UNIVERSIDAD PRIVADA DE TRUJILLO

CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

“CARACTERÍSTICAS DE UN SUB ESTÁNDAR PARA LA SEGURIDAD DE LA INFORMACIÓN EN LA MICRO Y PEQUEÑA EMPRESA DE LA PROVINCIA DE TRUJILLO, LA LIBERTAD – 2016”

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMÁTICA

AUTOR:

Br. HORNA CENTENO SHAYRA SABINA

ASESOR:

Dr. JORGE LORENZO HUAPAYA ESCOBEDO

TRUJILLO - PERÚ

2017

JURADO EVALUADOR

Dr. Óscar Romel Alcántara Moreno

Presidente

Ing. Víctor Guillermo Villar Paredes

Secretario

Mg. Julio Luis Tenorio Cabrera

Vocal

DEDICATORIA

A Dios, que me dio la fuerza y sabiduría para recorrer este largo camino.

A mi Madre, que me enseñó a salir adelante en momentos de adversidad y ser constante en la vida.

A cinco personas, que aun estando en la distancia son ejemplo de liderazgo, fortaleza, confianza, competitividad y esfuerzo.

AGRADECIMIENTO

A mis familiares, que gracias a sus consejos no hubiese podido cumplir mis metas.

Al Doctor Jorge Huapaya, que me apoyó en mi camino por la universidad, aportando valor y conocimientos en mi vida profesional.

PRESENTACIÓN

Señores Miembros del jurado:

De conformidad y en cumplimiento con los requisitos en el Reglamento de Grados y Títulos de la Universidad Privada de Trujillo y en el reglamento interno de la carrera profesional de Ingeniería de Sistemas e Informática para obtener el título profesional de Ingeniero de Sistemas e Informática ponemos vuestra consideración la presente tesis titulada: “CARACTERÍSTICAS DE UN SUB ESTÁNDAR PARA LA SEGURIDAD DE LA INFORMACIÓN EN LA MICRO Y PEQUEÑA EMPRESA DE LA PROVINCIA DE TRUJILLO, LA LIBERTAD – 2016”, con la finalidad de obtener el título profesional de Ingeniero de Sistemas e Informática.

Trujillo, Abril del 2017

Shayra Horna Centeno

Bachiller.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

RESUMEN

La tesis se titula “Características de un sub estándar adaptado para la Seguridad de la Información para la micro y pequeña empresa (Mype) de la provincia de Trujillo, La Libertad, 2016” .

El objetivo de esta tesis es determinar las principales características de un sub estándar mediante la adecuación de modelos y estándares internacionales para mejorar la seguridad de la información que se maneja en la micro y pequeña empresa de la ciudad de Trujillo; tomando como base el estándar ISO/IEC 27001.

Durante la investigación se identificó el estándar ISO/IEC 27001 y los modelos COBIT y BMI como objetos de estudio. Además se seleccionó los criterios para la selección de los controles, que se sustentan en tres elementos como: criterio económico, técnico y operativo; los cuales permitieron obtener como resultado diez dominios y veintiún controles que fueron aceptados por los expertos.

Se recomienda que en un estudio complementario debería considerar otros marcos de referencia, así como considerar el aspecto legal como criterio de selección en posteriores investigaciones. Asimismo tener en cuenta que dependiendo de las posibilidades técnicas, operativas y económicas la Mype, puede implementar el dominio 12 (Adquisición, desarrollo y mantenimiento de sistemas de información) que sugiere ISO 27001, así mismo, que los controles finales se alineen en un 100% a los criterios de técnicos, operativos y económicos, según las necesidades de la Mype.

PALABRAS CLAVES

Característica, Marco de referencia, Estándar, Seguridad de la información, Micro y pequeña empresa (Mype).

ABSTRACT

The thesis is entitled "Characteristics of a sub standard adapted for the Information Security for micro and small enterprises (Mype) of the province of Trujillo, La Libertad, 2016".

The objective of this thesis is to determine the main characteristics of a sub standard by adapting international models and standards to improve the information security that is handled in the micro and small business of the city of Trujillo; Based on the ISO / IEC 27001 standard.

During the research the ISO / IEC 27001 standard and the COBIT and BMI models were identified as objects of study. In addition, we selected the criteria for the selection of controls, which are based on three elements such as: economic, technical and operational criteria; Which allowed to obtain as a result ten domains and twenty-one controls that were accepted by the experts.

It is recommended that a complementary study should consider other frames of reference, as well as consider the legal aspect as a selection criterion in further research. Also take into account that depending on the technical, operational and economic possibilities of Mype, you can implement domain 12 (Acquisition, development and maintenance of information systems) that suggests ISO 27001, and also that the final controls are aligned in a 100 % to the technical, operational and economic criteria, according to the needs of the Mype.

KEYWORDS

Feature, Framework, Standard, Information Security, Micro and Small Business (Mype).

INTRODUCCIÓN

El propósito de la investigación es determinar, a partir de estándares internacionales las principales características de un sub estándar, orientado a mejorar la seguridad de la información en la micro y pequeña empresa (Mype)[1] de la ciudad de Trujillo.

La información es un recurso fundamental para todas las empresas, desde el momento que la información se crea, hasta el momento en que se destruye, la tecnología juega un papel importante. La tecnología es cada vez más avanzada y se ha convertido en omnipresente en las empresas y en el desarrollo social, público y entornos empresariales. (ISACA, COBIT 5 for Information Security, 2012)

La Seguridad de la Información se remonta al albor de los tiempos. La criptología o la ciencia de la confidencialidad de la información se remontan al inicio de nuestra civilización y ha ocupado algunas de las mentes matemáticas más brillantes de la historia, especialmente (y desafortunadamente) en tiempos de guerra.

Sin embargo, desde la llegada a todas partes de las redes de comunicación y en especial la internet, los problemas asociados a la seguridad de la información se han agravado considerablemente y nos afectan prácticamente a todos. […] La información es consustancial al negocio y su

[1]La expresión Mype se usa para designar a las Micro y Pequeñas Empresas. (Belaunde, 2014)

correcta gestión debe apoyarse en tres pilares fundamentales: confidencialidad, integridad y disponibilidad. (ITIL, s.f.)

Las Mype en la provicia de Trujillo estan orientadas a la venta de productos o ha brindar diversos servicios. Cada micro y pequeña empresa se desempeña en un ámbito especifico, interactuando con equipos informaticos que le apoyan sus actividades diarias para administrar la información logrando clientes satisfechos. Sin embargo, no cuentan con un modelo o sub estandar que mantenga la seguridad de la información, puesto que su implementacion no esta en el alcance de sus recursos.

En la problemática estan involucrados los administradores o responsables de la Mype quienes son los que manejan información importante que les permite la toma de decisiones con respecto al negocio; asimismo los clientes quienes seran beneficiados por los productos o servicios brindados.

En general, los responsables de las Mype desconocen sobre las medidas preventivas que les permitan garantizar y prevenir condiciones básicas de la seguridad de la información, lo cual las hace vulnerables ante cualquier amenaza del entorno, impactando negativamente en la calidad de la información y en consecuencia restando su capacidad como elemento catalizador para el logro de los objetivos del negocio y restando la posibilidad de generar valor para los clientes. Esto se origina por el hecho de no contar con ningún modelo o sub estándar que permita a los responsables de las Mype mantener la seguridad de la información en el negocio, beneficiando a los clientes posteriormente; debido a que tienen pocas posibilidades de implementar algún estándar sobre seguridad de la información, debido a sus

limitaciones económicas, técnicas y operativas; lo que determina que no cuente con medidas preventivas que resguarden y protejan la información, tanto del negocio como la del cliente.

El principal problema es que al no contar con medidas de seguridad de la información, en consecuencia, no se logre mantener la confidencialidad, integridad y disponibilidad de la misma; generando probables pérdidas económicas y aumentando los niveles de riesgo.

Lo descrito anteriormente determina la necesidad de definir cuáles son las características que se deben de considerar en un sub estándar para la seguridad de la información aplicable en la Mype de la provincia de Trujillo, región La Libertad.

La finalidad es determinar las principales características de un sub estándar mediante la adecuación de modelos y estándares internacionales para mejorar la seguridad de la información en la Mype de la ciudad de Trujillo, para ello se identificar de un número de estándares, normas y modelos en seguridad de la información para adecuar un sub estándar adaptado a la micro y pequeña empresa, definir criterios de seguridad de la información para construir la base de un sub estándar adaptado e identificar y validar los controles o características seleccionadas mediante juicio de expertos.

Capítulo I: PROBLEMA DE INVESTIGACIÓN

1.1. Formulación Del Problema:

¿Cuáles son las características que se deben de considerar en un sub estándar para la seguridad de la información aplicable en la Mype de la provincia de Trujillo, región La Libertad?

1.2. Objetivos

General:

Determinar las principales características de un sub estándar mediante la adecuación de modelos y estándares internacionales para mejorar la seguridad de la información en la Mype de la ciudad de Trujillo.

Específicos:

1. Identificar de un número de estándares, normas y modelos en seguridad de la información para adecuar un sub estándar adaptado a la micro y pequeña empresa.
2. Definir criterios de selección para construir la base de un sub estándar adaptado.
3. Identificar y validar los controles o características seleccionadas mediante juicio de expertos.

1.3. Justificación

Justificación económica: La micro y pequeña empresa de la región tiene limitaciones económicas, en consecuencia se justifica la definición de marcos de referencia para la seguridad de la información que permita la implementación de controles adecuados.

Justificación académica: No existen en el contexto nacional modelos o sub estándares adecuados al sector de la micro y pequeña empresa. Los marcos de referencia para la seguridad de la información, permiten mejorar, innovar y gestionar la seguridad de la información dentro y fuera de la organización, identifica, evalúa y controla los riesgos que afectan al negocio, brindando así una oportunidad de mejora y evitando generar pérdidas económicas. Cualquiera que sea el tamaño de la organización (grande, mediana, pequeña o microempresa, según la clasificación peruana) o naturaleza, hoy en día las organizaciones usan y requieren el recurso de información al cual se le cataloga como el principal, en consecuencia la seguridad de la misma es vital.

Capítulo II: MARCO TEÓRICO

2.1. Antecedentes

En el informe “Modelo Para Seguridad de la Información en TIC” (Jorge Burgos Salazar, Pedro G. Campos) , se realizó un modelo para seguridad de la información en TIC, este trabajo presenta un modelo para facilitar la obtención de un adecuado nivel de control de riesgos en tecnologías de información y comunicación (TIC), que permita entre otros evitar y/o disminuir las fallas en los sistemas, redes, internet y todo el patrimonio informático (hardware, software y datos) de taques o desastres, antes que éstos ocurran.

En el proyecto de investigación “Plan de Seguridad Para una Pequeña Empresa” (Ramírez, PLAN DE SEGURIDAD PARA UNA PEQUEÑA EMPRESA, 2008), se realizó el análisis de una pequeña empresa, donde identifico la falta de conciencia sobre la importancia de la seguridad informática, que la naturaleza de las amenazas ha cambiado, la vulnerabilidad de la pequeña empresa ante ataques informáticos, y la atención que requiere esta.

Un estudio realizado por el Instituto Nacional de Tecnologías de la Comunicación (INTECO, 2012), identifico puntos críticos que tienen las empresas con respecto a temas sobre la falsa sensación de seguridad, deficiencias en la cultura de seguridad, el tamaño de la empresa es un factor determinante (en negativo) para su nivel de protección, enfoque de la seguridad es excesivamente enfocado a la dimensión tecnológica, se cree que mientras más tecnología tengan es mejor su seguridad.

2.2. Bases teóricas científicas

2.2.1. Modelo de Negocios para la Seguridad de la Información (BMIS)

La consultora (BSC Consultores, 2010) extrajo del Manual de Preparación al Examen CISM – 2010 que, el Modelo de Negocios de Seguridad de la Información (BMIS, Business Model for Information Security), se originó en el Institute for Critical Information Infrastructure Protection, siendo El Information Systems Audit and Control Association (ISACA) quién desarrollo del Modelo de Gestión Sistémica de la Seguridad.

El BMIS usa un enfoque orientado al negocio para gestionar la seguridad de la información, basándose en conceptos fundamentales desarrollados por ISACA. El modelo utiliza el pensamiento sistémico con el propósito de aclarar relaciones complejas dentro de la empresa y, por ende, gestionar la seguridad más efectivamente. El modelo lo conforman los elementos y las interconexiones dinámicas que establecen los límites de un programa de seguridad de la información y configuran cómo funciona y reacciona al cambio interno y externo. El BMIS proporciona el contexto para marcos tales como Control Objectives for Information and Related Technology (COBIT).

La esencia de la teoría de sistemas es que “el sistema” debe ser visto holísticamente, no simplemente como la suma de sus partes, para así poder entenderlo con exactitud, dado que un enfoque holístico examina al sistema como una unidad de funcionamiento completo.

En (ISACA, The Business Model for Information Security, 2010), se cita un enfoque para la seguridad de la información representado de la Universidad de california, según la figura 1:

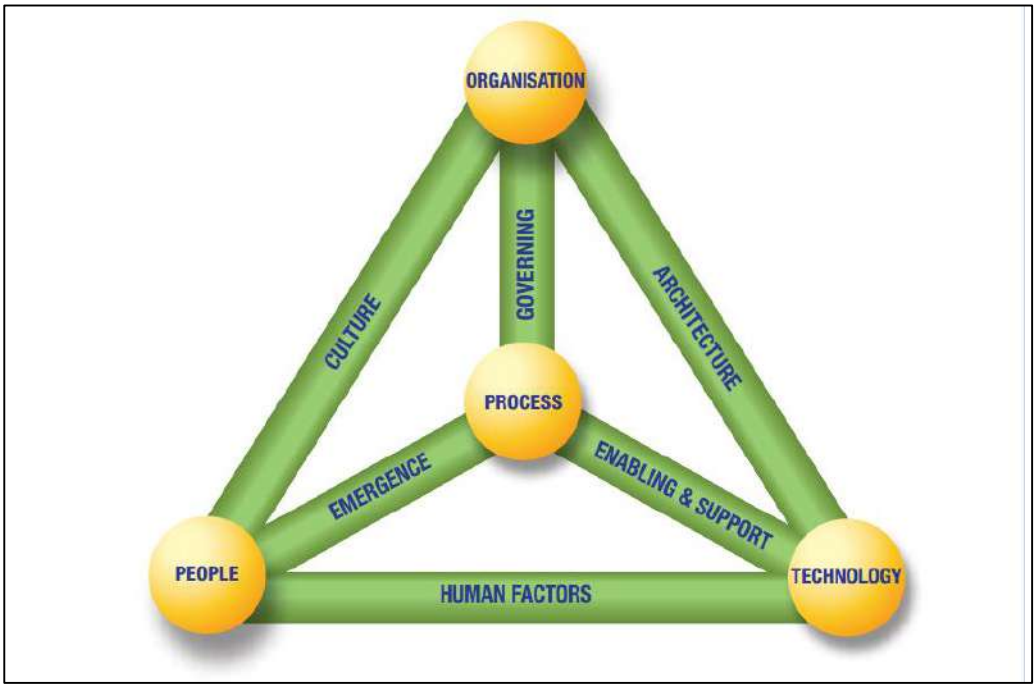


Figura 1: Vista general del modelo de negocio para la Seguridad de la Información (Fuente: The Business Model for Information Security (ISACA, The Business Model for Information Security, 2010, pág. 13))

En el modelo se aprecia una estructura tridimensional flexible, compuesta de cuatro elementos que interactúan entre sí. Si una de las partes del modelo es modificada, no es considerada o no es gestionada adecuadamente, es posible que el equilibrio del modelo esté en riesgo. Las interconexiones dinámicas actúan como elementos de tensión, ejerciendo una fuerza de empuje en respuesta a cambios en la empresa, lo que permite que el modelo se adapte según las necesidades. Los cuatro elementos del modelo son:

a. **Diseño y Estrategia de la Organización:** Una organización es representada por las personas, activos y procesos que interactúan entre sí con roles definidos y trabajando en equipo para alcanzar una meta común. La estrategia de la empresa especifica sus metas de negocio y los objetivos que se deben alcanzar, así como los valores y las misiones que se deben perseguir. Es la fórmula de la empresa para el éxito y establece su dirección básica. La estrategia se debe adaptar a los factores internos y externos.

