UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE ECONOMÍA Y EMPRESA

CARRERA DE CONTABILIDAD Y AUDITORÍA

TÍTULO:

Análisis para la Aplicación de la Norma ISO 27001 en Pymes del Sector Servicios de la Ciudad de Guayaquil, año 2022.

AUTOR:

Bonilla Sánchez, Steven Gonzalo

Trabajo de titulación previo a la obtención del título de

LICENCIADO EN CONTABILIDAD Y AUDITORÍA

TUTOR:

Ing. Com. Delgado Loor, Fabian Andrés. MBA

Guayaquil, Ecuador

7 de septiembre del 2023

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE ECONOMÍA Y EMPRESA

CARRERA DE CONTABILIDAD Y AUDITORÍA

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por **Bonilla Sánchez, Steven Gonzalo** como requerimiento parcial para la obtención del Título de: licenciado en Contabilidad y Auditoría.

TUTOR

f. _____

Ing. Com. Delgado Loor, Fabian Andrés. MBA

DIRECTOR DE LA CARRERA

f. _____

PhD. Said Diez Farhat

Guayaquil, a los 7 días del mes de septiembre del año 2023

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE ECONOMÍA Y EMPRESA

CARRERA DE CONTABILIDAD Y AUDITORÍA

DECLARACIÓN DE RESPONSABILIDAD

Yo, Bonilla Sánchez, Steven Gonzalo y

DECLARAMOS QUE:

El Trabajo de Titulación **"Análisis para la Aplicación de la Norma ISO 27001 en Pymes del Sector Servicios de la Ciudad de Guayaquil, año 2022"** previa a la obtención del Título de: **Licenciado en Contabilidad y Auditoría.**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de mi total autoría. En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del Trabajo de Titulación referido.

Guayaquil, a los 7 días del mes de septiembre del año 2023

AUTOR

Bonilla Sánchez, Steven Gonzalo

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE ECONOMÍA Y EMPRESA

CARRERA DE CONTABILIDAD Y AUDITORÍA

AUTORIZACIÓN

Yo, Bonilla Sánchez, Steven Gonzalo

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación en la biblioteca de la institución del Trabajo de Titulación **"Análisis para la Aplicación de la Norma ISO 27001 en Pymes del Sector Servicios de la Ciudad de Guayaquil, año 2022**", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

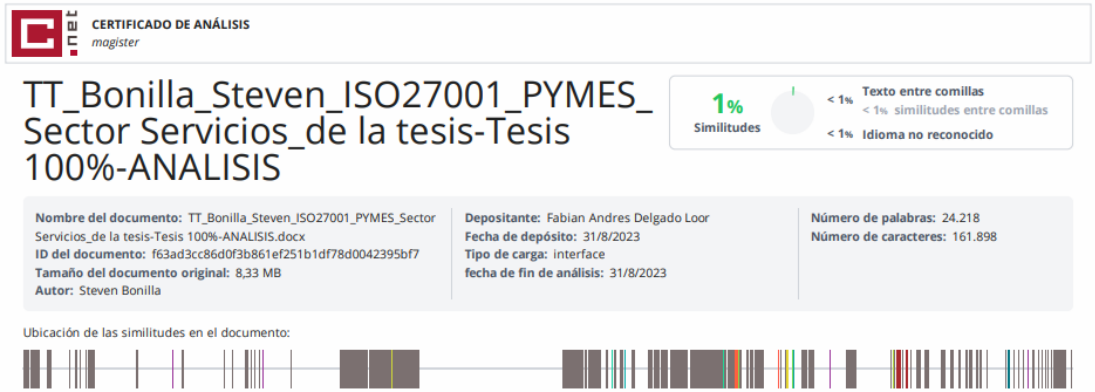
Guayaquil, a los 7 días del mes de septiembre del año 2023

AUTOR

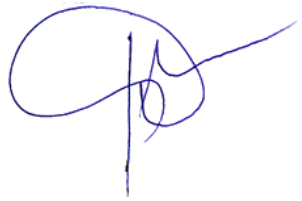
Bonilla Sánchez, Steven Gonzalo

REPORTE COMPILATIO

https://app.compilatio.net/v5/report/234b4dcbebb3173a60970ed9a357a647a6020b07/sources



TUTOR



f._____

Ing. Com. Delgado Loor, Fabian Andrés. MBA

AGRADECIMIENTO

A Dios por ser el guía de nuestra existencia y concederme el don del conocimiento, que me permitió culminar esta etapa dentro de mi vida estudiantil.

A todos los profesores quienes, a lo largo de mi carrera universitaria, mediante su esfuerzo y entrega, permitió que nosotros obtengamos valiosos conocimientos y experiencias, en la cual, será fundamental para el desarrollo personal y profesional de nuestra vida.

Finalmente, a mis familiares, amigos y compañeros, en donde, su apoyo incondicional, fue fundamental para el constante trabajo y sacrificio en la realización de la presente Tesis y adquisición del título profesional.

Steven Gonzalo Bonilla Sánchez

DEDICATORIA

Dedico este trabajo como muestra de devoción y gratitud eterna a mi padre Jesús Bonilla, quien siempre es ejemplo de superación y honradez durante mi vida estudiantil y personal; a mi madre Carmen Sánchez, quien con su esfuerzo y dedicación fue esencial para culminar lo iniciado; a mi hermano Billy Bonilla que cada día me daba ánimos para seguir adelante y culminar con éxito mis estudios y lograr el Título pretendido.

Steven Gonzalo Bonilla Sánchez

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE ECONOMÍA Y EMPRESA

CARRERA DE CONTABILIDAD Y AUDITORÍA

TRIBUNAL DE SUSTENTACIÓN

f. _____

Ph. D. Said Vicente Diez Farhat

DIRECTOR DE CARRERA

f. _____

Ec. Paola Guim Bustos, Mgs.

COORDINADORA DEL ÁREA

f. _____

PhD. Lorena Bernabé Argandoña, Econ.

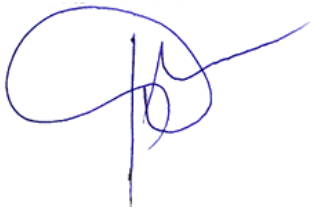
OPONENTE

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE ECONOMÍA Y EMPRESA

CARRERA DE CONTABILIDAD Y AUDITORÍA

CALIFICACIÓN



f. _____

Ing. Com. Delgado Loor, Fabian Andrés. MBA

TUTOR

Índice General

Lista de Tablas

Lista de Figuras

Resumen

En el presente trabajo de análisis de la aplicación de la norma ISO 27001 se estableció como objetivo general el analizar esta norma en PYMES del sector servicios de la ciudad de Guayaquil para el fomento de una gestión apropiada de seguridad de información con base en un diagnóstico del estado actual de la seguridad de la información en las Pymes seleccionadas. El estudio se enmarcó dentro de una investigación de carácter descriptivo. Los estudios descriptivos buscan especificar: (a) las propiedades, (b) las características y (c) los perfiles importantes de: (a) personas, (b) grupos, (c) comunidades o (d) cualquier otro fenómeno que se someta a un análisis. El método utilizado en la investigación fue: (a) Por juicio: el cual consiste en que los sujetos se seleccionan basados en: (a) conocimiento, (b) experiencia y juicio del investigador. Los principales resultados obtenidos por implementación de protección de datos: (a) nos muestra que las firmas auditoras implementaron el SGSI, (b) piensan que la implementación será un gasto adicional, (c) la no implementación puede sufrir amenazas de su información, (d) no se preocupan por la información. Los principales resultados obtenidos sobre seguridad de activos de información: (a) nos muestra que las firmas auditoras son importantes la seguridad de los activos de información porque quieren que sus datos sean protegidos de la mejor forma (b) indica que hay algunas firmas auditoras que si usan activos de información, pero se preocupan más por el funcionamiento del negocio de su firma para captar clientes y (c) finalmente protegen su información con pocos recursos, (d) muestra que para las firmas es clave porque el control de acceso impide que los usuarios no autorizados tengan información confidencial (e) falta implementar algunos controles fundamentales porque el objetivo de autenticar al usuario mediante: (a) preguntas personales, (b) huellas digitales y (c) tokens criptográficos. En conclusión, es importante que las organizaciones implementen el plan del SGSI porque identifican los controles de seguridad, los cuales: (a)salvaguardan, (b) controlan, (c) monitorean y (d) asignan responsabilidades, con el fin de: (a) evitar, (b) controlar, (c) transferir y (d) mitigar los riesgos detectados.

Palabras claves: Norma ISO 27001, SGSI, TIC, Sistema Informático, Riesgos, Vulnerabilidad, Seguridad Informática, PYMES.

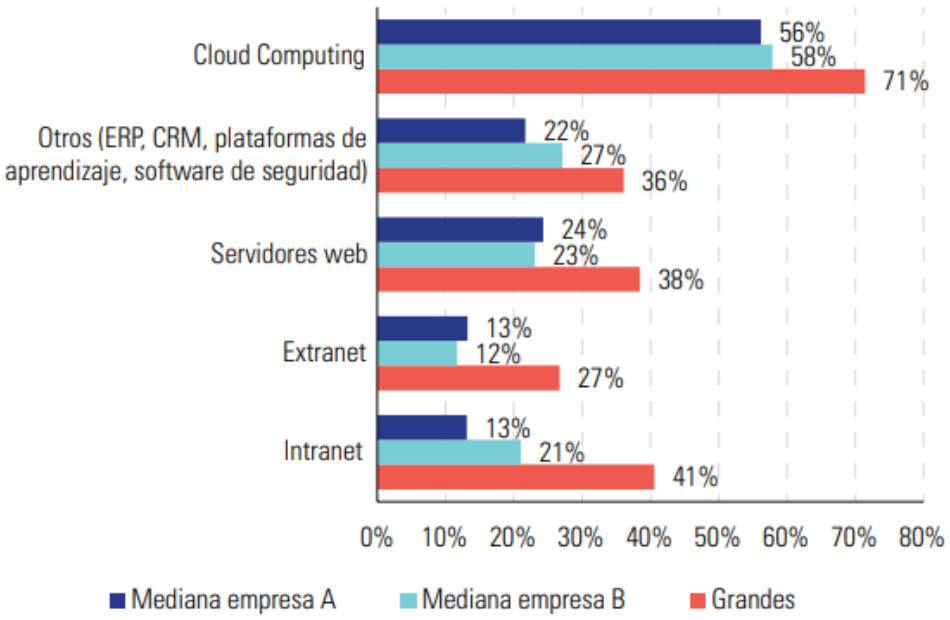
Introducción

Antecedentes

Tendencia Tecnológicas en PYMES ecuatorianas

Los resultados obtenidos del Módulo TIC de la Encuesta Estructural Empresarial realizada en el 2018 por parte del Instituto Nacional de Estadística y Censos (INEC), en la que participaron 4.088 empresas medianas y grandes (se excluyen micro y pequeñas) de sectores económicos como: (a) manufactura, (b) minería, (c) comercio, (d) construcción, y (e) servicios, denotaron que en el Ecuador el nivel de conexión a Internet se encuentra ampliamente extendido mediante banda ancha fija. En cuanto al uso avanzado de tecnología como Cloud Computing en las empresas o de gestión tipo ERP, CRM u otras, así como el uso de servidores o de la intranet, tuvo un bajo nivel de inversión. Cabe destacar que solo un aproximado del 30% de la población encuestada declararon invertir en tecnologías de información y comunicación (TIC) (Dini et. al, 2021). Resultados que se observan en la siguiente figura:

Figura 1
Tendencia de TICS



Nota. Tomado de *Transformación digital de las MIPYMES. Elementos para el diseño de políticas,* por Dini, Gligo y Patiño, 2021. Santiago de Chile. Naciones Unidas.

Durante el impacto de la crisis pandémica del 2020 ocasionada por la COVID-19, gran cantidad de las empresas recurrieron al uso intensivos de herramientas digitales para hacer frente a los desafíos de restricción de movilidad, propagación del virus, cierre de fronteras, entre otras situaciones. Este salto tecnológico permitió: (a) adaptación de teletrabajo, (b) realización de compras, (c) ventas online, (d) gestión de procesos de producción de forma remota. Sin embargo, el salto tecnológico constituyo grandes retos para las micro, pequeñas y medianas empresas y más aún sin el acompañamiento adecuado (Angelelli, Hennessey, & Henriquez, 2020).

La digitalización acelerada de las empresas en Ecuador represento una estrategia de negocios enfocada en la innovación y mejoramiento de los servicios para hacer frente a los desafíos de competitividad en el mercado durante la pandemia. Esto destacó la urgencia de la tecnificación de los negocios y de la aplicación de estrategias de ciberseguridad. No obstante, el asegurar el funcionamiento de la infraestructura tecnológica no ha sido tarea fácil debido a errores y fallas administrativas sobre los sistemas y la información. Es importante destacar, que pese a los retos que ha presentado la innovación, los propietarios de las empresas perciben sobre la importancia de la ciberseguridad y consideran viable invertir en sistemas de seguridad de información como la ISO27001 y el marco de gestión de riesgo COBIT 5.0 (Bueno et al., 2022).

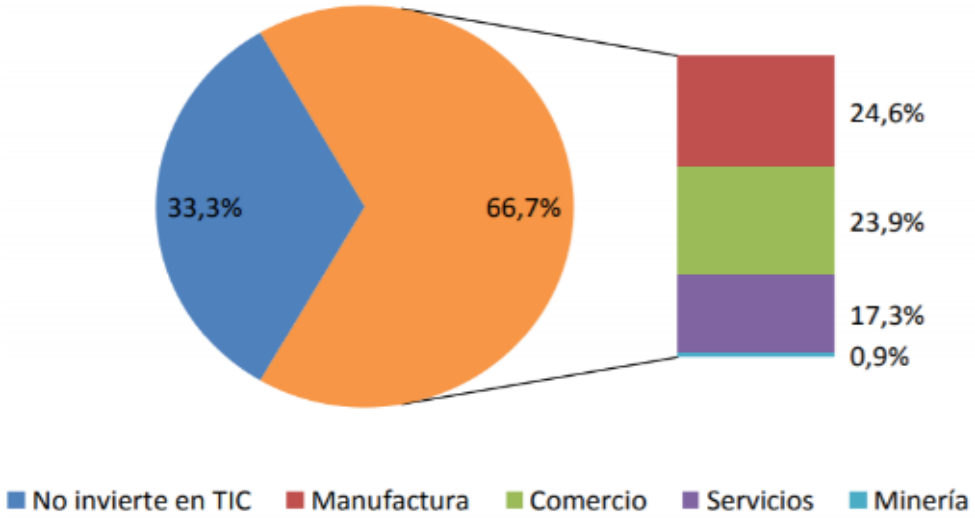
Otros estudios sobre la importancia de la información y de su gestión denotan la otra postura de las PYMES. En esta se evidenció que los sistemas de información básicos o complejos que poseen estos negocios se han visto afectadas por distintos ataques y amenazas sobre su información. Por tales motivos, los organismos internacionales han desarrollado estándares, metodologías y herramientas que permiten la gestión eficiente de la información, como en el caso de la ISO 27000. Esta norma promueve un sistema de gestión sobre la seguridad de información permitiendo el análisis de brecha y responder a los distintos riesgos de negocios sobre el alcance mencionado, otorgando resultados favorables para las empresas. Sin embargo, su

implementación se ve limitada por diversos aspectos como: (a) competencia de personal, (b) limitados recursos tecnológicos, (c) costo de implementación, (d) demás recursos para que el sistema de gestión y seguridad de la información funcione adecuadamente (Pruna et al., 2021).

Inversión en TICS en PYMES ecuatorianas

En un mercado globalizado las empresas buscan ser más competitivas, por tanto, la innovación es un factor determinante para su logro, considerando que las nuevas tecnologías proporcionan soluciones sustanciales en los modelos de negocio. Las tecnologías de información y de comunicación son consideradas como parte de las estrategias competitivas de las compañías. En concordancia con los datos levantados por del Instituto Nacional de Estadísticas y Censos, en el 2015 un 66,7% de las compañías invirtieron en TIC. De este grupo poblacional el 17,3% corresponde a entidades del sector servicios (Instituto Nacional de Estadística y Censos, 2015). A continuación, se muestran los resultados del censo sobre inversión en TIC.

Figura 2
Inversión en TICS



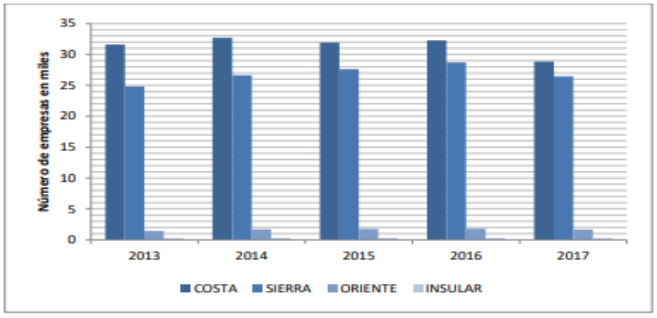
Nota. Tomado *de Empresas y Tecnología de Información y la Comunicación, de Instituto Nacional de Estadística y Censos*, 2015. Ecuador.

Durante el auge de la crisis pandémica, las empresas en el Ecuador aceleraron la adopción de las tecnologías de información. La mayor parte de la inversión se destinó a la compra de equipos de computación y programas de almacenamiento de información. Siendo el principal motor la incorporación de las actividades remotas como el teletrabajo. No obstante, las PYMES son las que presentan mayores retos tecnológicos debido a la desigualdad o brecha digital por la falta de conectividad y el analfabetismo digital (Microsoft, 2022).

Pese a que la innovación tecnológica representó una de las principales estrategias de negocios para hacer frente a los efectos de la crisis pandémica, el asegurar el correcto funcionamiento de la infraestructura tecnológica mediante la implementación de mecanismos de ciberseguridad representó uno de los grandes retos empresariales producto de los errores, fallas técnicas y administrativas sobre los sistemas y la información. Esta situación se origina por la falta de conocimiento sobre la ciberseguridad. De modo que, las buenas prácticas basado en normas internacionales como la ISO 27001 permiten la incorporación de controles para contrarrestar los efectos de los riesgos que afectan a la integridad, disponibilidad y confidencialidad de información (Bueno et al., 2022).

Conformación del Subsector de servicios

Figura 3
Distribución del sector de servicios



Nota. Tomado de *Estudios Sectoriales. Panorama del Sector de Servicio,* por Camino et al., 2018. Superintendencia de Compañías, Valores y Seguros (SCVS).

El sector de servicios desempeña una función significativa en la economía mundial, tanto en naciones avanzadas como en la mayoría de las economías en desarrollo, ya que actúa como el principal impulsor del crecimiento económico. Además, tiene una participación continua en cada una de las cadenas productivas que se generan en el sector empresarial formal, incluyendo la generación de empleo. En Ecuador estas empresas se concentran principalmente en las regiones Costa y Sierra, que en promedio comprenden el 52% y 45% del total de compañías, respectivamente como se describe en la figura tres (Camino et al., 2018).

Es importante destacar que el sector de servicios se subdivide en diversos grupos de subsectores como: (a) servicios de apoyo a la agricultura, (b) explotación de minas y recursos naturales, (c) reparación e instalación de maquinaria y equipo, (d) construcción y actividades inmobiliarias, (e) actividades comerciales, (f) transportes, (g) actividades de turismo y recreativas, (h) tecnología de información, (i) Actividades profesionales, científicas y técnicas; de servicio administrativo y de apoyo, y (j) otros servicios. Esta se categoriza de acorde con el Código de Categorías para Filiales Extranjeras de la CIIU de los servicios (Camino et al., 2018).

En relación con lo expuesto, la investigación se centrará en las empresas PYMES dedicada a las actividades de auditoría externas que forman parte del subsector de servicio Actividades Jurídicas y de Contabilidad. Actividad económica categoriza con el código CIIU M69. En el siguiente párrafo se describirá la conformación del subsector de firmas auditoras.

Subsector de firmas auditoras

En el Ecuador existen alrededor de 1,557 firmas auditoras constituidas bajo el control de la Superintendencia de Compañías, Valores y Seguros. Estas se, se enfocan en opinar sobre la razonabilidad de la información financiera mediante la emisión de informes de auditoría (Superintendencia de Compañías, Valores y Seguros, 2022). En la siguiente tabla se muestra su distribución por tamaño y su contribución en la generación de empleo.

