UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

FACULTAD DE CIENCIAS E INGENIERÍA

CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS:

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

PARA OPTAR EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas e Informática

AUTORES:

Bach. Córdova Salinas, José María
Bach. Remicio Canales, Wilian Eusebio

ASESOR:

Mg. Corilla Baquerizo, Eduardo Cancio

ORCID: 0000-0003-3472-2696

DNI Nº 20037930

Lima- Perú
2022

DEDICATORIA

A Dios

Por habernos permitido lograr esta meta y habernos bendecido con salud para cristalizar nuestros objetivos, además de su infinita bondad y amor.

A nuestras familias

Por apoyarnos cada día en todo momento, por sus consejos, valores y por su motivación constante para ser una persona de bien.

AGRADECIMIENTO

A los docentes, por sus lecciones y experiencias brindadas en formarnos como personas de bien y preparadas para los retos que pone la vida.

A la empresa Quantify Agency E.I.R.L. por facilitarnos la información necesaria para la realización de la presente investigación.

PRESENTACION

Señores miembros integrantes del jurado, en el marco del reglamento de "Grado de Bachiller y Título Profesional de la Universidad Peruana de Ciencias e Informática, aprobado por Resolución N° 373-2019-UPCI-R"; y en cumplimiento de los requisitos requeridos en el "Artículo N° 45, de la ley N° 30220; donde se indica que la obtención de grados y títulos se realiza de acuerdo a las exigencias académicas que cada universidad establezca", presentamos ante ustedes la tesis titulada "Modelo del Sistema de Gestión de Seguridad de la Información basado en la ISO 27001:2013 para minimizar los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency", la misma que se pone a vuestra consideración y evaluación para su aprobación y optar el Título Profesional de Ingeniero de Sistemas e Informática.

Atentamente. -

Bach. Córdova Salinas, José María.

Bach. Remicio Canales, Wilian Eusebio.

ÍNDICE

INDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

La presente investigación fue realizada en la empresa QUANTIFY AGENCY E.I.R.L., dedicada al asesoramiento empresarial referente a crear o mejorar la imagen corporativa de las organizaciones y cuya oficina está ubicada en el distrito de Miraflores, en Lima.

La finalidad de esta tesis fue "determinar la relación entre el modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 para minimizar los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency".

La metodología y el tipo de investigación fue aplicada, diseño no experimental y de nivel descriptivo correlacional; donde se utilizará la técnica de la encuesta y como instrumento de recolección de datos el cuestionario. La muestra probabilística final estuvo constituida por 10 personas trabajadores de la empresa.

Para el procesamiento de datos se aplicó el software estadístico SPSS, así como el análisis de fiabilidad se realizó con el alfa de Cronbach es de 0.922, por lo que se afirma que el instrumento posee un nivel excelente de fiabilidad siendo superior al mínimo aceptable de 0.7.

De los resultados obtenidos se concluyó que existe una correlación perfecta rho Spearman = 0.1 , donde el P = 0.000 < 0.05, se rechaza la H0, por lo tanto, sí existe correlación perfecta entre el modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 para minimizar los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.

De los resultados obtenidos muestran que sí existe relación muy alta del modelo del SGSI para minimizar los riesgos de seguridad en la empresa en Quantify Agency.

Palabras clave: Sistema de Gestión de Seguridad de la Información (SGSI), ISO/IEC 27001, Gestión de Riesgo.

ABSTRACT

This research was carried out in the company QUANTIFY AGENCY E.I.R.L., dedicated to business advice regarding creating or improving the corporate image of organizations and whose office is located in the district of Miraflores, in Lima.

The purpose of this thesis was “to determine the relationship between the information security management system model based on ISO 27001:2013 and the minimization of security risks in the systems area of the Quantify Agency company.

The methodology and type of research was applied, non-experimental design and correlational descriptive level; where the survey technique will be used and the questionnaire as a data collection instrument. The final probabilistic sample consisted of 10 workers of the company.

The SPSS statistical software was used in data processing, as well as the reliability analysis was performed with Cronbach's alpha of 0.922, so it is stated that the instrument has an excellent level of reliability, being higher than the minimum acceptable of 0.7.

From the results obtained, it was concluded that there is a perfect correlation, rho Spearman = 0.1 , where $P = 0.000 < 0.05$, H0 is rejected, therefore, there is a perfect correlation between the model of the information security management system based on the ISO 27001:2013 to minimize security risks in the systems area of the company Quantify Agency.

The results obtained show that there is a very high relationship of the Information Security Management System model to minimize security risks in the company in Quantify Agency.

Keywords: Information Security Management System (ISMS), ISO/IEC 27001, Risk Management.

I. INTRODUCCION

En estos tiempos de globalización, la seguridad de la información está siendo tomada de forma seria por las empresas, ya que esta se considera uno de los principales activos de una organización.

La seguridad de la información asegura la disponibilidad, integridad y confidencialidad de la información, con lo cual reduce considerablemente las vulnerabilidades y el mal uso de los activos.

Las empresas nuevas, como es el caso de Quantify Agency, no tienen bien definidas las políticas que deben implementar para la protección de su información, por lo que podrían sufrir ataques que ocasionen pérdida de información y tampoco tienen definida una respuesta o acción frente a este escenario.

Por tanto, la presente tesis se enfoca plantear un modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 para minimizar los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency., la cual servirá para la identificación de los riesgos y/o vulnerabilidades que pueden afectar a la empresa. Se realizará un diagnóstico del estado de la empresa con relación a la protección de su información, de tal forma que luego de la implementación, podremos brindar recomendaciones acordes a la normatividad vigente.

1.1. Realidad problemática

La tecnología ha permitido a las empresas desarrollarse y crecer de forma acelerada, pudiendo llegar a cualquier parte del mundo de forma inmediata.

Sin embargo, este avance tecnológico también trae formas avanzadas de recibir ataques, formas variadas de que nuestra información se pierda o sea modificada deliberadamente, formas en que los empleados de una organización no estén seguros de cómo reaccionar o qué deben hacer ante un posible ataque.

La Seguridad de la Información se ha establecido como un aspecto fundamental en las organizaciones, sean del tamaño que fueren, para la protección de los datos. Los datos se han convertido en uno de los activos más importantes de una empresa, por lo que esta debe garantizar su incorruptibilidad durante todo su ciclo de vida.

QUANTIFY AGENCY E.I.R.L. es una empresa que inició sus actividades en septiembre del 2019, dedicada, principalmente, al asesoramiento de imagen empresarial en la que realizan, en primer lugar, una investigación que les ayuda a comprender los puntos fuertes y débiles de la empresa; crean, luego, una estrategia donde buscan transformar las debilidades en fortalezas. Como paso siguiente, diseñan un impacto visual que sea a prueba de tiempo, profesional, limpio y conceptual y, por último, brindan la propuesta final que busca superar las expectativas del cliente.

Al ser una empresa relativamente nueva, no tienen bien definidas las políticas de seguridad que se apliquen en un momento dado, por lo que, en la presente investigación, se buscará plantear un modelo de sistema de gestión de seguridad de la información basado en la ISO 27001:2013 para minimizar los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency., de

forma que, al finalizar, cuente con políticas de seguridad definidas para el manejo de la seguridad de su información.

1.2. Planteamiento del problema

Delimitación del Problema

Espacial

La investigación se realizará en la empresa Quantify Agency, ubicada en el distrito de Miraflores, en Lima.

Temporal

Para la elaboración del proyecto, será considerar los datos del año 2021.

1.2.1. Problema General

¿Cómo se relaciona el modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 para minimizar los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency?

1.2.2. Problemas Específicos

a) ¿Cómo se relaciona el modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y la identificación de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency?

b) ¿Cómo se relaciona el modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y el análisis de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency?

c) ¿Cómo se relaciona el modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y la evaluación de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency?

1.3. Hipótesis de la investigación

1.3.1. Hipótesis General

Existe relación entre el modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 para minimizar los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.

1.3.2. Hipótesis Específicas

a) Existe relación entre el modelo del sistema de gestión de seguridad de la información y la identificación de riesgos de la información en el área de sistemas de la empresa Quantify Agency.
b) Existe relación entre el modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y el análisis de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.
c) Existe relación entre el modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y la evaluación de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.

1.4. Objetivos de la investigación

1.4.1. Objetivo General

Determinar la relación del modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 para minimizar los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.

1.4.2. Objetivos Específicos

a) Determinar la relación del modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y la identificación de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.

b) Determinar la relación del modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y el análisis de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.

c) Determinar la relación del modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y la evaluación de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.

1.5. Variables, dimensiones e indicadores

1.5.1. Variable Independiente

- ✓ Sistema de Gestión de Seguridad de la Información.

1.5.2. Variable Dependiente

- ✓ Riesgos de seguridad.

1.5.3. Dimensiones

- ✓ Requisitos del SGSI.
- ✓ Análisis de brechas.
- ✓ Controles de seguridad.
- ✓ Identificación de riesgos.
- ✓ Análisis de riesgos.
- ✓ Evaluación de riesgos.

1.5.4. Indicadores de las variables

- ✓ % de cumplimiento del SGSI.
- ✓ % de brechas.

- ✓ % de controles implementados.
- ✓ Nivel identificación de riesgos.
- ✓ Nivel de análisis riesgos.
- ✓ Nivel de evaluación riesgos.

