema a ser mejoradas, como por ejemplo, en lo que respecta a los operadores jurídicos y dirigentes de la fase procesal, fiscales, quienes tienen una inadecuada preparación en temáticas de delitos informáticos lo que les lleva a, en su mayoría, archivar este tipo de denuncias. Ecuador a pesar de tener una Subdirección de Delitos Informáticos le falta mayor inversión en grupos especializados que ayuden a mitigar o disminuir el impacto de estos delitos informáticos. (Santacruz y Hermoza, 2019)

Los delitos informáticos más usuales que se presentan en Ecuador son el Pharming y el Phishing los cuales se encuentran penados en la legislación ecuatoriana. El Pharming consiste en la suplantación de una página web oficial para solicitar información, mientras que el Phishing utiliza el envío de correos electrónicos para de igual manera solicitar información ya sea personal o bancaria. El Ecuador empezó a sancionar estos delitos informáticos a partir del año 2009 y desde entonces no se ha realizado una actualización a las leyes ocasionando que algunos delitos queden en la impunidad por falta de reglamentación. (Villon *et al.*, 2018)

La importancia de ciberseguridad en Ecuador y en el mundo radica en el aumento de la automatización de operaciones generadas por instituciones financieras, empresas públicas y otras, el Ecuador se implementó mediante Acuerdo Ministerial que todas las empresas públicas cuenten con un Esquema Gubernamental de Seguridad de la Información a partir del año 2013, pero, según el estudio realizado se evidencia que esto no ha sido suficiente para parar los ciberataques ya que estos han ido evolucionando de la mano con las tecnologías y los nuevos servicios que internet ofrece, uno de los que mayor impacto tiene en la sociedad son las redes sociales que han sido capaces de desorganizar estructuras sociales y políticas de forma impredecible. (Vargas *et al.*, 2017)

2.3 ¿Qué opciones tienen las empresas para evitar los ciberataques?

Muchos estudios se han realizado sobre cómo enfrentar el problema del ciberataque, una opción es la implementación del filtro Kalman en sistemas SCADA, esto para predecir los ataques cibernéticos y alertar a los ingenieros de sistemas sobre posibles contingencias que deben aplicar frente a los riesgos presentados, si bien los mecanismos presentados por otros estudios se basan en cómo mitigar el impacto de un ciberataque, esta propuesta

pretende que la empresa visualice los posibles impactos generados y de esta manera gestione dicho riesgo (Quiroz *et al.*, 2020).

Otra opción de seguridad de la información que podrían implementar las empresas lo plantean (Diéguez y Cares, 2019) mediante la comparación de dos métodos cuantitativos que buscan también ser presupuestariamente viable para las empresas, estos métodos son Answer Set Programation (ASP) y Programación Lineal (PL).

El modelo de auditoría de ciberseguridad CSAM se utiliza para evaluar la seguridad, su madurez y la preparación frente a la seguridad cibernética, además para detectar las necesidades para acrecentar la conciencia cibernética a nivel organizacional y personal. El modelo se puede implementar para llevar a cabo auditorías internas o externas de ciberseguridad, auditorías de ciberseguridad individuales o puede ser parte de cualquier programa de auditoría corporativa para mejorar los controles de ciberseguridad. El modelo de ciberseguridad que incluye todos sus componentes, fue validado satisfactoriamente por un caso de estudio realizado en una institución de educación superior canadiense en tres escenarios (1) Auditoría de todos los dominios del modelo, (2) Auditoría de varios dominios y (3) una auditoría de un único dominio y puede ser implementado en cualquier organización que puede ser cualquier empresa pequeña, mediana o grande, el modelo también es aplicable a cualquier organización sin fines de lucro. (Sabillon y Cano, 2019)

Por último, una solución planteada por (Morales *et al.*, 2019) es el uso de un sistema de seguridad perimetral como respuesta a minimizar el riesgo de sufrir ataques cibernéticos, este sistema incrementará la eficacia en el control de accesos y protección de los equipos, los permisos que se asignen en el sistema

garantizarán la seguridad de la información en cuanto a integridad, confidencialidad y disponibilidad de la misma.

3. Métodos y recursos

Para el desarrollo de este trabajo se realizó una investigación cuantitativa exploratoria haciendo énfasis en las amenazas y vulnerabilidades cibernéticas que hoy en día representan un mayor nivel de riesgo de afectación a las organizaciones e instituciones, públicas, privadas, y a las PYMES.