Tabla 1

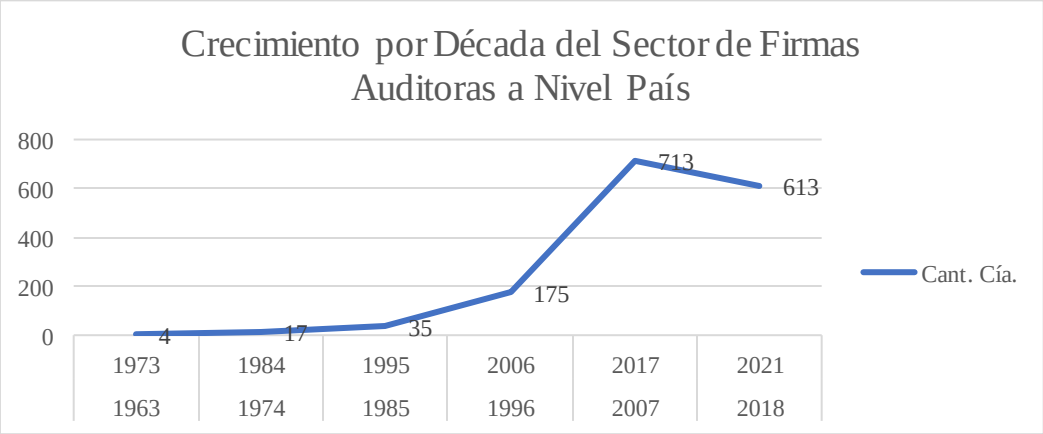
Distribución por Tamaño y Generación de Empleo

Tamaño	Mercado de Valores		Societario					
	Cant. de Cía.	Cant. Empleados	Cant. de Cía.	Cant. Empleados	Total, General de Cía.	% de Cía.	Total, General de Empleados	% de Empleados
Grande	3	480	3	2,846	6	0.39%	3,326	26.13%
Mediana	7	420	15	481	22	1.41%	901	7.08%
Microempresa	12	56	1,178	5,685	1,190	76.43%	5,741	45.09%
Pequeña	41	507	287	2,256	328	21.07%	2,763	21.70%
(En Blanco)			11	-	11	0.71%	-	0.00%
Total general	63	1,463	1,494	11,268	**1,557**		**12,731**	

Nota. Adaptado de "*Ranking de Empresas",* por Superintendencia de Compañías, Valores y Seguros, 2022. Ecuador

Las firmas auditoras en el Ecuador han presentado un crecimiento paulatino entre la década los periodos de 1973 al 2006- No obstante, en las últimas dos décadas su desarrollo ha sido notorio al incorporarse al mercado más de 1000 empresas enfocadas a atestiguar la información financieras de las compañías (Superintendencia de Compañías, Valores y Seguros, 2022).

Figura 4
Crecimiento de las Firmas Auditoras en el Ecuador por Década



Nota. Adaptado de *Ranking de Empresas,* por Superintendencia de Compañías, Valores y Seguros, 2021. Ecuador

En cuanto a la distribución provincial, la mayor concentración de firmas auditoras se centra en la provincia del Guayas y Pichincha con un 45% y 40% respectivamente. El 15% restantes de empresas se distribuye en otras 20 provincias (Superintendencia de Compañías, Valores y Seguros, 2022).

Tabla 2

Distribución Provincial de las Firmas Auditoras en el Ecuador

Región	Provincia	Cantidad de Cía.	%
Costa	El Oro	30	1.93%
	Esmeraldas	1	0.06%
	Guayas	**708**	**45.47%**
	Los Ríos	9	0.58%
	Manabí	40	2.57%
	Santa Elena	10	0.64%
Oriente	Napo	2	0.13%
	Orellana	1	0.06%
	Pastaza	2	0.13%
	Sucumbíos	1	0.06%
	Zamora Chinchipe	1	0.06%
Sierra	Azuay	56	3.60%
	Bolívar	1	0.06%
	Cañar	2	0.13%
	Chimborazo	8	0.51%
	Cotopaxi	4	0.26%
	Imbabura	12	0.77%
	Loja	12	0.77%
	Pichincha	**629**	**40.40%**
	Santo Domingo De Los Tsáchilas	14	0.90%
	Tungurahua	14	0.90%
Total, General		**1557**	

Nota. Adaptado de "*Ranking de Empresas",* por Superintendencia de Compañías, Valores y Seguros, 2022. Ecuador

En cuanto a su distribución a nivel cantonal, las firmas se concentran en la ciudad de Guayaquil y Quito en un 42.52% y 39.18% respectivamente. Esto se debe a la afluencia de compañías que requieren servicios externalizados de auditorías de estados financieros, para atestiguar la razonabilidad de su información financiera (Superintendencia de Compañías, Valores y Seguros, 2022).

Tabla 3

Distribución a Nivel de Ciudad de las Firmas Auditoras en el Ecuador

Ciudad	Cantidad de Cías.	%
Guayaquil	662	42.52%
Quito	610	39.18%
Cuenca	55	3.53%
Machala	27	1.73%
Manta	19	1.22%
Samborondón	18	1.16%
Otras 52 ciudades	166	10.66%
Total	**1557**	

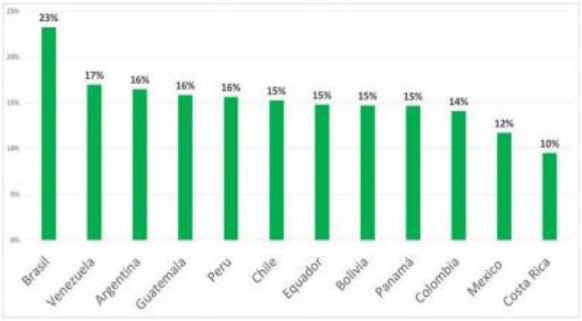
Nota. Adaptado de "*Ranking de Empresas",* por Superintendencia de Compañías, Valores y Seguros, 2022. Ecuador

En relación con los datos expuestos, se denota que la ciudad de Guayaquil concentra la mayor cantidad de firmas auditoras que forman parte del sector de servicio del país. De modo que, la investigación tomará en consideración a las PYMES que la conforman como población objeta de estudio.

Estadísticas de ataques que han sufrido las pymes en América latina.

Según el boletín de seguridad realizado (Kaspersky Lab., 2018) indico "Las pequeñas y medianas empresas son más propensas a recibir ataques por medio de emails (60%) y vectores offline (43%); es decir, USB contaminados". Se puede observar en la figura 2, que el país que ha sufrido de ataques informáticos es Brasil, Además, en el año 2017 Brasil también estuvo dentro de los 20 países más atacados a nivel mundial (Mejia & Romero, 2019). A continuacion, se muestra los paises afectados por ataques informaticos (Mejia & Romero, 2019).

Figura 5
Estadísticas de ataques informáticos a las Pymes a nivel mundial



Nota. Tomado de *Análisis de vulnerabilidad en un sistema de gestión de seguridad de información en un Pyme*, por Mejia y Romero, 2019. Universidad de Guayaquil de Ecuador.

Estadísticas mundiales de los sistemas de información

Una recopilación de información de la revista (Report, 2017), tomando en consideración Estados Unidos, Reino Unido, Alemania, Australia, Francia, Brasil, Japón, Italia, India, Canadá, Sudáfrica, el medio oriente (incluido el Emiratos Árabes Unidos y Arabia Saudita) demostró que el 47% corresponde a ataques maliciosos o criminales(externos), el 25% a fallas del sistema (internas)y el 28% a errores de falla humana de diferente índole (Mejia & Romero, 2019).

Figura 6
Estadísticas informáticas

Gráfico 1 Estadísticas Informáticas.

Nota. Tomado de *Análisis de vulnerabilidad en un sistema de gestión de seguridad de información en un Pyme*, por Mejia y Romero, 2019. Universidad de Guayaquil de Ecuador.

Definición del Problema

La liberación de eficiencias tecnológicas, la innovación de servicios a través de plataformas virtuales y la crisis de Covid-19 de 2019 han acelerado la transformación digital de los modelos de negocio tradicionales. Esto ha ocasionado diversos desafíos a nivel empresarial, como en el caso de la seguridad de la información (Pincay, 2021).

La situación presentada, se originó debido a la necesidad de las empresas en incorporar acciones de respuestas para adaptarse a los cambios constante del entorno económico, social, cultural, de salud y otros, para hacer frente al escenario pandémico. Esto incentivo a las empresas como las que pertenecen al sector de servicios tomar en consideración: (a) establecer planes de contingencia, en la que se establezcan políticas administrativas financieras, manejo de caja y capital de trabajo, (b) evaluar las diferentes alternativas de financiamiento, para la continuidad de sus operaciones, (c) desarrollar nuevas estrategias de negocio, (d) analizar la información financiera, donde se estime el impacto del COVID-19 y sobre la carga impositiva, y (e) definir protocolos de trabajos, mediante la evaluación de las estrategias de trabajo remoto, infraestructuras de comunicación y aplicación de las respectivas disposiciones laborales (Cornejo, 2021). Lo descrito denota diversas acciones tomadas por las

compañías, sin embargo, no enfocaron sus esfuerzos en lo referente en la seguridad de información, y su incidencia con la aceleración de la transformación digital de los modelos tradicionales de negocio.

Esta situación parte del auge sobre el manejo y administración de datos mediante el uso de infraestructuras ubicadas en la nube. La cual es considerada como una solución flexible y rentable para muchos servicios, representado un cambio importante en la tecnología de la información (IT) sobre recursos computacionales agrupados en ancho de banda, almacenamiento, servicios y aplicaciones. De manera que, la seguridad de información debe estar presente, no solo por la data que contiene o procesa, sino también porque en la actualidad está directamente relacionada con la privacidad del usuario. Sin embargo, las tecnologías están expuesta a diversidad de riesgos de seguridad de información como: (a) pérdida de datos, (b) sustracciones indebidas, (c) manipulaciones, (d) fraude, entre otros (Mártinez & Cruz, 2018).

En este contexto, las PYMES luchan constantemente para permanecer competitiva en el mercado, direccionado sus esfuerzos en reemplazar algunos procesos manuales por procesos automatizados con el propósito de agilizar la fluidez y sistematización de la información (financiera y no financiera), basadas en los principios de integridad, seguridad, veracidad, confiabilidad y equidad. Sin embargo, dichos cambios las exponen a diversidad de riesgos que indicien en la continuidad de las operaciones del negocio (Cornejo, 2021).

De la misma manera, con el panorama actual de las empresas que se encuentran en procesos de transformación digital como las PYMES, los desafíos en temas de ciberseguridad son notorios, lo cual se originan por factores como: (a) procesos internos, (b) cultura, (c) metodologías, (d) personas, entre otras. Además, en los dos últimos años con la aceleración en temas de desarrollo de tecnología y comercio electrónico también los delitos cibernéticos incrementaron a la par y en mayor proporción, hasta llegar a un 400% de incremento (Ramos, 2022).

En un estudio reciente sobre el manejo de información por parte de las PYMES en el Ecuador, se denotó que se encuentra dispersa, como, por ejemplo: (a) datos del personal, (b) informes, (c) cotizaciones, (d) documentos de contabilidad, (e) datos e información confidencial de clientes, entre otros. Esto se debe principalmente por su

almacenamiento en diferentes computadores sin seguridad, los cuales tienen acceso cualquier persona interna o en su efecto externas. Esto incide en la vulnerabilidad de posibles eventos como: perdida de información, y robo por terceros. Situación que se origina, por la poca importancia de implementar algún recurso tecnológico y la falta de conocimiento sobre seguridad de información (Jurado, Redín, & Jumbo, 2021).

Las prácticas de seguridad de información en las PYMES son diversas, pero comúnmente se centra en la restricción del acceso al sistema o parte del sistema. Asimismo, en lo referente a la modificación dentro de los límites de cada autorización. Sin embargo, las amenazas que se presentan se deben a que los propios usuarios no tienen en cuenta las vulnerabilidades que existen por el mal manejo de los sistemas y sus aplicativos, como, por ejemplo: (a) descargar archivos peligrosos, (b) eliminación de archivos importantes para el sistema, (c) programas maliciosos como virus o programas malignos, entre otros. De la misma manera, la falta de políticas relacionadas con: (a) confidencialidad, (b) integridad, y (c) disponibilidad de información (Figueroa et al., 2017).

En un estudio que se realizó a diversas empresas de categoría PYMES en Ecuador, se determinó la existencia de problemas de seguridad de información, las cuales se relacionan a factores con: (a) desconocimiento sobre aplicación de normas de seguridad de la información, (b) limitaciones en la administración de seguridad informática y de información, (c) mínima cultura en seguridad de información,(d) falta de responsables designados, (d) ausencia de políticas y procedimientos, (e) falencias en el manejo de activos informáticos, (f) competencia limitada del personal, entre otras. De manera que, resultó imperioso la aplicación de análisis y evaluación de riesgos, la verificación de controles de seguridad para la determinación de las causas de vulnerabilidades y en la búsqueda de soluciones aplicables para su mitigación. Por tanto, la ISO 27001 como sistema de gestión de seguridad de información controla las vulnerabilidades, amenazas y los riesgos de seguridad a que se ve expuesta las entidades (Solarte, Enriquez, & Benavides, 2015).

Lo expuesto, denota la importancia de que las empresas incluyan sistemas de seguridad de información para protección de esta. Además, de que impulsaría en el crecimiento empresarial. Entre los estándares más empleado se destaca la norma

ISO/IEC 27001 que forma parte de un conjunto de estándares desarrollados por la Organización Internacional de Estandarización. En esta se define un sistema de gestión de seguridad de la información que se aplica a todo tipo de empresas, como las de servicios.

Esto se debe a que la implantación oportuna de los requisitos de la ISO 27001 de seguridad de la información, permiten la reducción del impacto de los riesgos y amenazas. Además, promueve mejoras en la planificación, la gestión de la seguridad de los negocios, y garantías de continuidad d en caso de contingencia. Por consiguiente, da cumplimiento de normativas nacionales y mayores prestigios ante la competencia (Figueroa et al., 2017).

En relación con casos de éxitos, se destacan a las PYMES colombianas, en las cuales se ha promovido la importancia sobre la seguridad de los sistemas de información. En estas se denotaron que su alcance ha evolucionado favorablemente en las organizaciones y se ve reflejado en la implementación de diferentes mecanismos inmersos en la gestión tecnológica como la ISO 27001, permitiendo salvaguardar uno de los activos más importantes de los negocios como es la información. Esto ha permitido que las PYMES posean políticas y normas de seguridad implementadas que facilitan asegurar la integridad y la confiabilidad de los sistemas de información, incluyendo la disponibilidad de datos (Riascos et al., 2014).

En Ecuador, el sector servicios ocupa un lugar importante en la economía del país, ya que es uno de los principales motores del crecimiento. Además, proporciona gran parte de los empleos y agrega valor a otros sectores económicos mejorando sus ventajas competitivas y desempeño, como, por ejemplo: (a) sector manufacturero, (b) sector de comercio al por menor, (c) transporte, (c) servicios financieros, entre otros. Dicho en otras palabras, las actividades de servicios se encuentran integrados en las distintas etapas de una cadena de valor de los negocios (Camino, Bermudez, Chalen, Gutierrez, & Romero, 2018). Es importante destacar que, para propósito de la investigación se tomará en consideración el panorama actual de las **firmas de auditoría tipo PYMES** que pertenecen al subsector de actividades jurídicas y de contabilidad de la ciudad de Guayaquil, tomando en cuenta que como parte de sus

servicios es mantener la confidencialidad y protección apropiada de la información de sus clientes para evitar la fuga de datos confidenciales.

En relación con lo expuesto, se pretende el diseño de un análisis para la aplicación de la norma ISO 27001 en firmas de auditoría tipo PYMES, año 2022 que pertenecen al sector de servicios, como buenas prácticas enfocada en mantener la mejora continua en la gestión de la seguridad de información, lo cual contribuirá a la mitigación de riesgos de TICS y el cierre de brechas de controles.

Justificación de la Investigación

A nivel académico se pretende aportar con un análisis que contribuya al aprendizaje y entendimiento del alcance de la ISO 27001 como buenas prácticas enfocada en mantener la mejora continua de la seguridad de información, mediante acciones que permitan la mitigación de riesgos de seguridad de información y el cierre de brechas de controles. Esto se debe a que la norma presenta una serie de requisitos que se ajusta a todo tipo de negocio para proporcionar un modelo consistente que permite: (a) establecer, (b) implementar, (c) monitorear, (d) revisar y (e) mantener un Sistema de Gestión de Seguridad de la Información (SGSI). De igual forma, existen estudios enfocados en su implementación y seguimiento no explícitamente en el sector de servicio, sin embargo, permite la ilustración de enfoques para su adaptación. Esto permitirá que los estudiantes de la Universidad Católica de Santiago de Guayaquil cuenten con las competencias necesarias para formar parte de los equipos responsables en la adopción de nuevas prácticas relacionadas a la seguridad de información. De la misma manera, servirá de material de consultas para el desarrollo de nuevas investigaciones.

A nivel social y económico, el análisis podrá utilizarse como una guía didáctica para que las firmas de auditoría tipo PYMES que forman parte del sector de servicios puedan incorporar principios y prácticas relacionadas a la seguridad de información, considerando que la norma ISO 27001 posee requisitos que aportan un Sistema de Gestión de la Seguridad de la Información (SGSI), consistente en medidas orientadas a proteger la información, indistintamente del formato de la misma, contra cualquier amenaza, de forma que garanticemos en todo momento la continuidad de las actividades de la empresa.

Objetivos

Objetivo general

Analizar la aplicación de la norma ISO 27001 en PYMES del sector servicios de la ciudad de Guayaquil para el fomento de una gestión apropiada de seguridad de información con base en un diagnóstico del estado actual de la seguridad de la información en las Pymes seleccionadas.

Objetivos específicos

- Fundamentar teórica, conceptual, referencial, legal y de forma normativa que justifica la ISO 27001 y su aplicación en la seguridad de información en PYMES del sector servicios de la ciudad de Guayaquil.
- Establecer un análisis y el modo de recopilación de información sobre los problemas que inciden en la seguridad de información como riesgos (perdida de información, sustracciones, o adulteración de datos) y ausencia de controles en PYMES del sector servicios de la ciudad de Guayaquil.
- Realizar un diagnóstico del estado actual de la seguridad de la información en las Pymes seleccionadas para identificar las principales brechas y desafíos en la implementación de la Norma ISO 27001 en estas empresas.

Preguntas de investigación

- ¿Cuáles son los requisitos administrativos, técnicos y operativos que requiere una PYMES para aplicación de la ISO27001?
- ¿Cuáles son los problemas de seguridad de información que enfrentan las PYMES del sector servicios de la ciudad de Guayaquil?
- ¿Qué oportunidad representaría la ISO 27001 en la gestión de la seguridad de la información en PYMES del sector servicios de la ciudad de Guayaquil?

Limitación

La investigación durante su ejecución puede presentar limitaciones en diversos indoles como la obtención de estudios comparables relacionados ISO 27001, como: (a) casos de éxitos de implementación en empresas de servicios en Ecuador, (b) estudios sectoriales sobre el impacto de la seguridad de información en las PYMES, entre otras. De la misma manera, se podría presentar barreras que incidan en la participación de PYMES del sector servicios durante el levantamiento de datos primarios por situaciones como: (a) confidencialidad de información, (b) miedo de los participantes al informar las debilidades de negocios, (c) protección de la reputación de la entidad, entre otras. En concordancia con lo descrito, las limitantes se subsanarán promoviendo el levantamiento de datos mediante el uso de herramientas de comunicación como formularios de Microsoft o Google asegurando la confidencialidad de la razón social del negocio y el anonimato de los datos recogidos

con el propósito de obtener información más detallada sobre la problemática de estudio. Además, con el fin de prevenir la no obtención de información, se invitará a expertos en auditoría y consultoría seguridad de información que posean experiencia relacionada con la implantación de la ISO27001 y sobre los problemas que enfrentan las PYMES del sector de servicios. Datos que permitirán la elaboración de hallazgos para su discusión y servirán de base para el diseño del respectivo análisis.

Delimitación

El análisis se delimita en la ciudad de Guayaquil, considerando que en esta se concentra gran parte de las PYMES del sector. Esto se debe a que el sector presenta una creciente dependencia de la tecnología y de la información digital, lo que hace que la seguridad de la información sea especialmente relevante para estas empresas. En cuanto al tamaño de las empresas, nos centraremos en las PYMES, debido a que suelen presentar escases de recursos para implementar sistemas de seguridad de la información a gran escala, pero aun así se enfrentan a riesgos significativos de seguridad de la información. Además, se toma como población objetiva a las empresas dedicada a la actividad económica de servicios de auditorías, considerando que este tipo de negocio maneja información confidencial de sus clientes. Por tanto, la seguridad de información resulta imperiosa para prevenir diversidad de riesgos como: (a) perdida, (b) sustracciones, (c) robo, entre otras.

Geográfico: Ciudad de Guayaquil

Sectorial: Sector servicio

Subsector: Servicio Actividades Jurídicas y de Contabilidad (CIIU M69)

Actividad económica especifica: servicios de auditorías

Tamaño de Compañía: PYMES

Tiempo: 2023

Capítulo 1: Fundamentación Teórica

Marco Teórico

Teoría de la Empresa

La gestión interna de los negocios fue un tema secundario para la escuela clásica del pensamiento económico, por consiguiente, centró sus esfuerzos en investigaciones relacionadas con el entorno externo de las empresas, sin observar diversas situaciones que afectan a los procesos internos. Esta situación motivó a la teoría de la empresa a enfatizar sobre la falta de interés de las organizaciones para la realización de evaluaciones sobre sus procedimientos internos y la efectividad de los controles que aplicaban. Estas cuestiones surgidas en el contexto interno de los negocios que no se resolvieron en el ámbito de la teoría económica, se convirtió en el eje central de la teoría de la empresa, además, fue promovida por los requerimientos de las partes interesadas. De modo que, Coase en 1973 con la propuesta de "costo de transacción" promovió la importancia de considerar los parámetros internos de las empresas como gobierno y estructura de control en las evaluaciones internas. En esta teoría también destaca el alcance de los agentes en la aplicación de contratos para el direccionamiento de los esfuerzos para conseguir objetivos comunes, lo cual condujo a resultados favorables para los negocios (García et al., 2012).