1.5.5. Operacionalización de variables

Tabla 1. *Operacionalización de variables.*

Variable	Dimensión	Indicador	Escala de medición
Sistema de Gestión de Seguridad de la Información	Requisitos del SGSI	% de cumplimiento del SGSI	Totalmente en desacuerdo En desacuerdo Indiferente De acuerdo Totalmente de acuerdo
	Análisis de brechas	Nivel de brechas	
	Controles de seguridad	% de activos vulnerables	
Riesgos de seguridad	Identificación de riesgos	Nivel identificación de riesgos	Totalmente en desacuerdo En desacuerdo Indiferente De acuerdo Totalmente de acuerdo
	Análisis riesgos	Nivel de análisis riesgos	
	Evaluación riesgos	Nivel de evaluación riesgos	

Fuente: Elaboración propia.

1.6. Justificación del estudio

El presente proyecto se justifica porque su implementación es necesaria para reducir considerablemente los riesgos de la pérdida de información en el área de sistemas de la empresa.

Justificación Teórica

Proteger la información es primordial en cualquier organización, por tanto, se requiere siempre garantizar la confidencialidad, integridad y disponibilidad de esta mediante adecuadas políticas de seguridad.

Esta investigación busca aplicar la norma ISO/IEC 27001 para reducir el riesgo de pérdida de información en la empresa Quantify Agency. Mediante la aplicación de esta norma, se busca la identificación del riesgo y amenazas que pudieran comprometer su información y establecer medidas que ayuden a reducirlos a un nivel aceptable, de manera que pueda asumir, proteger y controlar estas amenazas por medio de procedimientos documentados y que las conclusiones de esta investigación incorporen conocimiento y pueda ser aprovechada en otras organizaciones que necesiten proteger su información.

Justificación Práctica

A causa de que ‘’Quantify Agency’’ no cuenta actualmente con una metodología que proteja la información, además de que carece de procesos que se puedan seguir para disminuir el riesgo de que la seguridad falle, fue necesaria la implementación de un SGSI que permita conocer y reducir al máximo los riesgos a fin de que, tanto usuarios como clientes, tengan la seguridad de que la información estará protegida.

Justificación Legal

Cada vez hay más leyes, reglamentos y requisitos Acuerdos contractuales relacionados con la seguridad de la información. Las buenas noticias es que la mayoría de ellos se pueden solucionar implementando la ISO 27001 ya que

esta regla le proporciona una metodología perfecta para cumplir con todos ellos.

Justificación Económica

La filosofía principal de ISO 27001 es prevenir la ocurrencia de incidentes de seguridad, y cada incidente, grande o pequeño, cuesta dinero; por lo tanto, al evitarlos, la empresa ahorrará mucho dinero.

1.7. Antecedentes nacionales e internacionales

1.2.1 Antecedentes internacionales

(Molano, 2017), Desarrolló la tesis titulada "Estrategia para implementar un sistema de gestión de seguridad de la información basado en la norma ISO 27001 en el área de TI para la empresa Market Mix. Universidad Católica de Colombia. Bogotá – Colombia". La investigación tiene como objetivo general: "Identificar la mejor estrategia en el proceso de implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001 en el área de TI para la empresa Market Mix".

La presente investigación:

Tuvo como objetivo "identificar una estrategia para la implementación de un Sistema de Gestión de Seguridad de la Información para el área de TI de la empresa Market Mix", los datos obtenidos fueron procesados y permitió identificar la estrategia óptima a aplicar para cumplir con sus objetivos.

La aplicación de estrategias y seguimiento constante de las actividades asignadas a los integrantes y permita identificar los riesgos al que se encuentran expuestos en la organización, así ser atacados y realizar las correcciones a fin de implementar mejoras continuas y proteger los activos de información y garantizar la continuidad de la empresa.

(Crespo, 2016), desarrollo la Tesis de "Metodología de Seguridad de la Información para la Gestión del Riesgo Informático Aplicable a MPymes. Universidad de Cuenca. Cuenca – Ecuador".

> La información es el activo más valioso para la organización o persona, lo que, para muchos es, una herramienta para crear la ventaja competitiva de la empresa. Sin embargo, el desconocimiento acerca de cómo proteger los activos de información, así como los estándares internacionales que establecen los procedimientos adecuados y lograr un nivel adecuado de protección, en las organizaciones, especialmente las del sector MIPYME. Se propone una metodología de SGSI para la gestión de riesgos informáticos aplicable al entorno empresarial y organizacional del sector MIPYME ecuatoriana. Para ello, se analizan comparativamente "varias metodologías ampliamente difundidas, tales como: Magerit, CRAMM (CCTA Risk Analysis and Management Method), OCTAVE-S, Microsoft Risk Guide, COBIT 5 y COSO III. Estas metodologías se utilizan internacionalmente en la gestión de riesgos de la información; a la luz de los marcos de referencia de la industria: ISO 27001, 27002, 27005 y 31000" (Crespo, 2016, pág. 2)

(Serna, Duran, & Sanchez, 2017), Desarrollaron la tesis titulada **"**Diseño de un sistema de gestión de la seguridad de la información para la secretaria de hacienda de rio de ORO-CESAR, basado en la norma ISO/IEC 27001:2013. Universidad Francisco de Paula Santander. Ocaña – Colombia". El objetivo general de la investigación fue: **"**Diseñar un sistema de gestión de la seguridad de la información para la Secretaría de Hacienda de Rio de Oro-Cesar, basado en la norma ISO/IEC 27001:2013**"**.

> Para el secretario de Hacienda de Río de Oro-Cesar es de vital importancia proteger la información y la infraestructura que soporta el sistema de información de la dependencia. Por lo tanto, este trabajo de grado se basó en el "Diseño de un Sistema de Gestión de Seguridad de la Información, basado en la norma internacional ISO/IEC27001:2013".
>
> Para llevar a cabo el Diseño del SGSI, inicialmente fue necesario un diagnóstico situacional del SGSI en la Secretaría de Hacienda de Rio de Oro-Cesar. A continuación, se determinó el estado de madurez desde el punto de vista de los procesos de misión de la unidad, frente a los requerimientos metodológicos y de acuerdo con los dominios y controles establecidos en el Anexo A de la norma ISO IEC-27001:2013.
>
> Posteriormente, se aplicó la "metodología para la Gestión de Riesgos, propuesta en la norma ISO/IEC 27005", identificando las principales vulnerabilidades y amenazas, que se encuentran expuestos los activos información de los sistemas del Ministerio de Hacienda, con el objetivo de aplicar el plan de tratamiento de riesgos de seguridad de la información, de acuerdo a los hallazgos encontrados y finalmente se definieron las políticas de seguridad de la información que brinden a la dependencia los lineamientos necesarios para proteger sus activos.

(Leon, 2019)**,** Efectuó una investigación titulada **"**Diseño de un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC27001 para entidades del estado. Universidad Nacional Abierta y a Distancia -UNAD. La Riohacha, Guajira – Colombia".

Cuyo objetivo general fue:

> **“**Diseñar un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001 que permita preservar la integridad, confidencialidad y disponibilidad de la información en las entidades del estado**”**.
>
> Este documento se basó en la elaboración y diseño de una guía de buenas prácticas y procedimientos sistémicos, que consisten en minimizar los riesgos y proteger la información, específicamente en las organizaciones y entidades estatales, con el fin de preservar la confidencialidad, integridad y disponibilidad de esta, a través de una herramienta de gestión relacionada con la seguridad y privacidad de los datos.
>
> Es por ello por lo que surgió la necesidad de desarrollar un sistema de gestión de seguridad de la información (SGSI) tomando como referencia la metodología definida por la norma ISO/IEC 27001. Con el fin de ponerlo a disposición de las entidades gubernamentales y que sea utilizado como guía para definir sus políticas de seguridad de la información.
>
> De esta forma, este documento busca brindar los lineamientos básicos y generales de cómo comenzar a diseñar y dimensionar el alcance para implementar el SGSI en una organización de Colombia.

(Guerrero, Navarro, Lizcano, & Felizzola, 2019), Efectuó una investigación titulada **“**Diseño del sistema de gestión de seguridad de la información SGSI basado en el estándar ISO 27001, en la Universidad Popular del Cesar, Seccional Aguachica. Universidad Francisco de Paula Santiago Ocaña. Ocaña – Colombia”. Cuyo objetivo general fue: **“**Diseñar el sistema de gestión de seguridad de la información SGSI basado en el estándar ISO 27001, en la Universidad Popular del

Cesar, Seccional Aguachica.**”**.

Mediante auditoría interna se visualiza que en la UPC Aguachica no existe un sistema basado en la norma ISO27001. “se realizó el análisis de la situación actual, identificando activos a los que se aplicó la norma, desarrollando un sistema de gestión y evidenciando los hallazgos encontrados, aplicables a la institución” (MINTIC, 2016), roles y responsabilidades.

1.2.2 Antecedentes nacionales

(Santos, 2016), En su investigación de tesis titulada **“**Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de software. Pontificia Universidad Católica del Perú. Lima Perú”.

Planteó como objetivo general: “Desarrollar un Sistema de Gestión de Seguridad de Información (SGSI) para una empresa de consultoría en desarrollo y calidad de software, tomando como marco normativo el estándar ISO/IEC 27001:2013”.

Actualmente, las empresas consultoras de desarrollo de software tienen muchos desafíos. Donde, destacan los relacionados con la seguridad de la información, debido al constante intercambio de información entre las empresas y sus clientes, existen riesgos potenciales que comprometen el éxito e incluso la supervivencia de la empresa.

La solución propuesta es un Sistema de Gestión de Seguridad Sistema de Información (SGSI), que tiene como marco la norma ISO 27001:2013.