   Los recursos constituyen el principal material para diseñar la estrategia y pueden ser de diferentes tipos (personas, equipos, conocimientos, técnicos). El diseño define la manera en que la organización implementa su estrategia. Los procesos, la cultura y la arquitectura son importantes para determinar el diseño.

b. **Los recursos humanos y los aspectos de seguridad que los rodean.** Define quién implementa (siguiendo el diseño) cada parte de la estrategia. Representa un colectivo humano y debe tener en cuenta valores, comportamientos y tendencias.

   Internamente, es fundamental que el responsable de Seguridad de la Información trabaje con los departamentos de recursos humanos y legales para resolver asuntos tales como: Estrategias de reclutamiento (acceso, verificación de antecedentes, entrevistas, roles y responsabilidades); Aspectos relacionados con el empleo (ubicación de la oficina, acceso a herramientas y datos, capacitación y concienciación, movimiento dentro de la empresa); Término de relaciones laborales (razones de la

desvinculación, momento de salida, roles y responsabilidades, acceso a los sistemas, acceso a otros empleados).

Externamente, los clientes, los proveedores, los medios y las partes interesadas, entre otros, pueden tener una fuerte influencia sobre la empresa y se deben considerar dentro de la postura de seguridad.

c. **Procesos:** Incluye mecanismos formales e informales (grandes y pequeños, simples y complejos) para realizar las tareas y proporcionar un vínculo vital con todas las interconexiones dinámicas. Los procesos identifican, miden, gestionan y controlan el riesgo, la disponibilidad, la integridad y la confidencialidad, además de asegurar la responsabilidad. Son resultado de la estrategia e implementan la parte operacional del elemento organización.

   Para que sean beneficiosos para la empresa, los procesos deben: Satisfacer los requerimientos del negocio y estar alineados con la política; Estar documentados y ser comunicados de forma adecuada a los recursos humanos apropiados; Ser revisados periódicamente, una vez establecidos, para asegurar su eficiencia y eficacia.

d. **Tecnología:** Conformada por todas las herramientas, aplicaciones y la infraestructura que incrementan la eficiencia de los procesos. Como elemento en evolución que experimenta cambios frecuentes, tiene sus propios riesgos dinámicos. Dada la típica dependencia de la tecnología que exhiben las organizaciones, constituye una parte esencial de la infraestructura de la empresa y es un factor crítico para alcanzar su misión.

La tecnología suele ser considerada por la dirección de la empresa como un instrumento para resolver las amenazas y los riesgos de seguridad. Aunque los controles técnicos son útiles para mitigar ciertos tipos de riesgos, la tecnología no se debe ver como una solución de seguridad de la información.

Los usuarios y la cultura de la organización tienen una gran influencia sobre la tecnología. Algunas personas aún desconfían de ella; algunas no han permitido avanzar a la velocidad que desean. Independientemente de la razón, los gerentes de seguridad de la información deben estar conscientes de que muchas personas intentarán burlar los controles técnicos.

2.2.2. **COBIT 5**

El framework COBIT 5, (ISACA, COBIT 5, 2012, pág. 14) se basa en cinco principios claves (mostrados en la figura 2) para el gobierno y la gestión de las TI empresariales: **Principio 1. Satisfacer las Necesidades de las Partes Interesadas**—Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos. **Principio 2: Cubrir la Empresa Extremo-a-Extremo** —COBIT 5 integra el gobierno y la gestión de TI en el gobierno corporativo: Cubre todas las funciones y procesos dentro de la empresa; COBIT 5 no se enfoca sólo en la “función de TI”, sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa; Considera que los catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin, es decir, incluyendo a todo

y todos – internos y externos – los que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionadas. **Principio 3: Aplicar un Marco de Referencia único integrado** —Hay muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI. Se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las Ti de la empresa. **Principio 4: Hacer Posible un Enfoque Holístico**—Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. **Principio 5: Separar el Gobierno de la Gestión** - establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos.

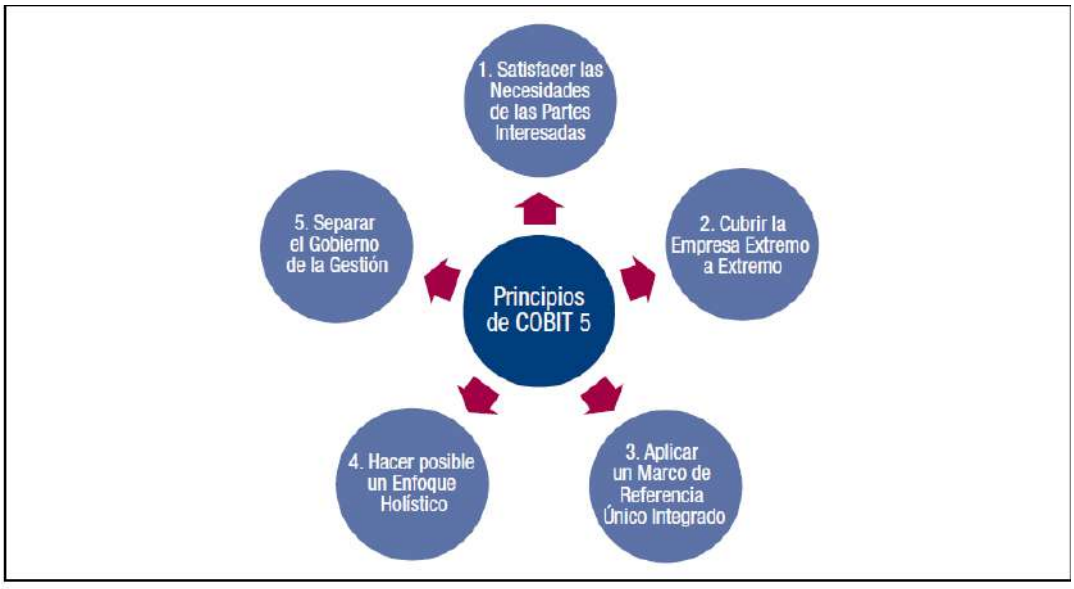


Figura 2: Principios de COBIT 5 (Fuente: (ISACA, COBIT 5, 2012, pág. 13))

COBIT 5 esta compuesto por 5 dominios y 37 procesos,en los cuales APO13(Alinear, Planificar y Organizar) Gestionar la Seguridad, DSS04 y DSS05 (Entregar, dar Servicio y Soporte) Gestionar la Continuidad y Gestionar los Servicios de Seguridad respectivamente y proporcionan una guía básica sobre cómo definir, operar y supervisar un sistema de gestión de la seguridad en general. Para ello ISACA implementa una guia profesional para la Seguridad de la Información - COBIT 5 for Information Security, brinda una vista general de dicha guía, describiendo lo útil que puede ser para la seguridad de la información, entre los beneficios que ofrece podemos citar a la letra:

"Reduced complexity and increased cost-effectiveness due to improved and easier integration of information security standards, good practices and/or sector-specific guidelines; Increased user satisfaction with information security arrangements and outcomes; Improved integration of information security in the enterprise; Informed risk decisions and risk awareness; Improved prevention, detection and recovery; Reduced (impact of) information security incidents; Enhanced support for innovation and competitiveness, Improved management of costs related to the information security function; Better understanding of information security." (ISACA, COBIT 5 for Information Security, 2012, pág. 15)

2.2.3. ISO/IEC 27000

Denominada como Serie de Norma ISO/IEC 27000**, e**stá documentada en (ISO, 2016), según se resumen a continuación:

La norma ISO, ISO/IEC 27000 es un conjunto de estándares desarrollados - o en fase de desarrollo - por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Según la (Universidad Nacional Autónoma de México, 2016) explica que, ISO-27000 se basa en la segunda parte del estándar británico BS7799 (BS7799:2). Está compuesta a grandes rasgos por: ISMS (Information Security Management System), valoración de riesgo y controles.

Son distintas las normas que componen la serie ISO 27000, para el presente proyecto de investigación se toma como referencia el estudio del ISO/IEC 27001 que según (ISO, 2016) fue publicada el 15 de Octubre de 2005 y revisada el 25 de Septiembre de 2013. Que constituye la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. En su Anexo A, numera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

2.2.4. ISO/IEC 27001:2005:

Este estándar está documentado en diversas formas, así en (ISO/IEC 2. , 2005) se puede leer los fundamentos sobre el : Enfoque del Proceso**,** promueve la adopción de un enfoque del proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización.

Una organización necesita identificar y manejar muchas actividades para poder funcionar de manera efectiva. Cualquier actividad que usa recursos y es manejada para permitir la transformación de Insumos en outputs, se puede considerar un proceso. Con frecuencia el output de un proceso forma directamente el Insumo del siguiente proceso.

La aplicación de un sistema de procesos dentro de una organización, junto con la identificación y las interacciones de estos procesos, y su gestión, puede considerarse un 'enfoque del proceso'.

Un enfoque del proceso para la gestión de la seguridad de la información presentado en este estándar internacional fomenta que sus usuarios enfaticen la importancia de: a) entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información; b) implementar y operar controles para manejar los riesgos de la seguridad de la información; c) monitorear y revisar el desempeño y la efectividad del SGSI; y d) mejoramiento continuo en base a la medición del objetivo.

Este estándar internacional adopta el modelo del proceso PDCA; Planear (establecer el SGSI) Establecer política, objetivos, procesos y

procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización; Hacer (implementar y operar el SGSI), Implementar y operar la política, controles, procesos y procedimientos SGSI.; Chequear (monitorear y revisar el SGSI), Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión y Actuar (mantener y mejorar el SGSI), Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoria interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.

El Sistema de gestión de seguridad de la información se describe en (ISO/IEC 2. , 2005) en el cual se detalla los procesos en el cual una organización debe considerar para poder gestionar la seguridad de la información dentro de ella.

2.2.5. Coeficiente de validación “V” de Aiken:

Según el artículo web publicado por el departamento de Psicología de la Pontificia Universidad Católica del Perú (Escurra, 2016), es un coeficiente que se computa como la razón de un dato obtenido sobre la suma máxima de la diferencia de los valores posibles. Puede ser calculado sobre las valoraciones de un conjunto de jueces con relación a un ítem o como las valoraciones de un juez respecto a grupo de ítem. Asimismo las valoraciones asignadas pueden ser dicotómicas (recibir valores de 0 ó 1) o politómicas (recibir valores de 0 a 5).

$$V = \frac{S}{(n(c-1))}$$

Formula N° 1

Siendo:

S = la sumatoria de s1

s1 = Valor asignado po r el juez i,

n = Número de jueces

c = Número de valores de la escala de valoración

2.3. Definición de términos básicos

2.3.1. **Característica:** “Dicho de una cualidad: Que da carácter o sirve para distinguir a alguien o algo de sus semejantes.” (Real Academia Española, 2016), en el contexto de la investigación se referirá a las características del modelo.

2.3.2. **Marco de Referencia**: “Es el conjunto de elementos conceptuales o características (teorías, leyes, principios, categorías, axiomas, formalizaciones matemáticas, paradigmas, modelos, criterios, etc...) que se refieren de forma directa al problema de investigación focalizado y que define, explica y predice lógicamente los fenómenos del universo al que este pertenece. Dichos elementos deben estar, en lo posible, relacionados lógicamente entre sí y constituir una estructura o varias unidades estructurales identificables.” (Cubillos, 2004)

2.3.3. **Estándar:** “Que sirve como tipo, modelo, norma, patrón o referencia.” (Real Academia Española, 2016)

Según PMI (Project Management Institute, 2015) define a un

estándar como un documento establecido por consenso, aprobado por un cuerpo reconocido, y que ofrece reglas, guías o características para que se use repetidamente.

2.3.4. **La Seguridad de la Información:** Según (Proviti: Risk & Business Consulting, Mayo 2015) se refiere que **“**Es una característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla los siguientes criterios; - Confidencialidad: La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados; - Integridad: La información debe ser completa, exacta y válida; - Disponibilidad: La información debe estar disponible en forma organizada para los usuarios autorizados cuando sea requerida; - Otras propiedades: Autenticidad, responsabilidad, no repudio, confiabilidad".

En (ISO/IEC 1. , 2005) se afirma: “Es la preservación de la confidencialidad, integridad y disponibilidad de la información; además, tambien puede estar involucradas otras propiedaades como la autenticidad, responsabilidad, no-repudio y con fiabilidad.”

2.3.5. **Micro y pequeña empresa (Mype):** El portal Trabajo del (Ministerio de Trabajo y Promoción del Empleo, 2016),la Micro y Pequeña empresa es la unidad económica constituida por una persona natural o jurídica, bajo cualquier forma de organización o gestión empresarial contemplada en la legislación vigente, que

tiene como objeto desarrollar actividades de extracción, transformación, producción, comercialización de bienes o prestación de servicios.

Según (INEI, 1995-1998) en el Perú las definiciones que se enuncian o adoptan varían según el tipo de enfoque que se utiliza: **Microempresa:** Son aquellas microempresas con potencial de crecimiento, tiene capacidad de generar excedentes y brindan ingresos y perspectivas de desarrollo interesantes a propietarios y trabajadores. Pueden ser considerados sujetos de créditos y de otros servicios no financieros por su estabilidad, potencial de crecimiento y capacidad de pago. En esta categoría, también se encuentran relaciones laborales familiares. Se tratan de unidades empresariales que cumplen con los requisitos mínimos de formalidad, sin que esto signifique que cumplan con todas, por lo que se le pueden calificar de "semiformales". En algunos casos, no cumplen con alguno de los aspectos laborales o con los registros municipales. Sin embargo, su carácter viable o de acumulación determina que sus necesidades tengan un sustento económico y no social, estando en tránsito hacia una formalidad regular, propia de su naturaleza de empresa emergente. **Pequeña empresa**: Está asociada al desarrollo económico, crecimiento y competitividad, estás empresas son unidades económicamente viables con capacidad de generar excedentes, crear empleo y contribuir a la competitividad del país. Son formales, desde el punto de vista, tributario, municipal y laboral, tienen

una organización con una elemental división del trabajo a nivel funcional y jerárquico. Generalmente es el propietario el que dirige la empresa, existiendo también relaciones familiares laborales. Utilizan servicios financieros y no financieros con regularidad a fin de explotar sus ventajas. Existe un mayor nivel de profesionalización en el empresario y sus trabajadores, así como una preocupación por la capacitación de la fuerza laboral. Utilizan tecnologías de información básicas, asimilan en sus procedimientos de gestión y producción el tema de la calidad.

Según indica el Anuario Estadístico Sub-Sector Mype e Industria del Ministerio de la Producción (Produción, 2016), en el Perú el 95% de las empresas está constituida por la Microempresa con un total de 1 607 305(empresas formales) y el 4,3% son pequeñas empresas (72 664), estas representan el 99.3% de empresas en todo el Perú, mientras que la Provincia de La Libertad tenemos 84 681 Microempresas y 3 110 de pequeñas empresas.

En el 2015 el 39,3% (661 mil 404 empresas) de las Mipyme (Micro, pequeña y mediana empresa) tuvieron ventas anuales menores o iguales a 2 UIT, es decir, presentaron una venta promedio mensual de alrededor de 642 Nuevos Soles. Esta realidad determina una de las principales limitaciones para que este sector pueda implantar tecnología con los estándares generalmente usados y recomendados.