La teoría de la empresa indicó que el objetivo principal de los negocios es concentrarse en la creación de beneficios económicos, por lo que enfatiza la importancia de la gestión interna. Coase (1973) destacó que "las empresas se clasifican como contratos que permiten la jerarquización de posiciones para mitigación de las incertidumbres que puedan afectar las operaciones del negocio" (p. 20). De modo que, la estructura contractual juega un rol importante en las empresas, permitiendo que los propietarios entreguen recursos y responsabilidades a los administradores (agentes) en la búsqueda de beneficios compartidos, basada en el cumplimiento de metas previamente acordadas. La teoría de la empresa se centra en elementos que se relacionan con el comportamiento de los agentes. Estos se desempeñan en distintas áreas de la organización enfatizando actividades de: (a)

dirección, (b) control y (c) supervisión. Es decir, dependerá de la estructura de propiedad y de los incentivos para la concentración de la propiedad del negocio, tales como (a) el número de propietarios y (b) sus relaciones con los directores (Coase, 1973).

La teoría de la empresa hace mención sobre los riesgos implícitos en el contexto de los negocios, en concordancia con la estructura de propiedad y relación de agentes (dueños, directores, empleados e inversionistas). De modo que, las prácticas de auditoría se enfocan en promover aseguramiento y atestiguamiento sobre la razonabilidad de la información financiera de las empresas. No obstante, no están exentas a situaciones de incertidumbres en sus prácticas que pueden incidir en su continuidad y reputación, como lo es el fraude y error al carecer de prácticas apropiadas que aseguren la calidad de los encargos de auditoría. Considerando el alcance de la teoría, las malas prácticas empresariales pueden ocasionar costos de no calidad que representan pérdidas económicas.

Las organizaciones, según la teoría de la empresa, representa una serie de contratos destinados a la creación de incentivos para aplicación de soluciones a problemas subyacentes con la coordinación interna. Esta situación impulsó a Coase para proponer a las empresas como sustituto de la coordinación interna, visión que fue compartida por otros defensores de la teoría de la empresa como Hart (1986), quien afirmó que "los procesos los procesos de negocios son complejos para no evidenciar la diferenciación del alcance de los contratos," (p. 18).

Los acuerdos de las empresas generan dudas persistentes sobre los derechos de propiedad, convirtiéndose en disputas que requieren la intervención de un juez para resolver las diferencias. Como agente principal en esta situación, la empresa es responsable de separarse de otros agentes en términos de toma de decisiones. Los niveles de producción organizacional se basan en variables que ningún agente principal, actuando solo o en parte, puede controlar en su totalidad. De modo que, requiere la participación de agentes adicionales. Los contratos son vistos en este contexto como expresión de las relaciones humanas en los negocios (Hart, 1986).

La idea de los costos de transacción se amplía cuando la atención se centra en eludir las restricciones contractuales. Esta práctica es imprevisible en el

mundo de los negocios donde los socios o accionistas deben tomar decisiones sobre incógnitas. La empresa fue fundada para frenar las acciones oportunistas de los agentes, lo que le hace velar por la gestión interna de la empresa. Sin embargo, no se reduce a una función de costos de transacción sino a acciones tomadas para fortalecer el sentido de identidad de la entidad (Williamson, 1975).

Coase (1937) señaló que a medida que aumentan los costos del mercado, la opción de internalización de las transacciones puede disminuir el impacto de los costos. En el contexto externo de los negocios, los recursos se promueven de manera eficiente o ineficiente sobre el número de empresas, que sustenta su desempeño. Williamson (1975) señaló que, aunque el uso de contratos no elimina por completo los costos de transacción, pueden disminuir el impacto de los contratos en la economía. Lo que indica que las empresas nacen de un arreglo contractual. En relación con la gestión de las firmas auditoras y sus servicios, la teoría de la empresa hace mención sobre la importancia de que los agentes promuevan mejoras internas adoptando prácticas como la de gestión de seguridad de la información que contribuye en la minimización de la exposición a riesgos de TIC que pueden incidir en la pérdida de información confidencial y continuidad de las operaciones del negocio.

Teoría Prospectiva

La teoría prospectiva explica cómo las personas toman decisiones en situaciones inciertas al tener una variedad de opciones financieras en una situación de riesgo. Esta teoría Fue creada para proporcionar un modelo descriptivo preciso de la toma de decisiones humanas y se basa en varios apartados empíricos tipo experimental sobre la conducta de elección humana. Es importante recalcar que dada decisión se basó principalmente entre una variedad de apuestas monetarias (Kahnema & Tversky, 2014). Esta teoría busca explicar la relación psicológica del ser humano con el comportamiento económico en momentos de inseguridad y desconfianza, esta conducta ha sido objeto de estudio en diversos ámbitos desde hace varios años y el riesgo es un factor que predomina previo y posterior a tomar una decisión.

La toma de decisiones bajo el análisis de riesgo clasifica los resultados como ganancias o utilidades si superan las expectativas y pérdidas si no alcanzan el punto de referencia. Los individuos deben evaluar el resultado en relación con su nivel de adaptación en relación con la superación de las expectativas. La sensibilidad y la aversión a la pérdida como paso final en la toma de decisiones son dos factores adicionales que esta teoría considera. El ser humano es aún más reacio a la hora de tomar decisiones en el día a día y pasa a depender del mercado para corregir lo irracional y construir marcos de contingencia con probabilidades de que ocurra un evento (Kahnema et al., 2014).

Las personas tratan los resultados que se consideran verdaderos o imposibles de formas muy diferentes. Esto se ilustra mediante la función de ponderación, que define la evaluación y contiene dos ideas críticas que se describen a continuación: (a) los resultados que se consideran ciertos, y (b) los resultados se consideran imposibles. La mayoría de las personas trata los sucesos extremadamente improbables como imposibilidades y los sucesos extremadamente probables como si fueran a ocurrir. Las personas también tienden a dar más importancia a los eventos de baja probabilidad. Asimismo, dan menos consideración psicológica a los resultados de probabilidad media y alta (Kahnema et al., 2014).

Los expertos han utilizado la teoría de la prospectiva en una variedad de situaciones, particularmente cuando se trata de relaciones internacionales y política comparada. La teoría se ha utilizado en política comparada para explicar la naturaleza del riesgo en la reestructuración económica de los países latinoamericanos, y se ha utilizado en relaciones internacionales para tratar de explicar la toma de decisiones que implican riesgos aparentemente irracionales, como continuar incurriendo en costos irrecuperables (McDermott, 2017). En conclusión, la teoría prospectiva describe cómo los individuos hacen una elección entre alternativas probabilísticas donde el riesgo está involucrado y la probabilidad de diferentes resultados es desconocida. De modo que, se denota la necesidad de que las empresas como en el caso de las firmas auditoras que ofrecen una variedad de servicio incorporen buenas prácticas de gestión de seguridad de información, como las que propone la ISO27001 para asegurar la protección de datos sensibles propios y de sus clientes.

Teoría de Gestión de Riesgo

La gestión de riesgos y sus requisitos son una nueva tendencia para muchas empresas, ya que enfrentan el desafío de comprender y gestionar la gestión de riesgos desde una nueva perspectiva. La identificación y análisis de riesgos es la tarea principal de la empresa. La gestión de riesgos está relacionada con la planificación estratégica. Como parte de la fase del ciclo de planificación estratégica, la identificación de riesgos debe realizarse al menos una vez al año mediante análisis paramétrico (entorno externo e interno). A medida que evoluciona el componente de gestión de riesgos del estándar de control interno de la empresa, puede afectar el logro de los objetivos declarados de la organización (Albán et al., 2018).

La incertidumbre es cuando no estás seguro de lo que sucederá en el futuro. El riesgo es una incertidumbre "importante" porque afecta el bienestar humano. Toda situación de riesgo es incierta, pero puede haber incertidumbre sin riesgo. Las organizaciones de todo tipo y tamaño enfrentan factores e influencias internos y externos que crean incertidumbre sobre cuándo se alcanzarán sus objetivos. Esta incertidumbre crea un riesgo de impacto en el logro de los objetivos organizacionales. Todos los procesos de gestión de riesgos tienen un factor común: identificación de riesgos, análisis, evaluación y tratamiento del nivel de riesgo. Sin embargo, el análisis del contexto es un aspecto esencial, porque es precisamente en él donde radica la especificidad de la acción a evaluar (Albán et al., 2018).

Se reconocen reglas internacionales y diversos modelos y herramientas de gestión de riesgos para crear procesos lógicos y sistemáticos para una toma de decisiones eficaz. Al respecto, dijo: "Los modelos identifican y preparan para posibles escenarios y son acciones tomadas para evitar y reducir los costos u otros impactos de un evento, no cuando ocurre el evento. Actuar en consecuencia". "El incidente ha ocurrido y ha resultado en el coste de restablecer la situación." Los procedimientos recomendados en AS/NZS 4360 (Standardisation Australia and New Zealand, 1999), ISO 31000 e ISO 31000 (Organización Internacional de Normalización, 2010) son enfoques para el desarrollo de la gestión de riesgos. Asimismo, determinadas industrias (aviación, transporte marítimo, gestión de proyectos, etc.) cuentan con

procesos de gestión de riesgos específicos de su situación y su documentación no hace referencia a normas (Albán et al., 2018).

Existen otros modelos para la gestión de riesgos que utilizan una serie de modelos de procesos lógicos y sistemáticos que pueden utilizarse en la toma de decisiones para aumentar la eficiencia y eficacia, entre ellos los llamados Boehm, McFarlan, Magerit, que se utilizan en gestión de proyectos (Albán et al., 2018).

Tanto los modelos estándar como otros modelos permiten la cuantificación de los niveles de riesgo. El cálculo del nivel de riesgo puede ser cuantitativo o cualitativo, aunque este último tiene incertidumbres, es el más aceptable. Los cálculos cuantitativos permiten evaluar el valor económico de los impactos, aunque los resultados pueden llevar tiempo y complicar la investigación (Albán et al., 2018).

Teoría de la seguridad de información

La seguridad informática, o seguridad de las tecnologías de la información, es un área de las tecnologías de la información que se enfoca en la protección de la infraestructura informática y todo lo relacionado con ella, especialmente la información que contiene o difunde. Para ello, existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes diseñadas para reducir los riesgos a los que puede estar expuesta la infraestructura o la información. La seguridad informática incluye software (bases de datos, metadatos, archivos), hardware y todo lo que una organización valora, y si esta información confidencial cae en las manos equivocadas, como por ejemplo convirtiéndose en información privilegiada, representa un riesgo (Universidad del Valle de México, 2020).

El análisis de riesgos, también conocido como evaluación de riesgos o PHA (abreviatura de Process Hazards Analysis en inglés), es el estudio de las causas de posibles amenazas y posibles eventos inesperados, así como de los posibles daños y consecuencias de estos. Este tipo de análisis se utiliza ampliamente como herramienta de gestión en la investigación financiera y de seguridad para identificar riesgos (métodos cualitativos) y evaluarlos de otro modo (generalmente métodos cuantitativos). El primer paso en el análisis es proteger o evaluar los activos. La evaluación de riesgos implica comparar el nivel de riesgo descubierto durante el

análisis con criterios de riesgo previamente definidos (Universidad del Valle de México, 2020).

Los elementos del sistema de información constan de 6 elementos claramente identificables:

- Base de datos: lugar donde se almacena toda la información necesaria para tomar una decisión. Esta información está organizada en registros específicos e identificables.
- Transacción: Corresponde a todos los elementos de la interfaz que permiten a los usuarios ver, agregar, modificar o eliminar registros de información específicos. · Informes: corresponde a todos los elementos de la interfaz a través de los cuales el usuario puede obtener uno o más registros y/o estadísticas (contar, sumar) según criterios de búsqueda y selección definidos.
- Proceso: Corresponde a todos los elementos que recuperan información de la base de datos y generan nuevos registros de información según una lógica predefinida. Estos procesos sólo los controla el usuario (por eso se muestra como una línea discontinua). Usuarios: Identifica a todas las personas que interactúan con el sistema, desde la alta dirección que recibe informes estadísticos hasta los usuarios operativos responsables de recopilar e ingresar información en el sistema.
- Procedimientos de gobernanza: corresponden al conjunto de reglas y políticas de la organización que rigen el comportamiento de los usuarios frente al sistema. En particular, deben garantizar que los usuarios no puedan en ningún caso obtener acceso directo a la base de datos.

La seguridad informática, o seguridad de las tecnologías de la información, es un área de las tecnologías de la información que se enfoca en la protección de la infraestructura informática y todo lo relacionado con ella, especialmente la información que contiene o difunde. Para ello, existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes diseñadas para reducir los riesgos a los que puede estar expuesta la infraestructura o la información. La seguridad informática incluye software (bases de datos, metadatos, archivos), hardware y todo

lo que una organización valora, y si esta información confidencial cae en las manos equivocadas, como información privilegiada, representa un riesgo. La definición de seguridad de la información no debe confundirse con la definición de "seguridad informática", ya que esta última sólo es responsable de la seguridad del entorno informático, pero la información se puede encontrar en diversos medios o formas, y no solo en los medios informáticos. La seguridad informática es una disciplina que se ocupa del desarrollo de estándares, procedimientos, métodos y técnicas encaminados a crear un sistema de información seguro y confiable. En pocas palabras, la seguridad en un entorno de red es la capacidad de identificar y abordar vulnerabilidades (Universidad del Valle de México, 2020).

Teoría de la mejora continua

Mantener la seguridad de la información corporativa requiere no solo implementar un sistema de gestión de seguridad de la información, sino también mantener y mejorar las medidas de seguridad. Si su empresa cuenta con un excelente sistema de gestión de seguridad de la información, no lo deje pasar por alto. La excelencia radica en la mejora continua del sistema, no sólo en su implementación. Todas las empresas, independientemente de su industria, enfrentan cada día muchos riesgos e incertidumbres provenientes de diversas fuentes. La norma ISO 27001 es una solución de mejora continua adecuada para evaluar diversos riesgos y establecer políticas y controles adecuados para garantizar la protección y protección de la información. Por tanto, el sistema de gestión de seguridad de la información de la norma ISO 27001 sigue un enfoque basado en los procesos utilizados en el ciclo de Deming, o ciclo de mejora continua, que incluye planificación, ejecución, verificación y operación (Seguridad de la información, 2018).

El ciclo de Deming en un sistema de gestión de seguridad de la información basado en la norma ISO 27001 tiene indicadores y medidas que pueden usarse para medir la efectividad de los distintos controles utilizados. De esta forma, proporciona datos reales relacionados con la seguridad de los sistemas de información. Utilizando estos datos, se pueden crear mecanismos de advertencia y se pueden realizar las correcciones apropiadas. Es importante señalar que la norma ISO 27001 es un sistema

activo e integrado en una empresa orientado hacia los objetivos comerciales y hacia adelante. En este sentido, es muy importante señalar que cada vez que una empresa introduce una nueva herramienta TIC, es necesario actualizar el análisis de riesgos para reducir y minimizar los riesgos de implementar la nueva herramienta (Seguridad de la información, 2018).

La certificación basada en la norma ISO 27001 se utiliza para implementar un sistema de gestión de seguridad de la información en una organización. Gracias a las nuevas tecnologías y a la globalización, la proliferación de sistemas informáticos ha traído beneficios, pero también peligros. La certificación ISO 27001 fue creada para promover la gestión de la seguridad de la información, es decir. apoyar sus principios fundamentales. Este estándar describe cómo gestionar la seguridad de la información en una organización. Por tanto, tiene 10 pilares:

- La certificación ISO 27001 garantiza que la información sea accesible sólo para el personal autorizado y no accesible para nadie sin la autorización adecuada.
- La información debe permanecer intacta y sólo puede ser modificada por personas con la autoridad adecuada.
- La información debe estar disponible cuando los usuarios autorizados deban tener acceso a ella.
- Debe existir un proceso, personas y tecnología para analizar el riesgo de la información.
- Las medidas anteriores deben prevenir o reducir los riesgos de seguridad de la información a través de un ciclo de mejora continua.
- La ISO 27001 define un sistema de parámetros que se deben seguir para gestionar la seguridad de la información.
- Implantación y operación del sistema. Cualquier organización que cumpla con la norma ISO 27001 debe tomar medidas para implementar y operar el sistema.
- Mantener y mejorar el sistema. Esta es otra filosofía que deben seguir las empresas certificadas según ISO 27001.

- Sistema de revisión. Se trata de una acción de mejora a realizar para detectar y reducir errores.
- Las empresas con certificación ISO 27001 tienen que comprometerse a la recertificación, lo cual es más difícil que obtenerla, porque en la primera auditoría te puedes permitir el lujo de no poner muchos controles, incluso los que ya están bien, pero en la recertificación mejores controles debe desarrollarse a medida que continúa el ciclo de mejora continua (Seguridad de la información, 2018).

Marco Conceptual

Sistema de gestión

Un sistema de gestión se compone de una serie de componentes conectados que nos ayudan a hacer crecer nuestra empresa. Se entiende por negocio la actividad a la que se dedica una organización, ya sea pública, privada, con o sin fines de lucro. Tanto las organizaciones públicas como las privadas se estructuran en torno a un sistema de gestión, que les permite producir los bienes y servicios que los clientes o usuarios necesitan (Calso et al., 2019). Por tanto, todas las empresas disponen de un sistema de gestión, que podrá estar más o menos dotado y/o formalizados, pero que sin lugar a dudas existirá, pues sin estos no serán posible desarrollar un negocio.

Los principales elementos que conforman un sistema de gestión son los siguientes: (a) procesos, representan un conjunto de actividades o tareas mediante las cuales unas entradas (inputs) se convierten en unas salidas o resultados (outputs), asimismo, constituyen los métodos de trabajo necesarios para poder generar los productos y servicios que se entregarán a los clientes (internos o externos), (b) productos y servicios, son el resultado de los procesos, que serán entregados a los clientes que los adquieran, (c) clientes y otras partes interesada, es el elemento que establece directa o indirectamente las características que han de tener los productos y servicios, (d) recursos, este elemento se emplea en los procesos para la creación de los productos y servicios, (e) infraestructura, son los edificios, máquinas, herramientas, vehículos y sistemas de información necesarios para desarrollar la actividad de la

organización, (f) materiales, materias primas, insumos, información, entre otros, utilizados principalmente en los procesos para la generación de los productos y servicios, y (g) estructura organizativa son los roles, responsabilidades y autoridades que las personas de la entidad utilizan para organizarse internamente y coordinar el trabajo (González et al., 2017).

Documentación del Sistema de Gestión de Calidad

Cada organización tiene un conjunto de documentos que utilizan como base para hacer crecer su empresa. Las organizaciones más simples suelen conservar registros manuales, instrucciones de funcionamiento de las máquinas, permisos o licencias necesarios para realizar la actividad, entre otros. Documentos que enumeran los resultados o dan prueba de las acciones tomadas (González et al., 2017).

Figura 7
Representación de la pirámide documental de un sistema de gestión

Nota. Tomado de *Sistema de Gestión de Calidad,* por González y Arciniegas, 2017. Colombia. Ecoe Ediciones.

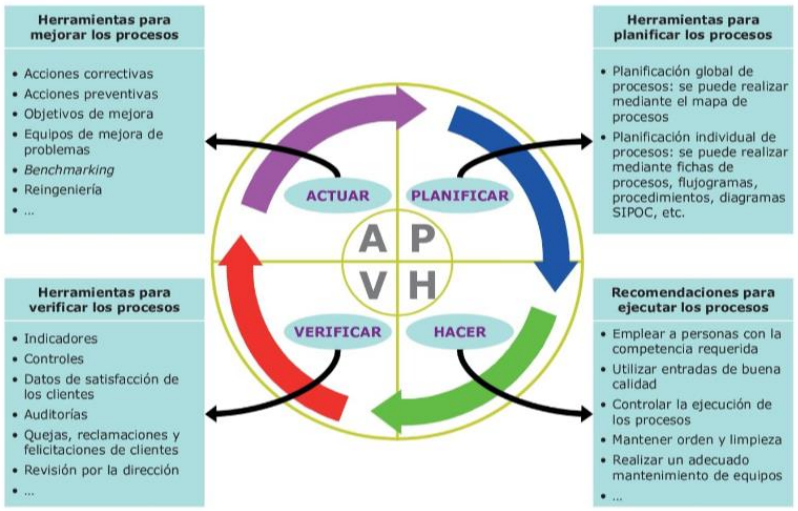
Todos los elementos descritos se encuentran interrelacionados entre sí, y globalmente conforman el sistema de gestión de la organización, mediante el que esta desarrolla su negocio. El sistema de gestión no es inmutable, por el contrario, cambia permanentemente, ya que, si uno de sus elementos cambia, también lo hace el sistema. Además, el funcionamiento del sistema de gestión es el resultado de la interacción de sus elementos, que deben acoplarse unos a otros y adaptarse a las influencias internas y externas que van apareciendo en el tiempo, y que marcan su comportamiento. Su importancia es de tal magnitud que todas las normas destacan que en el establecimiento del sistema de gestión se tengan en cuenta los procesos necesarios y sus interacciones (González et al., 2017).

