UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE GUAYAQUIL

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
INGENIERO DE SISTEMAS

CARRERA:

INGENIERÍA DE SISTEMAS

TEMA:
“IMPORTANCIA DE LA ISO 27001 EN LAS PYMES DE GUAYAQUIL:
CASO DE ESTUDIO TRANSNAVE”

AUTOR:

Kesli Lissette Preciado Oquendo

TUTOR:

Msg. Miguel Ángel Quiroz Martínez

Junio 2021

GUAYAQUIL-ECUADOR

DECLARATORIA DE RESPONSABILIDAD

Yo, **Kesli Lissette Preciado Oquendo**, declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del/los autor/es.

Firmado electrónicamente por:
KESLI LISSETTE
PRECIADO
OQUENDO

Firma del autor
Nombre: Kesli Lissette Preciado Oquendo
CI. 0953377140

Firma del tutor
Ing. Miguel Quiroz Martínez

IMPORTANCIA DE LA ISO 27001 EN LAS PYMES DE GUAYAQUIL: CASO DE ESTUDIO TRANSNAVE

Miguel Quiroz Martinez[1[0000-0002-8369-1913]] and Kesli Preciado Oquendo[1[0000-0003-0167-1677]]

[1] Universidad Politécnica Salesiana, Guayaquil, Ecuador
mquiroz@ups.edu.ec, kpreciado@est.ups.edu.ec

Abstract. En los años recientes, con la adaptación integral de la tecnología de la información, la seguridad de la información se ha convertido en un tema fundamental en la administración empresarial. Se han desarrollado varios estándares y pautas de seguridad y manejo de la información, como ISO / IEC 27001, ISO, COBIT, ITIL pero las empresas aún enfrentan obstáculos en el proceso de implementación. Este artículo presenta el estado actual del proceso de implementación de la norma ISO / IEC 27001 en las entidades y empresas de la gestión pública; con la finalidad de estudiar una empresa con un paradigma distinto a la comercialización de productos, se analizó el proceso de implementación de una empresa ubicada en Guayaquil dedicada a dar servicio de transporte naviero; Actualmente, existen muchas formas de implementar el Sistema de Gestión de Seguridad de la Información (SGSI) en pequeñas y medianas empresas basado en el Ciclo de mejora continua. Finalmente, Se propondrán algunos aspectos a considerar para implementar un SGSI en pymes. En este artículo, a través de una investigación cualitativa ha estudiado la forma en que las pymes enfrentan la seguridad de la información e identificar sus principales obstáculos al momento de implantar en la entidad un sistema de gestión de seguridad de la información (SGSI).

Abstract. In recent years, with the comprehensive adaptation of information technology (IT), ithe security of the information has become a fundamental issue in business management. Various information management, security standards and guidelines have been developed, such as ISO / IEC 27001, ISO, COBIT, ITIL but companies still face obstacles in the implementation process. This paper presents the current state of the implementation process of the ISO / IEC 27001 standard in public management entities and companies; In order to study a company with a paradigm other than the commercialization of products, the implementation process of a company located in Guayaquil dedicated to providing shipping service was analyzed; Currently, there are many ways to implement the Information Security Management System (ISMS) in small and medium-sized companies based on the Cycle of continuous improvement. Finally, some aspects to consider to implement an ISMS in SMEs will be proposed. In this article, through qualitative research, he has studied the way in which SMEs face information security and identify their main obstacles when implementing an information security management system (ISMS) in the entity.

Keywords: Seguridad, Información, SGSI, Ciberataque, Factores críticos de éxito.

1 Introducción

El uso frecuente de la tecnología de la información y comunicación (TIC) se ha convertido en un elemento taxativo para el éxito de cualquier entidad pública o privada y se ha convertido en una parte integral de los procesos administrativos de una empresa; la importancia de la información es cada vez más primordial en la gestión organizacional, ya que uno de sus propósitos básicos es prolongar su operatividad en el mercado; la implementación de tecnología ha traído amenazas, aumento de ciberataques y virus[1]. La sujeción de las tecnologías de la información ha aumentado y, en algunos casos, la tasa de pérdidas financieras es alta en comparación con las organizaciones que están estancadas y sin potencial de desarrollo, la diferencia entre las organizaciones exitosas es sin lugar a duda la información y su capacidad de transformarla para la toma efectiva de decisiones. Las pequeñas y medianas empresas deben conocer que la información obtenida dentro o fuera de la organización nos sitúa en una gestión real del desarrollo empresarial; por tanto, la cultura de seguridad de la información debe ser inculcada en todos los miembros que conforman la organización[2].