Lo que se desea probar en esta investigación es la poca trascendencia e impacto de las estrategias de ciberseguridad, puesto que no se han desarrollado en todos los sectores empresariales del país, motivo por el cual las pequeñas y medianas empresas de la ciudad de Cuenca no conocen, ni tienen implementado el concepto de ciberseguridad dentro de sus organizaciones.

Para confirmar o desechar la proposición, se decidió aplicar una encuesta donde se estableció como universo de estudio las pequeñas y medianas empresas de la ciudad de Cuenca, que cuenten con un número mínimo de 5 equipos de cómputo y máximo 50 unidades. Para la unidad de muestreo se seleccionaron las PYMES del sector industrial, comercial y de servicios. Para determinar el tamaño de la muestra se tomó como referencia información de la Cámara de Comercio de Cuenca, donde se establece la existencia de 300 PYMES, y se utilizó la fórmula de muestreo aleatorio simple de la siguiente manera:

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

En donde:

N = 300 unidades

Z = Percentil de la distribución normal con un nivel de confianza del 90%;

Z = 1.645

p = es la proporción esperada

p = 0.5

q = 1-p; complemento de la proporción esperada d es el margen de error;

E = 10%.

n: Tamaño de la muestra: 56 unidades

Para el presente trabajo de investigación, se han determinado las variables detalladas en la Tabla 1, mismas que resultaron de la revisión de la literatura.

Tabla 1 Definición de variables

VARIABLE		SIGNIFICADO
1.	**Costo – Beneficio**	Hace referencia a la relación entre la inversión y lo que se va a obtener de ella. Se quiere conocer si se lo ve como una inversión o un gasto.
2.	**Empleados**	Se busca verificar si es indispensable la existencia de empleados con conocimientos sobre ciberseguridades.
3.	**Filosofía Empresarial**	Se desea conocer si las PYMES están abiertas a las nuevas tendencias o prefieren lo tradicional.
4.	**Capacitación/Mantenimiento**	Hace referencia a que las ciberseguridades no son una única inversión inicial, sino que constantemente se debe mantener y capacitar al personal y eso implica mayor salida de dinero.
5.	**Capacidad de Reacción**	Hace referencia a la reacción que tiene la empresa frente al entorno o factores externos, si ésta es lenta o rápida

La calificación de las variables que se muestran en la Tabla 2, tendrá una escala ordinal, con valores que van del 1 al 5 siendo el más bajo y el más alto respectivamente.

Tabla 2 Escala de medición de variables

CALIFICACIÓN	SIGNIFICADO
1	No tiene importancia
2	Poca Importancia
3	Importante
4	Muy Importante
5	Indispensable

Posteriormente, dichas encuestas fueron analizadas y realizadas una correlación de variables mediante la técnica “Análisis de Varianza o ANOVA”. Este coeficiente de correlación es usado para medir la asociación entre dos variables, toma valores entre -1 y 1, indicando que un valor cercano a 0 se interpreta como independencia entre las variables mientras que si el valor es cercano a 1 o -1 indica correlación o dependencia ya sea directa o inversamente proporcional, respectivamente.

4. Resultados

Analizando los factores o barreras con mayor importancia según el criterio de los dueños o gerentes, se puede observar que “Costo – Beneficio” es la más influyente seguido de “Filosofía Empresa”. Además, se determinó que los gerentes o administradores de las empresas analizadas, no ven como una inversión a las ciberseguridades, más bien lo ven como un gasto debido a que no perciben ningún rendimiento monetario, este criterio para evaluar y diferenciar si es gasto o inversión no es el correcto, pues si bien es cierto no hay ingreso de efectivo, pero ayuda a prevenir pérdidas; y,

en la actualidad lo más importante son los activos intangibles que en este caso es la información. En las empresas industriales esto se traduce en: marcas, patentes, modelos, entre otros, los cuales pueden ser fácilmente sustraídos sino hay controles en los sistemas informáticos. De igual manera, en una empresa comercial lo más importante son los contactos de proveedores y clientes (intangibles) que han logrado captar durante su permanencia en el mercado y que seguramente le ha costado a estas compañía o sociedades conseguirlas, dicha información al ser de alta confidencialidad deberá manejarse con mucha delicadeza.