Ciclo PHVA

Es una buena práctica identificar los procesos para tener un punto de referencia que permita su comparación a la hora de determinar si es una falla del proceso u otro tipo de problema. Identificar actividades por función o departamento y organizarlas de acuerdo con objetivos, insumos o productos compartidos puede ser un sustituto de los procesos determinantes. Cada uno de los procesos enumerados debe responder siempre a la definición del proceso. El inventario de procesos finalizado servirá como guía para la documentación de procesos posterior. La información detallada de las operaciones, entradas, salidas, agentes implicados, controles, etc. estará a nuestro alcance gracias a la documentación de las mismas, lo que permite la identificación con precisión de cada proceso y en su caso introducir a posteriori posibles modificaciones (Parra, López, & Ramírez, 2019).

El ciclo de mejora continua PHVA debe aplicarse a los procesos determinados para gestionarlos de la forma más eficaz. Esto significa que los procesos deben ser cuidadosamente planificados (P), ejecutados de forma controlada (H), verificados en su desempeño (V), y si se encuentran discrepancias, incidencias o áreas de mejora, deben mejorarse (A) (Parra et al., 2019).

Figura 8
Gestión de Procesos mediante PHVA



Nota. Tomado de *gestión de la Competitividad Empresarial,* por Parra, López y Ramírez, 2019. Colombia. Ecoe Ediciones.

Se pueden encontrar muchos procesos diferentes en el sistema de gestión de una organización, y se pueden categorizar en las siguientes categorías: (a) procesos de gestión, estratégicos o de gestión, que son aquellos que la dirección ejecuta o en los que la dirección tiene un papel importante. Típicamente, su ámbito se restringe a los procesos involucrados en la estrategia y el control de gestión global, así como (b) los procesos operativos, también denominados procesos productivos, centrales, comerciales, principales, misionales, clave, etc. Estos son los procedimientos utilizados. para crear los bienes y servicios que se proporcionan a los clientes. Son únicos para cada negocio porque cada uno produce bienes y servicios únicos, y (c) los procesos de apoyo o auxiliares son aquellos que ayudan al crecimiento adecuado de los otros dos tipos de procesos al proporcionar típicamente recursos para su operación (Parra et al.,2019).

Tecnologías Centrales y de Gestión

Las tecnologías centrales permiten la transformación de datos de entrada en productos finales. Esta se basa en el conocimiento sobre las necesidades de la empresa, y encuentra formas de coordinar actividades como: (a) producción, (b) logística, (c) finanza, (d) administración, entre otras, tanto en los procesos administrativos como el desarrollo del software necesario para cada uno de los procesos anteriores (Scheel, 2017).

Las tecnologías de gestión son aquellas que utilizan conocimientos que parten de cambios sucesivos, transformando un carácter en otro para desarrollar procesos básicos que llamamos operaciones en una organización. Así como existen normas que rigen el diseño y fabricación de productos y procesos, también existen normas administrativas que definen los parámetros para la realización de actividades dentro del mismo ámbito regulatorio. La gestión de la tecnología, el conocimiento y la innovación en las organizaciones forma parte de la gestión tecnológica (Rodríguez, 2019).

La innovación puede referirse tanto a la tecnología básica relacionada directamente con los productos como a la tecnología de gestión vinculada con la gestión del mercado y la organización. Si una empresa no dispone de tecnologías de

gestión, no podrá utilizar su potencial de innovación, aunque sea tecnológicamente competente. Sin embargo, existen tecnologías centrales que también se utilizan para la gestión. Además, la innovación se vuelve aún más necesaria cuando hace que los productos existentes no sean competitivos debido a los avances tecnológicos, como: (a) los telégrafos, o (b) las máquinas de escribir, y se vuelve parcialmente innovadora cuando los productos existentes aún compiten entre sí, como: (a) teléfonos móviles y (b) Internet (Romero, 2018)

Tecnologías de la Información y la Comunicación (TIC)

Este nuevo concepto, introducido como TIC, tecnología de la información y la comunicación, se aplica a todo lo que implica la combinación de dos conceptos, comunicación e informática, que se ha producido desde la aparición de Internet. Las TIC abordan todos los aspectos sociales de la interacción de ambos conceptos. Estas nuevas tecnologías de la información se han convertido en herramientas informáticas que procesan, almacenan, sintetizan y recuperan información de todas las formas conocidas. También incluye todos los soportes y canales utilizados, como computadoras, internet, tecnología IP y más (Slusarczyk et al., 2018)

Ciclo Tecnológico

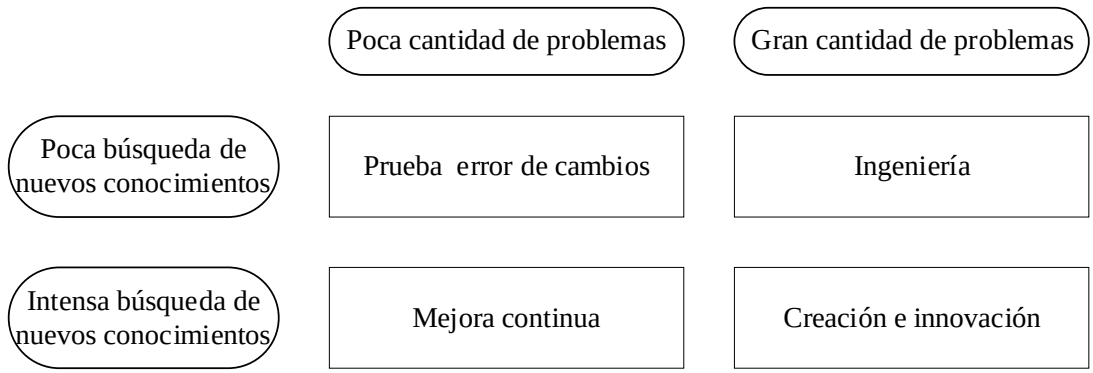
El ciclo tecnológico comienza cuando surge una nueva tecnología que puede ser incremental, es decir, que emerge lentamente, o fundamental o revolucionaria, es decir, a medida que la tecnología mejora con el tiempo y se expande. Este ciclo culmina cuando se vuelve más predominante, se vuelve dominante y comienza a desaparecer a medida que es reemplazada por una nueva tecnología fundamentalmente nueva o revolucionaria, que también declina, pero lo hace más lentamente. todavía te permite permanecer en un nicho. Esta a su vez generan nuevos ciclos de productos que no necesariamente se superponen. Estos ciclos se caracterizan por un patrón dominante y la posterior separación de sustitución de productos. Los lapsos de tiempo que ocurren están relacionados con la mejora continua del producto (Pérez, 2022). La forma dominante de tecnología está asociada con los procesos de innovación tecnológica subyacentes y las etapas de cambio gradual están asociadas con la

innovación paso a paso. Las grandes innovaciones que crean nuevos consumos, estos saltos tecnológicos, se trata de innovaciones fundamentales

Impacto Tecnológico en la Resolución de Problemas

La tecnología es un proceso de resolución de problemas en dos aspectos diferentes: (a) la medida en que un problema en particular requiere el descubrimiento de nuevos conocimientos adicionales, y (b) la variedad y complejidad del problema. y pedir buscar más que soluciones de una determinada manera (Franklin, 2016). Las bases estas dos dimensiones se definen a continuación distintos tipos de estrategias de innovación:

Figura 9
Impacto de la Tecnología en la Resolución de Problemas



Nota. Tomado de *Comportamiento Organizacional. Enfoque para América Latina*, Segunda Edición, por Franklin, 2016. Pearson Educación de México SA. de C.V. México.

Gestión de Procesos y la Innovación

La visión dentro de una empresa se basa en un organigrama que existe para funciones como: (a) administrativas, (b) financieras, (c) comerciales, (d) fabricación, entre otras. Esto ha permitido la partición de áreas por responsabilidad que limitan en divisiones individuales. Esto ocasionado el surgimiento de nuevas necesidades en las empresas para mantener su competitividad. Es claro que existen empresas conocidas y respetadas pero dispersas internamente, incapaces de tener capacidad de decisión y

otras pueden cumplir con una variedad de requisitos y con menos recursos, independientemente del tamaño de la empresa (Franklin, 2016).

Al considerar una empresa como un proceso, estas se dividen en dos categorías: (a) procesos críticos y (b) procesos de apoyo, la preparación de procesos importantes. Esto permite a la empresa realizar actividades multifuncionales que abordan diferentes perspectivas dentro de una organización enfocadas en el mismo objetivo general y en la satisfacción del cliente (Vasconcelos, 2019). De modo que, las empresas requieren una visión compartida que se comunica entre diferentes departamentos tratando de relacionar temas en otras áreas. Además, la gestión de procesos implica administrar el conocimiento y la tecnología para la continuidad de las operaciones del negocio. Por lo tanto, cada proceso contiene conocimiento tecnológico y cada mejora en estos procesos se considera innovación tecnológica.

Estructura Organizacional y la Tecnología

La estructura organizacional debe esforzarse por adaptarse a todos los requisitos tecnológicos. Esto se debe a la descentralización y centralización que existe en la toma de decisiones, gestión departamental y grupos. Este mecanismo de coordinación puede ser rígido o flexible. Estas deben de responder a todas las necesidades que plantea la naturaleza de la problemática tecnológica o de conocimiento (Slotnisky, 2018).

Tabla 4
Tecnología como Herramienta de Soluciones Organizacionales

Excepciones / Búsqueda de soluciones	Pocas	Muchas
No analizable	Organización artesanal.	Innovadora, basada en el conocimiento.
Analizable	Organización burocrática rutinaria.	De base tecnológica, fundamentada en el aprendizaje y la mejora continua.

Nota. Tomado de *Transformación Digital. Como las personas y Empresas deben Adaptarse a esta Revolución*, por Slotnisky, 2017. Digital House. Estados Unidos.

Cualquier cambio en la estructura de la organización debe realizarse de acuerdo con los procesos de transformación de insumos o datos, conocidos como: (a) servicios, (b) productos y (c) información interna. Esto se logra con diferentes tipos de tecnología relacionadas con las actividades de cada unidad dentro de la organización. (Slotnisky, 2018). Por lo tanto, la estructura organizacional debe generar información mediante el uso de tecnología de información y comunicación considerando que es el eje central de la entidad. Además, aporta nuevas soluciones a los problemas y oportunidades que se presentan en el contexto cambiante de los negocios.

Gestión del Cambio

Las organizaciones siempre están cambiando a medida que el entorno que las rodea se transforma. Con el tiempo, las organizaciones han tenido que desarrollar la capacidad de adaptación en sus procesos que son críticas para la supervivencia de los negocios. Sin embargo, la implementación de estos cambios no es una tarea fácil, para afrontar a los problemas que se presentan en los negocios (Rogers, 2018).

La gestión adecuada de los cambios en las organizaciones debe comenzar con el entendimiento de su contexto, como: (a) eventos externos, como las condiciones económicas, políticas, sociales y competitivas, y (b) eventos internos, como las

decisiones o Intereses administrativos, así como propuesta de valor, estructuras organizativas, sistemas y el personal. El control, en cambio se realiza mediante la evaluación, teniendo en cuenta que la iniciativa comienza en cada proceso (Bueno et al., 2017).

La intervención del cambio permite: (a) la comprensión del inicio de cada proceso, (b) la gestión (requisitos de entrada y salida), y (c) como estabilizar los resultados. Este conocimiento permite el desarrollo de diferentes acciones de mejoras. Sin embargo, la resistencia al cambio es muy frecuente y puede generarse por un individuo o la entidad en su conjunto. Esto se debe a que la condición de un proceso de cambios incluye etapas durante las cuales existe un sentimiento de negación, aceptación y adaptabilidad (Rogers, 2018).

En conclusión, un cambio es necesario cuando existe una evaluación de por medio y como resultado se denoten problemas en la dinámica que se desarrolla en un ambiente tecnológico, área, departamento, unidad de negocio o entidad. Este diagnóstico hace factible el proceso de cambio. Asimismo, determina el rumbo que se debe llevar a cabo según el propósito de la mejora.

La Tecnología de Información y su Influencia en la Mejora de los Negocios

Implementar un sistema de TI permite la automatización de los procesos empresariales. Esto se debe a que las tecnologías pueden incluso crear cambios en el flujo de información, permitiendo que más personas tengan acceso y compartan la información de manera ágil y oportuna. Esto debe a la simplificación de pasos o tareas secuenciales, eliminando retrasos en la toma de decisiones (Laudon, et al., 2016). Las nuevas tecnologías a menudo ayudan al surgimiento de nuevos modelos de negocios, pero en las formas antiguas buscan cambiar la forma en que interactuamos con la tecnología y la forma en que trabajamos.

Tipos de Sistemas Empresariales

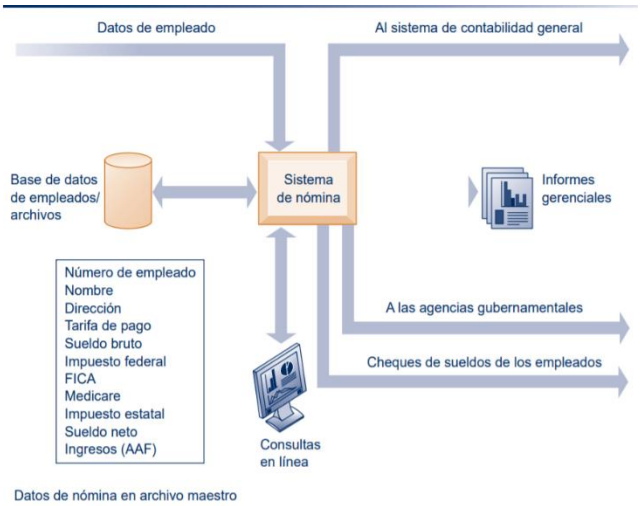
Una empresa equipada con sistemas le permiten soportar diferentes niveles de gestión dentro de la organización. Estos sistemas incluyen sistemas de procesamiento de transacciones (TPS) y sistemas de inteligencia comercial (BIS). A continuación, se describe el alcance de cada uno:

Sistema de Procesos Transaccionales.

Los negocios se esfuerzan por contar con sistemas que les permitan realizar un seguimiento de las actividades y transacciones esenciales de la organización, como: (a) ventas, (b) tarifas, (c) depósitos, y (d) más. Un sistema de procesamiento de transacciones (TPS) permite la generación de este tipo de información al ser un sistema computarizado para la ejecución y registro de transacciones diarias. El objetivo principal de este tipo de sistemas es responder preguntas comunes y poder rastrear cada transacción para la obtención de información de manera rápida, eficiente y actualizada (Laudon et al., 2016).

Los sistemas TPS proporcionan información a cada función empresarial. Por ejemplo, el sistema de nómina junto con el sistema de contabilidad importa nuevos datos al sistema de contabilidad para generar los informes de ingresos y gastos de la empresa. También le permite obtener datos del historial de nómina activados por el departamento de recursos humanos. Otros ejemplos incluyen recibir, a cambio, los salarios de los trabajadores, el seguro y los beneficios que les brinda el estado (Laudon, et al., 2016). A continuación, se muestra el desempeño de la TPS (Laudon, et al., 2016).

Figura 10
Sistema TPS de Nómina y Contabilidad

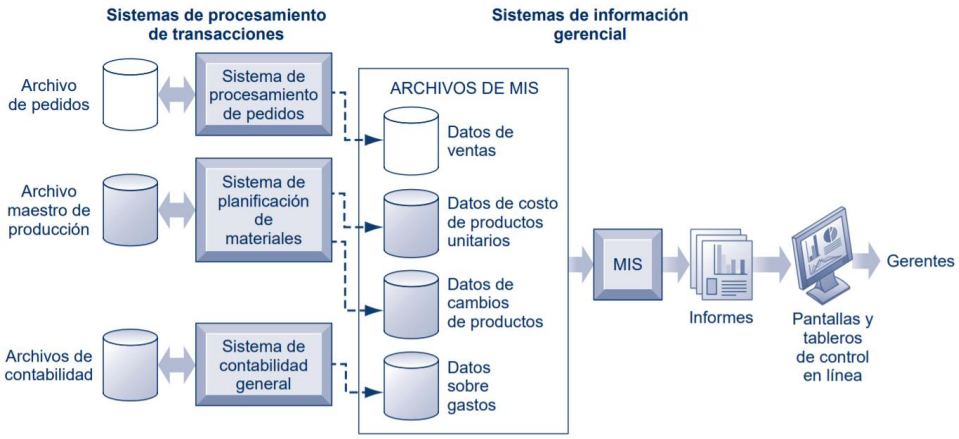


Nota. Tomado de *Sistema de Información Gerencial*, Decimocuarta, por Laudon y Laudon, 2016. Pearson Educación de México SA. de C.V. México.

Sistemas de Inteligencia de Negocios.

Las empresas que resuelven problemas de inteligencia de negocios se esfuerzan por la obtención de información que servirá de apoyo en la toma de decisiones. La inteligencia en el negocio, es un nuevo término que utiliza herramientas informáticas para: (a) administrar, (b) organizar y (c) analizar datos, con el fin de brindar acceso a datos para la toma de decisiones de los altos mandos. En el caso de los mandos intermedios, este tipo de sistema ayuda al control de las operaciones, y la toma de decisiones en cada etapa del proceso. Esto permitió la creación de un nuevo término, denominado Sistema de Información Gerencial (MIS), este proporciona informes de rendimiento actualizados de toda la organización. Esta información se utiliza para controlar y monitorear procesos dentro de la empresa, lo que ayuda a predecir posibles resultados en el futuro (Laudon et al., 2016).

Figura 11
Integración del Sistema de TPS con MIS



Nota. Tomado de *Sistema de Información Gerencial*, Decimocuarta, por Laudon y Laudon, 2016. Pearson Educación de México SA. de C.V. México.

Otros tipos de sistemas de Business Intelligence menos frecuentes son los denominados DSS, que son sistemas de apoyo para la decisión. Si bien los DSS se basan en información interna proporcionada por TPS y MIS, también se pueden usar para obtener datos externos, como precios calculados para el inventario o varios

productos. Estos diferentes sistemas son utilizados por super usuarios que buscan analizar y modelar el control y análisis de datos (Laudon et al, 2016).

En conclusión, la inteligencia de negocio y la aplicación de la tecnología ahora han hecho posible la gestión empresarial basada en datos. Esto ha permitido que usuarios se basen en gran medida en las herramientas de análisis de datos para la continuidad de sus operaciones.

Riesgos Tecnológicos

Las empresas se han vuelto más dependientes del uso de las tecnologías. Esta rápida adaptación ha permitido la creación de nuevos modelos de negocios que antes eran impensables. Algunos de estos nuevos modelos basados en tecnología están diseñados para brindar acceso a servicios e información en cualquier momento y desde cualquier dispositivo. Este nuevo desarrollo crea muchas oportunidades, pero conlleva nuevos riesgos, como: (a) aumento de los delitos cibernéticos, (b) robo de información, y (c) ataques a las redes de telecomunicaciones y los canales de venta en línea.

Los riesgos que se originan por la tecnología no deben verse como riesgos independientes, sino como riesgos estrechamente relacionados como parte fundamental del modelo de negocio. La adaptación de esta nueva tecnología ha propiciado que se conozcan las amenazas potenciales que plantea, lo que permite a la compañía controlarlas y gestionar adecuadamente. Los riesgos tecnológicos van de la mano con factores técnicos y humano. Asimismo, existen riesgos vinculados a la propia tecnología. Por otro lado, también existe el riesgo de que los empleados puedan estar motivados a cometer errores involuntarios sino de malicia (Auditores Internos de España, 2017).

Percepción del Riesgo Tecnológico.

Las organizaciones no mantienen la misma percepción de las TIC, la valoración de cada riesgo dependerá del tipo de negocio y gestión de riesgos que realicen. Aunque en cierto sentido el establecimiento de metas y misiones no se basa en la tecnología, es importante desde el punto de vista de la gestión de las TIC. La prestación de servicios y el desarrollo de productos, e incluso la gestión de una

empresa, dependen del cuidado de la estructura tecnológica subyacente y del personal operativo (Auditores Internos de España, 2017).

Los riesgos asociados con la gestión de TI se relacionan con la estructura organizativa, la gestión y los procesos de una empresa, lo cual se denomina gobierno de TI. Esta a su vez consta de cinco componentes: (a) estructura organizativa y de gestión, (b) gestión operativa o de soporte, (c) planificación estratégica y operativa, (d) provisión y evaluación de precios de servicios, y (e) organización de TI. y gestión de riesgos. Los riesgos asociados con la gestión de TI incluyen: (a) falta de planificación y ejecución, (b) fracaso en el logro de los objetivos, (c) pérdida de oportunidades comerciales, (d) posibles ineficiencias en los procesos comerciales, y (e) falta de control entre las operaciones de la organización y los objetivos estratégicos (Auditores Internos de España, 2017).

En conclusión, una buena estructura organizacional responsable de implementar las Tics siempre debe tener en cuenta la existencia de una separación de funciones. Los riesgos de implementación incluyen, sistemas operativos desarrollados en una intranet, software de seguridad o comunicaciones y capacidades de seguridad de bases de datos. Esto es para asegurar que la información sea completa y precisa.