En la llamada comunidad del conocimiento, el desarrollo de la tecnología de la información ha provocado cambios en el comportamiento de cada empleado de la organización, en esta sociedad el talento humano es la base de la transformación económica y tecnológica de este siglo; en Ecuador, las pymes han crecido en los últimos cinco años significativamente en su cartera de inversiones y producción, lo que crea más puestos de trabajo, pero en seguridad de TI se aíslan del progreso y esto los hace víctimas de ataques maliciosos al no implementan métodos efectivos de detección temprana aun de los ataques más comunes phishing o programa maligno[3].

La finalidad de esta investigación es individualizar y determinar algunas de las razones por las cuales las pymes se encuentran con obstáculos al implementar sistemas, planes, o esquemas para mitigar los riesgos de seguridad de la información independientemente de sus niveles de ingresos y producción, desde una perspectiva técnica a un plano de gestión empresarial y el nivel de compromiso que deben tener todos los que cumplen un rol de la organización, para lo cual se compararan diferentes empresas con el mismo objetivo de incrementar sus niveles de seguridad cumpliendo con el Esquema Gubernamental de Seguridad de la Información (EGSI), que en los últimos años el estado ecuatoriano exige a empresas públicas y estatales, cuyo organismo de control para este objetivo es el ministerio de telecomunicaciones[4].

Poco a poco las empresas empiezan a notar la gran ventaja que les proporciona un buen manejo de la información, no solo en seguridad sino también para poder establecer estrategias que les ayuden a sobresalir en su mercado, no obstante, las PyMes aun no le dan la relevancia a la protección y administración de su activo intangible más preciado; algunas de las fallas que las Pymes cometen regularmente son:

Desatender la infraestructura técnica.

El error más común es creer que los equipos de una red corporativa no son vulnerables. Sin embargo, contrariamente a esta consideración, esta es una de las formas más fáciles de estar expuesto a ataques cibernéticos como el phishing, que es donde se recopila información privada de un usuario presentándose como un contacto de confianza

de nuestra empresa, otro problema común en las empresas es el software malicioso. Este software descarga contenido malicioso en nuestras computadoras, encripta las unidades de almacenamiento de un equipo, y luego requiere un pago para devolver los datos robados. Esto es algo básico que muchos empleados de la organización no conocen, convirtiendo al usuario final la mayor vulnerabilidad de la seguridad de una empresa.[5]

No apreciar la información

La información actualmente es el activo intangible más preciado de una institución que se genera diariamente y todas las áreas generan información sensible e importante para un análisis dispuesto para la toma de decisiones gerenciales; el acceso ilimitado a ella sin definir roles de acceso pueden traer consecuencias en cuanto a la veracidad y disponibilidad de la información, las empresa no tienen definido que información ni a que niveles dentro de la organización le corresponde su custodio y divulgación.

Lo único necesario es un antivirus.

Varias empresas pequeñas y medianas necesitan incrementar el nivel de seguridad y al momento de pensar en proteger sus datos piensan en antivirus lo que genera una percepción falsa de seguridad descuidando otros factores técnicos y organizacionales.[6]

La base de seguridad es solo software o hardware.

Luego de que las empresas adquieren software como antivirus y equipos de hardware como firewall pueden llegar a sentirse más protegidos, dejando a un lado aspectos importantes de la información como sus accesos, custodios y aspectos legales de confidencialidad.

No establecer un plan de continuidad del negocio.

La mayoría de las empresas no tomarán medidas para prepararse para dificultades o urgencias que obstaculicen sus operaciones normales. La alta dirección es indiferente ante esto, pensando que "mi empresa no va a suceder" o "los planes de continuidad del negocio son caros y solo las grandes empresas con gran infraestructura tecnológica pueden permitírselo", y solo evalúan el costo[3].