2.4. Metodología de desarrollo

En consideración al enfoque de la investigación, la metodología empleada para la elaboración de un sub estándar, se describe a continuación:

2.4.1. Identificación de estándares, normas y modelos en Seguridad de la Información:

Para identificar los estándares, normas y modelos basados en seguridad de la información se consideró la técnica del Análisis Documental usando como instrumento “matrices comparativas”, y la palabra clave siguiente:” estándares, normas y modelos en Seguridad de la Información”, para consultar fuentes primarias en boletines, revistas, folletos y sitios web, en libros y revistas especializadas en google books y publicaciones científicas y afines en google académico, respectivamente. Mediante esta técnica se logró identificar los principales marcos de referencia en seguridad de la información, así como también sus características, los cuales permitió la selección de un estándar a seguir.

2.4.2. Determinación criterios de selección de acuerdo a los aspectos básico de factibilidad

Para determinar los criterios de selección se consideró los aspectos básicos de factibilidad que se refiere a económico (costos), operativo (condiciones y posibilidad de uso) y técnico (recursos y potenciales tecnológicos disponibles) de acuerdo a la naturaleza de la Mype, a partir de estos criterios se seleccionó los controles o características que conformarían el sub estándar. La técnica empleada para la recopilación de información fue el Análisis documental

y observación no participante de los criterios identificados y el instrumento fue tablas y la observación directa.

2.4.3. Selección de controles o características

Después de haber identificado el modelo estándar a seguir y de haber definido los criterios de selección, se aplicó el juicio de experto como fuente de información para la elaboración de la lista de verificación, en la cual se le asignó a cada criterio de selección un peso (1 -100) según la prioridad en la Mype, así como también se empleó la escala de Likert (0-4) variando sus alternativas según cada criterio, esto permitió la evaluación preliminar de cada objetivo de control.

Para realizar la selección de los controles o características se consideró solo a aquellos que tuvieron como resultado igual o mayor a 3, permitiendo obtener una lista de características, el cual se procedió a describir para ser la base de elaboración de la guía de juicio de expertos.

2.4.4. Validación de los dominios y controles

Construcción y validación del instrumento para validar el modelo para la seguridad de la información. Para la construcción y validación del instrumento se utilizó la técnica de juicio de expertos y el instrumento fue una lista de verificación en donde se describieron los controles seleccionados y la escala de calificación numérica a emplear (escala de Likert de 1- 5).

El criterio utilizado para la selección de los expertos para la validaciónpredel instrumento, se consideró a dos profesionales con trayectoria profesional reconocida en seguridad y TI. Los jueces no mantuvieron contacto

entre ellos, de los cuales según su visto bueno se procedió a la elaboración de la guía de juicio de expertos.

Aplicación del modelo al juicio de expertos: Se aplicó el juicio de expertos para que estos hicieran una valoración sobre los controles preseleccionados, así como una valoración completa de la misma. Se solicitó que valoraran cualitativamente cada objeto de control, pues se trata de una validación de contenido cuyos objetivos son analizar y valorar que los controles se adapten a la Mype, cumplan con los criterios técnicos, operativos y económicos y que permita mantener la seguridad de la información.

Se consideró tres objetivos generales para la validación de la guía: La adaptabilidad de los controles y objetivos definidos a las posibilidades de las Mype; que los controles y objetivos cumplan con los criterios de factibilidad económicos, operativos y Técnicos; y que los controles y objetivos permitan en cierto modo mantener la seguridad de la información en la Mype.

En cuanto a los expertos se consideró que tengan de 5 a 10 años de experiencia en TI, con 2 a 3 años en Seguridad de la información.

Observación: Luego de finalizada la evaluación de los expertos y considerando sus aportaciones y comentarios, se realizaron las modificaciones pertinentes en los controles, ya que sus sugerencias avalan concordancia entre el diseño del instrumento metodológico que se valida y su eficacia con respecto al objetivo para el que ha sido creado.

Validación: El proceso de validación permitió hacer los cambios en los controles a validar, en el cual se empleó el coeficiente de la V de Aiken y la técnica estadística T-Student para obtener el intervalo de confianza.

Capítulo III: MARCO METODOLÓGICO

2.1. Tipo y diseño de investigación

2.1.1. Según el tipo de investigación:

2.1.1.1. Por respuestas a problemas básicos del conocimiento:

Descriptiva – Deductiva

2.1.1.2. Por el enfoque de la investigación

Cualitativa

2.1.2. Según el diseño de la investigación:

Diseño no experimental transeccional o transversal

2.2. Población y Muestra

Por la naturaleza de la investigación la **población** no es conocida exactamente ya que la investigación se refiere a los estándares de Seguridad dela información; mientras que la **muestra** está representada por un estándar y dos modelos para la seguridad de la información que fueron elegidos de forma selectiva por ser los más usados en la región y en el país.

2.3. Hipótesis

Las características de un sub estándar para la seguridad de la información en la micro y pequeña empresa comprenderá por lo menos los siguientes elementos: Organización y cumplimiento, seguridad de recursos y entorno, sistemas y comunicaciones; y continuidad.

2.4. Variables:

Variable Categórica	Dimensiones	Medida	Técnicas e instrumentos de recolección de datos
Características de un sub estándar para la seguridad de la información en la micro y pequeña empresa	* Política de seguridad * Aspectos organizativos * Gestión de activos * Seguridad ligada a los recursos humanos * Seguridad física y del entorno * Gestión de comunicaciones * Control de acceso * Gestión de incidentes * Gestión de la continuidad del negocio * Cumplimiento	Escala de Likert 1 a 5	Guía de Verificación para el Juicio de expertos.

2.4.1. Técnica de análisis de datos

Se empleó el coeficiente V de Aiken y la técnica estadística T-Student (mencionado en el punto 2.2.5. pág. 18).

Capítulo IV: RESULTADOS

2.1. En relación a: Identificar de un número de estándares, normas y modelos en seguridad de la información para adecuar un sub estándar adaptado a la micro y pequeña empresa.

En la Tabla N° 1 se muestran los resultados de las características de los principales estándares identificados en seguridad de la información.

Tabla N° 1: Características de los principales estándares, normas y modelos en Seguridad de la Información

ISO 27001	BMIS	COBIT 5
Es un estándar que adopta un enfoque de procesos, estableciendo así un modelo de procesos para un Sistema de Gestión de Seguridad de la Información.	Es un modelo orientado al negocio para la gestión de la seguridad de la información.	Es un marco de trabajo integral con un enfoque holístico que permite a las TI ser gobernadas y gestionadas en toda la empresa.
Permite entender los requerimientos, necesidades y objetivos para la seguridad de la información en una organización.	Establece lo que se debe lograr en los distintos procesos de la organización (elemento de proceso) y al mismo tiempo establecer los límites sobre las actividades que mitiguen los riesgos.	Apoya a las empresas lograr sus objetivos para el gobierno y la gestión de las TI.
Ayuda a reducir los riesgos de la seguridad de la información mediante el análisis, implementación y ejecución de los controles necesarios y adecuados.	Los procesos deben servir a los objetivos de la organización a un nivel aceptable de previsibilidad, es decir, el riesgo.	Permite mantener el equilibrio entre generar beneficios y optimizar de los niveles de riesgo, así como el uso de recursos.

ISO 27001	BMIS	COBIT 5
Permite el seguimiento y revisión del Sistema de Gestión de Seguridad de la Información para evaluar su desempeño y efectividad de esta en la organización.	Abarca cuestiones de conservación de la organización, o la sostenibilidad.	Posibilita el gobierno y gestión de TI, considerando el negocio y sus partes externas.
Permite la mejora continua en base a los objetivos definidos.	Si una de las partes del modelo es modificada, no considerada o no gestionada adecuadamente, es posible que el equilibrio del modelo esté en riesgo.	Es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público.
Incluye objetivos de control y controles como parte del proceso del sistema de seguridad de la información.	Detalla los marcos de referencia los cuales permite la implementación de un tema en específico.	Integra los principales marcos y guías de ISACA como COBIT, ValIT, RiskIT y BMIS.

Fuente: Elaboración Propia

2.2. En la Tabla N° 2 se muestran los criterios de selección que se consideró para seleccionar los criterios.

Tabla N° 2: Criterios de Selección

Técnica	Operativa	Económica
Según el portal web (Universidad Monteávila, 2016) estudia la posibilidad tecnológica (existencia de los equipos para llevar a cabo los procesos), de infraestructura (existencia de instalaciones para los equipos), legal (existencia	Según (Hurtado, 2011, págs. 89,90) lo define con las siguientes preguntas, ¿Podrán los usuarios en el área comercial ser más productivos con estas tecnologías?, ¿Podrá los miembros del área de TIC soportarlas	Según (Hurtado, 2011, págs. 89,90) define que es la existencia (o no) de un balance entre los ingresos adicionales generados al implementar un proyecto; se refiere a los costos (personal,

Técnica	Operativa	Económica
de regulaciones), ambiental (evaluación del impacto) y geográfica (existencia de espacios y vías de acceso suficientes) que el proyecto pueda ser llevado a cabo satisfactoriamente con el menor riesgo posible. Es decir se refiere a los elementos necesarios y disponibles para realizar el ejercicio de implementar modelos, prácticas auditoria o de control de la información.	productivamente?, ¿Se podrán integrar estas tecnologías efectiva y eficientemente a los esquemas administrativos que usa la empresa en su unidad de las TIC? ; Es decir se refiere a las condiciones organizacionales y ambientales, que se expresan en términos de las competencias del personal, y en consecuencia la competitividad en el sector que permite orientar esfuerzos a acciones vinculadas con los objetivos centrales de la Mype.	servicios, materiales) que se requieren para adaptar nuevos modelos y que la inversión sea rentable, lo cual significa mayores limitaciones para la Mype estando en pleno crecimiento, considerando así un factor importante para su desarrollo.

Fuente: Elaboración Propia

2.3. En relación: Identificar y validar los controles o características seleccionadas mediante juicio de expertos.

En la selección de los controles para el sub estándar, en concordancia a las consideraciones técnicas, operativas y económicas definidas en la tabla N° 2 se realizó aplicando la escala de Likert de 0-4 según las ponderaciones que se especifican en la tabla N° 3. En el Anexo N° 1 se detalla el instrumento utilizado para esta selección.

Tabla N° 3: Pesos de criterios, escala y valor para selección de controles

CRITERIO POR COSTO	CRITERIO TÉCNICO	CRITERIO OPERATIVO	ESCALA	VALOR
Peso = 40	Peso = 40	Peso = 20	Muy bajo	0
			Bajo	1
			Medio	2
			Alto	3
			Muy alto	4

Fuente: Elaboración Propia

Como consecuencia se determinaron los controles que obtuvieron puntaje mayor o igual a 3 según se detalla en el Anexo N° 2. Asimismo dichos controles fueron agrupados considerando los objetivos de control en el ISO/IEC 27001 según como se muestra en la tabla N° 4 obteniéndose 27 controles, mientras que en la tabla N° 5 se describe lo que abarca cada control.

Tabla N°4: Dominios y controles requeridos

CONTROLES REQUERIDOS	
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	**Controles de Ref. - ISO 27001**
1. POLÍTICA DE SEGURIDAD	
Formulación y actualización de Políticas de seguridad	5.1.1 - 5.1.2
2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	
Acta de constitución, asignación de responsabilidades y autoridad, y acuerdo de confidencialidad.	6.1.1 - 6.1.8

CONTROLES REQUERIDOS	
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	**Controles de Ref. - ISO 27001**
Identificación y tratamiento de riesgos asociados a contratos con terceros	6.2.1 - 6.2.3
3. GESTIÓN DE ACTIVOS	
Inventario y uso de activos	7.1.1 - 7.1.3
4. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	
Ficha de responsabilidades, antecedentes y condiciones de contratación, incluye medidas disciplinaria	8.1 - 8.3
Inducción y capacitación en Seguridad de la información	
Devolución de activos y retiro de derechos de acceso	
5. SEGURIDAD FÍSICA Y DEL ENTORNO	
Acciones y controles de seguridad física contra amenazas ambientales	9.1
Emplazamiento y protección de equipos (incluye retiro , control fuera de las instalaciones y retorno)	9.2.1 - 9.2.7
Seguridad de instalaciones de cableado y accesorios	
6. GESTIÓN DE COMUNICACIONES Y OPERACIONES	
Gestión de cambios	10.1 - 10.9
Gestión de disponibilidad	
Gestión de servicios	
Protección contra código malicioso	
Gestión de intercambio de información	
Servicio de comercio electrónico	
Supervisión y registro de incidentes	
7. CONTROL DE ACCESO	
Políticas de control de acceso(Matriz de accesos) privilegios, contraseñas y responsable	11.1 - 11.2
Política de uso de red y control de conexión de red	11.4 - 11.6
Control de acceso al sistema operativo	
Procedimiento y control de contraseñas	
Control de acceso a aplicaciones e información	
8. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	
Registro de incidentes	13.1
Reporte e identificación de incidentes	

CONTROLES REQUERIDOS	
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	**Controles de Ref. - ISO 27001**
Análisis causa efecto	
9. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	
Planes de continuidad (Incluye pruebas y mantenimiento)	14
10. CUMPLIMIENTO	
Cumplimiento de los requisitos legales en concordancia de delitos informáticos	15

Fuente: Elaboración Propia

Tabla N° 5: Dominios y descripción de los controles requeridos

1. POLÍTICA DE SEGURIDAD	
Formulación y actualización de Políticas de seguridad	Se debe definir políticas de seguridad, esta se debe publicar y comunicar a todos los empleados y entidades externas relevantes, siendo revisada regularmente en intervalos planeados o si ocurren cambios significativos para así poder ser modificada. El documento que contiene las políticas de seguridad debe ser aprobado por la gerencia o por la persona responsable de la organización.
2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	
Acta de constitución, asignación de responsabilidades y autoridad, y acuerdo de confidencialidad.	Se deben definir claramente las responsabilidades, autoridades y los acuerdos de confidencialidad de la seguridad de la información
Identificación y tratamiento de riesgos asociados a contratos con terceros	Se deben identificar los riesgos que corre la información y los medios de procesamiento de información de la organización, así como el tratamiento a los riesgos identificados con terceros.
3. GESTIÓN DE ACTIVOS	

Inventario y uso de activos	Todos los activos deben estar claramente identificados, así como también identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con el de procesamiento de la información.
4. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	
Ficha de responsabilidades, antecedentes y condiciones de contratación, incluye medidas disciplinaria	Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros, estas también deben incluir las medidas disciplinarias, estando relacionada con la política de la seguridad de información de la organización.
Inducción y capacitación en Seguridad de la información	Se debe brindar capacitaciones tanto a los nuevos empleados como a los antiguos. Las capacitaciones deben tener información relevante sobre seguridad de la información, así como funciones, uso de activos, permisos, etc.
Devolución de activos y retiro de derechos de acceso	Esta acción se realiza cuando hay desvinculación del empleado, contratistas o terceros, esto evita cualquier fraude, pérdida o alteración de información.
5. SEGURIDAD FÍSICA Y DEL ENTORNO	
Acciones y controles de seguridad física contra amenazas ambientales	Se debe restringir el acceso a personal no autorizado, así como proteger los ambientes donde se encuentren los equipos de comunicación, datos, etc., contra desastres naturales o agentes externos.
Emplazamiento y protección de equipos (incluye retiro , control fuera de las instalaciones y retorno)	Se debe contar con la protección debida a los equipos, ya sea dentro del ambiente de trabajo o fuera de él, así como también el respectivo seguimiento cuando dicho equipo salga del área de trabajo y cuando retorne.
Seguridad de instalaciones de cableado y accesorios	Se deben proteger el cableado de energía eléctrica y de datos, evitando que estos puedan ser dañados.
6. GESTIÓN DE COMUNICACIONES Y OPERACIONES	

Gestión de cambios	Se debe controlar cualquier cambio en los medios y sistemas donde se procesa la información.
Gestión de disponibilidad	Se deben implementar controles de red, copias de seguridad de la información, controles de soporte para que la información y las aplicaciones se encuentren disponibles ante cualquier eventualidad.
Gestión de servicios	Se debe asegurar que los servicios brindados por terceros mantengan los controles de seguridad, definición del servicio y niveles de entrega que están incluidos en el contrato, así como realizar el monitoreo y revisión regularmente.
Protección contra código malicioso	Se deben implementar controles que permitan prevenir, detectar y recuperar para la protección de códigos maliciosos
Gestión de intercambio de información	Se deben implementar controles y definir políticas para intercambios formales de información a través de cualquier medio de comunicación.
Servicio de comercio electrónico	Se debe proteger la información relacionada con el comercio electrónico, ya que esta transita por la red pública y puede ser modificada fácilmente.
Supervisión y registro de incidentes	Se debe realizar la supervisión para identificar y registrar cualquier uso de información no autorizada, permitiendo así el análisis y tomar las medidas necesarias.
7. CONTROL DE ACCESO	
Políticas de control de acceso(Matriz de accesos) privilegios, contraseñas y responsable	Se debe definir, documentar y revisar las políticas de control de acceso, privilegio de usuario, gestión de contraseñas y responsables.
Política de uso de red y control de conexión de red	Se debe definir que los usuarios solo tengan acceso a los servicios los cuales han sido autorizados usar, además de restringir la capacidad de acceso de usuarios a la red.