ISO 27001

La ISO 27001 es un estándar internacional publicado por la Organización Internacional de Normalización (ISO) que describe cómo gestionar la seguridad de la información en las empresas. La última versión de la norma se publicó en 2013 y ahora se llama ISO/IEC 27001:2013. La primera versión se publicó en 2005 y se basa en la norma británica BS 7799-2 (Rojas, 2018).

ISO 27001 se puede implementar en cualquier tipo de organización, ya sea con fines de lucro, privada o pública, pequeña o grande. Escrito por los principales expertos mundiales en la materia, proporciona un análisis de la implementación de la gestión de la seguridad de la información en las organizaciones. También permite a las empresas obtener la certificación, lo que significa que un organismo de certificación independiente confirma que la organización ha implementado la seguridad de la información de acuerdo con la norma ISO 27001. ISO 27001 se ha

convertido en el estándar de seguridad de la información líder en el mundo y muchas empresas dan fe de su cumplimiento (Calder, 2017).

Alcance.

El eje central de la ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información de la empresa. Esto se hace examinando problemas potenciales que pueden afectar la información (es decir, evaluación de riesgos) y luego definiendo qué se debe hacer para evitar que esos problemas ocurran (es decir, mitigación o tratamiento de riesgos). Por tanto, la filosofía principal de ISO 27001 se basa en la gestión de riesgos: descubrir dónde están los riesgos y luego abordarlos sistemáticamente (Rojas, 2018).

Las medidas (o controles) de seguridad implementadas suelen ser políticas, procedimientos e implementaciones técnicas, como software y dispositivos. Sin embargo, en la mayoría de los casos las empresas ya poseen todo el hardware y software, pero lo utilizan de forma insegura; por lo tanto, una gran parte de la implementación de ISO 27001 consistirá en definir las reglas organizativas (como la documentación) necesarias para evitar violaciones de seguridad. Debido a que este tipo de implementación necesitará gestionar múltiples políticas, procedimientos, personas, activos, etc., ISO 27001 detalla cómo todos estos elementos pueden integrarse en un sistema de gestión de seguridad de la información (SGSI). La gestión de la seguridad de la información no se limita a la seguridad informática (por ejemplo, firewall, antivirus, etc.), sino que también está relacionada con la gestión de procesos, recursos humanos, protección legal, protección física, etc (Kosutic, 2016).

Importancia.

Al implementar este estándar para facilitar la seguridad de la información, la compañía puede obtener cuatro establecimientos básicos. El primero está relacionado con los requisitos de la ley, las regulaciones y los requisitos del contrato. La buena noticia es que la mayoría de estos problemas se pueden solucionar implementando la norma ISO 27001, ya que la norma proporciona los elementos y herramientas perfectos para garantizar el cumplimiento de todos estos requisitos. El segundo puede brindarle una ventaja competitiva, y si la empresa está certificada y sus competidores

no, puede obtener una ventaja sobre ellos ante los ojos de los clientes que se preocupan por la seguridad de su información. El tercero es reducir costes y evitar que se produzcan incidentes de seguridad. Cada incidente, por grande o pequeño que sea, generará costes. El cuarto beneficio contribuye a la mejora de la organización eliminando incertidumbres relacionadas o no con la seguridad de la información, reduciendo así el tiempo perdido de los empleados (Kenyon, 2019).

Sin embargo, algunos puntos son más importantes que otros a la hora de realizar una auditoría:

- Política de seguridad: debe incluir los objetivos de seguridad de la información de la organización, considerar los requisitos de seguridad comerciales, legales y contractuales, alinearse con la gestión general de riesgos, establecer criterios de evaluación de riesgos y ser aprobado por la junta.
- Asignación de responsabilidades de seguridad: A todas las actividades se les deben asignar responsabilidades. En el proceso de certificación cada tarea debe definirse de tal manera que una o varias personas de la organización puedan realizarla.
- Educación y formación en seguridad: Todos los empleados deben ser conscientes de la seguridad de la información.
- Registro de incidentes de seguridad: Se deben documentar los incidentes (incidentes) durante el proceso y se debe determinar su impacto y frecuencia. Definir controles de detección y respuestas ante dichos eventos.
- Gestión de la Continuidad del Negocio: El enfoque de la definición del SGSI debe ser mantener la continuidad del negocio, por lo que este objetivo no puede perderse en el proceso de implementación de un sistema de seguridad.
- Protección de registros organizacionales: la información es parte de los activos de una organización y, por lo tanto, debe preservarse y mantenerse. Los registros organizacionales, ya sean registros comerciales o relacionados con sistemas de seguridad, deben cumplir con las características básicas de confidencialidad, integridad y disponibilidad.

- Proteger los datos personales: Son parte de la información de la organización y por lo tanto necesitan ser protegidos.
- Propiedad intelectual: posee la licencia y/o permiso para utilizar el software dentro de la organización (Ladino et al., 2011).

Marco Referencial

Lema et al, (2018) en la investigación que se tituló: "*Análisis para la Aplicación de la Norma ISO 27001 en Pymes del Sector Servicios, año 2022," (p,1)* propuso un análisis para la incorporación de un sistema de gestión de seguridad de información fundamentado en los requisitos de la ISO/IEC 27001:2013. Estudio que parte de la problemática que detectada mediante el uso de la estrategia de análisis enfocada en la obtención de datos primarios. De los hallazgos detectados, se enfatiza la exposición a riesgos de seguridad de información que inciden en la vulnerabilidad, integridad, confidencialidad, y disponibilidad de la información de sus procesos. De la misma manera, de la fragilidad de los controles de seguridad de información. Dichos hallazgos permitieron promover mejoras en la seguridad de información mediante el análisis de incorporar la ISO 27001.

Mora (2021) en la investigación que tituló: *"Análisis para la Gestión de la Seguridad de la Información Alineada a la Norma ISO 27001 y Ciberseguridad," (p.1),* tuvo como objetivo el proponer un análisis para la adaptación de la gestión de la seguridad de la información, bajo los lineamientos de la ISO 27001 e ISO/IEC 27032. Este análisis de las vulnerabilidades existentes en la seguridad de los sistemas de información de las empresas. Por consiguiente, recomendó que, previo al proceso de implementación del análisis, se consideren todas las cláusulas del modelo de dicho análisis, por lo tanto, la participación de la dirección y gerencia es crítica al momento de llevar a cabo el proceso de toma de decisiones para implementar un marco de seguridad adecuado. Esto se debe a que la ISO 27001 se focalizada en la gestión de la seguridad de la información en base a un SGSI, la cual permite su implementa en toda organización. No obstante, la ISO/IEC 27032 no es aplicable en toda empresa y no es auditable, por lo tanto, es recomendable analizar y comprender la estructura

empresarial, al igual que sus objetivos y lineamientos, con la finalidad de determinar si el análisis presentado es acoplable a la organización.

Guerra et al., (2018) en el estudio que titularon: "*Propuesta de Implementación de un Sistema de Gestión de Seguridad de la Información basado en la Norma ISO 27001:2013 para la empresa Lovato City Gas S.A.S," (p.1),* parte de los problemas que se presentan en los servicios de instalación de gas para automotores, considerando los volúmenes de información que se generan diariamente por medio de diversos softwares (Softland, Gas Natural Fenosa, Revisiones Gazel) y herramientas. Además, mediante el uso de las técnicas e instrumentos de recopilación de información al direccionarse mediante un diseño de campo, permitió denotar diversas situaciones de riesgos de seguridad de información como: (a) pérdidas de datos confidenciales, (b) alteraciones de la información, (c) falta de políticas e infraestructura de protección, y (e) ausencia de controles de TIC. En relación con los hallazgos detectados, se estableció una propuesta de implementación de un sistema de gestión de seguridad de la información, cuyo propósito se enfoca en asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando los riesgos de seguridad de la información. Propuesta que se basó en los requisitos de la norma ISO 27001: 2013.

Marco Legal

Constitución de la República del Ecuador

De conformidad con lo dispuesto en el capítulo tercero "Medios de comunicación e información", se regula el libre acceso a las tecnologías de la información y la comunicación, artículo 16, numerales 2 y 3, la Constitución del Ecuador (2008) señaló que:

> Toda persona, individual o colectivamente, tiene derecho a: 2 El acceso universal a las TIC. 3. Crear medios de comunicación social y acceso igualitario a las frecuencias del espectro radioeléctrico para la gestión de las estaciones de radio y televisión públicas, privadas y públicas, así como de las redes de radio y televisión. Frecuencia libre para operación de redes inalámbricas. (p. 8).

El aporte de este apartado es sugerir que todas las personas físicas y jurídicas con sus propias formas y facilidades pueden poseer TIC y hacer un uso igualitario de todas las frecuencias y bandas disponibles, lo que demuestra que no existen barreras de acceso. Así, se pueden desarrollar tecnologías de la información y la comunicación innovadoras y accesibles a todo aquel que quiera incorporarlas a sus actividades.

Asimismo, profundizar en el tema del acceso gratuito a becas por diversidad, en su artículo 17, la Constitución (2008) determinó que:

> El Estado promoverá el pluralismo y la diversidad en las comunicaciones y en este sentido: 1. El Estado garantizará la asignación transparente y equitativa de las frecuencias del espectro radioeléctrico para la gestión de las estaciones de radio y la televisión pública. privados y públicos, así como el acceso a bandas libres para la operación de redes inalámbricas y asegurar que su uso se rija por el bien común. 2. Esto promoverá la creación y mejora de los medios de comunicación públicos, privados y sociales y el acceso universal a las tecnologías de la información y la comunicación, especialmente para aquellas personas y comunidades que no tienen ese acceso o lo tienen de forma limitada.

Con estas métricas, puede ver un camino claro para adoptar nuevas tecnologías sin temor a la reducción de personal, especialmente para aquellos que no tienen acceso o tienen acceso limitado, ya que esto tiene como objetivo fortalecer estas áreas, brindando un enfoque común que se aplica a todos.

Ley Orgánica de Telecomunicaciones

En la literatura de este estudio es necesario ampliar el tema de las telecomunicaciones para conocer las obligaciones, limitaciones y demás principios de este servicio y su principal instrumento, las TIC. Como se establece en el artículo de Ley Orgánica de Telecomunicaciones (2015) se reconocen los principales objetivos, de entre los cuales destacan:

> Impulsar el desarrollo y consolidación del sector de las telecomunicaciones. Promover la inversión nacional e internacional, pública o privada, en el desarrollo de las telecomunicaciones. Promover el desarrollo de productos y servicios de telecomunicaciones. Promover y fomentar la convergencia de redes, servicios y dispositivos. Estimular la disponibilidad de redes de telecomunicaciones rápidas y eficientes en todo el país, brindando a las personas acceso a Internet de banda ancha. Crear las condiciones ideales, garantizando a los ciudadanos el derecho al libre acceso y elección de los servicios públicos de telecomunicaciones de la más alta calidad, a precios razonables, y con información fidedigna y objetiva sobre el contenido y características del servicio público de telecomunicaciones. Promover la neutralidad tecnológica y la neutralidad de la red (p. 4).

Con este enfoque desde la Ley Orgánica de Telecomunicaciones, Se sustenta la intención del gobierno de mantener e incrementar la productividad de las telecomunicaciones, lo que beneficia al presente estudio por el poder transformador de las TIC y el apoyo de la comunidad, haciendo que estas tecnologías, que ya son poderosas y protegidas por los gobiernos, puedan posibilitar la innovación en la forma brindan servicios a todos los sectores de las economías de países con distintas industrias turísticas, una variable será explicada en las siguientes líneas.

Ley Orgánica de Protección de Datos Personales

En el Registro Oficial Suplemento No. 459 de 26 de mayo de 2021 se publicó la Ley Orgánica de Protección de Datos Personales. Tiene por objeto garantizar el derecho a la protección de datos personales, que incluye el acceso y decisión sobre la información y datos de este carácter, así como su correspondiente protección. En lo principal, la ley se refiere a las condiciones que se deben verificar para que el tratamiento de datos personales sea legítimo. Se refiere, también, a las formas a través de las cuales el titular de los datos personales puede manifestar su voluntad para el tratamiento de sus datos (Asamblea Nacional República del Ecuador, 2021).

Esta Ley regula, además, el contenido y alcance de los derechos: (a) a la información, (b) de acceso, (c) de rectificación y actualización, (d) de eliminación, (e)

de oposición, (f) a la portabilidad, (g) a no ser objeto de d una decisión basada única o parcialmente en valoraciones automatizadas, (h) de consulta pública y gratuita ante el Registro Nacional de Protección de Datos Personales, (i) a la educación digital. Por otro lado, consagra algunas categorías especiales de datos personales, como los datos sensibles, los de niños, niñas y adolescentes, los de salud y los de las personas con discapacidad; y se refiere al tratamiento especializado de estos datos. Finalmente, la ley consagra un régimen de sanciones para infracciones relacionadas con el tratamiento de datos personales. Las normas relativas al régimen sancionatorio no entrarán en vigor sino hasta dos años después de la publicación de la ley en el Registro Oficial (Asamblea Nacional República del Ecuador, 2021). En relación con lo expuesto, se denota la importancia de que las empresas posean sistemas de seguridad de información idóneos que aseguren la protección de datos tantos internos como de terceros.

Capítulo 2: Metodología de la Investigación

Diseño de la investigación

El diseño de una investigación es una estrategia general que adopta el investigador como forma de abordar un problema determinado, que permite identificar los pasos que deben seguir para efectuar su estudio. El diseño de la investigación ha de servir al investigador para concretar sus elementos, analizar la factibilidad de cada uno de los temas que formaran parte de los capítulos de dicho estudio. No obstante, también se utiliza para delimitar inicialmente la investigación, paso relevante para obtener el éxito deseado. Por supuesto, vale acotar que dicho diseño es flexible, porque un diseño no puede permanecer estático, ya que durante la evolución de la investigación puede variar en función de las acciones que se llevan a cabo A través del diseño de la investigación, se desarrolla el plan de acción a seguir durante la ejecución de la misma, además, en él se encuentran implícitas las líneas a seguir para la obtener un resultado. Sin embargo, como se mencionó anteriormente éste es flexible ya que debe incorporar los factores que emergen en cada una de sus fases y deben ser relevantes para alcanzar los objetivos deseados. De no ser así, los resultados que se obtienen podrían ser inapropiados con el contexto (Moreno, 2005).

Se usará el diseño experimental en este trabajo de investigación y dicho diseño es flexible porque ofrece varias ventajas al investigador que realiza su trabajo de investigación. La investigación experimental es un tipo de experimento y estudio en el que el investigador manipula y controla una o más variables independientes y observa la variable dependiente para medir cambios simultáneos.

El primer requisito para un experimento es manipular intencionalmente una o más variables independientes. Una variable independiente es una variable que se considera una posible causa de la relación entre las variables, y es un antecedente; el resultado causado por la causa se llama variable dependiente (resultado), es decir la causa es la variable independiente y el efecto es la variable dependiente.

Al formular una pregunta o hipótesis de investigación, los investigadores pueden considerar una o más variables independientes en su estudio. Si efectivamente existe una relación causal entre la variable independiente y la variable dependiente,

provocar intencionalmente un cambio en la primera variable también debe cambiar la segunda variable, por ejemplo, si la motivación es la causa del rendimiento académico, al cambiar el estímulo, el rendimiento académico debe cambiar (Agudelo & Aigneren, 2008).

Ventajas de la investigación experimental

Es muy importante probar nuevas ideas o teorías para poder beneficiarte de este tipo de investigación antes de tomar una decisión. Éstos son algunos de los beneficios de este tipo de encuestas:

- Los investigadores tienen más control sobre las variables para lograr los resultados deseados.
- La materia o industria no afecta la validez de la investigación experimental. Cualquier industria puede utilizarlo con fines de investigación. · Resultados específicos.
- Después de analizar los resultados, puedes aplicar tus conclusiones a ideas o situaciones similares.
- Capacidad para identificar supuestos de causa y efecto. Los investigadores pueden explorar más a fondo esta relación para obtener conocimientos más profundos.
- Los estudios experimentales son un punto de partida ideal. Los datos que recopila son la base para más ideas y más investigaciones. Estos estudios se pueden utilizar junto con otros métodos de investigación (Velázquez, 2022).

Tipo de investigación

El estudio se enmarcó dentro de una investigación de carácter descriptivo. Los estudios descriptivos buscan especificar las propiedades, las características y los perfiles importantes de personas, grupos, comunidades o cualquier otro fenómeno que se someta a un análisis. En definitiva, permiten medir la información recolectada para luego describir, analizar e interpretar sistemáticamente las características del fenómeno estudiado con base en la realidad del escenario planteado (Moreno, 2005).

Se usará la investigación descriptiva en este trabajo de investigación y dicho diseño, permitirá recopilar información sobre la población (firmas auditoras) y de que forma los problemas de seguridad de información como riesgos (filtración de información, perdida de datos, acceso no autorizado al sistema de información), afectan a las organizaciones mencionadas y cuales son los controles que pueden implementar para prevenir dichos inconvenientes. La investigación descriptiva se encarga de puntualizar las características de la población que está estudiando. La investigación descriptiva se encarga de especificar las características de la población de estudio. La investigación descriptiva es un método para intentar recopilar información cuantitativa que pueda utilizarse para el análisis estadístico de una muestra de población. Ventajas de la investigación descriptiva

Ventajas de la investigación descriptiva

Algunas de las principales ventajas de la investigación descriptiva son:

- **Realización de estudios en diferentes períodos de tiempo:** para determinar si existen similitudes o diferencias, se pueden realizar estudios en diferentes períodos de tiempo. Esto permite evaluar cualquier número de variables. Con fines de confirmación, el estudio de las condiciones actuales también se puede repetir para identificar tendencias.
- **Investigación por encuestas:** las encuestas son una herramienta de retroalimentación muy popular en la investigación de mercados. Para recopilar datos de calidad, las encuestas deben tener buenas preguntas y un equilibrio entre preguntas abiertas y cerradas. Este método de encuesta se puede realizar en línea o fuera de línea, lo que lo convierte en la primera opción para la investigación descriptiva cuando el tamaño de la muestra es grande.
- **Definir las características del entrevistado:** el propósito del uso de preguntas cerradas es sacar conclusiones específicas sobre el entrevistado. Busque patrones, rasgos y comportamientos. También puede comprender las actitudes u opiniones de los encuestados sobre fenómenos relacionados.

- **Entorno natural:** la investigación descriptiva brinda la oportunidad de realizar investigaciones en el entorno natural de los encuestados, lo que garantiza una recopilación de datos cualitativa y justa.
- **Forma una base para las decisiones:** dado que los datos recopilados en los estudios descriptivos son representativos de grupos más grandes y estables, es fácil tomar decisiones basadas en el análisis estadístico de estos datos (Velázquez, 2022).

Enfoque

La investigación es un proceso riguroso, exhaustivo y sistemático destinado a la resolución de problemas. Está organizado y garantizado para generar nuevos juicios lógicos o soluciones viables encaminadas a profundizar y crear conocimiento. El origen de la investigación científica es la necesidad humana de intentar resolver problemas cotidianos. Por tanto, para poder realizar una investigación es necesario definir un método que nos permita controlar el proceso con la suficiente eficacia como para obtener resultados que nos permitan explicar los fenómenos que nos ocupan. Así surge la metodología de investigación que informa nuestros resultados (Otero, 2018).

Hoy en día existen dos enfoques básicos de la investigación científica que tomaron su lugar en el siglo XX desde diferentes campos de estudio, y cuando llegue el siglo XXI, pueden estar seguros que comenzará con una tercera opción que ha sido probada, demostrada, incluyendo: el uso de métodos mixtos, una combinación de investigación cuantitativa y cualitativa en la investigación científica. Aún es necesario decirle a la nueva generación de investigadores que solo acumulando conocimientos en la práctica y el trabajo podrán convertirse en investigadores científicos (Otero, 2018).

Ambos métodos, el cuantitativo y el cualitativo, son paradigmas de la investigación científica porque utilizan procesos cuidadosos, sistemáticos y empíricos para generar conocimiento. Observan y evalúan fenómenos. Forman hipótesis o ideas basadas en observaciones y evaluaciones. El grado en que se puede demostrar que una hipótesis o idea es respaldada. Revisan estos supuestos o ideas basándose en evidencia o análisis

y desarrollan nuevas observaciones y juicios para aclarar, revisar y confirmar los supuestos e ideas; incluso crear otros (Otero, 2018).

En el enfoque **cuantitativo**, su proceso de investigación se centra en mediciones numéricas. Utiliza observaciones de procesos en forma de recopilación de datos y las analiza para obtener respuestas a las preguntas de investigación. El método utiliza análisis estadístico. Se deriva de la extracción de parámetros, medición, extracción de frecuencia y estadísticas generales. Esto crea una pregunta de investigación limitada y específica. Su pregunta de investigación es sobre un problema específico. Una vez que haya identificado su pregunta de investigación, revise lo que ha estudiado anteriormente. Esta actividad se denomina revisión de la literatura (Otero, 2018).