Requisitos formales para cumplir. Este sistema permite a los gerentes e involucrados gestionar y tomar decisiones adecuadas relacionada con la

> seguridad de información de la empresa, para asegurar los niveles adecuados de la confidencialidad, integridad y disponibilidad de la información crítica manejado como parte de su operación.
>
> Este modelo permite que el sistema funcione con el principio de mejora continua, que beneficia permanentemente a la organización, promoviendo una óptima gestión de la seguridad de su información.

(Porras, 2019), Desarrolló una tesis titulada **"**Sistema de gestión de seguridad de la información para la gestión de riesgos en activos de información. Universidad Peruana Los Andes. Huancayo – Perú".

> El objetivo general de la investigación fue: **"**Determinar la influencia de la implementación del Sistema de Gestión de Seguridad de la Información en la gestión de riegos en activos de información en la Empresa de BPO Contac Center Digitex, Lima".
>
> El estudio nos permitió distinguir claramente las ventajas obtenidas por haberlo implementado y la efectividad de alinearse con los procesos de negocio.
>
> El método de investigación fue de tipo Aplicada, nivel Explicativo, diseño Pre-experimental con Pre test y Post test. "fue considerado como población a los 114 controles del ANEXO A de la ISO 27001 y como muestra a 70 controles aplicables para el alcance definido, el resultado fue que la implementación del SGSI basado en controles de seguridad mejoró la madurez de la gestión de riesgos en los activos de información y el valor medio pasó de 3.65 a 5.22, se concluye que la implementación del SGSI genera resultados favorables en la gestión de Riesgos de los Activos de Información" (Porras, 2019, pág. 10)

(Castillo, 2016) , Desarrolló la investigación titulada “Sistema de gestión de seguridad de la información en la municipalidad distrital de Pira aplicando la norma ISO/IEC 27001:2013. Universidad Católica Los Ángeles de Chimbote. Huaraz – Perú”.

> Cuyo objetivo general de la investigación fue: “Evaluar el sistema de gestión de seguridad de la información en la Municipalidad Distrital de Pira basado en la norma ISO/IEC 27001:2013; la cual permitirá una mejor administración en los activos de información”.
>
> Este informe propone un “SISTEMA DE GESTIÓN DE SEGURIDAD PARA LA INFORMACIÓN EN EL MUNICIPIO DISTRITAL DE PIRA según la norma internacional ISO/IEC 27001:2013” porque las medidas de control cumplen los requisitos mínimos de seguridad de acuerdo con el diagnosticó la situación actual del municipio han sido parcialmente eficaces.
>
> Posteriormente, se desarrolló el SGSI en base a la fase de planificación del estándar. ISO/IEC 27001:2013 y en los controles. Como metodología de Análisis de Gestión de Se utilizó Risk MAGERIT versión 3.0. Orientado a todos los sectores de la organización. (Castillo, 2016, pág. 5)
>
> Una vez concluida la tesis, se dieron recomendaciones respecto al correcto uso y gestión de activos, seguridad de la información y los cambios que se requeridos para lograr mejores resultados en los sistemas de gestión de seguridad de la información en la Municipalidad Distrital de Pira.

Las conclusiones de la investigación de Castillo (2016) fueron:

a) “Ciertos procesos no cuentan con una buena gestión para su funcionamiento tales como: manuales, planos y recursos más necesarios.

b) Alto nivel de riesgos que existe en la gestión de los activos de información dentro del municipio, debido al poco control.

c) Tomar medidas preventivas y correctivas en los procesos que deban ser atendidos a la mayor brevedad posible en un nivel de seguridad para su mejor funcionamiento".

d) Informe basado en la norma ISO/IEC 27001:2013, soportado en la metodología MAGERIT versión 3.0, norma que permitió evaluar los riesgos de seguridad de la información, con el objetivo de "determinar en qué condiciones se encuentran y si están alineados con los objetivos del negocio. garantizando la integridad de su información en beneficio del municipio".

(Ochoa, 2019), Desarrolló la investigación titulada "Sistema web de gestión de seguridad de la información asistida por computadora basada en el estándar ISO 27001 en la universidad nacional José María Arguedas. Universidad Nacional José María Arguedas Cuyo. Andahuaylas – Perú".

Objetivo general de la investigación fue: **"**Desarrollar un Sistema web de gestión de seguridad de la información asistida por computadora basada en el estándar ISO 27001 en la Universidad Nacional José María Arguedas.".

Las conclusiones de la investigación de Ochoa (2017) fueron:

a) " Se analizó y diseñó los procesos y controles de gestión de la seguridad de la información en la Universidad.

b) Se construyó y probó eficientemente las medidas y controles de gestión de la seguridad de la información en la Universidad.

c**)** Se implementó y desplegó los controles del sistema de gestión de seguridad de la información en la Universidad".

(Vilca, 2017), Desarrolló una investigación titulada "Diseño e implementación de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos humanos de la empresa Geosurvey de la ciudad de Lima. Universidad de Huánuco. Huánuco. Perú".

Cuyo objetivo general de la investigación fue: **"**Determinar la mejora de implementar un sistema de gestión de seguridad de la información para la seguridad del área de recursos humanos de la empresa GEOSURVEY S.A**"**.

Tuvo como propósito "implementar un SGSI bajo la norma ISO 27002 para mejorar la seguridad en cuanto al uso de activos y tecnologías de la información en la empresa Geosurvey de la ciudad de Lima en el año 2016".

La metodología fue de "enfoque cuantitativo, tipo aplicativo; debido a que se utilizó la tecnología para resolver un problema, así mismo se utilizó el diseño pre-experimental de pre y post test, se realizó un experimento en condiciones controladas. Tanto la población como la muestra estuvo conformada por 33 trabajadores, al ser de tipo no probabilístico se tomó en cuenta a todos los trabajadores de las diferentes áreas de la empresa" (Vilca, 2017, pág. 8).

Para el proceso de recolección de datos se aplicó como técnica la encuesta e instrumento el cuestionario, los datos se procesaron con el software estadístico SPSS.

Se utilizaron las fases PDCA de la norma ISO 27002, para el diagnóstico de la gestión de riesgos de la organización, el desarrollo de la política de seguridad y con ello también el sistema de gestión de incidentes para poder controlar y mejorar la seguridad de la información de la empresa.

1.8. Marco teórico

Para la comprensión del proyecto presentado se deben tener en cuenta ciertos conceptos importantes, los cuales son elaborados, en los siguientes numerales:

1.8.1 Sistema de gestión de seguridad de la información

(Asociación Española para la Calidad, 2012), "Este sistema se basa en la norma UNE-ISO/IEC 27001:2007, forma parte del sistema general de gestión, se basa en un enfoque de riesgo comercial para establecer, implantar, operar, controlar , revisar, mantener y mejorar la seguridad de la información; sigue un enfoque basado en procesos que utilizan el ciclo de mejora continua o ciclo de Deming, o más conocido como PDCA (Plan-Do-Check-Act), también se basa en la norma UNE-ISO/IEC 27002:2009 que incluye una lista de los controles necesarios para alcanzar los objetivos de seguridad de información. El SGSI está diseñado para garantizar una selección de controles de seguridad que protegen los activos de información y dan confianza a las partes interesadas. El diseño y la implementación del SGSI de una organización están influenciados por las necesidades y objetivos comerciales, los requisitos de seguridad, los procesos, el tamaño y la estructura de la organización. Se espera que estos y sus sistemas de soporte cambien con el tiempo, ya que las situaciones simples requieren soluciones ISMS simples".

ISO/IEC 27001: 2013

ISO/IEC 27001:2014 explica que esta "Norma Internacional especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. El sistema de gestión de seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y da confianza a las partes interesadas de que los riesgos se gestionan adecuadamente". (ISO/CEI 27001, 2013).

"La Norma Internacional tiene 10 cláusulas, de las cuales las primeras tres (3) tratan sobre el contexto de la norma y los 7 restantes muestran los requisitos para la implementación del SGSI". (ISO/CEI 27001, 2013). (Ver figura).

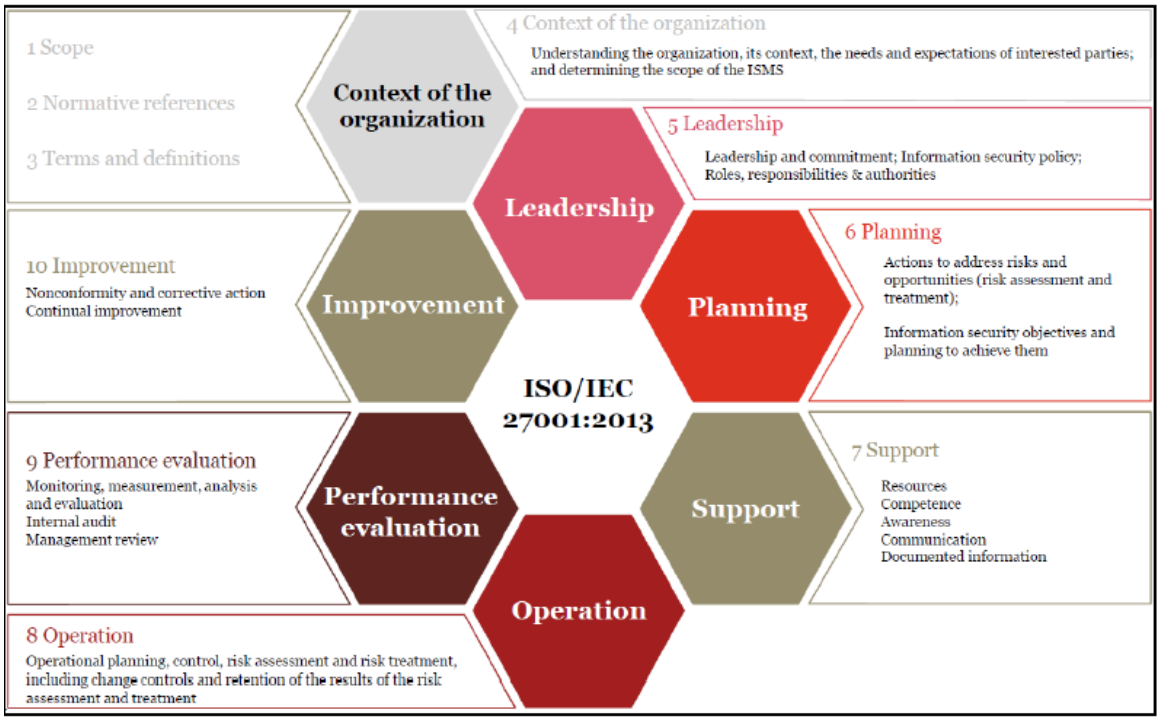


Figura 1. Cláusulas de la ISO/IEC 27001.
Fuente: Organización Internacional de Normalización (2013). ISO/IEC 27001.