Inversión tecnológica equivocada. Las pequeñas y medianas empresas tienen una inversión insuficiente en tecnología y, cuando lo hacen, generalmente obtienen equipos y software que no están en línea con el progreso de la tecnología sin pensar también en el desarrollo y crecimiento futuro de la empresa.

Un estudio elaborado por la compañía de seguridad Kaspersky denominado “Informe Especial ¿Quién le espía?” señala que ninguna empresa está exenta de sufrir ciberataques. Sin los mayores ataques son hacia las pymes que son más vulnerables a esta problemática por su mayor falta de recursos y también por su menor concienciación en este aspecto, además de considerarse una vía abierta y de confianza para obtener información de empresas más grandes debido a sus relaciones y comunicaciones comerciales.[3]

2 Materiales y Métodos

Los trabajos relacionados a la investigación muestran los resultados de implementaciones de esquemas de seguridad de la información en diferentes empresas clasificadas como medianas o pequeñas, y una inmersión de las recomendaciones y requisitos de la ISO 27001 además del MAGERIT como una ayuda para realizar evaluaciones y determinación de niveles de riesgo en sistemas de información.

2.1 Materiales

Como materiales podemos establecer que necesitamos conocer a profundidad la norma ISO 27000 sus requisitos y recomendaciones para su aplicación, esta va de la mano también con saber evaluar e identificar los niveles de riesgo en los que se encuentra una organización, para esto el MAGERIT ofrece un método de análisis y tratamiento para la mitigación de riesgos desarrollado por el Comité de Estrategia de TIC para responder a la percepción de las entidades en su conjunto confían cada vez más en las tecnologías de la información para cumplir con su objetivo[4].
La razón para tomar como guía de evaluación de vulnerabilidades tecnológicas a MAGERIT está estrechamente vinculada con el uso frecuente de la tecnología, que aporta grandes beneficios a la organización, pero también trae consigo algunos riesgos, que deben ser mitigados mediante medidas de seguridad que fomenten la confianza; conocer y dominar esta metodología puede ayudarnos a identificar y definir los riesgos que tienen nuestros sistemas de información como por ejemplo lo sistemas contables. Aplicar un esquema de seguridad de la información se debe tener en cuenta los niveles de riesgos y las áreas más vulnerables, para esto la ISO 27001 establece una estructura de 6 fases a seguir para su implementación[7].

Alcance y campo de aplicación Auditoria inicial. El alcance del SGSI se define como: Determinar qué información queremos protege; comprender esto es crucial, porque debemos considerar la responsabilidad de proteger la información, sin importar dónde, cómo y quién acceda a esta información; con base en el análisis de riesgos, podemos obtener un informe analizando el cumplimiento de los hitos de control para establecer un plan para su aplicación y su estado de cumplimiento, además de ayudarnos a preparar la declaración de aplicabilidad[5].

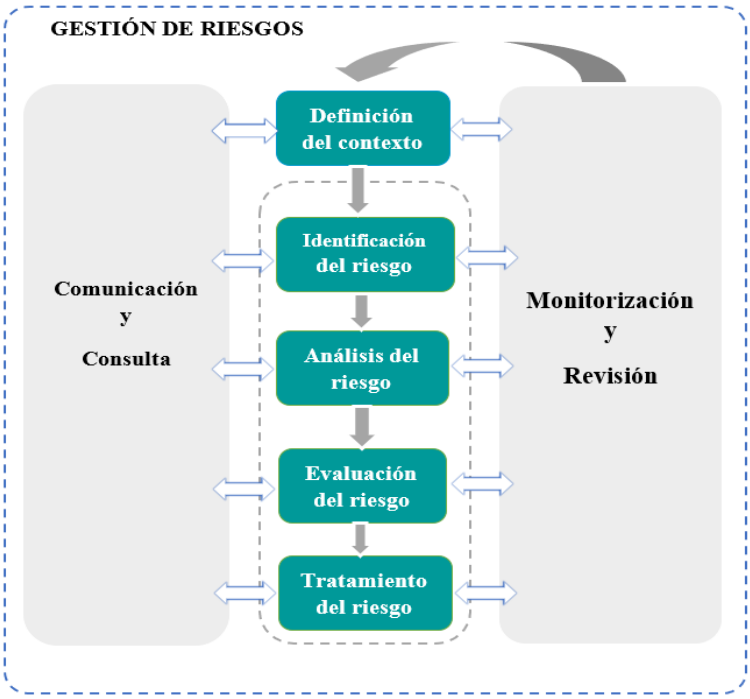
Análisis del entorno de una organización. Esta fase incide en definir en qué proporción los aspectos internos y externos pueden intervenir en el objetivo de la organización y su eficacia para lograr los efectos previstos del SGSI. Es decir, problemas que pueden perjudicar la seguridad de la información por agentes externos e internos en las que están inmersas las actividades organizacionales; se trata de definir el efecto en la seguridad de la información establecido por los siguientes factores[8]:

- Como se administra su organización.
- Conocimientos y aptitudes organizacionales.
- La cultura de la organización.

- Las relaciones contractuales.
- La influencia de condiciones ambientales.
- Predisposición del mercado y normas regulatorias.
- Los progresos tecnológicos.
- El vínculo con proveedores externos.

Gestión del riesgo. Como se ha visto, el proceso comienza con la evaluación del contexto como punto de partida. Esto asegura que el riesgo sea tratado por las necesidades reales de las partes interesadas en términos de seguridad de la información. El resultado del proceso de evaluación de riesgos es información valiosa, así como los riesgos de seguridad de la información, tomando en cuenta el entorno empresarial de la organización, en este proceso de identificación de riesgos, debemos determinar los activos de información, sus riesgos y determinar posibles acciones ante eventos adversos[8].

Fig. 1. Ciclo de gestión del riesgo



Selección de controles a implementar. Esta fase se basa en la auditoria inicial y la contextualización de la organización herramientas de análisis con la que podremos elegir de acuerdo con las necesidades de la empresa los activos de información que se deben proteger, estableciéndolos controles con una declaración de aplicabilidad obtenida de la auditoria inicial realizada para detectar los riesgos existentes y sin control[9].

Declaración de aplicabilidad. Este documento es un requisito que se encuentra en la norma ISO 27000 donde se listan los hitos y su nivel de cumplimiento, pero también se puede utilizar para realizar un control interno del avance de las medidas de seguridad aplicadas en una organización[11].

Revisión del sistema. No se trata solo de centrarse en la obtención de los certificados ISO 27000, sino que debemos tener en cuenta que la gestión de seguridad de la información correctamente implantado podria ser la clave para alinear los procesos de TI con los procesos generales de una empresa. Esta integración de la seguridad de la información en los procesos organizacionales nos ayudará fundamentalmente a reducir el nivel general de riesgo.

2.2 Métodos

La investigación realizada es cualitativa y cuantitativa. Para el estudio del proceso de implementación de ISO 27001 Se ha analizado información de la empresa TRANSNAVE, quien fue participe de EGSI v1, esta fue tomada de su página web puesto que la LOTAIP exige a instituciones del estado informar al público su administración; se realizó el análisis de los artículos de investigación con la finalidad de presentar los resultados a nuestro enfoque de seguridad para la información en PyMes de Guayaquil.
En varios artículos que estudian o evalúan factores críticos de éxito en la implementación de la seguridad de información" respecto al rol e interpretación del usuario y con datos tomado de cada institución. Los autores proponen un modelo con varios factores críticos de éxito y sus indicadores para la implementación de políticas y medidas para mitigar riesgos conforme a la norma ISO 27001[12]; en la tabla 2 se presenta la descripción de los factores críticos considerados por diversos autores en cada una de las categorías establecidas.

Tabla 2. Agentes críticos de éxito en la implementación de la ISO 27001

Ref.	Dimensión	Indicador
[13]	Compromiso de la Alta Gerencia	Apoyo y compromiso
		Resistencia al cambio
		Motivación
		Necesidades del negocio
		Administración del presupuesto
[6]	Cultura Organizacional	Idioma
		Conducta y actitud
		Sistema de valores
		Perspectivas del cambio social
		Motivaciones
[14]	Misión de la Organización	Claridad
		Alineamiento
		Cumplimiento
		Seguridad
[16]	Recurso y presupuesto	Aplicación optima de recursos y materiales
		Apoyo óptimo de activos humanos
		Provisión según necesidades empresariales