Control de acceso al sistema operativo	Se debe controlar los accesos al sistema operativo mediante procedimientos de registro, donde se identifiquen a los usuarios que acceden a los sistemas. Los sistemas deben cerrarse luego de un periodo de inactividad definido.
Procedimiento y control de contraseñas	Se deben definir procedimientos y controles para las contraseñas, donde se indique el periodo de renovación de contraseñas, longitud de contraseñas, caracteres especiales, etc.
Control de acceso a aplicaciones e información	Se debe restringir el acceso a los usuarios a cierta información o aplicativos que no están de acuerdo a su función en concordancia con la política de control de acceso definida.
8. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	
Registro de incidentes	Mediante el registro de incidentes, se puede identificar los problemas, fecha de ocurrencia, área donde ocurrió el incidente, verificar el estado en que se encuentra, las medidas tomadas para su solución, etc.
Reporte e identificación de incidentes	Mediante el reporte de los incidentes de seguridad de la información se identifican las oportunidades de mejora.
Análisis causa efecto	Se debe definir controles para la evaluación de incidentes, así como también medidas a tomar ante cual eventualidad, el responsable del incidente y las oportunidades de mejora.
9. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	
Planes de continuidad (Incluye pruebas y mantenimiento)	Se debe desarrollar e implementar planes de continuidad que permitan mantener o restaurar las operaciones y asegurar la disponibilidad de la información en niveles y tiempo requerido luego de una interrupción, así como prueba, mantenimiento y re-evaluación de los planes de continuidad, esto servirá para asegurar que estén actualizados y sean efectivos.
10. CUMPLIMIENTO	

Cumplimiento de los requisitos legales en concordancia de delitos informáticos	Se debe cumplir con los requisitos legales establecidos por la ley, como la ley de protección de datos personales, estándares de seguridad, etc.

Fuente: Elaboración Propia

Los controles definidos en la tabla N° 5 se sometieron a una validación preliminar, lo que permitió obtener 23 controles según se muestra en la tabla N° 6.

Tabla N° 6: Dominios y controles después de la Preliminar

CONTROLES REQUERIDOS	
1. POLÍTICA DE SEGURIDAD	
Formulación y actualización de Políticas de seguridad	Se debe definir políticas de seguridad, esta se debe publicar y comunicar a todos los empleados y entidades externas relevantes, siendo revisada regularmente en intervalos planeados o si ocurren cambios significativos para así poder ser modificada. El documento que contiene las políticas de seguridad debe ser aprobado por la gerencia o por la persona responsable de la organización.
2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	
Acta de constitución, asignación de responsabilidades y autoridad, y acuerdo de confidenciad.	Se deben definir claramente las responsabilidades, autoridades y los acuerdos de confidencialidad de la seguridad de la información.
3. GESTIÓN DE ACTIVOS	

CONTROLES REQUERIDOS	
Inventario y uso de activos	Todos los activos deben estar claramente identificados, así como también identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con el de procesamiento de la información.
4. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	
Inducción y capacitación en Seguridad de la información	Se debe brindar capacitaciones tanto a los nuevos empleados como a los antiguos. Las capacitaciones deben tener información relevante sobre seguridad de la información, así como funciones, uso de activos, permisos, etc.
Devolución de activos y retiro de derechos de acceso	Esta acción se realiza cuando hay desvinculación del empleado, contratistas o terceros, esto evita cualquier fraude, pérdida o alteración de información.
5. SEGURIDAD FÍSICA Y DEL ENTORNO	
Acciones y controles de seguridad física contra amenazas ambientales	Se debe restringir el acceso a personal no autorizado, así como proteger los ambientes donde se encuentren los equipos de comunicación, datos, etc., contra desastres naturales o agentes externos.
Emplazamiento y protección de equipos (incluye retiro , control fuera de las instalaciones y retorno)	Se debe contar con la protección debida a los equipos, ya sea dentro del ambiente de trabajo o fuera de él, así como también el respectivo seguimiento cuando dicho equipo salga del área de trabajo y cuando retorne.
Seguridad de instalaciones de cableado y accesorios	Se deben proteger el cableado de energía eléctrica y de datos, evitando que estos puedan ser dañados.
6. GESTIÓN DE COMUNICACIONES Y OPERACIONES	

CONTROLES REQUERIDOS	
Gestión de cambios	Se debe controlar cualquier cambio en los medios y sistemas donde se procesa la información.
Gestión de disponibilidad	Se deben implementar controles de red, copias de seguridad de la información, controles de soporte para que la información y las aplicaciones se encuentren disponibles ante cualquier eventualidad.
Protección contra código malicioso	Se deben implementar controles que permitan prevenir, detectar y recuperar para la protección de códigos maliciosos
Gestión de intercambio de información	Se deben implementar controles y definir políticas para intercambios formales de información a través de cualquier medio de comunicación.
Servicio de comercio electrónico	Se debe proteger la información relacionada con el comercio electrónico, ya que esta transita por la red pública y puede ser modificada fácilmente.
7. CONTROL DE ACCESO	
Políticas de control de acceso(Matriz de accesos) privilegios, contraseñas y responsable	Se debe definir, documentar y revisar las políticas de control de acceso, privilegio de usuario, gestión de contraseñas y responsables.
Política de uso de red y control de conexión de red	Se debe definir que los usuarios solo tengan acceso a los servicios los cuales han sido autorizados usar, además de restringir la capacidad de acceso de usuarios a la red.
Control de acceso al sistema operativo	Se debe controlar los accesos al sistema operativo mediante procedimientos de registro, donde se identifiquen a los usuarios que acceden a los

CONTROLES REQUERIDOS	
	sistemas. Los sistemas deben cerrarse luego de un periodo de inactividad definido.
Procedimiento y control de contraseñas	Se deben definir procedimientos y controles para las contraseñas, donde se indique el periodo de renovación de contraseñas, longitud de contraseñas, caracteres especiales, etc.
Control de acceso a aplicaciones e información	Se debe restringir el acceso a los usuarios a cierta información o aplicativos que no están de acuerdo a su función en concordancia con la política de control de acceso definida.
8. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	
Registro de incidentes.	Mediante el registro de incidentes, se puede identificar los problemas, fecha de ocurrencia, área donde ocurrió el incidente, verificar el estado en que se encuentra, las medidas tomadas para su solución, etc.
Reporte e identificación de incidentes	Mediante el reporte de los incidentes de seguridad de la información se identifican las oportunidades de mejora.
Evaluación de incidentes	Se debe definir controles para la evaluación de incidentes, así como también medidas a tomar ante cual eventualidad, el responsable del incidente y las oportunidades de mejora.
9. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	
Planes de continuidad (Incluye pruebas y mantenimiento)	Se debe desarrollar e implementar planes de continuidad que permitan mantener o restaurar las operaciones y asegurar la disponibilidad de la información en niveles y tiempo requerido luego de una interrupción, así como prueba, mantenimiento y re -evaluación de los planes de continuidad, esto

CONTROLES REQUERIDOS	
	servirá para asegurar que estén actualizados y sean efectivos.
10. CUMPLIMIENTO	
Cumplimiento de los requisitos legales en concordancia de delitos informáticos	Se debe cumplir con los requisitos legales establecidos por la ley, como la ley de protección de datos personales, estándares de seguridad, etc

Fuente: Elaboración Propia

Los 23 controles pre seleccionados se validaron mediante juicios de expertos, empleando el coeficiente de la V de Aiken (la guía de aplicación se sustentan en el Anexo N° 4), de acuerdo a las consideraciones descritas en la tabla N°7, se obtuvo como resultado los controles mostrados en la tabla N° 8, los cuales alcanzaron un puntaje entre 0.88 y 0.98 según el intervalo de confianza definido que se muestran a continuación en la tabla N° 9 y se detalla en el Anexo N° 5.

Tabla N° 7: Consideraciones para Juicio de Expertos

Objetivos de la Validación	Determinar el grado de importancia d los controles para la Mype.
Expertos	De 5 a 10 años de experiencia en TI, con 2 a 3 años en Seguridad de la información, soporte y riesgos.
Modo de validación	Aplicación individual de la guía a cada experto sin que estos estén comunicados
Intervalo de confianza	Mayor e igual a 0.9

Fuente: Elaboración Propia

Tabla N° 8: Controles finales seleccionados

N°	Controles
1	Formulación y actualización de Políticas de seguridad
2	Acta de constitución, asignación de responsabilidades y autoridad, y acuerdo de confidencialidad.
3	Inventario y uso de activos
4	Inducción y capacitación en Seguridad de la información
5	Devolución de activos y retiro de derechos de acceso
6	Acciones y controles de seguridad física contra amenazas ambientales
7	Emplazamiento y protección de equipos (incluye retiro , control fuera de las instalaciones y retorno)
8	Seguridad de instalaciones de cableado y accesorios
9	Gestión de cambios
10	Gestión de disponibilidad
11	Protección contra código malicioso
12	Gestión de intercambio de información
13	Servicio de comercio electrónico
14	Políticas de control de acceso(Matriz de accesos) privilegios, contraseñas y responsable
15	Política de uso de red y control de conexión de red
16	Procedimiento y control de contraseñas
17	Control de acceso a aplicaciones e información
18	Reporte e identificación de incidentes
19	Evaluación de incidentes
20	Planes de continuidad (Incluye pruebas y mantenimiento)
21	Cumplimiento de los requisitos legales en concordancia de delitos informáticos

Fuente: Elaboración Propia

Tabla N° 9: Intervalos de confianza

N° de controles	Escala	Intervalos de confianza
2	Mala	0 > y < 0.87
18	Buena	0.87 >= y =< 0.98
3	Excelente	0.98 >= 1

Capítulo V: DISCUSIÓN

Los resultados de esta investigación definen la propuesta de un modelo o sub estándar de Seguridad de la información para la Micro y pequeña empresa, basado en los resultados obtenidos.

En relación a la identificación de los estándares, normas y modelos se concluyó que el ISO 27001 describe los objetivos de control y controles recomendables en cuanto a seguridad de la información, COBIT 5 define objetivos de control y procesos basados en gobierno de TI, mientras que BMIS define elementos e interconexiones dinámicas orientadas al negocio con una visión holística; estos dos últimos consideran a la seguridad de la información como parte de TI. Esto se relaciona con lo dicho por (Jorge Burgos Salazar, Pedro G. Campos) explica que para la correcta administración de la seguridad de la información, se deben establecer y mantener acciones que busquen cumplir con los tres requerimientos de mayor importancia para la información, que son: confidencialidad, integridad y disponibilidad, debido a que organizaciones internacionales han definido estándares y normas que apoyan en diferente medida el cumplimiento de los requerimientos indicados anteriormente, detalló los más usados mundialmente incluyendo a COBIT e ISO 27001 de la serie 27000 siendo estos son principales normas, estándares y leyes relacionadas con la gestión de seguridad de información.

En relación a la definición de criterios de selección, se consideró tres criterios que se alinean con las posibilidades y recursos de las Mype como técnica, económica y operativa, relacionándose con las áreas de factibilidad

definidas por (Perez, 2016) las cuales considera a técnica, financiera, operacional, geográfico, tiempo, recursos, legal y política**.**

Con respecto a la selección de los controles, se realizó considerando los criterios definidos anteriormente, de los cuales se obtuvo 10 dominios y 27 controles, que fueron las bases para la construcción del instrumento aplicado al juicio de expertos. El instrumento fue previamente validado por dos expertos en el área antes de su aplicación, ellos realizaron sugerencias permitiendo realizar modificaciones finales en la guía para así tener la versión final y luego su aplicación.

Los 23 controles seleccionados anteriormente, fueron validados mediante Juicio de expertos con el uso del coeficiente de la V de Aiken, cuyo resultado es el que se detalla en el Anexo N° 6; y el uso de la T-Student para hallar el intervalo con un nivel de confianza del 99%, destacando a “Inventario y uso de activos y Acciones y controles de seguridad física contra amenazas ambientales” que obtuvieron como resultado 1 en la V de Aiken, lo cual significa que son considerados Obligatorios e indispensables en la Mype, caso contrario paso con “registro de incidentes y control de acceso al sistema operativo”, los cuales obtuvieron una V de Aiken menor 0.87 considerándose necesaria pero no indispensable, pues siendo su resultado menor a lo deseado se eliminaron dichos controles, para garantizar la validez del modelo, obteniendo 0.931 la V de Aiken total.

Capítulo VI: PROPUESTA

Descripción del Modelo para la Seguridad de la Información (Sub Estándar) en la Micro y Pequeña empresa (Mype) de la provincia de Trujillo - Región La Libertad

4.1. Consideraciones iniciales del modelo

La seguridad de la información busca proteger los recursos de la empresa como son la información, las comunicaciones, el hardware y el software que le pertenecen, para ello se seleccionan y establecen los controles apropiados.

La micro y pequeña empresa (Mype) según la clasificación en el Perú, desempeñan un papel fundamental en la economía peruana ya que éstas representan el 99,5% de empresas. Actualmente las Mypes no cuentan con niveles tecnológicos que les permitan adaptarse a los nuevos flujos de información y a mantener dicha información segura.

La Seguridad de la información contribuye con la misión de la empresa, protegiendo así sus recursos físicos, financieros, reputación, posición legal, empleados y otros activos tangibles e intangibles.

El estándar ISO 27001 recomienda la implementación de controles para garantizar la Seguridad de la Información en una empresa. Dichos controles no se pueden aplicar en toda su magnitud en una Mype ya que por su naturaleza ésta tiene limitaciones en recursos, por esta razón se evalúo cada control del estándar ISO 27001, identificando cuales serían los eventualmente necesarios

para que las Mype puede implementarlos para gestionar y mantener la seguridad de la información.

Gestionar un Sistema de Gestión de Seguridad de la Información (SGSI) desde su establecimiento hasta mejorarlo continuamente permite que la micro y pequeña empresa (Mype) mantenga la seguridad de la información así como identificar los riesgos que enfrenta.

4.2. Objetivos del modelo

- Establecer controles para la Mype con el fin de garantizar la seguridad de la información
- Permitir realizar mejoras continuas empleando recursos disponibles en la Mype.
- Evaluar o diagnosticar el grado de control de la seguridad de la información

4.3. Principios del modelo

- Eficiencia. El uso racional de los recursos informáticos, alcanzando el objetivo definido.
- Eficacia: capacidad para lograr los objetivos propuestos.