Ciclo PHVA

Esta norma internacional adopta el modelo de proceso "Planificar-Hacer-Verificar-

Actuar" (PHVA) o la "rueda de Deming", que se aplica a la estructura de todos los procesos de un sistema de gestión. Se muestra cómo un sistema de gestión utiliza como entrada los requisitos y las expectativas de las partes interesadas, y cómo se producen, con las acciones y procesos necesarios, los resultados de seguridad de la información que cumplan con los requisitos y expectativas.

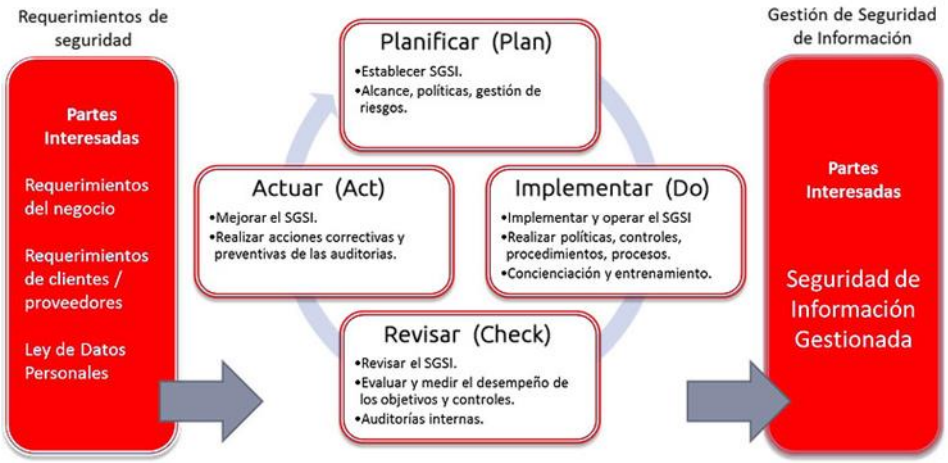


Figura 2. Ciclo de Deming.
Fuente: ISO 27001:2013.

Planificar (establecer el sistema de gestión): "Establecer la política, los objetivos, los procesos y procedimientos relacionados con la gestión de riesgos y la mejora de la seguridad de la información para proporcionar resultados en línea con las políticas mundiales y los objetivos de la organización. (ISO 27001:2013)

Hacer (implementar y operar el sistema de gestión): Implementar y operar la política, controles, procesos y procedimientos del sistema de gestión.

Verificar (monitorear y revisar el sistema de gestión): Evaluar y, si procede, medir las actuaciones del proceso frente a la política, los objetivos y la experiencia práctica e informar los resultados a la gerencia para su revisión.

Actualizar (mantener y mejorar el sistema de gestión): Llevar a cabo las acciones correctivas y preventivas, sobre la base de los resultados de la auditoría interna y

revisión por la dirección, u otra información relevante para la mejora continua de dicho sistema".

A continuación, se detallan las 10 cláusulas:

- **Cláusula 1:** Ámbito: "incluye requerimientos para la valoración y tratamiento de riesgos de la seguridad de la información de cualquier empresa o Compañía" (Columba Bernardo, 2017).
- **Cláusula 2:** Referencias normativas: "Se hace una referencia normativa en parte, o en su totalidad, a la norma ISO/IEC 27000, Information Technology. Security Technology Techniques. Information Security Management Systems. Overview and Vocabulary" (ISO/IEC 27001, 2013).
- **Cláusula 3:** Términos y definiciones: "Se aplican términos y definiciones proporcionados en ISO/IEC 27000". (ISO/IEC 27001, 2013).
- **Cláusula 4:** Contexto de la Organización: "Se determinan aspectos como el conocimiento de la organización, comprensión de las necesidades y expectativas de las partes interesadas". (Columba Bernardo, 2017).
- **Cláusula 5:** Liderazgo: "La alta dirección debe demostrar liderazgo y compromiso respecto al SGSI" (ISO/IEC 27001, 2013).
- **Cláusula 6:** Planificación: "Cuando se planifica el SGSI, la organización debe considerar lo referente a comprender la organización y comprender las necesidades y expectativas de las partes interesadas para asegurar que el SGSI pueda lograr los objetivos esperados" (ISO/IEC 27001, 2013).
- **Cláusula 7:** Soporte: "En este punto, muestra los recursos, competencias e información documentada; así como el trabajo de concientización y comunicación que debe realizar la organización para la implementación del SGSI" (ISO/IEC 27001, 2013).

- **Cláusula 8:** Operación: “La organización debe planificar implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información” (ISO/IEC 27001, 2013).
- **Cláusula 9:** Evaluación de desempeño: “La organización debe evaluar el desempeño de la seguridad de la información y la efectividad del sistema de gestión de seguridad de la información determinando los métodos de monitoreo, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos” (ISO/IEC 27001, 2013).
- **Cláusula 10:** Mejoras: “Cuando en las evaluaciones (Cláusula 9) se identifican no conformidades, la organización debe tomar acciones correctivas, y estas deben ser apropiadas de acuerdo con los efectos de las no conformidades encontradas” (ISO/IEC 27001, 2013).

El anexo A “es la serie más conocida de objetivos de control de seguridad para la implementación ISO / IEC 27001: 2013” y consiste en:

- “14 dominios de control: Principales tópicos que cubren la mayoría de los aspectos de la seguridad de la información.
- 34 objetivos de control: Objetivos de los controles propiamente dichos.
- 114 controles: Controles aplicables a ser implementados en el programa del sistema de gestión”.

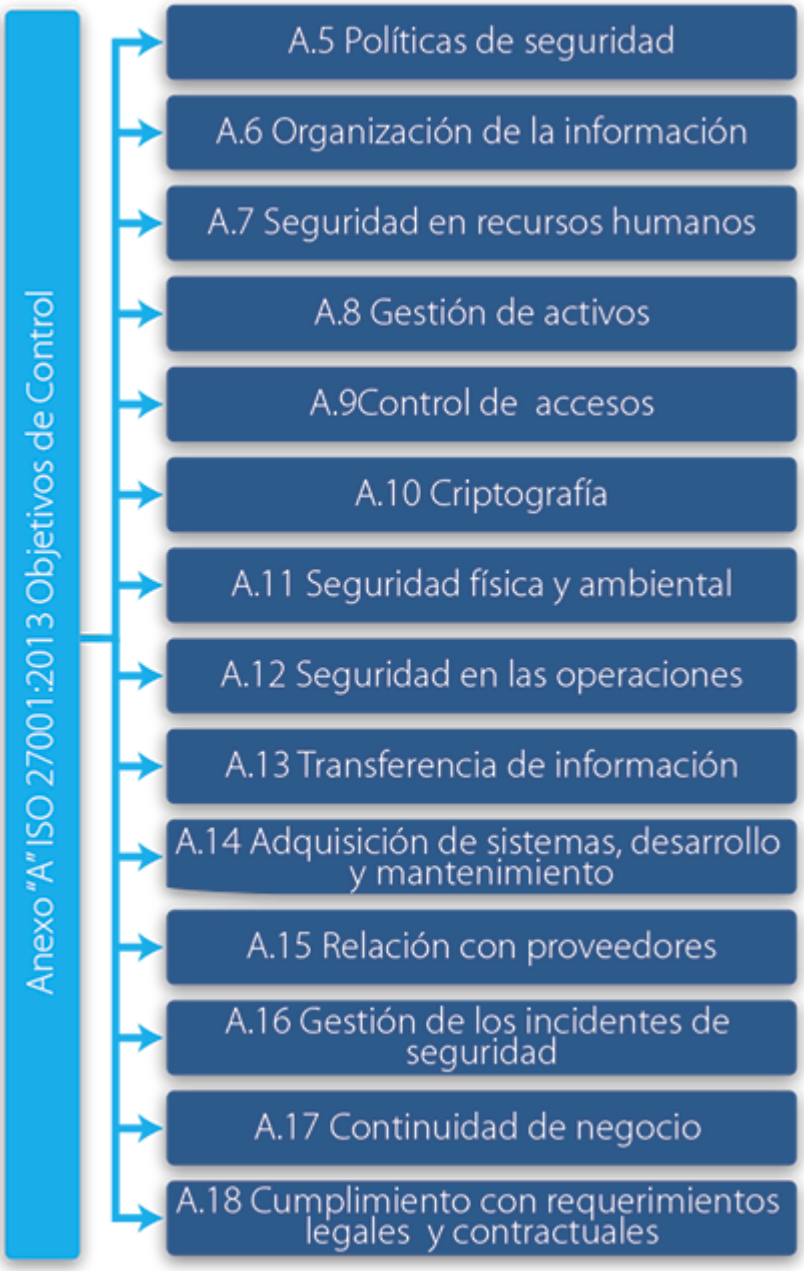


Figura 3. Dominios de la ISO 27001:2013.