La Tabla 3 que se detalla a continuación, resume los resultados promedio obtenidos por sector económico, determinando así, que la rama de servicios da mayor importancia a las ciberseguridades y se preocupa en reforzar sus controles informáticos. Este sector está consciente de las deficiencias informáticas y sabe que es necesario tener resguardada la información, lo cual es lógico pues al dedicarse a los servicios su actividad y desarrollo depende de las bases de datos y sistemas de información que puedan tener.

Tabla 3 Resultados por sector económico

sector	costo beneficio	empleados	filosofia y empresa	capacitacion mantenimiento	capacidad de adaptacion
Industrial	4	3	2	3	2
Comercial	3	2	4	3	2
Servicios	4	3	3	2	4

Como se puede observar en la Tabla 4, el estadístico de prueba es mayor al valor crítico, o dicho de otra forma F calculado es mayor a F dado, entonces se rechaza la hipótesis nula de que las medias de los grupos (sectores económicos) son iguales,

concluyéndose con un 95% de confianza, que a nivel poblacional existen variaciones considerables entre actividades empresariales, y el sector de servicios es el más interesado y preocupado en la implementación de ciberseguridades.

Tabla 4 Resultados del análisis de varianza

ANÁLISIS DE VARIANZA						
Origen de las variaciones	***Suma de cuadrados***	***Grados de libertad***	***Promedio de los cuadrados***	***F***	***Probabilidad***	***Valor crítico para F***
Entre grupos	25,7	4	6,425	3,347 2481	0,0112 0165	2,4179 625
Dentro de los grupos	374,3	195	1,919487			
Total	400	199				

En la Tabla 5 se muestran los resultados del análisis de correlación entre variables; en la cual, se puede observar que la variable “Filosofía Empresa” se relaciona con casi todas y de forma inversa, es decir cuando un dueño o gerente adopta medidas menos tradicionales, esto involucraría:

1. Considerar a la ciberseguridad como inversión,
2. Contar con personal que tengan conocimientos en sistemas de información,
3. Menor presupuesto para capacitación a personal, pues ya cuentan con las bases necesarias.

Esto a su vez se verá reflejado en personal proactivo, con una mayor capacidad de reacción frente a los cambios

organizacionales, fortaleciendo la eficiencia, eficacia y economía en las empresas u organizaciones.

Tabla 5 Análisis de correlación

	Costo-Beneficio	***Empleados***	***Filosofía***	***Capacitación***	***Adaptación***
Costo-Beneficio	-	0,023412	0,294772	-0,27131	0,038274
Empleados	0,563623	-	0,48274	-0,4231	0,94727
Filosofía	-0,9489131	-0,94613424	-	-0,8439	-0,382
Capacitación	-0,5049367	-0,92462424	0,5149921	-	-0,0472
Adaptación	-0,1094482	0,51505450	-0,2097849	0,802706498	-

5. Debate

La barrera más grande en la implementación de ciberseguridades que las pequeñas y medianas empresas ven es el “Costo – Beneficio” lo cual indica que aún no se ve como inversión a las salidas de dinero por concepto de ciberseguridad, es decir este resultado es similar al obtenido por (Ribagorda Garnacho, 2018). El comportamiento de la mayor parte de las empresas no es proactivo, sino reactivo es decir tiene que pasar eventos desfavorables para que las organizaciones tomen decisiones que implican correcciones en varias actividades que realizan y que podían haberse detectado y evitado a tiempo, siendo esto lo contrario con la propuesta presentada por (Quiroz et al., 2020).

Otra tendencia que tienen nuestras empresas es aplicar medidas para cumplir con la normativa, es decir el Estado presiona para que se adopten nuevas políticas lo cual es lamentable porque debería ser el mismo sector privado el que impulse nuevos mecanismos, pero las empresas del país (no solo de Cuenca) están acostumbradas a que haya regulaciones para actuar. Tal cual como lo indica (Vargas Borbua et al., 2017).

Por el momento, se puede optar a que el Sector Público entre a regular esta situación porque es de mucha importancia para toda la sociedad no sólo para las empresas. Siendo necesario vincular la auditoría gubernamental con la informática forense para proteger los recursos mediante el custodio de la evidencia electrónica, así como lo indica (Caraguay, 2020).