[12]	Formación y Capacitación	Continuidad Instrucción en seguridad de activos Formación y formación en temas de seguridad
[13]	Alineamiento con el negocio	Alineamiento con los objetivos de la organización.
	Competencias de TI	Proyectos bien estructurados con enfoque holístico. Programa de trabajo bien estructurado
[16]	Desarrollo de controles de seguridad	Evaluación de riesgos Selección de hitos de cumplimiento Documentación Cumplimiento de la Políticas de Seguridad y Adaptación al modelo empresarial

3 Resultados

Para realizar esta investigación, con base en los resultados de la revisión de diferentes trabajos, se planteó una encuesta basada en factores críticos de éxito para evaluar la implementación de la norma ISO en tres empresas públicas con la finalidad de obtener información pública mediante la ley orgánica de transparencia de acceso a la información; utilizando la matriz lado a lado, para elaborar preguntas en relación con el nivel de cumplimento del EGSI y su nivel de satisfacción en relación con los controles de seguridad. Las calificaciones basadas en la matriz lado a lado tienen las siguientes respuestas probables: nivel de importancia que comprende valores de 1 a 5 y nivel de satisfacción también comprendida en una escala de 1 a 5 entre insatisfecho y muy satisfecho

Una vez realizada la encuesta se tomó el mejor resultado para definir una línea de base además de realizar una investigación en el ranking que propone el Ministerio de Telecomunicaciones periódicamente en donde se indica la fase y el nivel de cumplimiento de cada institución

Tabla 3. Empresas del caso de estudio

	E1	E2	E3
Tipo	Estatal	Publica	Publica
Número de empleados	100	488	156
Ingreso anual	$1.995.450	$14.044.502	$298.863.304
Financiamiento	Fondos propios	Fondos propios	Recursos Fiscales /y Autogestión

En la fase comparativa se realizó el análisis por cada factor crítico por lo que obtendremos el nivel de cumplimiento de cada factor de éxito por cada una de las empresas públicas establecidas en la tabla 3.

Tabla 4. Resultados del estudio de implementación del Esquema gubernamental de seguridad de la información en empresas públicas.

Factores críticos de éxito	*E1*	*E2*	*E3*	*Prácticas Empresariales*
Compromiso de la Alta Gerencia	40%	90%	70%	Los gerentes de las instituciones encargan en los comités de gestión empresarial la implementación de los mecanismos de seguridad de la información.
Cultura Organizacional	30%	100%	100%	La carencia de profesionales en seguridad de la información ha obligado a quienes carecen de aptitudes necesarias, improvisar sus funciones, para obtener un nivel de cumplimiento aceptable ante las entidades de control.
Misión de la Organización	30%	62%	80%	Los objetivos de la organización no están alineados con el activo de la información para estrategias empresariales y toma de decisiones.
Recurso y presupuesto	10%	20%	60%	La adquisición de equipos y recursos informáticos para la seguridad de la información se considera un gasto. El presupuesto siempre debe ser ajustado a la necesidad principal de la empresa y su modelo de negocio.
Formación y Capacitación	25%	63%	70%	El presupuesto para la formación del personal en seguridad de la información es muy reducido, generalmente la seguridad no forma parte del plan de capacitación anual.
Alineamiento con el negocio	23%	70%	70%	Las instituciones públicas reglamentariamente deben implementar el EGSI norma ISO / IEC 27001. El comité está presidido por representantes de la alta dirección y es responsable de aprobar las medidas de control de seguridad y los niveles de riesgo aceptables.
Competencias de TIC	70%	90%	87%	El personal de TI en algunas instituciones públicas tiene los conocimientos y habilidades necesarios, pero no son especializados ni capacitados en la norma ISO / IEC 27000.
Desarrollo de verificación de seguridad	40%	96%	100%	Las normas de seguridad de la información se aprueban y publican solamente con el fin de cumplir con la ordenanza del MINTEL. Las políticas y controles de seguridad se consideran barreras para la gestión.