4.4. Criterios considerados del modelo

Los criterios Disponibilidad, Confidencialidad e Integridad o también conocidos como categorías son considerados como los 3 pilares que permiten garantizar la Seguridad de la información en las empresas, según.

- Disponibilidad: “La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada” (ISO/IEC 13335-1:2004).

La información debe estar disponible en forma organizada para todos los usuarios autorizados cuando esta sea requerida.

- Confidencialidad: “La propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no-autorizados” (ISO/IEC 13335-1:2004).

  La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados.

- Integridad: “La propiedad de salvaguardar la exactitud e integridad de los activos”. (ISO/IEC 13335-1:2004).

  La información debe ser completa, exacta y válida.

Existen otros criterios, pero estos se enfocan en otros ámbitos de la seguridad de la información, como las auditorias de sistemas. Los criterios son Autenticidad, responsabilidad, no repudio, confiabilidad.

4.5. Costos de implementación

La implementación de los controles del modelo propuesto implica un costo mínimo que tiene que ser asumido por la Mype, considerando que esta última no cuenta con el personal y herramientas necesarias (Ver Anexo N° 7).

4.6. Controles para la Seguridad de la Información

Los controles enumerados en la siguiente tabla se derivan de ISO 27001. La lista de controles son considerados necesarios en la Mype, pero esta puede adaptar los controles según sus requerimientos.

Controles para la Seguridad de la Información

DOMINIOS Y CONTROLES	
1. POLÍTICA DE SEGURIDAD	
Formulación y actualización de Políticas de seguridad	Se debe definir políticas de seguridad, esta se debe publicar y comunicar a todos los empleados y entidades externas relevantes, siendo revisada regularmente en intervalos planeados o si ocurren cambios significativos para así poder ser modificada. El documento que contiene las políticas de seguridad debe ser aprobado por la gerencia o por la persona responsable de la organización.
2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	
Acta de constitución, asignación de responsabilidades y autoridad, y acuerdo de confidenciad.	Se deben definir claramente las responsabilidades, autoridades y los acuerdos de confidencialidad de la seguridad de la información.
3. GESTIÓN DE ACTIVOS	
Inventario y uso de activos	Todos los activos deben estar claramente identificados, así como también identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con el de procesamiento de la información.
4. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	
Inducción y capacitación en Seguridad de la información	Se debe brindar capacitaciones tanto a los nuevos empleados como a los antiguos. Las capacitaciones deben tener información relevante sobre seguridad de la información, así como funciones, uso de activos, permisos, etc.
Devolución de activos y retiro de derechos de acceso	Esta acción se realiza cuando hay desvinculación del empleado, contratistas o terceros, esto evita cualquier fraude, pérdida o alteración de información.
5. SEGURIDAD FÍSICA Y DEL ENTORNO	
Acciones y controles de seguridad física contra amenazas ambientales	Se debe restringir el acceso a personal no autorizado, así como proteger los ambientes donde se encuentren los equipos de comunicación, datos, etc., contra desastres naturales o agentes externos.

DOMINIOS Y CONTROLES	
Emplazamiento y protección de equipos (incluye retiro , control fuera de las instalaciones y retorno)	Se debe contar con la protección debida a los equipos, ya sea dentro del ambiente de trabajo o fuera de él, así como también el respectivo seguimiento cuando dicho equipo salga del área de trabajo y cuando retorne.
Seguridad de instalaciones de cableado y accesorios	Se deben proteger el cableado de energía eléctrica y de datos, evitando que estos puedan ser dañados.
6. GESTIÓN DE COMUNICACIONES Y OPERACIONES	
Gestión de cambios	Se debe controlar cualquier cambio en los medios y sistemas donde se procesa la información.
Gestión de disponibilidad	Se deben implementar controles de red, copias de seguridad de la información, controles de soporte para que la información y las aplicaciones se encuentren disponibles ante cualquier eventualidad.
Protección contra código malicioso	Se deben implementar controles que permitan prevenir, detectar y recuperar para la protección de códigos maliciosos
Gestión de intercambio de información	Se deben implementar controles y definir políticas para intercambios formales de información a través de cualquier medio de comunicación.
Servicio de comercio electrónico	Se debe proteger la información relacionada con el comercio electrónico, ya que esta transita por la red pública y puede ser modificada fácilmente.
7. CONTROL DE ACCESO	
Políticas de control de acceso(Matriz de accesos) privilegios, contraseñas y responsable	Se debe definir, documentar y revisar las políticas de control de acceso, privilegio de usuario, gestión de contraseñas y responsables.

DOMINIOS Y CONTROLES	
Política de uso de red y control de conexión de red	Se debe definir que los usuarios solo tengan acceso a los servicios los cuales han sido autorizados usar, además de restringir la capacidad de acceso de usuarios a la red.
Procedimiento y control de contraseñas	Se deben definir procedimientos y controles para las contraseñas, donde se indique el periodo de renovación de contraseñas, longitud de contraseñas, caracteres especiales, etc.
Control de acceso a aplicaciones e información	Se debe restringir el acceso a los usuarios a cierta información o aplicativos que no están de acuerdo a su función en concordancia con la política de control de acceso definida.
8. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	
Reporte e identificación de incidentes	Mediante el reporte e identificación de los incidentes de seguridad de la información se identifican las oportunidades de mejora.
Evaluación de incidentes	Se debe definir controles para la evaluación de incidentes, así como también medidas a tomar ante cual eventualidad, el responsable del incidente y las oportunidades de mejora.
9. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	
Planes de continuidad (Incluye pruebas y mantenimiento)	Se debe desarrollar e implementar planes de continuidad que permitan mantener o restaurar las operaciones y asegurar la disponibilidad de la información en niveles y tiempo requerido luego de una interrupción, así como prueba, mantenimiento y re -evaluación de los planes de continuidad, esto servirá para asegurar que estén actualizados y sean efectivos.
10. CUMPLIMIENTO	
Cumplimiento de los requisitos legales en concordancia de delitos informáticos	Se debe cumplir con los requisitos legales establecidos por la ley, como la ley de protección de datos personales, estándares de seguridad, etc.

4.7. Prueba de cumplimiento.

Para identificar los controles a implementar o para evaluar si estos fueron implementados correctamente, las actividades que requiere un esquema metodológico se detalla a continuación:

N°	ACTIVIDADES	DESCRIPCIÓN
1	Preparar un cuestionario con las preguntas formuladas.	Tomar como referencia los dominios y controles propuestos.
2	Construir un instrumento para hacer auditoria tomado como referencia los dominios y controles definidos.	Cuestionario (Ver Anexo N°8) con opciones de respuesta dicotómica (CUMPLE - NO CUMPLE).
3	Determinar fuentes informantes.	Personas interesadas en la Mype.
4	Aplicación del instrumento.	-
5	Procesar la información obtenida.	-
6	Identificar los controles no cumplidos.	Para todas respuesta que el resultado fue NO.
7	Hacer un programa de implementación y mejora continua.	Definir los responsables.

Fuente: Elaboración Propia

CONCLUSIONES

1. Se identificaron un estándar y dos modelos los cuales se detalla a continuación:

Tabla N° 10: Resumen de estándares y modelos para la seguridad de la información

	ISO 27001	BMIS	COBIT 5
ENFOQUE	Procesos	Negocio	Sistemas
ORIENTACIÓN	Requerimientos, necesidades y objetivos	Lograr de procesos	Apoya a los objetivos de gobierno
PERMITE	Reducir los riesgos de la seguridad de la información	Los procesos cumplan objetivos de la organización	Mantener el equilibrio entre beneficios y optimizar de los niveles de riesgo
OBJETIVO	Evaluación desempeño y efectividad de la organización.	Conservación o sostenibilidad de la organización.	Gobierno y gestión de T.I.
BENEFICIOS	Mejora continua en base a objetivos definidos.	Mantener el equilibrio del modelo y disminuir riesgos.	Genérico y útil para toda empresa.
CONSIDERA	Dominios, objetivos de control y controles.	Marcos de referencia específicos.	Integración de marcos de referencia y guías de ISACA.

Fuente: Elaboración Propia

2. Los criterios para la selección de los controles se sustentan en tres elementos como se muestra en la tabla a continuación:

Tabla N° 11: Resumen de criterios de selección

TÉCNICA	OPERATIVA	ECONÓMICA
Disponibilidad de elementos necesarios (equipos, instalaciones, ambiente, etc.) que la Mype requiere para implementación de controles.	Disponibilidad de personal capacitado para cumplir con las funciones asignadas.	Disponibilidad de ingresos económicos que permitan cubrir con los costos que se requiere.

Fuente: Elaboración Propia

3. Diez fueron los dominios y veintiuno los controles que aceptaron los expertos como figura en la siguiente tabla:

Tabla N° 12: Resumen de dominios y controles del proceso de selección para el sub estándar

DOMINIOS ISO 27001	Total de controles	Porcentaje de controles	Controles pre seleccionados	Controles seleccionados	Controles validados
5. Política de seguridad.	2 de 2	100%	1	1	1
6. Aspectos organizativos de la seguridad de la información.	4 de 11	36%	2	2	1
7. Gestión de activos.	2 de 5	40%	1	1	1
8. Seguridad ligada a los recursos humanos.	6 de 9	67%	3	2	2
9. Seguridad física y del entorno.	4 de 13	31%	3	3	3
10. Gestión de comunicaciones y operaciones.	9 de 32	28%	7	5	5
11. Control de acceso.	8 de 25	32%	5	4	4
12. Adquisición, desarrollo y mantenimiento de sistemas de información.	0 de 16	0%	0	0	0
13. Gestión de incidentes en la seguridad de la información.	2 de 5	40%	3	3	2
14. Gestión de la continuidad del negocio.	2 de 5	40%	1	1	1
15. Cumplimiento.	2 de 10	20%	1	1	1
TOTAL	**41 de 133**	**40%**	**27**	**23**	**21**

Fuente: Elaboración Propia

RECOMENDACIONES

1. Un estudio complementario debería considerar otros marcos de referencia.
2. Se recomienda considerar el aspecto legal como criterio de selección en posteriores investigaciones.
3. Tener en cuenta que dependiendo de las posibilidades técnicas, operativas y económicas la Mype, puede implementar el dominio 12 (Adquisición, desarrollo y mantenimiento de sistemas de información) que sugiere ISO 27001.
4. En posteriores investigaciones se recomienda que los controles finales se alineen en un 100% a los criterios de técnicos, operativos y económicos, según las necesidades de la Mype.

REFERENCIAS

Belaunde, G. (20 de enero de 2014). Mypes y Pymes: No Confundir. *Diario Gestión*.

BSC Consultores. (2010). *http://www.bscconsultores.cl/index.html.* Obtenido de http://www.bscconsultores.cl/descargas/D.3%20Modelo%20de%20Negocios%20para%20la%20Seguridad%20de%20la%20Informacin.pdf

Cubillos, A. (2004). *Marco de Referencia.* Obtenido de http://trabajodegradouamerica.wikispaces.com/file/view/MarcoReferencia.pdf

Escurra, L. M. (Noviembre de 2016). *Pontificia Universidad Católica del Perú.* Obtenido de Pontificia Universidad Católica del Perú : http://ezproxybib.pucp.edu.pe/index.php/psicologia/article/viewFile/4555/4534

Hurtado, F. (2011). Dirección de proyectos. En F. Hurtado, *Dirección de Proyectos: Una Introducción con base en el marco del PMI* (pág. 89_90). EE. UU: Palibrio.

INEI. (1995-1998). *Determinates del Empleo Adecuado en las Micro y Pequeñas Empresas en el Perú*. Obtenido de http://proyectos.inei.gob.pe/web/biblioineipub/bancopub/Est/Lib0165/cap311.htm

ISACA. (2010). *The Business Model for Information Security.*

ISACA. (2012). COBIT 5. En ISACA, *COBIT 5.*

ISACA. (2012). COBIT 5 for Information Security. En ISACA, *COBIT 5 for Information Security.*

ISO. (05 de enero de 2016). *ISO 27000*. Recuperado el 05 de enero de 2016, de ISO 27000: http://www.iso27000.es/iso27000.html

ISO/IEC, 1. (2005). *Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.* Obtenido de https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

ISO/IEC, 2. (2005). *Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos.* Obtenido de https://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf

ITIL. (s.f.). *Osiatis*. Obtenido de http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_seguridad/vision_general_gestion_de_la_seguridad/vision_general_gestion_de_la_seguridad.php

Jorge Burgos Salazar, Pedro G. Campos. (s.f.). *Modelo Para Seguridad de la Información en TIC.* Concepción - Chile.

Ministerio de Trabajo y Promoción del Empleo. (Julio de 2016). *Trabajo*. Obtenido de http://www.trabajo.gob.pe/mostrarContenido.php?id=541&tip=9

Perez, J. L. (Noviembre de 2016). *Proyectum*. Obtenido de Proyectum: http://www.proyectum.lat/2011/03/14/8-criterios-para-el-contenido-de-un-estudio-de-factibilidad/

Poggi, E. (2006). *Marcos de referencia para la gestión de TI.* Buenos Aires - Argentina.

Produción, M. d. (Setiembre de 2016). *Produce.* Obtenido de http://www.produce.gob.pe/documentos/estadisticas/anuarios/anuario-estadistico-mype-2015.pdf

Project Management Institute. (Agosto de 2015). *Project Management Institute*. Obtenido de http://americalatina.pmi.org/latam/pmbokguideandstandards/whatisastandar.aspx

Proviti: Risk & Business Consulting. (Mayo 2015). Sistema de Gestión de Seguridad de la Información(SGSI) y Gestión de Riesgos de Seguridad de la Información.

Ramírez, J. C. (2008). *Plan de Seguridad para una pequeña empresa.* Madrid.

Real Academia Española. (22 de febrero de 2016). *Real Academia Española*. Obtenido de http://www.rae.es/

Real Academia Española. (s.f.). *Real Academia Española*. Obtenido de http://www.rae.es/

Roberto Hernández Sampieri, Carlos Fernández Collado, Pilar Baptista Lucio. (2006). Metodología de la Investigación. En *Metodología de la Investigación.* México. Obtenido de https://competenciashg.files.wordpress.com/2012/10/sampieri-et-al-metodologia-de-la-investigacion-4ta-edicion-sampieri-2006_ocr.pdf

Rosalva Bautista Nieves , Wilber Vidal Marín. (2014). *Marco de Gobierno de TI en las empresas.*

Taboada, N. M. (2014). *Metodológia de la Investigación Científica.* Trujillo: EDUNT.