Fuente: ISO 27001:2013.

Fases para la implementación del SGSI

El Sistema de Gestión de La Seguridad de la Información que propone la Norma ISO 27001 se puede resumir en las siguientes fases:

Figura 4. Fases de la implementación de la ISO 27001.
Fuente: ISO 27001:2013.

1.8.2 Riesgos

"Efecto que genera incertidumbre sobre el logro de los objetivos de seguridad de información" (ISO/IEC 27000: 2014).

Valoración de riesgos

Consiste en establecer el contexto, identificación de riesgos, análisis de riesgos, y evaluación de riesgos.

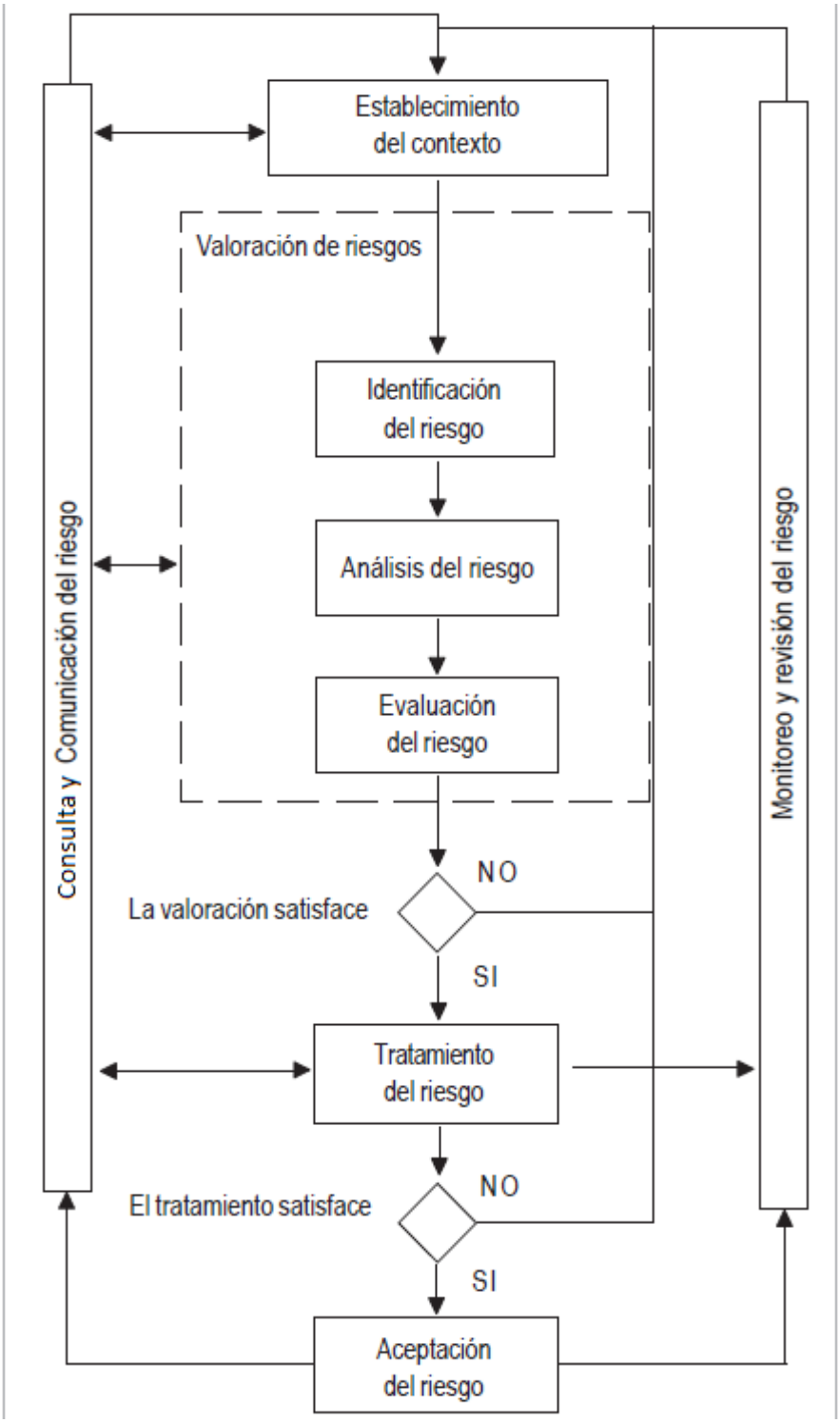


Figura 5. Enfoque de evaluación de riesgos según ISO 27005
Fuente: ISO 27005

Identificación de riesgos

Los riesgos potenciales deberían aparecer en la lista de riesgos.

El inicio de este enfoque es la identificación de los activos de información que pueden ser afectados en su integridad, confidencialidad y disponibilidad.

A partir de la lista de los activos debería ser realizado el análisis del riesgo para establecer un plan de tratamiento de riesgos que está en conformidad con lo dispuesto en la política de SGSI, y alineado con las expectativas de negocio de la empresa.

El análisis de los controles que dentro de la organización debe consistir en evaluar los posibles controles y permitir concluir así las estrategias que se recomiendan que son ventajosas para la organización.

Análisis de Riesgos

De acuerdo con el capítulo 5.4.3 de la ISO 31000. “El análisis del riesgo implica desarrollar una comprensión del riesgo.

El análisis del riesgo proporciona elementos de entrada para la evaluación del riesgo y para tomar decisiones acerca de si es necesario tratar los riesgos, así como sobre las estrategias y los métodos de tratamiento del riesgo más apropiados.

El análisis del riesgo implica la consideración de las causas y las fuentes del riesgo, sus consecuencias positivas y negativas, y la probabilidad de que estas consecuencias puedan ocurrir. Se deberían identificar los factores que afectan a las consecuencias y a la probabilidad. El riesgo se analiza determinando las consecuencias y su probabilidad, así como otros atributos del riesgo. Un suceso puede tener múltiples consecuencias y puede afectar a múltiples objetivos.

También se deberían tener en cuenta los controles existentes, así como su eficacia y su eficiencia.

La forma de expresar las consecuencias y la probabilidad, así como la manera en que éstas se combinan para determinar un nivel de riesgo, debería corresponder al tipo de riesgo, a la información disponible y al objetivo para el que se utiliza el resultado de la apreciación del riesgo. Todos estos datos deberían ser coherentes con los criterios de riesgo. También es importante considerar la interdependencia de los diferentes riesgos y de sus fuentes.

La confianza en la determinación del nivel de riesgo y su sensibilidad a las condiciones previas y a las hipótesis se debería considerar en el análisis y comunicar de manera eficaz a las personas que han de tomar decisiones y, cuando corresponda, a otras partes interesadas. Factores tales como las diferencias de opinión entre expertos, la incertidumbre, la disponibilidad, la calidad, la cantidad y la validez de la pertinencia de la información, o las limitaciones respecto a modelos establecidos se deberían indicar y pueden resaltarse".

Estimación de las consecuencias:

- "Los impactos estimados se pueden expresar en términos cualitativos cuantitativos.
- El valor de impacto por lo general depende del valor y la importancia de los activos afectados por el escenario de incidentes.
- Esta estimación se puede obtener mediante un análisis de impacto en el negocio (BIA)".

Evaluación de incidentes

"Después de identificar las hipótesis de incidentes correspondientes y la estimación de sus consecuencias, se debe estimar la probabilidad de ocurrencia de cada escenario. Es necesario estimar la probabilidad realista

de un incidente de seguridad de un activo a la vista de las amenazas dominantes y las vulnerabilidades, los impactos asociados a los activos y los controles de seguridad ya implementadas para proteger los activos".

La probabilidad se define como el "grado de probabilidad para que ocurra un evento", señalando que la probabilidad es en general (y en especial en la norma ISO 3534-1) definida como "un número real en el intervalo de 0 a 1, asociado a un evento al azar" y tomando nota de que "se puede utilizar la frecuencia más que la probabilidad para describir el riesgo", y que "el grado de creencia de la probabilidad se puede elegir una clase o como un rango, tal como rara o improbable / moderada / probable / casi segura, o increíble / improbable / probable / ocasional / probable / frecuente".

Determinación del nivel de riesgos

Una vez que se establece "un registro de todas las fuentes de riesgo en la forma de una lista genérica de posibles incidentes, los riesgos asociados con cada incidente deben ser evaluados, lo que lleva a un inventario jerárquico de los posibles escenarios de incidentes.

La estimación del riesgo asignará entonces un valor cualitativo o cuantitativo a la probabilidad de un escenario de incidentes y sus consecuencias".

Evaluación de riesgos

Consiste en "comparar el nivel estimado de riesgos contra los criterios de evaluación de riesgos y los criterios de aceptación de riesgos, y luego priorizarlos".

La evaluación de riesgos es necesaria antes de tomar una decisión sobre las posibles opciones para el tratamiento de riesgos.