Adicionalmente, los resultados obtenidos en la presente investigación están acorde a lo propuesto por (Tates Almeida y Recalde Herrera, 2019), en el sentido de establecer una política de Estado, pero con la inclusión del sector privado, más aún en el contexto actual en que se están desarrollando las actividades (Teletrabajo) y se requiere de políticas que garanticen la seguridad de la información.

6. Conclusiones

La globalización ha traído consigo la aparición de nuevas tecnologías apoyadas por el uso de internet, las mismas que han generado grandes desarrollos en el mundo. Si bien es cierto, el computador ha sido un instrumento de gran ayuda, pero de doble filo, pues por un lado ha permitido sin duda alguna conectar al mundo, disminuyendo distancias y agilitando diferentes procesos de la vida cotidiana; pero, por otro lado, también ha permitido la aparición de varios problemas. Uno de ellos es la delincuencia informática, que se apoya en el delito instrumentado por el uso de

la computadora a través de redes telemáticas y la interconexión, aunque no es el único medio. Son muchos los delitos informáticos que ya han sido generados y a medida que la tecnología e Internet se desarrollen, aparecerán muchos más.

La criminalidad informática constituye un reto considerable tanto para las diferentes personas ya sean naturales o jurídicas de un país, como para los legisladores y principales autoridades del Estado; ya que a pesar de la normativa vigente que penalizan este tipo de delitos, el índice de fraudes informáticos no disminuye sino al contrario, va en aumento a nivel mundial.

Lo más importante es que tanto las personas y las diferentes empresas u organizaciones en calidad de víctimas potenciales, tomen conciencia de la importancia de implementar métodos más rígidos de seguridad informática, no únicamente para contrarrestar los perjuicios que puede generar un fraude informático sino más bien para prevenirlos. Como se demostró en el presente trabajo de investigación, el sector de servicios es el que lidera la inversión en ciberseguridad, dentro de esta rama se encuentran las instituciones financieras, lo cual resulta bastante coherente dicho resultado. Otro aspecto que se podría analizar a futuro es que si estos controles de las instituciones financieras son por iniciativa propia o por obligatoriedad (cumplimiento de normativa). En base a los resultados expuestos, la interrogante planteada es válida debido a que la filosofía empresarial de las compañías y sociedades ecuatorianas es reactiva, es decir se limita al cumplimiento de la base legal.

Una posible alternativa a esta situación es que la Superintendencia de Compañías (órgano supervisor de sociedades y compañías del Ecuador), solicite a los auditores externos un apartado detallado sobre los sistemas informáticos y su nivel de

riesgo a ciberataques, dentro del Informe de Control Interno de las empresas a las que realicen las revisiones obligatorias. De esta manera, se podrá actualizar indicadores de la exposición a delitos informáticos y concientizar a las empresas sobre las inversiones en controles de los sistemas. La finalidad sería que la mayor cantidad de empresas sientan la necesidad de establecer políticas de inversión respecto a ciberseguridad, que se adapten a su realidad económica, financiera y operativa.

7. Bibliografía

ALZAMORA, E. (2013). Impacto de las prácticas de auditoría en la disminución de fraude en las organizaciones. Revista Enfoque Disciplinario, 25-30.

ANCHUNDIA-BETANCOURT, C. E. (2017). Ciberseguridad en los sistemas de información de las universidades. Dominio de las Ciencias.

ACOSTA, MARÍA GABRIELA, & BENAVIDES, MERCK MILKO, & GARCÍA, NELSON PATRICIO (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. Revista Venezolana de Gerencia, 25(89),351-368. Disponible en: https://www.redalyc.org/articulo.oa?id=290/29062641023

BAEZ, A., VILLAGÓMEZ, M., CEVALLOS, M. (2017). La auditoría forense. En el espacio social de la ciencia y la tecnología. Corporación Educativa SER, 698-716.

CAAMAÑO, E., GIL, R. (2020). Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional. Novum, Revista de Ciencias Sociales Aplicadas, 61-80.

CARAGUAY, S. (2020). Aplicación de informática forense en auditorias gubernamentales para la deteminacion de indicios de responsabilidad penal con delitos informáticos en Ecuador, México y Perú, 2007-2019. Estado & Comunes, 135-153.