Universidad Monteávila. (Agosto de 2016). *Universidad Monteávila*. Obtenido de Universidad Monteávila: http://www.uma.edu.ve/moodle_uma/course/info.php?id=28

Universidad Nacional Autónoma de México. (Enero de 2016). *Redes y Seguridad*. Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/ISO27.php

ANEXOS

ANEXO N° 1: "SELECCIÓN DE DOMINIOS Y CONTROLES"

	RAZÓN PARA SELECCIONAR EL ELEMENTO															
	COSTO-Peso = 40					TÉCNICA-Peso= 40					OPERATIVA= Peso = 20					
DOMINIOS, OBJETIVOS DE CONTROL Y CONTROLES	Muy Bajo	Bajo	Medio	Alto	Muy Alto	Podría prescindirse	Poco importante	Muy importante	Necesario	Indispensable	Muy Baja	Baja	Media	Alta	Muy alta	Promedio Total
	4	3	2	1	0	0	1	2	3	4	4	3	2	1	0	
5. POLÍTICA DE SEGURIDAD.																
5.1 Política de seguridad de la información.																
5.1.1 Documento de política de seguridad de la información.	4								3					1		3
5.1.2 Revisión de la política de seguridad de la información.	4								3					1		3
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.																
6.1 Organización interna.																
6.1.1 Compromiso de la Dirección con la seguridad de la información.	4						1					3				2.6
6.1.2 Coordinación de la seguridad de la información.	4							2					2			2.8
6.1.3 Asignación de responsabilidades relativas a la seg. de la informac.	4								3					1		3
6.1.4 Proceso de autorización de recursos para el tratamiento de la información.		3						2				3				2.6
6.1.5 Acuerdos de confidencialidad.	4								3					1		3
6.1.6 Contacto con las autoridades.	4							2					2			2.8
6.1.7 Contacto con grupos de especial interés.	4							2					2			2.8
6.1.8 Revisión independiente de la seguridad de la información.			2				1					3				1.8
6.2 Terceros.																
6.2.1 Identificación de los riesgos derivados del acceso de terceros.	4								3				2			3.2
6.2.2 Tratamiento de la seguridad en la relación con los clientes.				1			1					3				1.4
6.2.3 Tratamiento de la seguridad en contratos con terceros.		3								4				1		3

	RAZÓN PARA SELECCIONAR EL ELEMENTO															
	COSTO-Peso = 40					TÉCNICA-Peso= 40					OPERATIVA - Peso = 20					
DOMINIOS, OBJETIVOS DE CONTROL Y CONTROLES	**Muy Bajo**	**Bajo**	**Medio**	**Alto**	**Muy Alto**	**Podría prescindirse**	**Poco importante**	**Muy importante**	**Necesario**	**Indispensable**	**Muy Baja**	**Baja**	**Media**	**Alta**	**Muy alta**	**Promedio Total**
	4	**3**	**2**	**1**	**0**	**0**	**1**	**2**	**3**	**4**	**4**	**3**	**2**	**1**	**0**	
7. GESTIÓN DE ACTIVOS.																
7.1 Responsabilidad sobre los activos.																
7.1.1 Inventario de activos.	**4**								**3**					**1**		**3**
7.1.2 Propiedad de los activos.	**4**							**2**					**2**			**2.8**
7.1.3 Uso aceptable de los activos.	**4**								**3**					**1**		**3**
7.2 Clasificación de la información.																
7.2.1 Directrices de clasificación.		**3**						**2**					**2**			**2.4**
7.2.2 Etiquetado y manipulado de la información.		**3**						**2**					**2**			**2.4**
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.																
8.1 Antes del empleo.																
8.1.1 Funciones y responsabilidades.	**4**								**3**					**1**		**3**
8.1.2 Investigación de antecedentes.		**3**							**3**			**3**				**3**
8.1.3 Términos y condiciones de contratación.	**4**								**3**					**1**		**3**
8.2 Durante el empleo.																
8.2.1 Responsabilidades de la Dirección.		**3**					**1**						**2**			**2**
8.2.2 Concienciación, formación y capacitación en seguridad de la información.	**4**								**3**					**1**		**3**
8.2.3 Proceso disciplinario.		**3**						**2**					**2**			**2.4**
8.3 Cese del empleo o cambio de puesto de trabajo.																
8.3.1 Responsabilidad del cese o cambio.	**4**							**2**					**2**			**2.8**
8.3.2 Devolución de activos.	**4**								**3**					**1**		**3**
8.3.3 Retirada de los derechos de acceso.	**4**								**3**					**1**		**3**
9. SEGURIDAD FÍSICA Y DEL ENTORNO.																
9.1 Áreas seguras.																
9.1.1 Perímetro de seguridad física.			**2**					**2**					**2**			**2**
9.1.2 Controles físicos de entrada.		**3**								**4**		**2**				**3.2**
9.1.3 Seguridad de oficinas, despachos e instalaciones.			**2**					**2**					**2**			**2**
9.1.4 Protección contra las amenazas externas y de origen ambiental.		**3**								**4**				**1**		**3**
9.1.5 Trabajo en áreas seguras.		**3**						**2**					**2**			**2.4**
9.1.6 Áreas de acceso público y de carga y descarga.			**2**					**2**					**2**			**2**
9.2 Seguridad de los equipos.																
9.2.1 Emplazamiento y protección de equipos.		**3**								**4**				**1**		**3**
9.2.2 Instalaciones de suministro.			**2**					**2**				**3**				**2.2**
9.2.3 Seguridad del cableado.		**3**								**4**			**2**			**3.2**
9.2.4 Mantenimiento de los equipos.		**3**						**2**				**3**				**2.6**
9.2.5 Seguridad de los equipos fuera de las instalaciones.		**3**					**1**					**3**				**2.2**
9.2.6 Reutilización o retirada segura de equipos.	**4**						**1**						**2**			**2.4**
9.2.7 Retirada de materiales propiedad de la empresa.							**1**						**2**			**0.8**

	RAZÓN PARA SELECCIONAR EL ELEMENTO															
	COSTO-Peso = 40					TÉCNICA-Peso= 40					OPERATIVA - Peso = 20					
DOMINIOS, OBJETIVOS DE CONTROL Y CONTROLES	**Muy Bajo**	**Bajo**	**Medio**	**Alto**	**Muy Alto**	**Podría prescindirse**	**Poco importante**	**Muy importante**	**Necesario**	**Indispensable**	**Muy Baja**	**Baja**	**Media**	**Alta**	**Muy alta**	**Promedio Total**
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.																
10.1 Responsabilidades y procedimientos de operación.																
10.1.1 Documentación de los procedimientos de operación.		3						2					2			2.4
10.1.2 Gestión de cambios.		3								4				1		3
10.1.3 Segregación de tareas.			2				1					3				1.8
10.1.4 Separación de los recursos de desarrollo, prueba y operación.			2				1					3				1.8
10.2 Gestión de la provisión de servicios por terceros.																
10.2.1 Provisión de servicios.		3								4			2			3.2
10.2.2 Supervisión y revisión de los servicios prestados por terceros.		3								4			2	1		3.2
10.2.3 Gestión del cambio en los servicios prestados por terceros.			2					2				3				2.2
10.3 Planificación y aceptación del sistema.																
10.3.1 Gestión de capacidades.			2					2					2			2
10.3.2 Aceptación del sistema.			2					2					2			2
10.4 Protección contra el código malicioso y descargable.																
10.4.1 Controles contra el código malicioso.		3								4				1		3
10.4.2 Controles contra el código descargado en el cliente.		3						2					2			2.4
10.5 Copias de seguridad.																
10.5.1 Copias de seguridad de la información.		2								4		3				3
10.6 Gestión de la seguridad de las redes.																
10.6.1 Controles de red.		3								4				1		3
10.6.2 Seguridad de los servicios de red.			2					2					2			2
10.7 Manipulación de los soportes.																
10.7.1 Gestión de soportes extraíbles.	4								3				2			3.2
10.7.2 Retirada de soportes.		3						2					2			2.4
10.7.3 Procedimientos de manipulación de la información.		3						2					2			2.4
10.7.4 Seguridad de la documentación del sistema.		3						2					2			2.4
10.8 Intercambio de información.																
10.8.1 Políticas y procedimientos de intercambio de información	4								3					1		3
10.8.2 Acuerdos de intercambio.		3						2					2			2.4
10.8.3 Soportes físicos en tránsito.		3						2					2			2.4
10.8.4 Mensajería electrónica.		3						2					2			
10.8.5 Sistemas de información empresariales.							1					3				1
10.9 Servicios de comercio electrónico.																
10.9.1 Comercio electrónico.	4								3					1		3
10.9.2 Transacciones en línea.		3					1						2			2
10.9.3 Información públicamente disponible.		3					1						2			2

DOMINIOS, OBJETIVOS DE CONTROL Y CONTROLES	RAZÓN PARA SELECCIONAR EL ELEMENTO															
	COSTO-Peso = 40					TÉCNICA-Peso= 40					OPERATIVA= Peso = 20					
	Muy Bajo	Bajo	Medio	Alto	Muy Alto	Podría prescindirse	Poco importante	Muy importante	Necesario	Indispensable	Muy Baja	Baja	Media	Alta	Muy alta	Promedio Total
10.10 Supervisión.																
10.10.1 Registros de auditoría.		3				0						3				1.8
10.10.2 Supervisión del uso del sistema.		3					1						2			2
10.10.3 Protección de la información de los registros.		3				0							2			1.6
10.10.4 Registros de administración y operación.		3					1					3				2.2
10.10.5 Registro de fallos.		3					1					3				2.2
10.10.6 Sincronización del reloj.	4					0						3				2.2
11. CONTROL DE ACCESO.																
11.1 Requisitos de negocio para el control de acceso.																
11.1.1 Política de control de acceso.	4								3					1		3
11.2 Gestión de acceso de usuario.																
11.2.1 Registro de usuario.		3						2					2			2.4
11.2.2 Gestión de privilegios.	4								3					1		3
11.2.3 Gestión de contraseñas de usuario.	4								3					1		3
11.2.4 Revisión de los derechos de acceso de usuario.		3						2					2			2.4
11.3 Responsabilidades de usuario.																
11.3.1 Uso de contraseñas.		3						2					2			2.4
11.3.2 Equipo de usuario desatendido.		3						2					2			2.4
11.3.3 Política de puesto de trabajo despejado y pantalla limpia.		3						2					2			2.4
11.4 Control de acceso a la red.																
11.4.1 Política de uso de los servicios en red.	4								3					1		3
11.4.2 Autenticación de usuario para conexiones externas.			2					2				3				2.2
11.4.3 Identificación de los equipos en las redes.		3								4			2			3.2
11.4.4 Protección de los puertos de diagnóstico y configuración remotos.		3						2				3				2.6
11.4.5 Segregación de las redes.		3						2				3				2.6
11.4.6 Control de la conexión a la red.	4								3				2			3.2
11.4.7 Control de encaminamiento (routing) de red.			2				1					3				1.8
11.5 Control de acceso al sistema operativo.																
11.5.1 Procedimientos seguros de inicio de sesión.		3					1						2			2
11.5.2 Identificación y autenticación de usuario.		3						3						1		2.6
11.5.3 Sistema de gestión de contraseñas.			2				1					3				1.8
11.5.4 Uso de los recursos del sistema.		3					1						2			2
11.5.5 Desconexión automática de sesión.		3					1						2			2
11.5.6 Limitación del tiempo de conexión.	4								3					1		3
11.6 Control de acceso a las aplicaciones y a la información.																
11.6.1 Restricción del acceso a la información.	4								3					1		3
11.6.2 Aislamiento de sistemas sensibles.			2				1					3				1.8
11.7 Ordenadores portátiles y teletrabajo.																
11.7.1 Ordenadores portátiles y comunicaciones móviles.				1			1				4					1.6
11.7.2 Teletrabajo.				1			1				4					1.6

	RAZÓN PARA SELECCIONAR EL ELEMENTO															
	COSTO-Peso = 40					TÉCNICA-Peso= 40					OPERATIVA= Peso = 20					
DOMINIOS, OBJETIVOS DE CONTROL Y CONTROLES	**Muy Bajo**	**Bajo**	**Medio**	**Alto**	**Muy Alto**	**Podría prescindirse**	**Poco importante**	**Muy importante**	**Necesario**	**Indispensable**	**Muy Baja**	**Baja**	**Media**	**Alta**	**Muy alta**	**Promedio Total**
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.																
12.1 Requisitos de seguridad de los sistemas de información.																
12.1.1 Análisis y especificación de los requisitos de seguridad.			**2**			**0**					**4**					**1.6**
12.2 Tratamiento correcto de las aplicaciones.																
12.2.1 Validación de los datos de entrada.		**3**					**1**				**4**					**2.4**
12.2.2 Control del procesamiento interno.			**2**				**1**				**4**					**2**
12.2.3 Integridad de los mensajes.			**2**				**1**				**4**					**2**
12.2.4 Validación de los datos de salida.			**2**				**1**				**4**					**2**
12.3 Controles criptográficos.																
12.3.1 Política de uso de los controles criptográficos.			**2**				**1**				**4**					**2**
12.3.2 Gestión de claves.			**2**				**1**				**4**					**2**
12.4 Seguridad de los archivos de sistema.																
12.4.1 Control del software en explotación.			**2**				**1**				**4**					**2**
12.4.2 Protección de los datos de prueba del sistema.			**2**				**1**				**4**					**2**
12.4.3 Control de acceso al código fuente de los programas.			**2**				**1**				**4**					**2**
12.5 Seguridad en los procesos de desarrollo y soporte.																
12.5.1 Procedimientos de control de cambios.			**2**				**1**				**4**					**2**
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.			**2**				**1**				**4**					**2**
12.5.3 Restricciones a los cambios en los paquetes de software.			**2**				**1**				**4**					**2**
12.5.4 Fugas de información.				**1**			**1**				**4**					**1.6**
12.5.5 Externalización del desarrollo de software.			**2**				**1**				**4**					**2**
12.6 Gestión de la vulnerabilidad técnica.																
12.6.1 Control de las vulnerabilidades técnicas.			**2**				**1**				**4**					**2**
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.																
13.1 Notificación de eventos y puntos débiles de seguridad de la información.																
13.1.1 Notificación de los eventos de seguridad de la información.	**4**								**3**					**1**		**3**
13.1.2 Notificación de puntos débiles de seguridad.	**4**								**3**					**1**		**3**
13.2 Gestión de incidentes y mejoras de seguridad de la información.																
13.2.1 Responsabilidades y procedimientos.		**3**					**1**						**2**			**2**
13.2.2 Aprendizaje de los incidentes de seguridad de la información.		**3**						**2**						**1**		**2.2**
13.2.3 Recopilación de evidencias.		**3**						**2**					**2**			**2.4**

	RAZÓN PARA SELECCIONAR EL ELEMENTO															
	COSTO-Peso = 40					TÉCNICA-Peso= 40					OPERATIVA= Peso = 20					
DOMINIOS, OBJETIVOS DE CONTROL Y CONTROLES	**Muy Bajo**	**Bajo**	**Medio**	**Alto**	**Muy Alto**	**Podría prescindirse**	**Poco importante**	**Muy importante**	**Necesario**	**Indispensable**	**Muy Baja**	**Baja**	**Media**	**Alta**	**Muy alta**	**Promedio Total**
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.																
14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.																
14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.		**3**					**1**						**2**			**2**
14.1.2 Continuidad del negocio y evaluación de riesgos.			**2**					**2**				**3**				**2.2**
14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.			**2**							**4**		**3**				**3**
14.1.4 Marco de referencia para la planificación de la cont. del negocio.		**3**						**2**					**2**			**2.4**
14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.			**2**							**4**		**3**				**3**
15. CUMPLIMIENTO.																
15.1 Cumplimiento de los requisitos legales.																
15.1.1 Identificación de la legislación aplicable.		**3**								**4**				**1**		**3**
15.1.2 Derechos de propiedad intelectual (DPI).			**2**					**2**				**3**				**2.2**
15.1.3 Protección de los documentos de la organización.		**3**						**2**				**3**				**2.6**
15.1.4 Protección de datos y privacidad de la información de carácter personal.		**3**							**3**			**3**				**3**
15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.			**2**					**2**				**3**				**2.2**
15.1.6 Regulación de los controles criptográficos.			**2**				**1**					**3**				**1.8**
15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.																
15.2.1 Cumplimiento de las políticas y normas de seguridad.			**2**				**1**					**3**				**1.8**
15.2.2 Comprobación del cumplimiento técnico.			**2**				**1**					**3**				**1.8**
15.3 Consideraciones sobre las auditorías de los sistem. de información.																
15.3.1 Controles de auditoría de los sistemas de información.		**3**						**2**					**2**			**2.4**
15.3.2 Protección de las herramientas de auditoría de los sist. de inform.		**3**						**2**					**2**			**2.4**

ANEXO N° 2: "CONTROLES CON MAYOR PUNTAJE SELECCIONADOS"