La naturaleza de las “decisiones relativas a la evaluación del riesgo y los criterios de evaluación de riesgos que se utilizarán para tomar esas decisiones, se habrán decidido al establecer el contexto.

Estas decisiones y el contexto deberían ser revisados en más detalle en este momento cuando más se sabe sobre los riesgos particulares identificados.

Para evaluar los riesgos, las organizaciones deberían comparar los niveles de riesgo con los criterios de evaluación de riesgos definidos en el establecimiento del contexto.

Los criterios de evaluación de riesgos utilizados para tomar decisiones deberían ser compatibles con el contexto para la gestión de riesgos externo e interno y deben tener en cuenta los objetivos de la organización y las opiniones de las partes interesadas, etc. Las decisiones tomadas en la actividad de la evaluación del riesgo se basan principalmente en el nivel de riesgo aceptable. Sin embargo, las consecuencias, la posibilidad y el grado de confianza en la identificación y el análisis de riesgos deben también considerarse”. La agregación de múltiples riesgos bajos o medios puede resultar en mucho mayor riesgo global y la necesidad de ser abordados en consecuencia.

Priorización de Riesgos

Una vez que se establece de una manera jerárquica el inventario de los escenarios de posibles incidentes, es necesario definir criterios para una clasificación simple de los riesgos para su priorización.

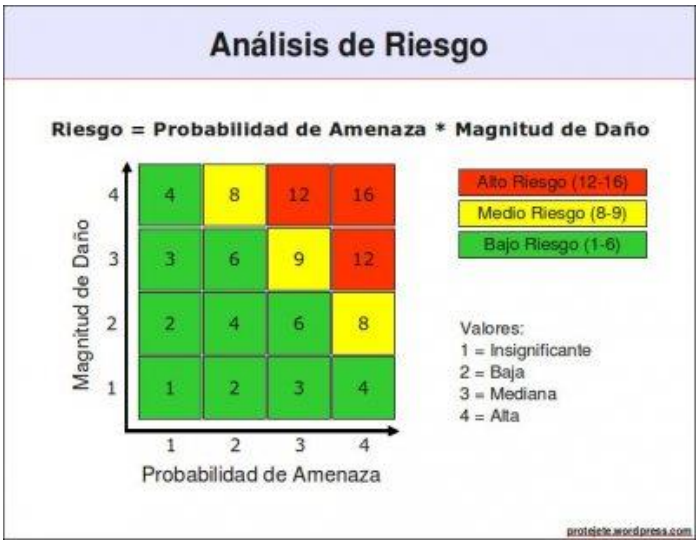


Figura 6. Matriz de riego.

El riesgo cero no existe, pero es posible definir un umbral por debajo del cual es aceptable no hacer nada para reducir el riesgo.

En el otro extremo de la escala, hay un umbral más allá del cual el riesgo es inaceptable, entonces se debe hacer todo lo posible para eliminar su fuente, o reducir los riesgos de forma fiable. El riesgo de un desastre nuclear es un claro ejemplo de riesgo inaceptable, que llevó a algunos opositores a la demanda de una prohibición total del uso de la energía nuclear, cualquiera que sea el costo de las alternativas para la empresa.

Es evidente que el umbral de aceptación de riesgos y la tolerancia reflejan la actitud de la organización y de la sociedad en relación con el riesgo. Una vez establecido, no se debe cambiar.

El proceso sistemático descrito anteriormente, sin aportar soluciones prefabricadas, identifica el debate y aclara las elecciones que habrán de formularse. Este proceso permite, una vez hechas las elecciones, comunicarse de manera efectiva y mejorar la coherencia interna de las acciones de la compañía en relación con sus opciones fundamentales.

Se pueden asignar zonas definidas en cualquier matriz de riesgo para clasificar a cada incidente genérico potencial, y definir el tipo de medidas requeridas en cada caso.

1.8.3 Minimizar los riesgos de seguridad

Domínguez (2007) Afirma que **"**La liquidez es el grado en que una empresa puede hacer frente a sus obligaciones corrientes, en la medida de su liquidez a corto plazo.

La liquidez implica, por tanto, la capacidad puntual de convertir los activos en líquidos o de obtener disponible para hacer frente a los vencimientos a corto plazo. Algunos autores se refieren a este concepto de liquidez con el término de solvencia, definiéndola como la capacidad que posee una empresa para hacer frente a sus compromisos de pago. Podemos definir varios grados de solvencia.

El primer lugar tenemos la solvencia final, expresada como la diferencia existente entre el activo total y el pasivo exigible. Recibe este nombre de solvencia final porque se sitúa en una perspectiva que podemos considerar última: La posible liquidación de una empresa.

Con esta solvencia final medimos si el valor de los bienes de activo respalda la totalidad de las deudas contraídas por la empresa. Recordemos que esta medida es la que suele figurar en las notas o resúmenes sobre suspensiones" (p. 49).

1.9. Definición de términos básicos

Activos de información. Como menciona Dutton, J. (2016), Un activo de información "es cualquier pieza o colección de información almacenada en el patrimonio de la

organización, definida y administrada como una sola unidad para que podamos entenderla, compartirla y protegerla eficazmente y obtener el máximo valor de ella. Es algo que no podemos reemplazar sin costo, tiempo, habilidad y recursos".

Amenaza. "Causa potencial de un incidente inesperado, que podría resultar e daño a un sistema o a la organización" (ISO/IEC 27000: 2014).

Confidencialidad. "Propiedad de la limitación o restricción de la información a individuos, entidades o procesos no autorizados" (ISO/IEC 27000: 2014).

Control. "Medida que modifica el riesgo. Los controles incluyen cualquier proceso, política, dispositivo, práctica u otras acciones que modifiquen el riesgo" (ISO/IEC 27000:2018).

Controles de Seguridad de Gestión. "Son aquellos controles procedimentales, administrativos y/o documentales que establecen las reglas a seguir para la protección del entorno" (ACOSTA RODRÍGUEZ, 2018).

Disponibilidad. "Propiedad de la información de ser accesible o usable cuando sea demandada por una entidad autorizada" (ISO/IEC 27000: 2014).

Evaluación de riesgos. "Proceso global de identificación, análisis y estimación de riesgos" (ISO/IEC 27000:2018).

Estimación de riesgos. "Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables" (ISO/IEC 27000:2018).

Información. La información "es un activo que, al igual que otros activos de negocio importantes, es esencial para la misión de una organización y por lo tanto necesita ser protegida de forma adecuada. La información puede ser almacenada en muchas

formas, incluyendo: forma digital (por ejemplo: archivos de datos almacenados en medios electrónicos u ópticos), forma material (por ejemplo: en el papel), así como la información no estructurada en la forma de conocimiento de los empleados" (ISO/IEC 27000: 2014).

Integridad. "Propiedad de [la información de] exactitud y completitud" (ISO/IEC 27000: 2014).

ISO/IEC 27001:2013 Tecnología de Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de Información. Requerimientos. "Es la última versión del estándar que establece los requisitos para los sistemas de gestión de seguridad de información. Define los requerimientos necesarios para el adecuado establecimiento, implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI)" (ISO/IEC 27000: 2014).

Objetivo de control. "Declaración que describe lo que se debe lograr como resultado de la implementación de controles" (ISO/IEC 27000:2018).

Riesgo. "Efecto que genera incertidumbre sobre el logro de los objetivos de seguridad de información" (ISO/IEC 27000: 2014).

Sistema de Gestión de Seguridad de Información. Un Sistema de Gestión de Seguridad de la Información (SGSI) "consiste en políticas, procedimientos, directrices, recursos asociados y actividades, gestionadas colectivamente por una organización, en la búsqueda de la protección de sus activos de información" (ISO/IEC 27000: 2014).

Seguridad de información. La seguridad de información "incluye tres dimensiones principales: la confidencialidad, disponibilidad e integridad. Consiste en la aplicación y gestión de medidas de seguridad apropiadas, lo que implica la consideración de una

amplia gama de amenazas, con el fin de garantizar el éxito y continuidad del negocio, de manera sostenida, y la minimización de los impactos de los incidentes de seguridad de la información" (ISO/IEC 27000: 2014).

Sistema de gestión. "Utiliza un marco de recursos para lograr los objetivos de una organización. El sistema de gestión incluye la estructura organizativa, políticas, planificación de actividades, responsabilidades, prácticas, procedimientos, procesos y recursos". (ISO/IEC 27000: 2014).

Vulnerabilidad. "Debilidad de un activo o control que puede ser explotada por una o más amenazas" (ISO/IEC 27000: 2014).

II. METODO

2.1. Tipo y diseño de la investigación

Tipo de investigación

La presente tesis, es aplicada.

Según los autores Hernández (2006), “plantean respecto a este estudio que puede identificarse como aquel tipo de investigación que tiene fines prácticos en el sentido de solucionar problemas detectados en un área del conocimiento. Está ligada a la aparición de necesidades o problemas concretos y al deseo del investigador de ofrecer solución a estos”. (pág. 128).

Diseño de la investigación

- **No Experimental**

Para el diseño de la investigación se ha considerado una investigación descriptiva y de corte transversal, es decir, consiste en que el investigador obtiene los datos o información en un solo momento de la investigación. Estos hechos son medidos y descritos. Según manual de la Universidad Jaime Bausate y Meza “el Diseño no experimental consiste en no manipular variables, básicamente se observa un hecho o fenómeno tal y como se presentan en la realidad con la intención de analizarlo”.

Nivel de la investigación

Esta investigación fue de nivel descriptivo correlacional.