Analizando la empresa TRANSNAVE desde estos factores críticos se muestra que dentro de la misión de la organización en sus “Regulaciones y procedimientos

internos aplicables a la entidad"[18] no se establecen los procesos en base a la seguridad de la información descuidando así su activo intangible más importante para la toma de decisiones. El autor señala que el apoyo del nivel de toma de decisiones es uno de los fatores críticos más importantes en el éxito de implementación de un SGSI, debido al poder de tomar decisiones y proporcionar los recursos y materiales necesarios para un proyecto como este; finalmente este concepto debe integrarse y darle mayor relevancia a la seguridad de la información alineando esta con las metas de la empresa[7], así el éxito de esta cultura se debe a que todas las personas de la empresa la comparten, interiorizan y se comunican con ella. Esta cultura debe ser el camino y guía que nos oriente para lograr los resultados esperados en la organización. Refiriéndonos a recursos y presupuesto de acuerdo con la información generada por la empresa naviera en el 2019, este destino de su presupuesto de gasto anual el 0,31%[18] además que el porcentaje de personal de tecnología fue de tan solo el 1% en referencia a su nómina.

4 Discusión

De acuerdo con los resultados de esta investigación y caso de estudio de la empresa se puede evidenciar que las empresas medianas o pequeñas se enfrentan a mayores obstáculos ya que los factores críticos para el éxito se repiten como un común denominador en cada implementación ya que su cultura organizacional, visión general y presupuestos están sujetas al rendimiento de su modelo de negocio.

Cultura organizacional y visión de la Gerencia

Uno de los factores principales y el que determina el inicio del proyecto, de acuerdo con la norma ISO 27001 es la participación de la gerencia o alta dirección de una empresa. No estamos hablando de expresiones persuasivas, ya que una empresa debe asumir desde el principio que el sistema de gestión de la seguridad de la información afectará la gestión y objetivos de la empresa, y se requiere que todas las decisiones y acciones posteriores solo puedan ser ejecutadas por la dirección de la organización. No es posible delegar la seguridad de la información a una sola área considerándolo solamente como tema técnico que reemplaza a los estratos inferiores de la organización, por lo que los riesgos e impactos comerciales deben ser gestionados para que la responsabilidad provenga de la gestión organizacional.[10]

Presupuesto y proyectos de inversión.

Aunque no hay una regla establecida acerca de qué porcentaje del presupuesto anual de una empresa deba dedicarse a los proyectos de tecnología esto dependerá del modelo de negocio al que se dedique la empresa y su entorno; el presupuesto de tecnología puede llegar a ser un valor importante para una empresa que se dedique a la tecnología ya sea como servicios o ventas. Sin embargo, en giros de negocios diferentes se pueden manejar porcentajes muy bajos; una empresa que desea implementar un proyecto tecnológico tendrá que evaluar su rentabilidad mediante algunos conceptos como viabilidad comercial, técnica, administrativa, financiera; estos conceptos de análisis

determinan si la empresa cuenta con funciones de gestión interna para lograr una correcta implementación y una gestión empresarial eficaz; cuando se trata de un proyecto de empresa en constante cambio y crecimiento, se trata de definir la estructura empresarial existente que adoptará la organización, la designación de sus diferentes departamentos y las designación de roles y funciones de sus empleados; cabe destacar que el costo de gestión del proyecto no debe derivarse de este análisis.[17]

Inversión económica. Evidentemente, la seguridad no es gratuita, por lo que se requiere un cierto grado de inversión en base a la evaluación de riesgos y estándares para asumir o minimizar diferentes niveles de riesgo, y siempre teniendo en cuenta la situación financiera de la empresa; para la organización todos los análisis previos deben traducirse en números y luego combinarse para obtener indicadores financieros que permitan a la gerencia decidir finalmente si es conveniente implementar el proyecto. Para ello la gerencia piensa instintivamente en presupuesto, liquidez ", que le permitirá calcular la tasa interna de retorno) y, periodo de recuperación de la inversión, que los niveles de toma de decisiones definen como base para realizar la decisión final.[15]

Instalaciones. Las instalaciones de la organización deben estar preparadas para proporcionar un nivel de seguridad acorde con los riesgos de la empresa.

Equipos. En algunos casos, debemos contar con equipos específicos para brindar un sistema de defensa o detección de intrusos en nuestro sistema de información, aumentando así el nivel de seguridad, aunque la norma no especifique los equipos necesarios estos serán determinados por una auditoria inicial.