	RAZÓN PARA SELECCIONAR EL ELEMENTO															
	COSTO -Peso = 40					TÉCNICA-Peso= 40					OPERATIVA)= Peso = 20					
DOMINIOS, OBJETIVOS DE CONTROL Y CONTROLES	Muy Bajo	Bajo	Medio	Alto	Muy Alto	Podría prescindirse	Poco importante	Muy importante	Necesario	Indispensable	Muy Baja	Baja	Media	Alta	Muy alta	Promedio Total
5. POLÍTICA DE SEGURIDAD.	4	3	2	1	0	0	1	2	3	4	4	3	2	1	0	
5.1 Política de seguridad de la información.																
5.1.1 Documento de política de seguridad de la información.	4								3					1		3
5.1.2 Revisión de la política de seguridad de la información.	4								3					1		3
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.																
6.1.3 Asignación de responsabilidades relativas a la seg. de la informac.	4								3					1		3
6.1.5 Acuerdos de confidencialidad.	4								3					1		3
6.2 Terceros.																
6.2.1 Identificación de los riesgos derivados del acceso de terceros.	4								3				2			3.2
6.2.3 Tratamiento de la seguridad en contratos con terceros.		3								4				1		3
7. GESTIÓN DE ACTIVOS.																
7.1 Responsabilidad sobre los activos.																
7.1.1 Inventario de activos.	4								3					1		3
7.1.3 Uso aceptable de los activos.	4								3					1		3
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.																
8.1 Antes del empleo.																
8.1.1 Funciones y responsabilidades.	4								3					1		3
8.1.2 Investigación de antecedentes.		3							3			3				3
8.1.3 Términos y condiciones de contratación.	4								3					1		3
8.2 Durante el empleo.																
8.2.2 Concienciación, formación y capacitación en seg. de la informac.	4								3					1		3
8.3 Cese del empleo o cambio de puesto de trabajo.																
8.3.2 Devolución de activos.	4								3					1		3
8.3.3 Retirada de los derechos de acceso.	4								3					1		3
9. SEGURIDAD FÍSICA Y DEL ENTORNO.																
9.1 Áreas seguras.																
9.1.2 Controles físicos de entrada.		3								4		2				3.2
9.1.4 Protección contra las amenazas externas y de origen ambiental.		3								4				1		3
9.2 Seguridad de los equipos.																
9.2.1 Emplazamiento y protección de equipos.		3								4				1		3
9.2.3 Seguridad del cableado.		3								4			2			3.2
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.																
10.1 Responsabilidades y procedimientos de operación.																

	RAZÓN PARA SELECCIONAR EL ELEMENTO															
	COSTO -Peso = 40					TÉCNICA-Peso= 40					OPERATIVA)= Peso = 20					
DOMINIOS, OBJETIVOS DE CONTROL Y CONTROLES	Muy Bajo	Bajo	Medio	Alto	Muy Alto	Podría prescindirse	Poco importante	Muy importante	Necesario	Indispensable	Muy Baja	Baja	Media	Alta	Muy alta	Promedio Total
10.1.2 Gestión de cambios.		3								4				1		3
10.2 Gestión de la provisión de servicios por terceros.																
10.2.1 Provisión de servicios.		3								4			2			3.2
10.2.2 Supervisión y revisión de los servicios prestados por terceros.		3								4			2	1		3.2
10.3 Planificación y aceptación del sistema.																
10.4 Protección contra el código malicioso y descargable.																
10.4.1 Controles contra el código malicioso.		3								4				1		3
10.5 Copias de seguridad.																
10.5.1 Copias de seguridad de la información.		2								4		3				3
10.6 Gestión de la seguridad de las redes.																
10.6.1 Controles de red.		3								4				1		3
10.7 Manipulación de los soportes.																
10.7.1 Gestión de soportes extraíbles.	4								3				2			3.2
10.8 Intercambio de información.																
10.8.1 Políticas y procedimientos de intercambio de información.	4								3					1		3
10.9 Servicios de comercio electrónico.																
10.9.1 Comercio electrónico.	4								3					1		3
11. CONTROL DE ACCESO.																
11.1 Requisitos de negocio para el control de acceso.																
11.1.1 Política de control de acceso.	4								3					1		3
11.2 Gestión de acceso de usuario.																
11.2.2 Gestión de privilegios.	4								3					1		3
11.2.3 Gestión de contraseñas de usuario.	4								3					1		3
11.4 Control de acceso a la red.																
11.4.1 Política de uso de los servicios en red.	4								3					1		3
11.4.3 Identificación de los equipos en las redes.		3								4			2			3.2
11.4.6 Control de la conexión a la red.	4								3				2			3.2
11.5 Control de acceso al sistema operativo.																
11.5.6 Limitación del tiempo de conexión.	4								3					1		3
11.6 Control de acceso a las aplicaciones y a la información.																
11.6.1 Restricción del acceso a la información.	4								3					1		3
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.																
13.1 Notificación de eventos y puntos débiles de seguridad de la información.																
13.1.1 Notificación de los eventos de seguridad de la información.	4								3					1		3

	RAZÓN PARA SELECCIONAR EL ELEMENTO															
	COSTO -Peso = 40					TÉCNICA-Peso= 40					OPERATIVA)= Peso = 20					
DOMINIOS, OBJETIVOS DE CONTROL Y CONTROLES	Muy Bajo	Bajo	Medio	Alto	Muy Alto	Podría prescindirse	Poco importante	Muy importante	Necesario	Indispensable	Muy Baja	Baja	Media	Alta	Muy alta	Promedio Total
13.1.2 Notificación de puntos débiles de seguridad.	4								3					1		3
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.																
14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.																
14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.			2							4		3				3
14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.			2							4		3				3
15. CUMPLIMIENTO.																
15.1 Cumplimiento de los requisitos legales.																
15.1.1 Identificación de la legislación aplicable.		3								4				1		3
15.1.4 Protección de datos y privacidad de la información de carácter personal.		3							3			3				3

ANEXO N° 3: “DOMINIOS, OBJETIVOS DE CONTROL Y CONTROLES SELECCIONADOS”

DOMINIOS, OBJETIVOS DE CONTROL Y CONTROLES DEL ISO/IEC 27001	TOTAL DE CONTROLES SELECCIONADOS
5. POLÍTICA DE SEGURIDAD.	
5.1 Política de seguridad de la información.	
5.1.1 Documento de política de seguridad de la información.	2
5.1.2 Revisión de la política de seguridad de la información.	
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	
6.1 Organización interna.	
6.1.3 Asignación de responsabilidades relativas a la seguridad de la información.	2
6.1.5 Acuerdos de confidencialidad.	
6.2 Terceros.	
6.2.1 Identificación de los riesgos derivados del acceso de terceros.	2
6.2.3 Tratamiento de la seguridad en contratos con terceros.	
7. GESTIÓN DE ACTIVOS	
7.1 Responsabilidad sobre los activos.	
7.1.1 Inventario de activos.	2
7.1.3 Uso aceptable de los activos.	
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	
8.1 Antes del empleo.	
8.1.1 Funciones y responsabilidades.	3
8.1.2 Investigación de antecedentes.	
8.1.3 Términos y condiciones de contratación.	
8.2 Durante el empleo.	
8.2.2 Concienciación, formación y capacitación en seguridad de la información	1
8.3 Cese del empleo o cambio de puesto de trabajo.	
8.3.2 Devolución de activos.	2
8.3.3 Retirada de los derechos de acceso.	

DOMINIOS, OBJETIVOS DE CONTROL Y CONTROLES DEL ISO/IEC 27001	TOTAL DE CONTROLES SELECCIONADOS
9. SEGURIDAD FÍSICA Y DEL ENTORNO.	
9.1 Áreas seguras.	
9.1.2 Controles físicos de entrada.	2
9.1.4 Protección contra las amenazas externas y de origen ambiental.	
9.2 Seguridad de los equipos.	
9.2.1 Emplazamiento y protección de equipos.	2
9.2.3 Seguridad del cableado.	
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.	
10.1 Responsabilidades y procedimientos de operación.	
10.1.2 Gestión de cambios.	1
10.2 Gestión de la provisión de servicios por terceros.	
10.2.1 Provisión de servicios.	2
10.2.2 Supervisión y revisión de los servicios prestados por terceros.	
10.4 Protección contra el código malicioso y descargable.	
10.4.1 Controles contra el código malicioso.	1
10.5 Copias de seguridad.	
10.5.1 Copias de seguridad de la información.	1
10.6 Gestión de la seguridad de las redes.	
10.6.1 Controles de red.	1
10.7 Manipulación de los soportes.	
10.7.1 Gestión de soportes extraíbles.	1
10.8 Intercambio de información.	
10.8.1 Políticas y procedimientos de intercambio de información.	1
10.9 Servicios de comercio electrónico.	
10.9.1 Comercio electrónico.	1
11. CONTROL DE ACCESO.	
11.1 Requisitos de negocio para el control de acceso.	

DOMINIOS, OBJETIVOS DE CONTROL Y CONTROLES DEL ISO/IEC 27001	TOTAL DE CONTROLES SELECCIONADOS
11.1.1 Política de control de acceso.	1
11.2 Gestión de acceso de usuario.	
11.2.2 Gestión de privilegios.	2
11.2.3 Gestión de contraseñas de usuario.	
11.4 Control de acceso a la red.	
11.4.1 Política de uso de los servicios en red.	3
11.4.3 Identificación de los equipos en las redes.	
11.4.6 Control de la conexión a la red.	
11.5 Control de acceso al sistema operativo.	
11.5.6 Limitación del tiempo de conexión.	1
11.6 Control de acceso a las aplicaciones y a la información.	
11.6.1 Restricción del acceso a la información.	1
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	
13.1 Notificación de eventos y puntos débiles de seguridad de la información.	
13.1.1 Notificación de los eventos de seguridad de la información.	2
13.1.2 Notificación de puntos débiles de seguridad.	
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	
14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	
14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.	2
14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.	
15. CUMPLIMIENTO.	
15.1 Cumplimiento de los requisitos legales.	
15.1.1 Identificación de la legislación aplicable.	2
15.1.4 Protección de datos y privacidad de la información de carácter personal.	
Total	**41**

Fuente: Elaboración Propia

ANEXO N° 4: "GUÍA PARA LA VALIDACIÓN POR JUICIO DE EXPERTOS DE LOS CONTROLES REQUERIDOS DE SEGURIDAD DE LA INFORMACIÓN EN LA PEQUEÑA Y MICROEMPRESA (MYPE) DE LA PROVINCIA DE TRUJILLO - REGIÓN LA LIBERTAD"

Nombre: …….....

Institución Laboral:……..

Cargo:……..

Parte I: Información general

La encuesta está referida a los controles para garantizar la Seguridad de la Información en la pequeña y microempresa (Mype). Los controles han sido definidos a partir de la norma ISO 27001 considerando aquellos controles mínimos para la Mype, dadas sus limitaciones en recursos y costos.

Parte II: Instrucciones

Cada control debe ser calificado considerando las siguientes opciones:

1.- No necesario: puede ser no considerado

2.- Opcional: podría considerarse

3.- Necesario: es necesario pero no indispensable

4.- Indispensable: es necesario y no puede dejar de considerarse

5.- Obligatorio: no puede dejar de ser considerado

Parte III: Controles requeridos

Califique para cada uno de los controles entre 1 y 5 considerando las premisas definidas líneas arriba

EVALUACIÓN DE CONTROLES (Marque en OPCIONES DE EVALUACIÓN con una X el VALOR QUE CONSIDERE A SU JUICIO)

CONTROLES REQUERIDOS			OPCIONES DE EVALUACIÓN				
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	**DESCRIPCIÓN**	**Controles de Ref. - ISO 27001**	**1**	**2**	**3**	**4**	**5**
1. POLÍTICA DE SEGURIDAD							
Formulación y actualización de Políticas de seguridad	Se debe definir políticas de seguridad, esta se debe publicar y comunicar a todos los empleados y entidades externas relevantes, siendo revisada regularmente en intervalos planeados o si ocurren cambios significativos para así poder ser modificada. El documento que contiene las políticas de seguridad debe ser aprobado por la gerencia o por la persona responsable de la organización.	5.1.1 - 5.1.2					
2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN							
Acta de constitución, asignación de responsabilidades y autoridad y acuerdo de confidenciad.	Se deben definir claramente las responsabilidades, autoridades y los acuerdos de confidencialidad de la seguridad de la información.	6.1.1 - 6.1.8					

CONTROLES REQUERIDOS			OPCIONES DE EVALUACIÓN				
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	**DESCRIPCIÓN**	**Controles de Ref. - ISO 27001**	**1**	**2**	**3**	**4**	**5**
3. GESTIÓN DE ACTIVOS							
Inventario y uso de activos	Todos los activos deben estar claramente identificados, así como también identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con el de procesamiento de la información.	7.1.1 - 7.1.3					
4. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS							
Inducción y capacitación en Seguridad de la información	Se debe brindar capacitaciones tanto a los nuevos empleados como a los antiguos. Las capacitaciones deben tener información relevante sobre seguridad de la información, así como funciones, uso de activos, permisos, etc.	8.1 - 8.3					
Devolución de activos y retiro de derechos de acceso	Esta acción se realiza cuando hay desvinculación del empleado, contratistas o terceros, esto evita cualquier fraude, pérdida o alteración de información.						

CONTROLES REQUERIDOS			OPCIONES DE EVALUACIÓN				
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	**DESCRIPCIÓN**	**Controles de Ref. - ISO 27001**	**1**	**2**	**3**	**4**	**5**
5. SEGURIDAD FÍSICA Y DEL ENTORNO							
Acciones y controles de seguridad física contra amenazas ambientales	Se debe restringir el acceso a personal no autorizado, así como proteger los ambientes donde se encuentren los equipos de comunicación, datos, etc., contra desastres naturales o agentes externos.	9.1					
Emplazamiento y protección de equipos (incluye retiro , control fuera de las instalaciones y retorno)	Se debe contar con la protección debida a los equipos, ya sea dentro del ambiente de trabajo o fuera de él, así como también el respectivo seguimiento cuando dicho equipo salga del área de trabajo y cuando retorne.	9.2.1 - 9.2.7					
Seguridad de instalaciones de cableado y accesorios	Se deben proteger el cableado de energía eléctrica y de datos, evitando que estos puedan ser dañados.						
6. GESTIÓN DE COMUNICACIONES Y OPERACIONES							
Gestión de cambios	Se debe controlar cualquier cambio en los medios y sistemas donde se procesa la información.	10.1 – 10.9					
Gestión de disponibilidad	Se deben implementar controles de red, copias de seguridad de la información, controles de soporte para que la información y las aplicaciones se encuentren disponibles ante cualquier eventualidad.						