Este enfoque cuantitativo se basa en una revisión de la literatura orientada al tema y concluye con el marco teórico del estudio. Las hipótesis que surjan de estas recopilaciones de datos se probarán para demostrar la exactitud del estudio. Si los resultados confirman o concuerdan con la hipótesis, se presenta evidencia a su favor. Cuando se demuestra que están equivocadas, se descartan en busca de mejores explicaciones y nuevas hipótesis (Otero, 2018).

Población

La población es la totalidad del fenómeno a estudiar, en donde las unidades de población poseen una característica común, la cual se estudia y da origen a los datos de la investigación (Moreno, 2005).

De acuerdo al catastro de la Super de Compañías, Valores y Seguros, las firmas auditoras de la ciudad de Guayaquil son 212

Se usará la población basada en las firmas auditoras de la ciudad de Guayaquil. En esta investigación se evitarán que existan los posibles sesgos en la población porque se elegirá a profesionales del área de sistemas de las dichas entidades. El sesgo de muestreo, o una muestra de estudio sesgada, ocurre cuando los miembros de la población objetivo son mal seleccionados debido a un muestreo insuficiente o excesivo.

Cómo evitar el sesgo de muestreo

El sesgo de muestreo puede evitarse hasta cierto punto. A continuación, se ofrecen algunos consejos para evitar el sesgo de muestreo:

- Definir población y marco muestral
- Asegúrese de que la población objetivo se ajuste al marco muestral
- Evite el muestreo por conveniencia, no es la mejor solución
- Determinar los objetivos del estudio.
- Dar a los encuestados igualdad de oportunidades para participar
- La duración de la encuesta es corta o razonable.
- Simplifique las encuestas
- Seguimiento (Velázquez, 2022).

Técnica e instrumentos de recolección de información

Es uno de los pasos más trascendentes en el proceso de investigación científica. Debe ser uno de los ejes principales del estudio, porque de él proviene la información que se analiza para transmitir los resultados del estudio (Moreno, 2005).

Cualquier herramienta de recolección de datos debe cumplir dos requisitos básicos: validez y confiabilidad. La validez se determina revisando la presentación del contenido, la comparación del indicador con el ítem que mide la variable correspondiente. La validez se evalúa como el hecho de que una prueba ha sido ideada, formulada y aplicada de tal manera que mide lo que se supone que debe medir. La validez es el grado en que la prueba utilizada realmente mide lo que se pretende medir; es decir, la validez se considera específica de un conjunto porque involucra un propósito particular y un grupo particular de sujetos (Moreno, 2005).

Se usará el enfoque cuantitativo en este trabajo de investigación y la herramienta que se utilizará es la encuesta.

Se utilizará la encuesta del 2022, la cual fue elaborada por los por los Ings. José Córdova y William Remicio y validada cuantitativamente por tres expertos: Ing. De Sistemas y Computo, Karina Saravia Aguilar, Mg. En Educación con Mención en Docencia y Gestión, Sabina Acosta Salvador, Magister en Gestión Tecnológica de la

Información, José González Calderón. Los expertos mencionados validaron esta encuesta con un alfa de Cronbach de 0.85.

Se usará la escala de Likert en las diversas preguntas de la encuesta que deberán responder los encuestados. En base a los puntos de vista de los profesionales encuestados permite medir el nivel de seguridad de los sistemas de las organizaciones y sus respuestas ayudan a determinar lo que se puede implementar para mejorar los sistemas de seguridad de información en las entidades mencionadas.

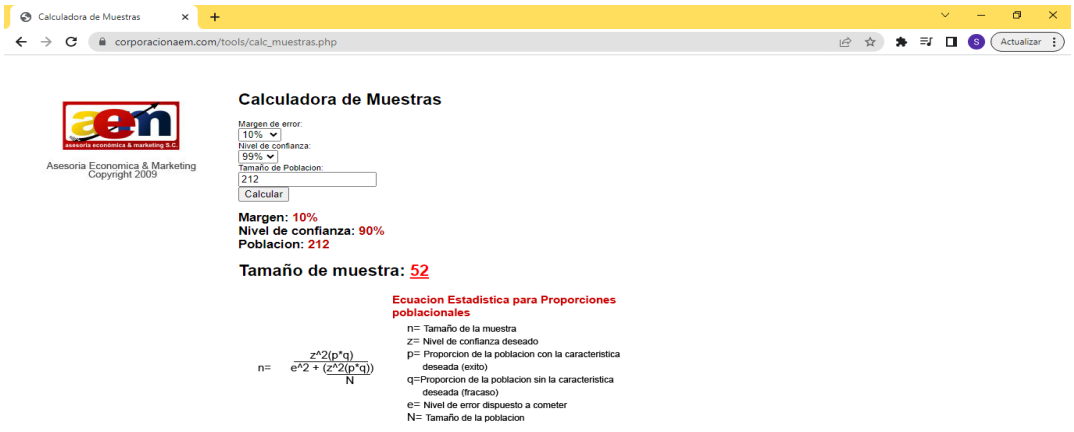
La encuesta elaborada por los autores mencionados, se encuentra en los Anexos de este trabajo de investigación.

Muestra

Es el subconjunto o parte del universo o el todo que se estudiará. Existen programas para obtener múltiples componentes de ejemplo como fórmulas, lógica, etc. Una muestra es una parte representativa de la población (Lopez, 2004).

Se hizo el calculo de la muestra mediante una formula utilizando 212 como tamano de poblacion, un 90% de nivel de confianza y 10% de margen de error, se determino que el tamano de la muestra es de 52. En otras palabras, se encuestara a 52 firmas auditoras.

Figura 12
Porcentaje sobre el cálculo de la muestra



Muestreo

Es el método utilizado para seleccionar a los componentes de la muestra del total de la población. Consiste en un conjunto de reglas, procedimientos y criterios mediante los cuales se selecciona un conjunto de elementos de una población que representan lo que sucede en toda esa población.

El realizar el diseño muestral es importante porque:

- Permite que el estudio se realice en menor tiempo.
- Se incurre en menos gastos.
- Posibilita profundizar en el análisis de las variables.
- Permite tener mayor control de las variables a estudiar (López, 2004).

Tipos de muestreo

Se dividen en dos grupos: el probabilístico y el no probabilístico.

Muestreo no probabilístico

El muestreo no probabilístico se emplea cuando es difícil obtener la muestra por el método de muestreo probabilístico. Este método una técnica de muestreo que no realiza procedimientos de selección al azar, sino que se basan en el juicio personal del investigador para realizar la selección de los elementos que pertenecerán a la muestra. En esta técnica no se conoce la probabilidad de seleccionar a cada elemento de la población y también no todos cuentan con las mismas probabilidades de ser seleccionados para la muestra.

Aunque este método no es muy representativo bajo los criterios del investigador, pero no se garantiza la representatividad. Entre los métodos no probabilísticos los más utilizados son: muestreo por cuotas, muestreo intencional o de conveniencia, muestreo de bola de nieve y muestreo por juicio.

Por juicio: El método de muestreo no probabilístico, el cual consiste en que los sujetos se seleccionan con base del conocimiento y juicio del investigador. Es decir, el investigador utiliza su juicio o experiencia para seleccionar a los elementos que pertenecerán a la muestra, ya que considera que son más representativos de la población en estudio.

Este método es recomendable utilizarlo cuando el responsable de realizar el estudio conoce estudios anteriores similares o idénticos y sabe con exactitud que la muestra fue útil para el estudio, de igual manera cuando la población es chica por tanto el investigador conoce a la población (Parra & Vásquez, 2017).

En esta técnica de muestreo no probabilístico, las muestras se seleccionan basándose únicamente en el conocimiento y la credibilidad del investigador. En otras palabras, los investigadores eligen solo a aquellos que estos creen que son los adecuados (con respecto a los atributos y la representación de una población) para participar en un estudio de investigación (Ortega, 2022).

En este trabajo de investigación, el tipo de muestreo que se utilizará es el muestreo no probabilístico por juicio. Este metodo nos permitió seleccionar muestras de profesionales del area de sistemas de las firmas de auditoras. El muestreo realizado es un gran aporte a este trabajo de investigación porque ayuda a determinar como la seguridad de información afecta a la poblacion mencionada.

Se encuestará a los profesionales del área de sistemas de las firmas auditoras de la ciudad de Guayaquil, que tengan conocimientos y experiencia sobre la seguridad de la información y protección de datos.

Resultados de la investigación

De acuerdo a la utilización de las técnicas y recolección de información, se detalla el análisis respectivo de la información sobre la seguridad de la información y protección de datos de las firmas auditoras en la ciudad de Guayaquil, en la cual, se observa y describe el comportamiento que tienen para mitigar los posibles riesgos de información, pero principalmente conocer las acciones que toman ante los diversos problemas que se presenten en el área de sistemas de las entidades mencionadas.

Análisis de los resultados

Según la muestra obtenida de este trabajo de investigación, se hicieron encuestas a profesionales del área de sistemas de las 52 firmas auditoras de la ciudad de Guayaquil.

Los encuestados eligieron su respuesta en base a los diferentes puntajes de la escala de Likert:

1-Totalmente en desacuerdo

2-En desacuerdo

3-Indiferente

4-De acuerdo

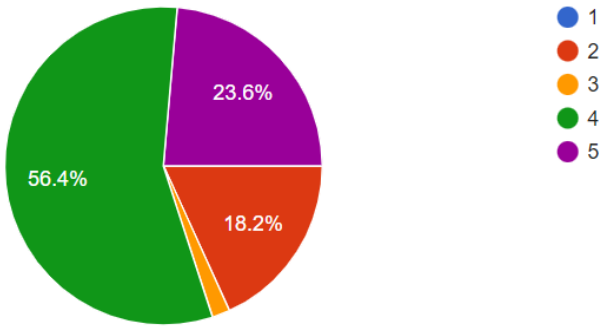
5-Totalmente de acuerdo

Las encuestas realizadas reflejan los siguientes resultados:

1. ¿Usted piensa que las firmas auditoras cumplen los requisitos del sistema de gestión de la seguridad de la información?

El 56.40% (color verde-de acuerdo) nos muestra que gran parte de las firmas auditoras cumplen los requisitos del SGSI, pero el 18.20% (color café-en desacuerdo) indica que las entidades mencionadas no pueden cumplir por la falta de capacidad y gestión.

Figura 13
Porcentaje sobre el cumplimiento de los requisitos del sistema de gestión de la seguridad de la información por parte de las firmas auditoras



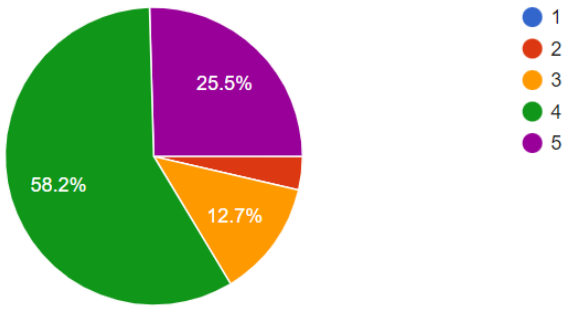
2. ¿Es fundamental la implementación del sistema de gestión de la seguridad de la información en las firmas auditoras?

En resumen, el 58.20% (color verde-de acuerdo) nos muestra que gran parte de las firmas auditoras si quieren implementar el SGSI porque quieren proteger sus datos.

El 12.70% (color amarillo-indiferente) piensan que al implementar tendrán un gasto adicional y sino implementan pueden sufrir amenazas de su información, entonces

mejor no se preocupan y mejor continúan realizando sus actividades como por ejemplo procesos para captar clientes, procesos para capacitar a los empleados, etc. Esto provoca que aún no se decidan en que momento implementarlo y puede ser que al final si implementen el SGSI para salvaguardar su información.

Figura 14
Porcentaje sobre la implementación del sistema de gestión de la seguridad de la información en las firmas auditoras

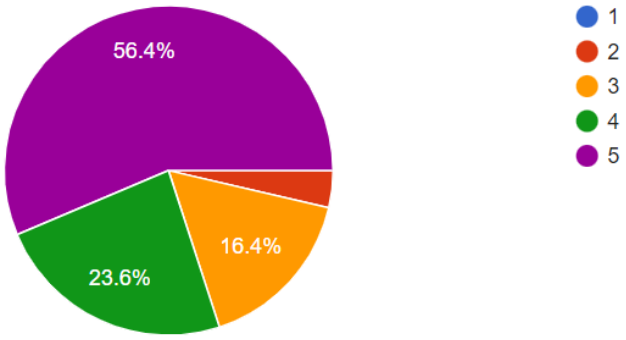


3. ¿Cree usted que es importante la seguridad de los activos de información?

El 56.40% (color morado-de acuerdo) nos muestra que para todas las firmas auditoras son importantes la seguridad de los activos de información y más aún las grandes firmas auditoras que contratan servicios para que sus datos sean protegidos con las seguridades más altas posibles y tratar de evitar filtración y perdida de información.

A pesar que todos dijeron que son importantes, pero el 16.40% (color amarillo-indiferente) indica que hay algunas firmas auditoras por ejemplo firmas auditoras pequeñas o que recién empiezan si usan activos de información, pero se preocupan más por el funcionamiento del negocio de su firma para captar clientes. Finalmente, protegen su información con sus pocos recursos, pero no pueden tener el 100% de seguridad como lo tienen las grandes firmas auditoras.

Figura 15
Porcentaje sobre la seguridad de los activos de información



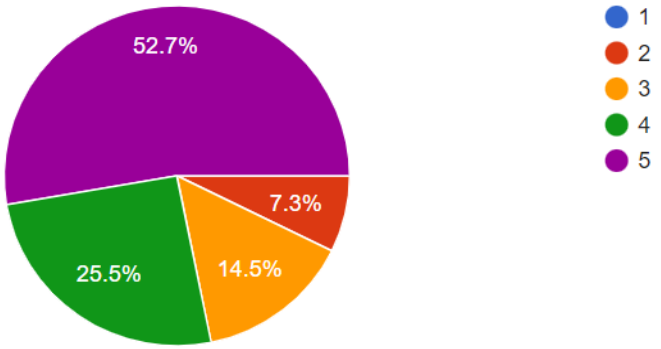
4. ¿El diseño de un Sistema de Gestión de la Seguridad de Información para las firmas auditoras mejorará la protección de los activos de información?

El 52.70% (color morado-de acuerdo) nos muestra que para todas las firmas es importante porque dicho diseño tiene un enfoque de seguridad tecnológica que se centra en automatizar los controles de seguridad de los datos, por tanto, la seguridad por diseño está pensada para prevenir cualquier fallo de seguridad tecnológica para no reparar los problemas que se presenten después.

El 14.50% (color amarillo-indiferente) indica que hay algunas firmas auditoras que hacen su diseño de SGSI con el software no muy avanzado y como las grandes firmas si tienen. Estas firmas auditoras pequeñas al tener un sistema se pueden decir básico, aunque quiera agregarle muchos controles de seguridad, no podrá ejecutarlos todos porque el software es limitado y solo puede aplicar la mayoría de controles, pero no en su totalidad. Al no ejecutar la totalidad de los controles de seguridad, el sistema es vulnerable y pueden producirse fallos en los procesos de control de acceso a la información del sistema, ataques de posibles hackers, filtración y perdida de información, entre otros problemas.

Figura 16

Porcentaje sobre el diseño de un Sistema de Seguridad de Información para las firmas auditoras y como mejorará la protección de los activos de información



5. ¿El diseño y la implementación de controles de seguridad de la información permitirá reducir los riesgos a los activos de información?

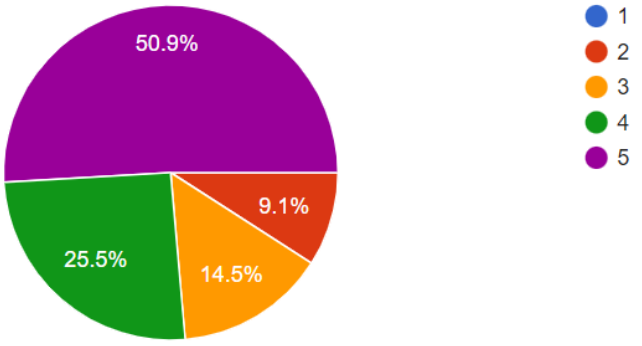
El 50.90% (color morado-de acuerdo) nos muestra que para todas las firmas es importante porque mediante el análisis y evaluación de riesgos basado en activos de información, permite identificar claramente todas aquellas amenazas que pueden impactar negativamente en la seguridad de los activos por ejemplo: dispositivos, hardware y software, bases de datos, archivos, ordenadores y sistemas de almacenamiento, incluso, personas y otros recursos críticos que se deben proteger para garantizar la confidencialidad, integridad y disponibilidad de la información.

El 14.50% (color amarillo-indiferente) indica que hay algunas firmas auditoras que implementan su diseño de SGSI y los controles de seguridad en su software pero que sus sistemas no son tan avanzados como de las grandes firmas auditoras.

Los sistemas de las grandes firmas auditoras pueden identificar cada uno de los activos que tienen algún valor para la organización y que es importante proteger, esto incluye activos para el procesamiento, transmisión, tratamiento o almacenamiento de la información. En este punto es fundamental definir quién es el propietario del activo, es decir, la persona o área responsable de este y por ende, el que debe establecer e implementar las medidas y controles para su adecuada protección. Contar con este inventario, que debe mantenerse actualizado, permite a las organizaciones tener claridad de todos sus activos de información y tomar las medidas necesarias para protegerlos.

Figura 17

Porcentaje sobre el diseño y la implementación de controles de seguridad de la información y reducción de los riesgos a los activos de información



6. ¿Para usted al contar con menores controles de seguridad de la información representa desventaja?

El 47.30% (color morado-de acuerdo) nos muestra que para todas las firmas es importante y permite que se den cuentas que no son suficientes controles y por tanto deben aumentar y reforzar dichos controles. Por ejemplo, para fortalecer los controles de seguridad de la información se debe hacer lo siguiente:

Adoptar de manera rutinaria un análisis de vulnerabilidades y gestión de actualizaciones

Realizar una revisión de seguridad con un enfoque táctico, estratégico y técnico para las amenazas de ciberseguridad

Actualizar periódicamente los sistemas operativos y todo el software instalado en los equipos e implementar un programa de respaldos periódicos de la información

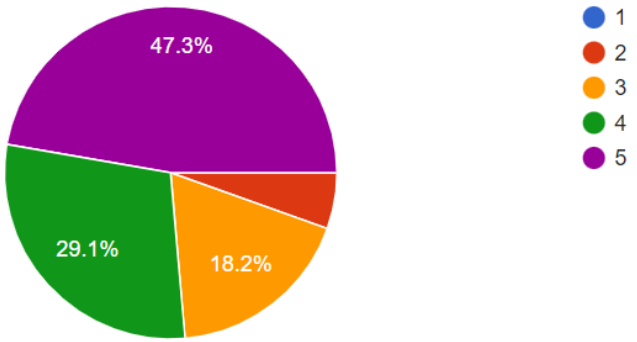
Realizar programas de concientización para los colaboradores de todos los niveles

Ejecutar un plan de acción ante un incidente cibernético

El 18.20% (color amarillo-indiferente) indica que para algunas firmas auditoras es una desventaja porque las firmas auditoras de gran renombre que tienen un buen o

avanzado software estarán mayor preparadas antes posibles ataques de hackers, filtración de información, perdida de datos, desastres naturales, entre otros problemas. En otras palabras, las firmas auditoras grandes tendrán menores problemas para afrontar situaciones de alto riesgo, a diferencia de firmas auditoras pequeñas que sufrirán cuando se les presenten esas situaciones de alto riesgo.

Figura 18
Porcentaje sobre los controles de seguridad de la información



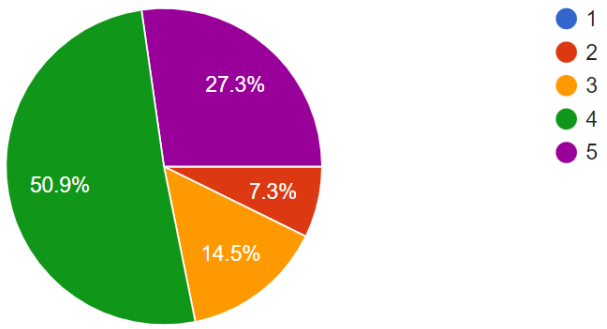
7. ¿Los controles sobre las vulnerabilidades de los sistemas de información en las firmas auditoras, mejorará la protección de la información de dichas entidades?

El 50.90% (color verde-de acuerdo) nos muestra que gran parte de las firmas auditoras implementan controles sobre las vulnerabilidades de los sistemas de información en las firmas auditoras porque se han convertido en una tarea importante para las empresas y dichos controles de seguridad informática necesitan ser adecuadamente establecidos, implementados, operados, monitorizados, revisados, mantenidos y mejorados; para mantener un sistema de seguridad informática efectivo a lo largo del tiempo.

Por otro lado, el 14.50% (color amarillo-indiferente) indica que dichas entidades han implementado los controles de seguridad de información, pero mencionan que aun así los sistemas pueden sufrir varios ataques cibernéticos y producir perdida de información. En este caso, para reducir la complejidad de los problemas y aumentar la efectividad de la gestión de la seguridad de la información es posible automatizar determinadas acciones y controles. La automatización de controles de seguridad

informática implica que la operación, monitorización y la revisión de estos se realice de forma automática por herramientas de hardware y software, sin intervención humana en esas acciones.