Según Hernández Sampieri (2014). “Los estudios descriptivos permiten detallar situaciones y eventos, es decir cómo es y cómo se manifiesta determinado fenómeno y busca especificar propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis”. (p. 125).

Es correlacional, según Hernández Sampieri (2014. "Tiene como finalidad conocer la relación o grado de asociación que exista entre dos o más conceptos, categorías o variables en una muestra o contexto particular" (p. 93).

Enfoque de la investigación

El enfoque del de la tesis fue cuantitativo ya que según la definición de Hernández: "Utiliza la recolección y el análisis de datos para contestar preguntas de investigación y probar hipótesis establecidas previamente y confía en la medición numérica, el conteo y frecuentemente en el uso de la estadística para establecer con exactitud patrones de comportamiento de una población" (Hernández Etal, 2003; p.5).

2.2. Población y muestra

- ✓ **Población**

  La población del estudio está conformada por todas las personas que laboran en la empresa Quantify Agency, que son un total de 10 personas, siendo de las áreas de Gerencia, Contabilidad, Administración y los especialistas.

- ✓ **Muestra**

  Para la muestra que se tomara el 100% de la población que son (10 personas).

2.3. Técnicas para la recolección de datos

- ✓ **Técnicas**

  Las técnicas que se utilizaran para el análisis y verificación del proyecto de tesis son las siguientes:

  - **Encuestas:**

    Según (Palella Stracuzzy & Martins Pestana, Metodologia De La Investigacion Cuantitativa, 2017) la encuesta "es una técnica destinada a obtener datos de varias personas cuyas opiniones interesan al investigador.

Para ello, a diferencia de la entrevista, se utiliza un listado de preguntas escritas que se entregan a los sujetos quienes, en forma anónima, las responden por escrito".

- **Entrevistas:**

  Según (Palella Stracuzzy & Martins Pestana, Metodologia De La Investigacion Cuantitativa, 2017) es una técnica "que permite obtener datos mediante un diálogo que se realiza entre dos personas cara a cara: el investigador y del entrevistado; la intención es obtener información que posea este último".

✓ **Instrumentos**

Cuestionarios:

Según Hernández Sampieri (1997), el cuestionario "es tal vez el más utilizado para la recolección de datos; este consiste en un conjunto de preguntas respecto a una o más variables a medir".

2.4. Validez y confiabilidad de instrumentos

Validez del instrumento:

Para la validación de la encuesta, se utilizará el coeficiente Kappa:

$$K = Po - Pe / (1-Pe)$$

Donde:

Pe = Porcentaje esperado por puro azar.

Po = Porcentaje observado.

Para la validación del contenido se recurrió al Juicio de tres expertos.

Tabla 2.
Juicio de Expertos.

N°	Expertos	Promedio de ponderación
1	Ing. Karina Saravia Aguilar	85 %
2	Mg, Acosta Salvador Sabina Gualvertina	86 %
3	Mg. Gonzales Calderón José Ramos	86 %

Ponderado	86%

Fuente: Elaboración propia.

Criterio de confiabilidad de instrumento

La confiabilidad de la Encuesta será medida usando el coeficiente Alpha de Cronbach.

Tabla 3.
Prueba de confiabilidad del instrumento.

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,922	30

Fuente: Elaboración propia.

De los resultados Alpha de Cronbach con valor de 0,922, por lo que se afirma que el instrumento posee un nivel excelente de fiabilidad, lo cual indica que el cuestionario sobre el SGSI y el Riesgo de seguridad tiene un alto grado de consistencia interna y repetitividad, siendo confiable su aplicación.

Según lo mencionado por (Ñaupas, Mejia, Novoa, & Villagomez, 2014, pág 217) "un instrumento es fiable cuando las mediciones no varían significativamente ni en tiempo ni en aplicación a diferentes personas. La confiabilidad es la prueba que genera confianza cuando, al aplicarse en condiciones iguales o similares los resultados son siempre los mismos.

Se sugieren los siguientes criterios para evaluar los coeficientes de alfa de Cronbach":

- "Coeficiente alfa > 0.9 es excelente.
- Coeficiente alfa > 0.8 es bueno.
- Coeficiente alfa > 0.7 es aceptable.

- Coeficiente alfa > 0.6 es cuestionable.
- Coeficiente alfa > 0.5 es pobre.
- Coeficiente alfa < 0.5 es inaceptable" (Ñaupas, Mejia, Novoa, & Villagomez, 2014, pág 217).

2.5. Procesamiento y análisis de datos

Para el estudio se utilizó la técnica de la encuesta y entrevista que tuvo como instrumento el cuestionario, dirigida a la empresa Quantify Agency que resulten seleccionados en la muestra del estudio.

Los resultados obtenidos fueron procesados y tabulados utilizando el Microsoft Excel y para efectuar el análisis se procedió a utilizar la herramienta de software IBM SPSS 22. En dicho análisis se relacionó con las variables dependientes.

2.6. Aspectos éticos

La presente investigación tuvo en consideración los siguientes aspectos éticos:

- Fiabilidad de la información obtenida de la empresa.
- Veracidad de los resultados obtenidos.
- Respeto por los resultados obtenidos en el desarrollo de la investigación, sin alterar ninguno de ellos.
- Respeto a la propiedad intelectual, citándose a los autores de los textos de la documentación comprendida en la bibliografía utilizados en la investigación.

III. RESULTADOS

3.1. Resultados descriptivos

Para determinar en qué medida el modelo del sistema de gestión de seguridad de la información se relaciona con la mitigación de riesgos de información en el área de sistemas de la empresa Quantify Agency y de sus respectivas dimensiones se realizó con los puntajes promedios recopilados a través de la encuesta de la investigación realizada y el criterio tomado es el siguiente:

Tabla 4.
Niveles del sistema de gestión de seguridad de la información para minimizar los riesgos de información

Nivel y rango	**Malo**	**Regular**	**Bueno**
Sistema de gestión de seguridad de la información	**23 - 37**	**38- 51**	**52- 60**
Requisitos del SGSI	4 - 9	10 - 15	15 - 20
Análisis de brechas	4 - 9	10 - 15	15 - 20
Controles de seguridad	4 - 9	10 - 15	15 - 20
Riesgos de seguridad	**23 - 37**	**38- 51**	**52- 60**
Identificación de riesgos	4 - 9	10 - 15	15 - 20
Análisis de riesgos	4 - 9	10 - 15	15 - 20
Evaluación de riesgos	4 - 9	10 - 15	15 - 20

Fuente: Elaboración propia.

Tabla 5.

Descriptivos de la variable Sistema de gestión de seguridad de la información.

Sistema de Gestión de Seguridad de la Información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	2	20,0	20,0	20,0
	Bueno	8	80,0	80,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico de barras:

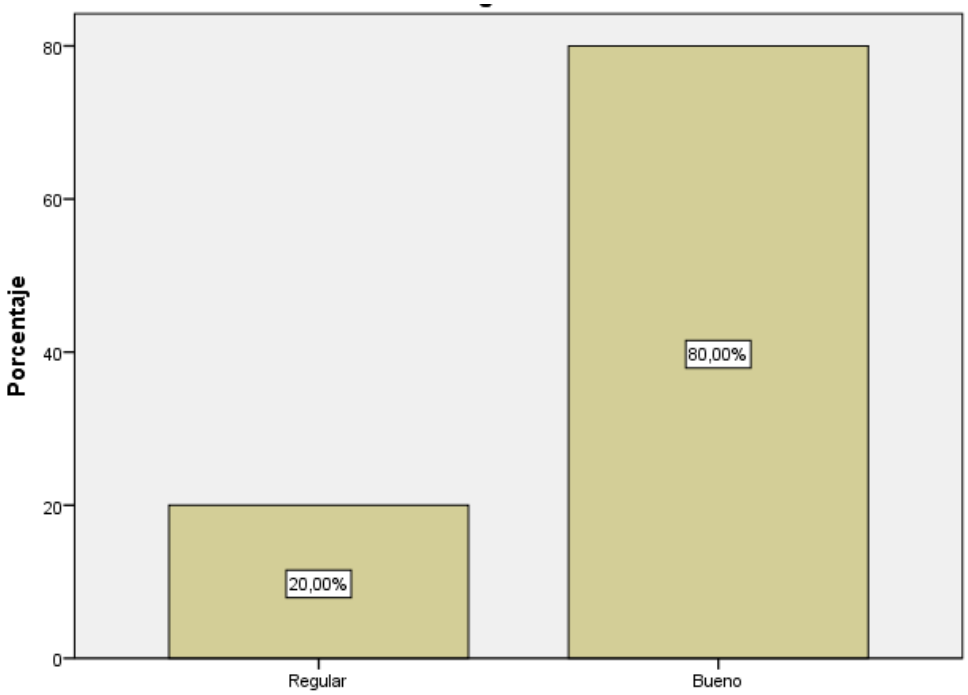


Figura 7. Descriptivos de la variable de Sistema de gestión de seguridad de la información.

.

Nota: Se observa que del total de usuarios encuestados califica que el 80% Bueno, 20% Regular, los. nivel del Sistema de gestión de seguridad de la información.

Tabla 6.

Descriptivos de la dimensión de requisitos del SGSI

Requisitos del SGSI

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bueno	10	100,0	100,0	100,0

Fuente: Elaboración propia.