CONTROLES REQUERIDOS			OPCIONES DE EVALUACIÓN				
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	**DESCRIPCIÓN**	**Controles de Ref. - ISO 27001**	**1**	**2**	**3**	**4**	**5**
Protección contra código malicioso	Se deben implementar controles que permitan prevenir, detectar y recuperar para la protección de códigos maliciosos						
Gestión de intercambio de información	Se deben implementar controles y definir políticas para intercambios formales de información a través de cualquier medio de comunicación.						
Servicio de comercio electrónico	Se debe proteger la información relacionada con el comercio electrónico, ya que esta transita por la red pública y puede ser modificada fácilmente.						
7. CONTROL DE ACCESO							
Políticas de control de acceso(Matriz de accesos) privilegios, contraseñas y responsable	Se debe definir, documentar y revisar las políticas de control de acceso, privilegio de usuarios, gestión de contraseñas y responsables.	11.1 - 11.2					
Política de uso de red y control de conexión de red	Se debe definir que los usuarios solo tengan acceso a los servicios los cuales han sido autorizados usar, además de restringir la capacidad de acceso de usuarios a la red.	11.4 - 11.6					

CONTROLES REQUERIDOS			OPCIONES DE EVALUACIÓN				
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	**DESCRIPCIÓN**	**Controles de Ref. - ISO 27001**	**1**	**2**	**3**	**4**	**5**
Control de acceso al sistema operativo	Se debe controlar los accesos al sistema operativo mediante procedimientos de registro, donde se identifiquen a los usuarios que acceden a los sistemas. Los sistemas deben cerrarse luego de un periodo de inactividad definido.						
Procedimiento y control de contraseñas	Se deben definir procedimientos y controles para las contraseñas, donde se indique el periodo de renovación de contraseñas, longitud de contraseñas, caracteres especiales, etc.						
Control de acceso a aplicaciones e información	Se debe restringir el acceso a los usuarios a cierta información o aplicativos que no están de acuerdo a su función en concordancia con la política de control de acceso definida.						
8. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN							
Registro de incidentes	Mediante el registro de incidentes, se puede identificar los problemas, fecha de ocurrencia, área donde ocurrió el incidente, verificar el estado en que se encuentra, las medidas tomadas para su solución, etc.	13.1					
Reporte e identificación de incidentes	Mediante el reporte de los incidentes de seguridad de la información se identifican las oportunidades de mejora.						

CONTROLES REQUERIDOS			OPCIONES DE EVALUACIÓN				
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	**DESCRIPCIÓN**	**Controles de Ref. - ISO 27001**	**1**	**2**	**3**	**4**	**5**
Evaluación de incidentes	Se definen controles para la evaluación de incidentes, así como también medidas a tomar ante cual eventualidad, el responsable del incidente y las oportunidades de mejora.						
9. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO							
Planes de continuidad (Incluye pruebas y mantenimiento)	Se debe desarrollar e implementar planes de continuidad que permitan mantener o restaurar las operaciones y asegurar la disponibilidad de la información en niveles y tiempo requerido luego de una interrupción, así como prueba, mantenimiento y re-evaluación de los planes de continuidad, esto servirá para asegurar que estén actualizados y sean efectivos.	14					
10. CUMPLIMIENTO							
Cumplimiento de los requisitos legales en concordancia de delitos informáticos	Se debe cumplir con los requisitos legales establecidos por la ley, como la ley de protección de datos personales, estándares de seguridad, etc.	15					

Controles que usted agregaría:

Parte III: Valoración general

1. No cumple 2. Cumple parcialmente 3. Cumple 4. Cumple totalmente

(Marque con una X su valoración)

	1	2	3	4
Los Controles definidos se adaptan a las posibilidades de las Mypes				
Los Controles cumplen en general con los criterios de factibilidad Técnicos, Operativos y económicos.				
Los Controles permiten en cierto modo mantener la seguridad de la información de una Mype.				

Observaciones y Recomendaciones

Gracias por su valioso aporte a la investigación

ANEXO N° 5: “PROCESO PARA HALLAR EL INTERVALO DE CONFIANZA”

T- Student

$$\mu = \bar{X} \pm t \cdot \frac{\delta}{\sqrt{n}}$$

Donde:

$\bar{x}$**= promedio de la V Aiken**
t= T - Student
$\delta =$ **Desviación estándar**
n= número de jueces

Por lo tanto:

$\bar{x}$**= 0,93**
t= 2.99 **
n = 8
$\delta =$ **0.0498 *****

Resolviendo:

$$\mu = 0,93 \pm 2,99 \cdot \frac{0.048}{\sqrt{8}}$$

$$\mu = 0.93 \pm 0.052$$

$$\mu = 0,87 \pm 0.98$$

$$0.87 \leq \mu \leq 0.98$$

**** (n-1)= 7 => Grado de Libertad**
Nivel de confianza 99%

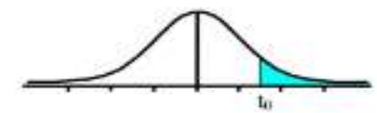
$$1 - \alpha = 0.99$$
$$-\alpha = 0.99 - 1$$
$$\alpha = 0.01$$

=> Nivel de significación
Ubicado en la tabla T-Student tenemos: 2,99

*** $\delta =$ **Desviación estándar**

$$s = \sqrt{\frac{\sum_{i=1}^{n} (x_i - \bar{x})^2}{n-1}}$$

Tabla t-Student



Grados de libertad	0.25	0.1	0.05	0.025	0.01	0.005
1	1.0000	3.0777	6.3137	12.7062	31.8210	63.6559
2	0.8165	1.8856	2.9200	4.3027	6.9645	9.9250
3	0.7649	1.6377	2.3534	3.1824	4.5407	5.8408
4	0.7407	1.5332	2.1318	2.7765	3.7469	4.6041
5	0.7267	1.4759	2.0150	2.5706	3.3649	4.0321
6	0.7176	1.4398	1.9432	2.4469	3.1427	3.7074
7	0.7111	1.4149	1.8946	2.3646	2.9979	3.4995
8	0.7064	1.3968	1.8595	2.3060	2.8965	3.3554

ANEXO N° 6: “VALIDACIÓN DE CONTROLES MEDIANTE JUICIO DE EXPERTOS”

Jueces	Dominio 1	Dominio 2	Dominio 3	Dominio 4		Dominio 5			Dominio 6					Dominio 7					Dominio 8			Dominio 9	Dominio 10
	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16	C17	C18	C19	C20	C21	C22	C23
Juez 1	0.750	0.750	1.000	0.500	1.000	1.000	1.000	1.000	0.750	1.000	1.000	0.750	1.000	1.000	0.750	0.750	0.750	1.000	0.500	0.500	0.500	0.750	1.000
Juez 2	1.000	0.750	1.000	0.750	1.000	1.000	0.750	1.000	1.000	1.000	0.750	1.000	1.000	1.000	1.000	0.750	0.750	1.000	1.000	1.000	1.000	1.000	1.000
Juez 3	1.000	0.750	1.000	1.000	1.000	1.000	0.500	1.000	0.500	1.000	1.000	0.750	0.750	0.500	0.750	0.500	1.000	0.750	0.750	1.000	0.750	1.000	1.000
Juez 4	0.750	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	0.750	1.000	1.000	1.000	1.000
Juez 5	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	0.250	1.000	1.000	0.750	1.000	1.000	1.000	1.000
Juez 6	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
Juez 7	1.000	1.000	1.000	1.000	1.000	1.000	1.000	0.500	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	0.750
Juez 8	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	0.750	0.750	0.750	0.750	1.000	1.000	1.000	1.000	1.000	1.000	0.750	1.000	1.000	1.000
Total por Objetivo	0.938	0.906	1.000	0.906	1.000	1.000	0.906	0.938	0.906	0.969	0.938	0.906	0.938	0.938	0.938	0.781	0.938	0.969	0.844	0.906	0.906	0.969	0.969
Total por Dominio	0.961	0.906	1.000	0.953		0.948			0.931					0.913					0.885			0.969	0.969

Valor mínimo	1
Categorías	4

Escala de Likert	1	2	3	4	5
Valor de Likert en decimales	0	0.25	0.5	0.75	1
Valor de Likert en porcentaje	0%	25%	50%	75%	100%

“RESUMEN DE CONTROLES VALIDADOS MEDIANTE JUICIO DE EXPERTOS”

N °	Controles	V Aiken
1	Formulación y actualización de Políticas de seguridad	0.938
2	Acta de constitución, asignación de responsabilidades y autoridad y acuerdo de confidencialidad.	0.906
3	Inventario y uso de activos	1
4	Inducción y capacitación en Seguridad de la información	0.906
5	Devolución de activos y retiro de derechos de acceso	1
6	Acciones y controles de seguridad física contra amenazas ambientales	1
7	Emplazamiento y protección de equipos (incluye retiro , control fuera de las instalaciones y retorno)	0.906
8	Seguridad de instalaciones de cableado y accesorios	0.938
9	Gestión de cambios	0.906
10	Gestión de disponibilidad	0.969
11	Protección contra código malicioso	0.938
12	Gestión de intercambio de información	0.906
13	Servicio de comercio electrónico	0.938
14	Políticas de control de acceso(Matriz de accesos) privilegios, contraseñas y responsable	0.938
15	Política de uso de red y control de conexión de red	0.938
16	Control de acceso al sistema operativo	0.781
17	Procedimiento y control de contraseñas	0.938
18	Control de acceso a aplicaciones e información	0.969
19	Registro de incidentes	0.844
20	Reporte e identificación de incidentes	0.906
21	Evaluación de incidentes	0.906
22	Planes de continuidad (Incluye pruebas y mantenimiento)	0.969
23	Cumplimiento de los requisitos legales en concordancia de delitos informáticos	0.969
	V Aiken Total	0.931

ANEXO N° 6: “JUECES CONSIDERADOS PARA LA APLICACIÓN DE LA GUÍA DE JUICIO DE EXPERTOS”.

- Experto: Ing. Liliana Vigo Pereyra

  N° CIP: 70724

- Experto: Ing. Freddy Infantes Quiroz

  N° CIP: 139578

- Experto: Ing. Agustín Ullón Ramírez

  N° CIP: 137602

- Experto: Ing. Hebert Abanto Cabrera

  N° CIP: 106421

- Experto: Ing. Litzi Valeriano Valverde

  Centro Laboral: Edpyme Acceso Creditico S.A – Coordinadora de Operaciones y sistemas

- Experto: Ing. Mercedes Napán Aranda

  N° CIP: 153064

- Experto: Doc. Jorge Huapaya Escobedo

  N° CIP: 17215

- Experto: Ing. Noelia Gutiérrez

  Centro Laboral: Caja Municipal de Ahorro y Crédito Trujillo – Jefe de Riesgo Operacional

ANEXO N° 7: “COSTOS DE IMPLEMENTACIÓN DEL MODELO EN LA MYPE”.

PERSONAL			**INVERSIONES**				**GASTOS CORRIENTES**				**OTROS GASTOS**	
DESCRIPCIÓN	CANTIDAD	MONTO	DESCRIPCIÓN	CANTIDAD	UNIDAD DE MEDIDA	MONTO	DESCRIPCIÓN	CANTIDAD	UNIDAD DE MEDIDA	MONTO	DESCRIPCIÓN	MONTO
Analista	1	1000	Laptop	1	Unid.	1500	Útiles de escritorio	-	-	200	Gastos elegibles	100
			Impresora	1	Unid.	500	Materiales de red y comunicaciones	-	-	250	Gastos de gestión	100
			CD	12	Unid.	50						
			USB	2	Unid.	80						
			Otros equipos de almacenamiento	-	-	130						
TOTAL		**1000**	**TOTAL**			**2260**	**TOTAL**			**450**	**TOTAL**	**200**
TOTAL INVERSIÓN								**3910**				

ANEXO N° 8: "CUESTIONARIO PARA AUDITORIA DE CONTROLES EN LA MYPE".

Nombre de la Empresa: _____

Responsable: _____ **Fecha:** _____

CONTROLES AUDITADOS		OPCIONES DE EVALUACIÓN	
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	**DESCRIPCIÓN**	**Cumple**	**No cumple**
1. POLÍTICA DE SEGURIDAD			
Se formulan y actualizan políticas de seguridad	-Define políticas de seguridad. -Publica y comunica las políticas de seguridad a todos los empleados y entidades externas relevantes. -Revisa regularmente las políticas de seguridad en intervalos planeados o si ocurren cambios significativos para así poder ser modificada. -El documento que contiene las políticas de seguridad debe es aprobado por la gerencia o por la persona responsable de la organización.		
2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN			
Existe acta de constitución, asignación de responsabilidades y autoridad y acuerdo de confidencialidad.	-Define claramente las responsabilidades, autoridades y los acuerdos de confidencialidad de la seguridad de la información		
3. GESTIÓN DE ACTIVOS			
Existe inventario y uso de activos	-Los activos están claramente identificados. -Las reglas para el uso aceptable de la información y los activos asociados con el de procesamiento de la información están identificados, documentados e implementados.		
4. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS			

Inducción y capacitación en Seguridad de la información	-Brinda capacitaciones tanto a los nuevos empleados como a los antiguos. -Las capacitaciones tienen información relevante sobre seguridad de la información, así como funciones, uso de activos, permisos, etc.		
Devolución de activos y retiro de derechos de acceso	-Se realiza la devolución de activos y retiro de accesos cuando hay desvinculación del empleado, contratistas o terceros, evitando cualquier fraude, perdida o alteración de información.		
5. SEGURIDAD FÍSICA Y DEL ENTORNO			
Se manejan acciones y controles de seguridad física contra amenazas ambientales	-Se restringe el acceso a personal no autorizado. -Se protege los ambientes donde se encuentren los equipos de comunicación, datos, etc, contra desastres naturales o agentes externos.		
Existe procedimiento de emplazamiento y protección de equipos (incluye retiro , control fuera de las instalaciones y retorno)	-Cuenta con la protección debida a los equipos, ya sea dentro del ambiente de trabajo o fuera de él. -Se realiza el respectivo seguimiento cuando dicho equipo salga del área de trabajo y cuando retorne.		
Seguridad de instalaciones de cableado y accesorios	-Protege el cableado de energía eléctrica y de datos, evitando que estos puedan ser dañados.		
6. GESTIÓN DE COMUNICACIONES Y OPERACIONES			
Existe la gestión de cambios	-Controla cualquier cambio en los medios y sistemas donde se procesa la información.		
Existe la gestión de disponibilidad	-Implementa controles de red, copias de seguridad de la información, controles de soporte para que la información y las aplicaciones se encuentren disponibles ante cualquier eventualidad.		
Existe protección contra código malicioso	-Implementa controles que permitan prevenir, detectar y recuperar para la protección de códigos maliciosos		

Existe la gestión de intercambio de información	-Implementa controles y definir políticas para intercambios formales de información a través de cualquier medio de comunicación.		
Servicio de comercio electrónico	-Protege la información relacionada con el comercio electrónico, ya que esta transita por la red pública y puede ser modificada fácilmente.		
7. CONTROL DE ACCESO			
Existe políticas de control de acceso(Matriz de accesos), privilegios, contraseñas y responsables	-Define, documentar y revisar las políticas de control de acceso, privilegio de usuario, gestión de contraseñas y responsables.		
Existe política de uso de red y control de conexión de red	-Define que los usuarios solo tengan acceso a los servicios los cuales han sido autorizados usar. -Restringe la capacidad de acceso de usuarios a la red.		
Existe procedimiento y control de contraseñas	-Define procedimientos y controles para las contraseñas, donde se indique el periodo de renovación de contraseñas, longitud de contraseñas, caracteres especiales, etc.		
Existe procedimiento de control de acceso a aplicaciones e información	-Restringe el acceso a los usuarios a cierta información o aplicativos que no están de acuerdo a su función en concordancia con la política de control de acceso definida.		
8. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN			
Existe registro de incidentes	-Registra incidentes. Mediante el registro se puede identificar los problemas, fecha de ocurrencia, área donde ocurrió el incidente, verificar el estado en que se encuentra, las medidas tomadas para su solución, etc.		
Existe la evaluación de incidentes	-Define controles para la evaluación de incidentes, así como también medidas a tomar ante cual eventualidad, el responsable del incidente y las oportunidades de mejora.		

9. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO			
Existe planes de continuidad (incluye pruebas y mantenimiento)	-Desarrollar e implementar planes de continuidad que permitan mantener o restaurar las operaciones y asegurar la disponibilidad de la información en niveles y tiempo requerido luego de una interrupción. -Prueba, mantiene y re-evalúa de los planes de continuidad, esto servirá para asegurar que estén actualizados y sean efectivos.		
10. CUMPLIMIENTO			
Existe procedimientos de cumplimiento de los requisitos legales en concordancia de delitos informáticos	-Cumple con los requisitos legales establecidos por la ley, como la ley de protección de datos personales, estándares de seguridad, etc.		