Figura 19
Porcentaje de los controles sobre las vulnerabilidades de los sistemas de información en las firmas auditoras

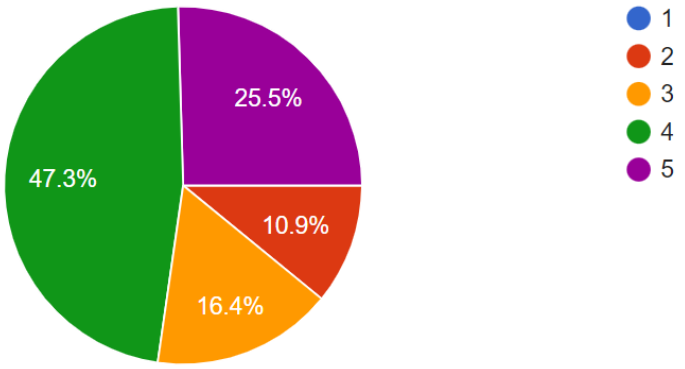


8. ¿La implementación del plan del SGSI permitirá mitigar los riesgos de información?

El 47.30% (color verde-de acuerdo) nos muestra que gran parte de las firmas auditoras implementan el plan del SGSI porque dicho plan tiene como base la identificación de los controles de seguridad, en el cual, se hace la selección de salvaguardas, incluyendo políticas, controles, monitoreo y asignación de las responsabilidades, con el fin de evitar, controlar, transferir y mitigar los riesgos detectados.

El 16.40% (color amarillo-indiferente) indica que dichas entidades tienen la intención y hasta han implementado el plan del SGSI, pero de acuerdo con sus niveles económicos de cada firma auditora. En el caso de grandes firmas auditoras, podrán cumplir con la mayoría y totalidad del plan, pero en firmas auditoras pequeñas cumplirán el plan en su mayoría o mitad y hasta veces menos de la mitad, porque los recursos de las firmas auditoras pequeñas son pocos y limitados.

Figura 20
Porcentaje sobre la implementación del plan del SGSI



9. ¿Cree usted que es clave que las firmas auditoras implementen controles que eviten el acceso no autorizado a los sistemas de información?

El 50.90% (color morado-de acuerdo) nos muestra que para todas las firmas es clave porque el control de acceso impide que los infiltrados u otros usuarios no autorizados se hagan con la información confidencial (como los datos de clientes y la propiedad intelectual). Además, reduce el riesgo de filtrado de datos por parte de los empleados y mantiene a raya las amenazas web. En vez de manejar los permisos de forma manual, las organizaciones con mayor seguridad dependen de soluciones de administración de identidad y acceso para implementar directivas de control de acceso.

El 16.40% (color amarillo-indiferente) indica que hay algunas firmas auditoras si tienen controles de acceso, pero no al nivel de grandes firmas auditoras. Les falta implementar algunos controles fundamentales porque el objetivo de autenticar al usuario es simplemente si alguien es quien dice ser por medio de alguno de estos factores: algo que sabes (preguntas personales), algo que eres (huellas digitales) y algo que tienes (tokens criptográficos).

Y para ello, existen diferentes tipos de autenticación:

Inicio de sesión único (SSO). Es una función de seguridad que permite a los usuarios iniciar sesión en varios sitios web y aplicaciones con una única cuenta. Simplifica el proceso de inicio de sesión para los usuarios, ya que solo necesitan recordar un nombre de usuario y una contraseña para acceder a todos los sitios web y aplicaciones. SmartLogin es un buen ejemplo de este tipo de autenticación.

Autenticación multifactor (MFA): Los usuarios acceden a los recursos protegidos mediante la combinación de dos o más elementos, como una contraseña y un token de seguridad.

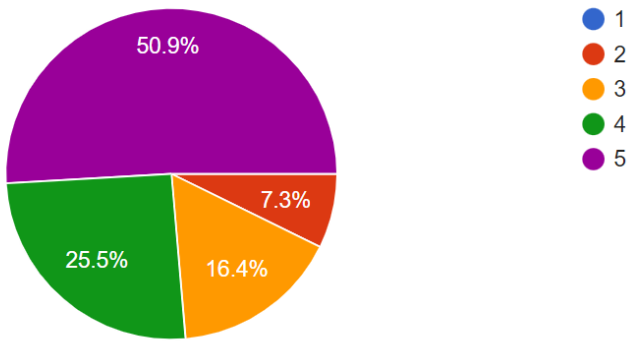
Autenticación basada en riesgos: Se centra en la identificación y el análisis de los factores de riesgo que pueden afectar a la seguridad de un sistema, y solicita al usuario MFA solo en caso de detectar la presencia de un riesgo mayor.

Autenticación basada en tokens: Los usuarios acceden a los recursos protegidos mediante un token de seguridad, que puede ser un código de acceso o una tarjeta física.

Autenticación basada en certificados: Los usuarios acceden a los recursos protegidos mediante un certificado de seguridad digital.

Autenticación biométrica: Los usuarios acceden a los recursos protegidos mediante la verificación de una característica física única, como la huella dactilar o la voz.

Figura 21
Porcentaje sobre la implementación de controles que eviten el acceso no autorizado a los sistemas de información



10. ¿Usted considera que al implementar ERP es importante para los sistemas de seguridad de información?

El 56.40% (color morado-de acuerdo) nos muestra que para todas las firmas es importante el ERP porque la información del sistema deberá estar concentrada en un único servidor, con su respectiva restricción de acceso al mismo y tener sólo personal especializado para el uso del equipo. También es importante tener restringido el acceso al servidor mediante la red de la empresa, que sólo ciertos usuarios o personal del área de sistemas tengan acceso al mismo.

El 14.50% (color amarillo-indiferente) indica que algunas firmas auditoras mencionan que si usan ERP pero que hay algunas falencias de los ERP e igual usan el ERP porque ofrecen varias seguridades en los sistemas para dichas entidades. Algunos de las falencias que presentan los ERP, por ejemplo, Software obsoleto: Los mejores proveedores de ERP son implacables en su batalla contra los nuevos y emergentes riesgos de seguridad.

Cada vez que se identifica un riesgo de este tipo, se desarrolla un parche de seguridad que se distribuye a los clientes. En el pasado, algunas empresas han ignorado o retrasado la aplicación de estas actualizaciones durante largos períodos de tiempo, lo cual ha dejado a sus sistemas vulnerables. Esto es especialmente cierto en el caso de ERP más antiguos que han sufrido numerosas personalizaciones y soluciones alternativas, lo cual hace que la implementación de parches sea más problemática de gestionar.

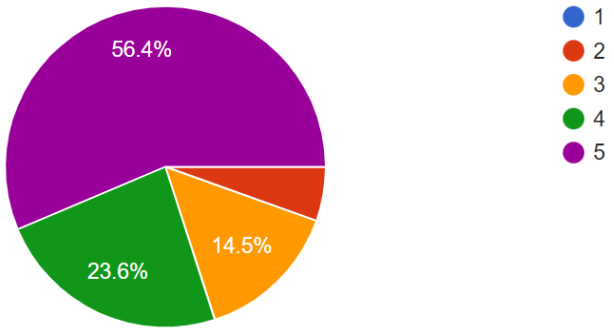
Corrección: las actualizaciones y parches de seguridad deben implementarse regularmente a pesar del riesgo de interrupciones y tiempo de inactividad porque surgen nuevas amenazas todo el tiempo. La aplicación de parches y actualizaciones para ERP on-premise requiere un enfoque basado en riesgos para priorizar a aquellos con más implicaciones de seguridad y, si bien no es un proceso fácil ni disruptivo, es clave para mitigar los riesgos.

Incumplimiento de los estándares de seguridad y control: A medida que los sistemas de ERP se integran cada vez más en más departamentos, el alcance de los datos

vulnerables se hace cada vez más diverso, incluyendo cosas como información segura del producto, registros médicos o propiedad intelectual. Cuanto más sensibles sean los datos (financieros, médicos o legales, por ejemplo), más probabilidades habrá de que tengan sus propios protocolos de seguridad y almacenamiento. Si no se respetan, o no se tienen en cuenta, estos protocolos pueden dar lugar no solo al posible incumplimiento de esos datos, sino también a sanciones e incluso repercusiones legales en caso de incumplimiento.

Corrección: hoy, los mejores ERP, con bases de datos modernas, pueden facilitar la automatización y el control centralizados de una variedad de protocolos de compliance para una amplia variedad de tipos de datos. Esto significa que los equipos de TI pueden trabajar con especialistas de toda la empresa para determinar inicialmente los estándares de seguridad correctos y, a continuación, automatizar los sistemas y los dashboards de usuario para garantizar que se cumplan los protocolos correctos en el futuro.

Figura 22
Porcentaje sobre la implementación de ERP a los sistemas de seguridad de información



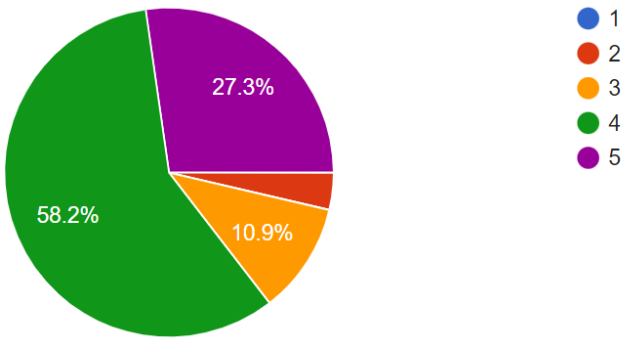
11. ¿Cree usted que las firmas auditoras mejoraran la seguridad de información al recurrir a terceros?

El 58.20% (color verde-de acuerdo) nos muestra que gran parte de las firmas auditoras recurren a terceros porque la protección de la información de la empresa es una responsabilidad compartida entre la organización y los terceros con los que se

establecen relaciones comerciales. Frente a ello, se toman una serie de acciones que van desde la selección adecuada de colaboradores y proveedores externos. Para ello, se debe valorar objetivamente aspectos de calidad, precio, plazos de entrega, reputación, capacidad técnica y de seguridad.

Por otro lado, el 10.90% (color amarillo-indiferente) indica que dichas entidades tienen la intención y hasta han recurrido a terceros, pero el manejo de la información durante el proceso de transferencia o intercambio con terceros implica riesgos de pérdida, alteración, robo o uso indebido de los datos. Por ello, se deben establecer medidas de seguridad, como el uso de medios de transmisión seguros, como canales cifrados o redes privadas virtuales (VPN), que impidan el acceso no autorizado o la interceptación de los datos. Además, verificar la identidad y autorización de los terceros que reciben o envían la información, mediante sistemas de autenticación y control de acceso, aplicar técnicas de anonimización o pseudoanonimización de la información cuando sea posible, para reducir el impacto potencial en caso de divulgación o compromiso de los datos e implementar mecanismos de registro y auditoría para rastrear y verificar las operaciones realizadas con la información durante el proceso de transferencia o intercambio con los terceros.

Figura 23
Porcentaje sobre las firmas auditoras que recurren a terceros para mejorar la seguridad de información



Capítulo 3: Resultados de la Investigación

Matriz de resultados

Según las investigaciones realizadas en este trabajo, se determinó los principales ataques y vulnerabilidades que sufren los sistemas de información, en donde, se comprobó que las empresas como las PYMES son atacadas e indefensas ante situaciones que afectan los datos almacenados en sus sistemas. Los principales ataques son los detallados a continuación:

Tabla 5
Vulnerabilidades a los sistemas

Principales ataques/ vulnerabilidades	Comportamiento/ fuentes	Impacto / Afectaciones
Phishing Producidos por hackers que acceden a cualquier tipo de información, también pueden ser producidos por bucaneros, que son actores que dependen específicamente de la red de internet	Se encargan de crear páginas webs falsas, a los que direccionan los correos correcciones, o a través de ingeniería social con sugerencias de actualizaciones de seguridad a las que acceden los usuarios	• Logra acceder a información confidencial de la empresa. • Infectan de virus los equipos tecnológicos de los departamentos.
Inserción de Dispositivos externos Producidos por personales internas o externas de la empresa	Se encargan de introducir memorias, pendrive, discos duros, lectores y demás dispositivos	• Robo de información • Infección de los activos tecnológicos de la empresa. • Genera costos de reparación de equipos

Según sección de la tabla **Software desactualizado** Los Softwares desactualizados son blanco de virus en pueden atrapar en la red de internet. Los atacan ciberdelincuentes	Los hackers atacan los softwares que los usuarios utilizan con más frecuencia	• Intervención a redes corporativas • Acceso a redes de wifi de la empresa • Fuentes de Ransomware
Falta de controles de acceso al talento humano.	Toda persona tiene acceso a todos los sistemas de información	• Manipulación de la información • Robo de información
Pérdidas de información por falta de copias de seguridad	Falta de uso de copias de seguridad debido a falta de cultura de cuidado de la información	• Inactividad de la empresa por falta de registros • Cierre de la empresa
Falta de firma de contratos de confidencialidad	Nadie cuida la información de la empresa	• Venta de información • Mal uso de información de la empresa

Nota. Tomado de *Análisis de vulnerabilidad en un sistema de gestión de seguridad de información en un Pyme*, por Mejia y Romero, 2019. Universidad de Guayaquil de Ecuador.

Los softwares son importantes porque eliminan las acciones y ataques que afectan a los sistemas de las empresas. Cabe recalcar que esta es una acción preventiva que ayuda a mitigar daños menores, mayores o de cualquier tipo a la empresa. Los principales softwares son los detallados a continuación:

Tabla 6
Softwares a utilizar

Ataque	Software a utilizar
Malware	• Free eScan Anti-Virus Toolkit
Virus	• Bitdefender
Troyano	• Tencent
Spyware	• AdwCleaner
AdWare	• SpyBot Search & Destroy
Ransomware	• WinPatrol
Phishing	• Kaspersky Internet Security
Denegación de servicio distribuido (DDoS)	• Avast
Trashing (cartoneo)	• Enhanced Mitigation Experience Toolkit

Nota. Tomado de *Análisis de vulnerabilidad en un sistema de gestión de seguridad de información en un Pyme*, por Mejia y Romero, 2019. Universidad de Guayaquil de Ecuador.

Plan de seguridad

Se desarrollará un plan de seguridad que consiste en llevar a cabo objetivos estratégicos, mediante políticas de seguridad para que empresas como las PYMES puedan estar en un riesgo aceptable y tengan menos probabilidades que le ocurran situaciones que pueden afectar a su sistema y sean capaces de hacer frente a adversidades que se presenten.

En este plan se usarán medidas de protección, con la cual, se quiere dar la mayor seguridad posible, pero dependerá del tipo de sistema que posea la empresa. Se detallan las medidas de protección que pueden implementar en su sistema:

Control de acceso a la información

- **Control de acceso a la información**: El empleado o usuario debe de tener acceso a información rigurosamente necesaria para realizar sus actividades diarias y así cumplir con las labores asignadas.
- **Conocer el tipo de información:** La empresa puede tener información baja, media y alta, pero dependerá de la interacción que exista con el personal, entrevistas y reuniones y se deberá calificarla según su criticidad.
- **Establecer mediante documentación:** Las designaciones del personal y el tipo de información que puede manejar.
- **Autorización de permisos de acceso a la información:** Se realiza de forma individual, grupal o por perfiles profesionales, generando diversos grupos de acceso al sistema, en la cual, cada trabajador debe ingresar al grupo que estrictamente le corresponda y no debe entrar a otro grupo que no le corresponde con los datos de su usuario.
- Establecer como se debe acceder al sistema y actualizar la base de datos de usuarios que han sido modificados o eliminados.

Copias de seguridad

En el Ecuador, varias empresas como las PYMES no poseen la cultura de crear copias de seguridad porque no están muy familiarizado con ese tema, pero es fundamental que toda empresa debe cumplir debido a que la cantidad de datos que maneje la empresa se pueden respaldar ante situación que pueda ocurrir.

Se deben generar copias diarias, copias totales realizadas una vez por semana, copias mensuales, y almacenar anualmente, esto ayuda a la empresa que en un momento desafortunado no cese sus actividades comerciales diarias porque al usar la copia de seguridad, se cargan los datos guardados en el sistema y se retoman sus actividades, evitando el más mínimo impacto en la empresa.

Establecer el nivel de criticidad de la información a guardar, la información es de alta importancia debe ser encriptada para evitar que cualquier persona tenga acceso a esos datos. Además, hay que considerar factores como incendios o destrucción del bien inmueble, por tanto, se debe realizar copias en la nube.

Almacenamiento en la nube

Generalmente se utiliza como un medio para cargar datos cuando ocurren situaciones como incendios o algún otro desastre natural. Esta herramienta necesita poca inversión, y se delega a terceros la confiabilidad de la información.

Es importante que antes de acceder a un servicio de información en la nube se debe de leer los términos y condiciones.

Hay que tener en cuenta que se debe almacenar únicamente datos de la empresa, no personales. Un punto principal en el almacenamiento de la nube es verificar las políticas de las empresas de las cuales se contrata el servicio de seguridad de la nube, debido a que, si es de otros países, se debe adaptar al entorno y a las políticas establecidas en otros lugares.

Cifrado de la información

Se debe utilizar técnicas de codificación de la información evitando que el personal no autorizado pueda acceder de forma fácil al sistema. Por eso, se deben de considerar algunos aspectos:

- **La clave debe tener alto grado de dificultad y contiene:** Números, combinación de mayúsculas y minúsculas, incluya mínimo un carácter especial, tener longitud mayor a 8 caracteres.
- **No debe contener:** Información personal, secuencia de números (1234). no repita caracteres.
- **Consejos adicionales:** La contraseña es de conocimiento personal, no anotar la contraseña en papeles, no incluir contraseña en documentos electrónicos.

Conclusiones

En el presente, varios sistemas de información son vulnerados por ciberdelincuentes, quienes se aprovechan de las debilidades existentes y extraen información relevante, que en la mayoría de los casos es utilizada con fines extorsivos o vendidas a competencias directas de las empresas, de allí radica que es fundamental que las organizaciones inviertan recursos en el área de sistemas para salvaguardar los activos de información.

En este trabajo de investigación se realizó encuestas a profesionales del área de sistemas y mediante el juicio profesional de ellos, se pueda conocer los diversos problemas que pueden ocurrir en la seguridad de información de las empresas. Algunos inconvenientes como: (a) ataques de posibles hackers, (b) filtración y perdida de información, (c) accesos no autorizados, se pueden suscitar en las organizaciones. Por eso, los resultados obtenidos mediante las encuestas aportan a este trabajo de investigación para la implementación de un análisis que permitirá: (a) encontrar soluciones a inconvenientes que puedan ocurrir, (b) mejorar la protección de los datos de los sistemas de las PYMES del sector servicios de la ciudad de Guayaquil.

Estas empresas han implementado la ISO 27001 porque es especializada en el tema de la seguridad de información. Dicha norma define de manera genérica, independientemente de los factores ambientales de organización: (a) entorno, (b) contexto, (c) activos de las TIC, (d) información, (e) cultura organizacional, tanto internos como externos a la misma y de los activos de los procesos de la organización: (a) políticas, (b) procedimientos, (c) procesos, cómo se: (a) planifica, (b) implanta, (c) verifica y (c) controla un Sistema de Gestión de Seguridad de la Información (SGSI), a partir de la realización de: (a) un análisis de riesgos y (b) de la planificación e implantación de la respuesta a los mismos para su mitigación, es decir, cualquier empresa u organización puede desplegar un SGSI siguiendo este estándar.

Es importante que cualquier organización implemente el plan del SGSI porque dicho plan tiene como base la identificación de los controles de seguridad, en el cual, se hace la selección de: (a) salvaguardas, (b) controles, (c) monitoreo y (c) asignación de las responsabilidades, con el fin de: (a) evitar, (b) controlar, (c) transferir y (d) mitigar los

riesgos detectados. El establecer controles de seguridad de información que permitan que: (a) la información esté disponible a quienes tienen permiso para acceder a ella, (b) que se mantenga íntegra desde su origen hacia su destino y (c) que sea conocida solo para quien esté dirigida, es decir, solo puede: (a) ingresar la persona autorizada y (b) hacer uso de la información con el fin de mejorar y (c) continuar con los procesos que existen dentro del sistema de la entidad.

La mayoría de PYMES no cuentan con la seguridad necesaria en sus sistemas informáticos, porque gran parte de los propietarios: (a) ignoran o subestiman la importancia y (b) el uso de la información que hay en sus empresas o simplemente creen que al ser sus empresas pequeñas no las convierten en blancos y (c) como consecuencia están expuestas a diferentes tipos de ciberataques debido a las vulnerabilidades que tienen sus sistemas. Por eso, la aplicación de la norma ISO 27001 y la ejecución de controles de seguridad permite: (a) proteger la información de los sistemas de las empresas mencionadas.

Recomendaciones

Se recomienda que varias entidades puedan ejecutar los sistemas de planificación de recursos empresariales ERP, son los sistemas que abarcan toda la información de la empresa tanto: (a) de sus usuarios y (b) sus clientes, de allí radica la importancia de que las empresas adopten medidas para proteger su principal activo que es la información. Además, pueden poner en funcionamiento: (a) el uso de Sistemas de Detección de Intrusos-IDS y (b) Sistemas de Prevención de intrusos-IPS, son herramientas que permiten: (a) monitorear toda nuestra infraestructura tecnológica y (b) de redes, generando alertas en caso de que personal no autorizado quiera acceder a la información del sistema de la entidad.