Personas. Dentro de la organización, las responsabilidades relacionadas con la seguridad de la información deben definirse para todos los empleados, las personas juegan un papel fundamental en el uso y procesamiento de la información. Estos pueden generar operaciones de control muy importantes dentro de la organización, tales como: permisos de acceso de los usuarios, operaciones que requieren la aprobación de cierto personal de gestión, almacenamiento de información; así mismo la empresa debe asegurar que las personas estén aptas sobre la base de una educación, formación o experiencia adecuadas por lo que es necesario demostrar la capacidad del personal en seguridad de la información a través de información registrada.[4]

5 conclusiones

En el futuro, nosotros propusimos afrontar los factores críticos ya mencionados en esta investigación, que debe analizar una pyme al momento de iniciar con el proyecto para cumplir con la norma ISO 27001, pensando que la información es una de las mayores ventajas que tiene una empresa

6 Referencias

1. Condori, H.: Un Modelo de Evaluación de Factores Críticos de Éxito en la Implementación de la Seguridad en Sistemas de Información para determinar su influencia en la intención del usuario. 184 (2012).
2. Echeverría, H. et al.: Cita sugerida (APA, sexta edición). Univ. y Soc. 9, 2,

313–318 (2019).
3. Especial, I.: ¿Quién le espía?
4. Hsu, C. et al.: The impact of ISO 27001 certification on firm performance. Proc. Annu. Hawaii Int. Conf. Syst. Sci. 2016-March, 4842–4848 (2016). https://doi.org/10.1109/HICSS.2016.600.
5. Lluch, C.: Guía de iniciación a actividad profesional; implantación de SGSI según la norma ISO 27001. Coit. 46 (2012).
6. Lomprey, G.R.: Critical Elements of an Information Security Management Strategy. 97204, July 2008, 1–96 (2008).
7. LOTAIP: Art. 7 de la Ley Orgánica de Transparencia y Acceso a la Información Pública - LOTAIP. Gad Munic. Milagro. 593 4, 1–11 (2017).
8. Martínez Cortes, J.F.: Seguridad de la Información en pequeñas y medianas empresas (pymes). Polux - Univ. Pilot. Colomb. 8 (2015).
9. MINTEL: Guia Para La Implementación De L Esquema Gubernamental De Seguridad De La Información (Nte Inen Iso/Iec 27001:2017). Regist. Of. (2020).
10. Monev, V.: Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002. 2020 34th Int. Conf. Inf. Technol. InfoTech 2020 - Proc. September, 17–18 (2020). https://doi.org/10.1109/InfoTech49733.2020.9211066.
11. Parra Giraldo, Á.M.: Iso 27001 para pymes. Medellín-Colombia. 1–147 (2014).
12. S, D.M.: Un modelo de evaluación de factores críticos de éxito en la implementación de la seguridad en sistemas de información respecto a la intención del usuario. 9, 1, 9–22 (2012).
13. Sadeghi, R.A.: Identifying Key Success Factors in the Implementation of Information Security Systems on Service Businesses: A Case Study of the Private Banks of Tehran. Am. J. Theor. Appl. Bus. 2, 4, 28–37 (2016). https://doi.org/10.11648/j.ajtab.20160204.11.
14. Sataloff, R.T. et al.: No 主観的健康感を中心とした在宅高齢者における健康関連指標に関する共分散構造分析Title.
15. Sussy, B. et al.: Implementación de la NTP ISO / IEC 27001 en las Instituciones Públicas: Caso de Estudio ISO / IEC 27001 Implementation in Public Organizations: A Case Study. 1, 410–416 (2015).
16. Tu, Z., Yuan, Y.: Critical success factors analysis on effective information security management: A literature review. 20th Am. Conf. Inf. Syst. AMCIS 2014. 1–13 (2014).
17. Velasco, J. et al.: Benefits of implementing an ISMS according to the ISO 27001 standard in the ecuadorian manufacturing industry. Proc. - 3rd Int. Conf. Inf. Syst. Comput. Sci. INCISCOS 2018. 2018-Decem, 294–300 (2018). https://doi.org/10.1109/INCISCOS.2018.00049.
18. Literal a3) Regulaciones y procedimientos internos Estatuto Orgánico de Gestión Organizacional por Procesos.pdf.