CÁSERES, G., DE LA TORRE, C. (2017). Auditoria Forense como medio para combatir la corrupción. Revista Arje, 88-97.

DIÉGUEZ, M., & CARES, C. (2019). Comparación de dos enfoques cuantitavos para seleccionar controles de seguridad de la información. Revista Ibérica de Sistemas y Tecnologías de la Información.

ESPINOZA, W. (2016). La tecnología de la información como herramienta construccionista para el auditor financiero hibrido. Fides Et Ratio, 17-35.

GAVILANES MOLINA, A. F., & PROAÑO ESCALANTE, R. A. (2018). Estrategia para responder a incidentes de inseguridad informática ambientado en la legalidad ecuatoriana. Sistema de Información Científica Redalyc.

GIL VERA, V. D., & GIL VERA, J. C. (2017). 7. Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. Scientia Et Technica.

GÓMEZ-GIACOMAN, C., & BOLAÑOS-BURGOS, F. (2015). Estudio cualitativo de la relación de las leyes y la pericia informática en el Ecuador. RECIBE; Revista electrónica de Computación, Informática, Biomédica y Electrónica.

HERNÁNDEZ, I., & MARINO MEDINA, L. (2020). Planes tácticos sobre la gestión de procesos externalziados. SIC, 82-84.

LERMA GANGOITI, A. (2020). Los Sistemas de Gestión como herramienta de Seguridad. SIC, 88- 89.

MARTÍNEZ, E. D. (2020). La automatización, Ciberseguridad y TI. SIC, 116-119.

MORALES CARRILLO, J. J., AVELLAN ZAMBRANO, N., LENTONG ZAMBRANO, T. J., & ZAMBRANO BRAVO, M. (2020). Proceso de Ciberseguridad: Guía Metodológica para su implementación. Revista Ibérica de Sistemas e Tecnologias de Informação, 41-50.

MORALES, F., TOAPANTA, S., & TOASA, R. (2019). Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información. Revista Ibérica de Sistemas y Tecnologías de la Información.

OSWALDO BRAVO, R. C. (2017). Deloitte. Ecuador. Obtenido de https://www2.deloitte.com/ec/es/misc/search.html#qr=SEGURIDAD%20DE%20LA%20 INFORMACION

RIBAGORDA GARNACHO, A. (2018). Panorama Actual de la Ciberseguridad. Visión Global, 13-26.

ROJAS PARRA, J. H. (2016). Análisis de la penalización del cibercrimen en países de habla hispana.

Revista LOGOS CIENCIA & TECNOLOGÍA, 220-232.

RIASCOS ERAZO, S. C., AGUILERA CASTRO, A., & ÁVILA FAJARDO, G. P. (2015). Seguridad de los sistemas de información en las Pymes de Santiago de Cali (Colombia). Libre Empresa.

RUIZ, D., & HURTADO, J. (2020). Thin Security, o como maximizar la efectividad de la ciberseguridad para sobrevivir en el mundo Post COVID 19. SIC, 78-80.

SABILLON, R., & CANO M., J. J. (2019). Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas

y naciones. Revista Ibérica de Sistemas e Tecnologias de Informação, 33-48.

SANTACRUZ, H., & HERMOZA, M. (2019). Los delitos informáticos y su tipificación en la legislación penal ecuatoriana. Revista Ibérica de Sistemas y Tecnologías de la Información.

SIC. (2020). La gestión de múltiples soluciones, que no se integran, sigue en la cúspide de retos de los responsables españoles de ciberseguridad. SIC, 118-121.

SUCUNZA, F. (2020). Retos de la ciberseguridad en virtualización OT. SIC, 106-108.

TATES ALMEIDA, C. A., & RECALDE HERRERA, L. (2019). La ciberseguridad en el Ecuador, una propuesta de organización. Revista de Ciencias de Seguridad y Defensa, 156-169.

VARGAS BORBUA, R., RECALDE HERRERA, L., & REYES CH., R. P. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. URVIO, Revista Latinoamericana de Estudios de Seguridad, 31-45.

VILLON, H., SOJOS, M., MENDOZA, C., GUARDA, T., & CLERY, A. (2018). Delitos informáticos penalizados por la legislación ecuatoriana. Revista Ibérica de Sistemas y Tecnologías de la Información.