Se recomienda capacitar al personal con: (a) programas relacionados a la seguridad de la información y (b) las vulnerabilidades que el sistema de información puede presentar. De esta manera, el personal del área de sistemas estará actualizado sobre: (a) las diversas amenazas y (b) ataques que puedan ocurrir en el sistema.

Por otro lado, se recomienda que el área de sistemas monitoree constantemente: (a) el sistema y (b) los datos que hay en ella, ayuda a que las organizaciones: (a) detecten y conozcan las vulnerabilidades a las cuales la información estará expuesta, (b) el realizar pruebas de penetración-Pentesting, son buenas estrategias que ayudan a lograr esto. Es fundamental contar con el personal capacitado para que estén preparados a: (a) posibles incidentes que puedan ocurrir, (b) al cierre de brechas, (c) al análisis de vulnerabilidades de los sistemas y (d) establecer medidas que permitan la mitigación de cualquier tipo de ataque o pérdida de información.

Es fundamental realizar trabajos de auditoria cada cierto periodo de tiempo para verificar que la seguridad del sistema sea la más óptima, debido a que el avance de la tecnología con: (a) cambios y mejoras en los softwares y (b) las apariciones de nuevos hardware, obliga que las empresas ejecuten controles cada cierto tiempo.

Anexos

Anexo 1 Autorización para el uso de la encuesta validada

En este trabajo de investigación se trabajará con una encuesta validada, sin embargo, se solicitó la autorización a los autores de la encuesta Ings. José Córdova y William Remicio, quienes a través de una carta autorizaron el uso de la misma.

José María Córdova Salinas

jcordovas87 · Instagram

Ver perfil

31 jul 2023 04:05

Buenas noches estimado José María Córdova Salinas, me contacto por este medio con usted y le comento que estaba buscando información en el internet y me salió este trabajo y menciona que usted lo hizo junto a otra persona. Si en verdad este es su trabajo, le pido la autorización para usar las encuestas u otra información de su trabajo de investigación. El motivo del uso de su información es que soy un estudiante universitario y necesito su información para mi trabajo de tesis de investigación sobre la seguridad de información. Por favor espero me pueda ayudar con mi pedido y yo pueda continuar y mejorar mi trabajo de tesis de investigación en base al aporte de su información.

En espera de una pronta respuesta

Atentamente,

Steven Bonilla
Estudiante de CPA

https://repositorio.upci.edu.pe/handle/upci/634

"Modelo del Sistema de Gestión de Seguridad de la Información basado en la ISO 27001:2013 para minimizar los riesgos de seguridad en el área de...

Dom, 15:31

Hola Steven, disculpame, recién veo tu mensaje.

Lun, 03:30

Hola, no hay problema pero por favor me puedes ayudar con tu autorización para usar tu información para mi trabajo de tesis

Lun, 06:01

Si, está bien, no te olvides de citar correctamente para que no te lo detecte cómo plagio.

Lun. 08:42

Lun, 03:30

Hola, no hay problema pero por favor me puedes ayudar con tu autorización para usar tu información para mi trabajo de tesis

Lun, 06:01

Si, está bien, no te olvides de citar correctamente para que no te lo detecte cómo plagio.

Lun, 08:42

Claro y gracias por tu apoyo

👍👍

Anexo 2: Instrumento de recolección de datos

"Encuesta para determinar el modelo del Sistema de Gestión de Seguridad de la Información para minimizar los riesgos de seguridad en el área de sistemas de las firmas auditoras en la ciudad de Guayaquil "

La presente encuesta tiene como objetivo: Obtener información que permita desarrollar de forma eficiente el modelo de sistema de gestión de seguridad de la información que ayude a minimizar los riesgos de seguridad en el área de sistemas de las firmas auditoras en la ciudad de Guayaquil.

Los encuestados responderán las preguntas según su juicio profesional.
En cada pregunta deben escoger una de las diversas puntuaciones de la escala valorativa, en donde, 5 es la máxima puntuación-totalmente de acuerdo, 1 es la mínima puntuación-totalmente desacuerdo.

Tabla 7

Escala valorativa

ESCALA VALORATIVA

INDICE	INTERVALO	PUNTUACION
A	Totalmente en desacuerdo	1
B	En desacuerdo	2
C	Indiferente	3
D	De acuerdo	4
E	Totalmente de acuerdo	5

Tabla 8

Cuestionario

CUESTIONARIO	ESCALA VALORATIVA				
Sistema de Gestión de Seguridad de la Información	**1**	**2**	**3**	**4**	**5**
1. ¿Usted piensa que las firmas auditoras cumplen los requisitos del sistema de gestión de la seguridad de la información?					

2. ¿Es fundamental la implementación del sistema de gestión de la seguridad de la información en las firmas auditoras?					
3. ¿Cree usted que es importante la seguridad de los activos de información?					
4. ¿El diseño de un Sistema de Gestión de la Seguridad de Información para las firmas auditoras mejorará la protección de los activos de información?					
5. ¿El diseño y la implementación de controles de seguridad de la información permitirá reducir los riesgos a los activos de información?					
6. ¿Para usted al contar con menores controles de seguridad de la información representa desventaja?					
7. ¿Los controles sobre las vulnerabilidades de los sistemas de información en las firmas auditoras, mejorará la protección de la información de dichas entidades?					
8. ¿La implementación del plan del SGSI permitirá mitigar los riesgos de información?					
9. ¿Cree usted que es clave que las firmas auditoras implementen controles que eviten el acceso no autorizado a los sistemas de información?					
10. ¿Usted considera que al implementar ERP es importante para los sistemas de seguridad de información?					
11. ¿Cree usted que las firmas auditoras mejoraran la seguridad de información al recurrir a terceros?					

Referencias

Figueroa, J., Rodríguez, R., Bone, C., & Saltos, J. (2017). *La seguridad informática y la seguridad de la información.* Ecuador: Pol. Con. (Edición núm. 14) Vol. 2 No 12.

Agudelo, V., & Aigneren, A. (2008). *CEO-Diseños de investigación experimental y no-experimental*. Obtenido de https://bibliotecadigital.udea.edu.co/handle/10495/2622

Albán, V., Soler, C., & Oñate, A. (2 de Septiembre de 2018). *La teoría de redes y la gestión de riesgos-Revista Universidad y Sociedad de la universidad Politécnica de Chimborazo del Ecuador*. Obtenido de http://scielo.sld.cu/scielo.php?pid=S2218-36202018000400239&script=sci_arttext&tlng=en

Angelelli, P., Hennessey, M., & Henriquez, P. (2020). *Respuestas al COVID-19 desde la ciencia, la innovación y el desarrollo productivo.* Banco Interamericano de Desarrollo.

Arciniegas, J., & González, Ó. (2020). *Sistemas de Gestión de la Calidad.* Colombia: Ecoe Ediciones.

Asamblea Nacional República del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales.* Quito: Quinto Suplemento No. 459 Registro Oficial. Obtenido de https://drive.google.com/file/d/1UhmqRQpkkBjWs5iGGiB_oOxKeRdaX2Ut/view

Bueno, G., & Haz, L. (2022). *Ciberseguridad post covid-19 y su impactoen las pymes del Ecuador.* Ecuador: Universidad Estatal Península de Santa Elena. doi:https://doi.org/10.29018/issn.2588-1000vol6iss46.2022pp103-12

Bueno, J., & Ferreira, M. (2017). *La ruta de la transformación digital. Descubre las claves de digitaliziación en las empresas.* España: Edición Kindle.

Calder, A. (2017). *ISO27001/ISO27002: Una guía de bolsillo.* México: Edición Kindle.

Calso, & Pardo. (2019). *Guía práctica para la integración del sistema de gestión ISO 9001, ISO 14001 e ISO 45001.* México: Alphaeditorial.

Camino, S., Bermudez, N., Chalen, A., Gutierrez, P., & Romero, D. (2018). *Panorama del Sector de Servicio.* Ecuador: Estudios Sectoriales. Obtenido de https://investigacionyestudios.supercias.gob.ec/wp-content/uploads/2019/01/PANORAMA-DE-LAS-ACTIVIDADES-DE-SERVICIOS-EN-EL-ECUADOR-2013-2017.pdf

Coase, R. (1973). *The Nature of The Firm*. John Wiley & Sons, Ltd. Obtenido de https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1468-0335.1937.tb00002.x

Cornejo, J. (2021). *COVID-19 ¿desafío u oportunidad para nuevas herramientas tecnológicas en los negocios?* Perú: PWC Perú. Obtenido de https://desafios.pwc.pe/covid-19-desafio-u-oportunidad-para-nuevas-herramientas-tecnologicas-en-los-negocios/

Dini, M., Gligo , N., & Patiño, A. (2021). *Transformación digital de las MIPYMES. Elementos para el diseño de políticas.* Santiago de Chile: Naciones Unidas.

Obtenido de https://www.cepal.org/es/publicaciones/47183-transformacion-digital-mipymes-elementos-diseno-politicas

Franklin, E. (2016). *Comportamiento Organizacional. Enfoque para América Latina.* México: Pearson Educación de México SA. de C.V.

García Alejandro, & Leticia, E. (2012). *Teoría de la empresa: las propuestas de Coase, Alchian y Demsetz, Williamson, Penrose y Nooteboom*. Scielo. Obtenido de https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0188-33802012000100002

González, Ó., & Arciniegas, J. (2017). *Sistema de Gestión de Calidad*. Colombia: Ecoe Ediciones.

Hart, O. (1986). *Una Perspectiva Económica sobre la Teoría de la Empresa. Columbia Law Review*. Columbia Law Review. .

Instituto Nacional de Estadística y Censos. (2015). *Empresas y TIC (Tecnología de Información y la Comunicación)*. Ecuador: Instituto Nacional de Estadística y Censos. Obtenido de https://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Economicas/Tecnologia_Inform_Comun_Empresas-tics/2015/2015_TICEMPRESAS_PRESENTACION.pdf

Jurado, F., Redín, E., & Jumbo, J. (2021). *LA SEGURIDAD DE LA INFORMACIÓN DE LAS MICROEMPRESAS EN EL ECUADOR*. Quito, Ecuador: Revista Científica ECOCIENCIA. Obtenido de https://revistas.ecotec.edu.ec/index.php/ecociencia/article/view/600/386

Kahnema, D., & Tversky, A. (2014). *Teoría prospectiva: un análisis de la decisión bajo riesgo.* Taylor & Francis Online.

Kenyon, B. (2019). *ISO 27001 Controls: A Guide to implementing and auditing.* UK: Itgp.

Kosutic, D. (2016). *Seguro y Simple. Una Guía para la Pequeña Empresa para la Implementación de la ISO 27001 con medios propios.* Croacia: Advisera Expert Solutions Ltd.

Ladino, M., Villa, P., & López, A. (2011). *Fundamentos de ISO 27001 y su aplicación en las empresas-Scientia Et Technica-Universidad Tecnológica de Pereira de Colombia*. Obtenido de https://www.redalyc.org/pdf/849/84921327061.pdf

Lopez, P. (2004). *Punto Cero*. Obtenido de http://www.scielo.org.bo/pdf/rpc/v09n08/v09n08a12.pdf

Mártinez, C., & Cruz, Y. (2018). *Tendencias tecnológicas y desafíos de la seguridad informática.* Azuay, Ecuador: Pol. Con. (Edición núm. 19) Vol. 3, No 5.

McDermott, R. (2017). *Prospect Theory*. Europa: Britannica. Obtenido de https://www.britannica.com/topic/prospect-theory

Mejia, G., & Romero, S. (Septiembre de 2019). *ANÁLISIS DE VULNERABILIDAD EN UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN UNA PYME DEL SECTOR COMERCIAL*. Obtenido de http://repositorio.ug.edu.ec/bitstream/redug/44386/1/TESIS%20MEJIA%20Y%20ROMERO%202019.pdf

México, U. d. (2020). *Studocu*. Obtenido de https://www.studocu.com/es-mx/document/universidad-del-valle-de-mexico/informatica/teoria-de-la-informacion/33014435

Microsoft. (2022). *Impacto de la pandemia: 9 de cada 10 pymes aceleraron su proceso de transformación digital en Ecuador.* News Center Microsoft Latinoamérica.

Obtenido de https://news.microsoft.com/es-xl/impacto-de-la-pandemia-9-de-cada-10-pymes-aceleraron-su-proceso-de-transformacion-digital-en-ecuador/

Moreno, P. (2005). *Metodología de investigación. En El profesorado de Educación Física y las competencias básicas en TIC en el desarrollo de su actividad profesional*. Obtenido de http://biblioteca.udgvirtual.udg.mx/jspui/bitstream/123456789/3830/1/Metodolgia_investigaci%c3%b3n.pdf

Ortega, C. (2022). *Muestreo no probabilístico: definición, tipos y ejemplos-QuestionPro*. Obtenido de https://www.questionpro.com/blog/es/muestreo-no-probabilistico/

Otero, A. (2018). *Enfoques de investigación*. Obtenido de https://www.researchgate.net/profile/Alfredo-Otero-Ortega/publication/326905435_ENFOQUES_DE_INVESTIGACION/links/5b6b7f9992851ca650526dfd/ENFOQUES-DE-INVESTIGACION.pdf

Paredes, M. (2021). *"DISEÑO DE UN ESQUEMA DE SEGURIDAD INFORMÁTICA, CON BASE EN EL ESTÁNDAR ISO 27001, PARA LA EMPRESA NEGYSERT S.A., UNA PYME PRESTADORA DE SERVICIOS TECNOLÓGICOS BAJO MODALIDAD SAAS."*. Guayaquil-Ecuador. Obtenido de https://www.dspace.espol.edu.ec/handle/123456789/54424

Parra, G., & Angela, M. (2014). *ISO 27001 PARA PYMES*. Medellin-Colombia. Obtenido de https://reunir.unir.net/bitstream/handle/123456789/3128/AngelaMaria_Parra_Giraldo.pdf?sequence=1&isAllowed=y

Parra, L., & Vásquez, M. (2017). *Licenciatura en Ciencias Empresariales-Universidad del Istmo* . Obtenido de https://www.gestiopolis.com/wp-content/uploads/2017/02/muestreo-probabilistico-no-probabilistico-guadalupe.pdf

Parra, M., López, L., & Ramírez, E. (2019). *Gestión de la Competitividad Empresarial.* Colombia: Ecoe Ediciones.

Pérez, M. (2022). *Business Intelligence. Técnicas, Herramientas y Aplicaciones*. México: Alfaomega.

Pincay, B. (2021). *Economía digital, sus efectos tributarios.* Ecuador: PwC Ecuador. Obtenido de https://www.pwc.ec/es/entrevistas-de-temas-de-interes/Economia-digital-sus-efectos-tributarios.html

Pruna, F., Redín, E., & Jumbo, j. (2021). *La Seguridad de la Información de las Microempresas en el Ecuador.* Ecuador: Revista Científica ECOCIENCIA. Obtenido de https://revistas.ecotec.edu.ec/index.php/ecociencia/article/view/600/386

Ramos, S. (2022). *Cuáles son los desafíos que enfrentan las empresas en temas de transformación digital.* Ecuador: Forbes Digital. Obtenido de https://www.forbes.com.ec/liderazgo/desde-cero-dinero-7-pasos-crear-tu-marca-personal-aumentar-visibilidad-tu-carrera-profesional-n33800

Riascos, S., Aguilera, A., & Ávila, G. (2014). *Seguridad de los sistemas de información en las Pymes de Santiago de Cali (Colombia).* Colombia: Universidad del Valle – Colombia.

Rodríguez, N. (2019). *Tecnología de la Información y Comunicación TIC.* Colombia: Editorial Artesy Letras.

Rogers, D. (2018). *Guía Estrategica para la Transformación Digital. Reiventa tu negocio para la era digital.* México.

Rojas, H. (2018). *Plan De Implementación De La ISO/IEC 27001:2013.* España: Editorial Academica Espanola.

Romero, P. (2018). *Tecnología de la Información y la Comunicación.* México: Pearson Educación.

Scheel, C. (2017). *Las TIC un nuevo modelo de negocio.* México: Editorial Trillas.

Seguridad de la información-¿Qué importancia tiene la mejora continua en la seguridad de la información? (27 de Septiembre de 2018). Obtenido de https://www.pmg-ssi.com/2018/09/que-importancia-tiene-la-mejora-continua-en-la-seguridad-de-la-informacion/

Slotnisky, D. (2018). *Transformación Digital. Como las personas y Empresas deben Adaptarse a esta Revolución.* Estados Unidos: Digital House.

Slusarczyk, M., Pozo, J., & Perurena, L. (2018). *Gestión de las TIC en las empresas en la era de conocimiento.* España: Editorial Academica Espñola.

Solarte, F., Enriquez, E., & Benavides, M. (2015). *Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001.* Ecuador: Revista Tecnológica ESPOL –RTE, Vol. 28, N. 5, 492-507. Obtenido de http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321

Superintendencia de Compañías, Valores y Seguros. (2022). *Ranking de Empresas.* Ecuador: Superintendencia de Compañías, Valores y Seguros.

Vasconcelos, J. (2019). *Informática I.* Madrid: Editorial Patria.

Velázquez, A. (20 de Agosto de 2022). *Investigación experimental: Qué es, tipos y cómo realizarla-QuestionPro*. Obtenido de https://www.questionpro.com/blog/es/investigacion-experimental/

Velázquez, A. (s.f.). *Investigación experimental: Qué es, tipos y cómo realizarla-QuestionPro*. Obtenido de https://www.questionpro.com/blog/es/investigacion-experimental/

Williamson, O. (1975). *The Theory of The Firm as Governance Structure: From Choice to Contract.* Obtenido de https://www.researchgate.net/publication/4734059_The_Theory_of_the_Firm_as_Governance_Structure_From_Choice_to_Contract

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Bonilla Sánchez, Steven Gonzalo** con C.C: #0929463578 autor del trabajo de titulación: **Análisis para la Aplicación de la Norma ISO 27001 en Pymes del Sector Servicios de la Ciudad de Guayaquil, año 2022**, previo a la obtención del título de Licenciado en Contabilidad y Auditoría en la Universidad Católica de Santiago de Guayaquil.

1.- Declaramos tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizamos a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 7 de septiembre de 2023

f. 

Bonilla Sánchez, Steven Gonzalo
CC. 0929463578

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	Análisis para la Aplicación de la Norma ISO 27001 en Pymes del Sector Servicios de la Ciudad de Guayaquil, año 2022.		
AUTOR (ES)	Bonilla Sánchez, Steven Gonzalo		
REVISOR(ES)/TUTOR(ES)	Ing. Com. Delgado Loor, Fabian Andrés. MBA		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Economía y Empresa		
CARRERA:	Contabilidad y Auditoría		
TITULO OBTENIDO:	Licenciado. Contabilidad y Auditoría		
FECHA DE PUBLICACIÓN:	7 de septiembre de 2023	**No. DE PÁGINAS:**	87
ÁREAS TEMÁTICAS:	Norma ISO 27001 en Pymes del Sector Servicios de la Ciudad de Guayaquil, año 2022		
PALABRAS CLAVES/ KEYWORDS:	Norma ISO 27001, SGSI, TIC, Sistema Informático, Riesgos, Vulnerabilidad, Seguridad Informática, PYMES.		

RESUMEN/ABSTRACT (150-250 palabras):
En el presente trabajo de análisis de la aplicación de la norma ISO 27001 se estableció como objetivo general el analizar esta norma en PYMES del sector servicios de la ciudad de Guayaquil para el fomento de una gestión apropiada de seguridad de información con base en un diagnóstico del estado actual de la seguridad de la información en las Pymes seleccionadas. El estudio se enmarcó dentro de una investigación de carácter descriptivo. Los estudios descriptivos buscan especificar: (a) las propiedades, (b) las características y (c) los perfiles importantes de: (a) personas, (b) grupos, (c) comunidades o (d) cualquier otro fenómeno que se someta a un análisis. El método utilizado en la investigación fue: (a) Por juicio: el cual consiste en que los sujetos se seleccionan basados en: (a) conocimiento, (b) experiencia y juicio del investigador. Los principales resultados obtenidos por implementación de protección de datos: (a) nos muestra que las firmas auditoras implementaron el SGSI, (b) piensan que la implementación será un gasto adicional, (c) la no implementación puede sufrir amenazas de su información, (d) no se preocupan por la información. En conclusión, es importante que las organizaciones implementen el plan del SGSI porque identifican los controles de seguridad, los cuales: (a)salvaguardan, (b) controlan, (c) monitorean y (d) asignan responsabilidades, con el fin de: (a) evitar, (b) controlar, (c) transferir y (d) mitigar los riesgos detectados.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** 0989559577	E-mail: stbonilla19@gmail.com
CONTACTO CON LA INSTITUCIÓN (COORDINADOR DEL PROCESO UTE):	**Nombre:** Bernabé Argandoña Lorena Carolina	
	Teléfono: +593-4-2206953 Ext. 1635	
	E-mail: lorena.bernabe@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	