Gráfico de barras:

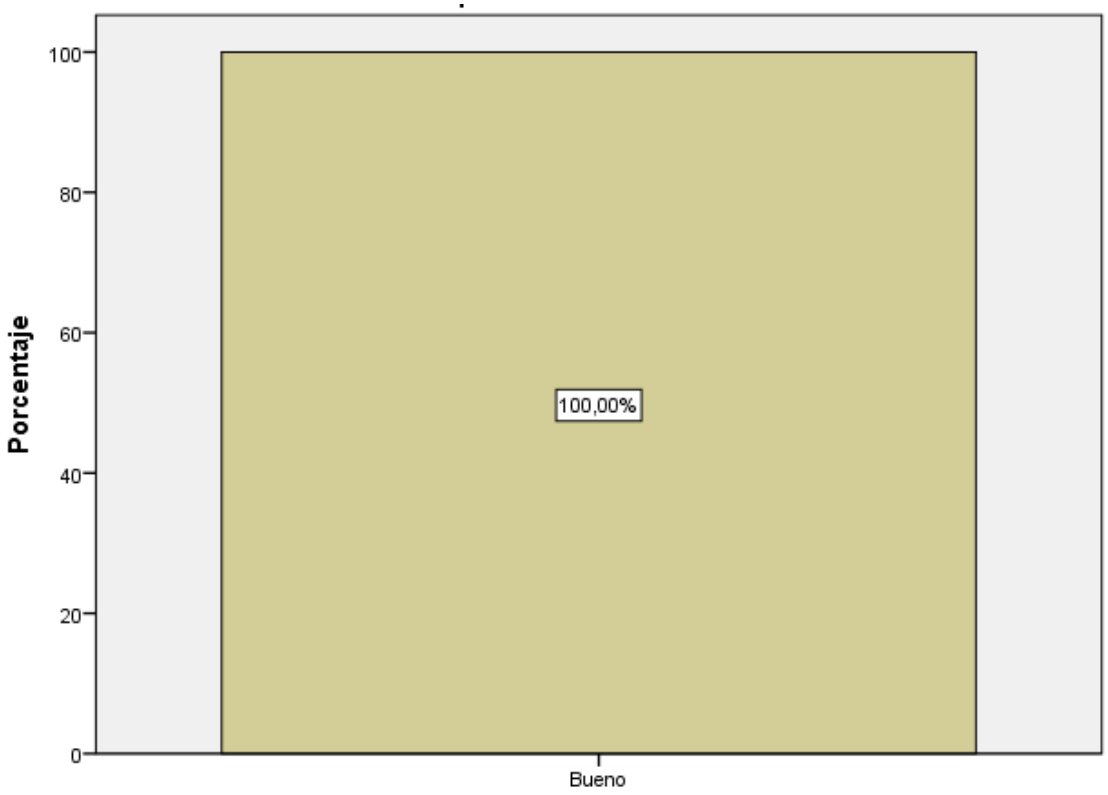


Figura 8. Descriptivo del nivel de requisitos del SGSI.

Nota: Se puede observar que de los usuarios encuestados considera que el 100% es Bueno en los niveles requisitos del SGSI.

Tabla 7.
Descriptivo de la dimensión de análisis de brechas.

Análisis de brechas

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	6	60,0	60,0	60,(
	Bueno	4	40,0	40,0	100,(
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico de barras:

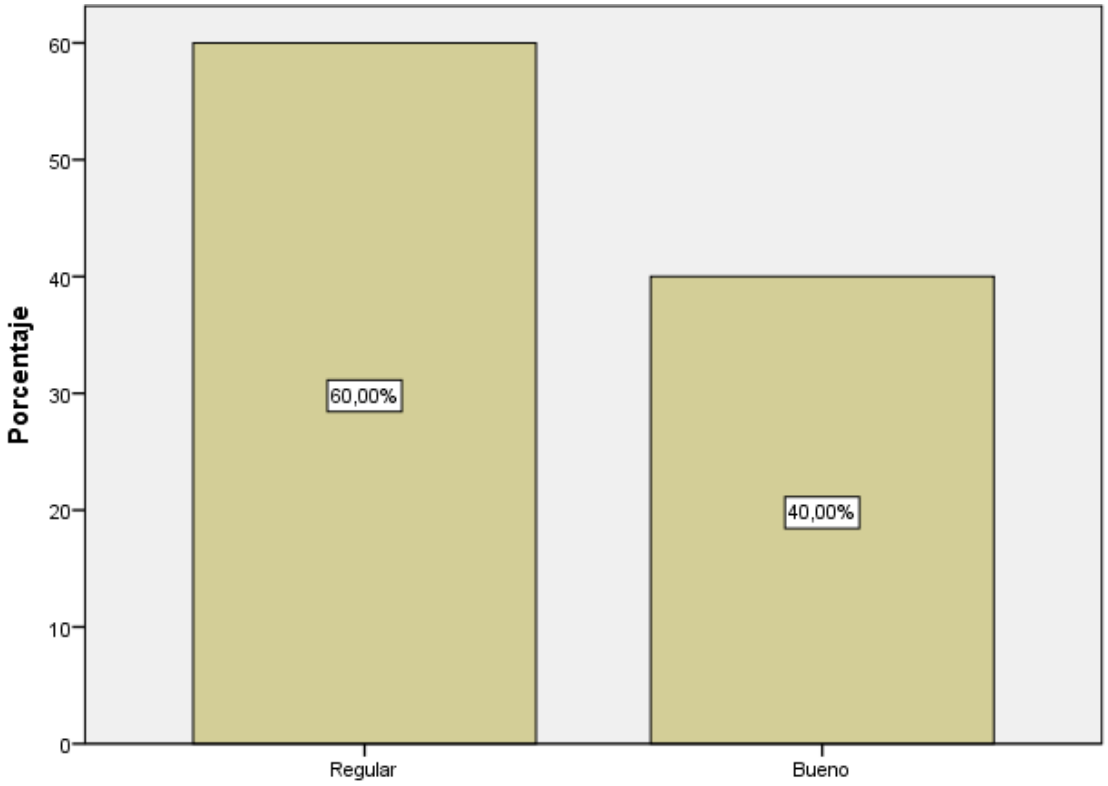


Figura 9. Descriptivo de los niveles de análisis de brechas.

Nota: Se observa que del total de usuarios encuestados consideran que el 60% es Regular y el 40% Bueno los niveles del análisis de brechas.

Tabla 8.
Descriptivo de la dimensión controles de seguridad.

Controles de seguridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	2	20,0	20,0	20
	Bueno	8	80,0	80,0	100
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico de barras:

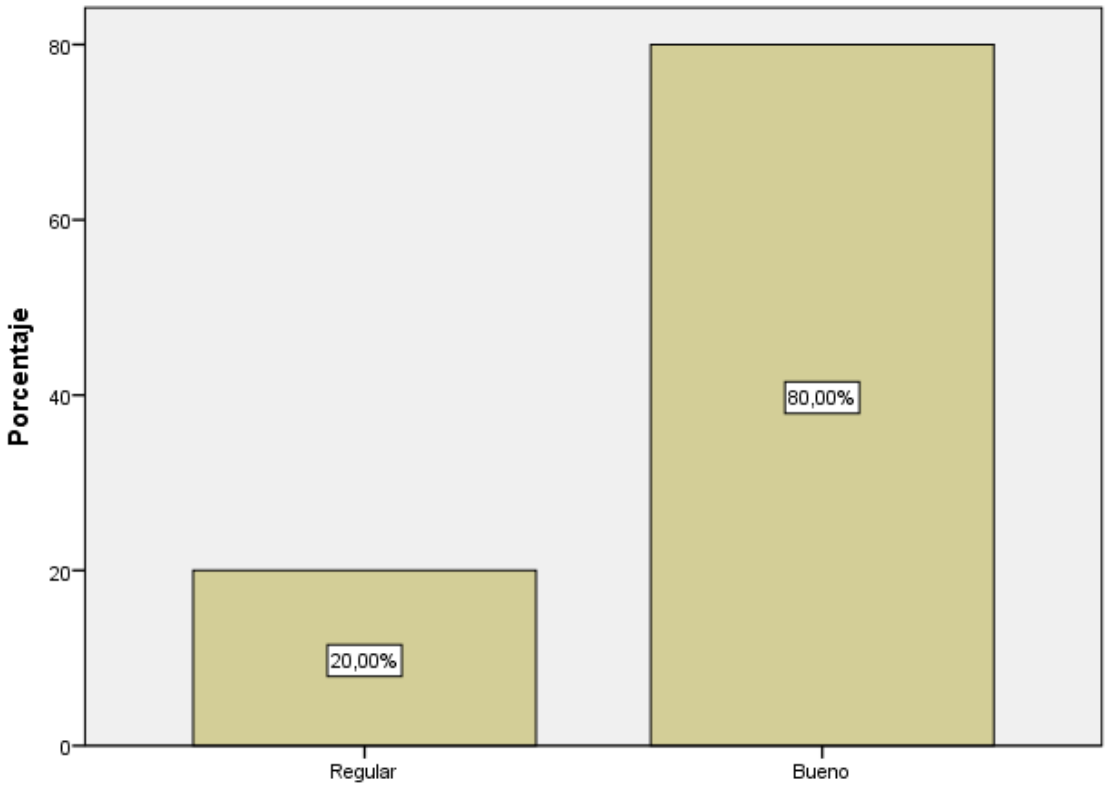


Figura 10. Descriptivo de los niveles de controles de seguridad.

Nota: Se observa que del total de usuarios encuestados consideran que el 80% es Bueno y el 20% Regular los niveles de controles de seguridad.

Tabla 9.
Descriptivo de la variable riesgos de seguridad.

Riesgos de seguridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	9	90,0	90,0	90,0
	Bueno	1	10,0	10,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico de barras:

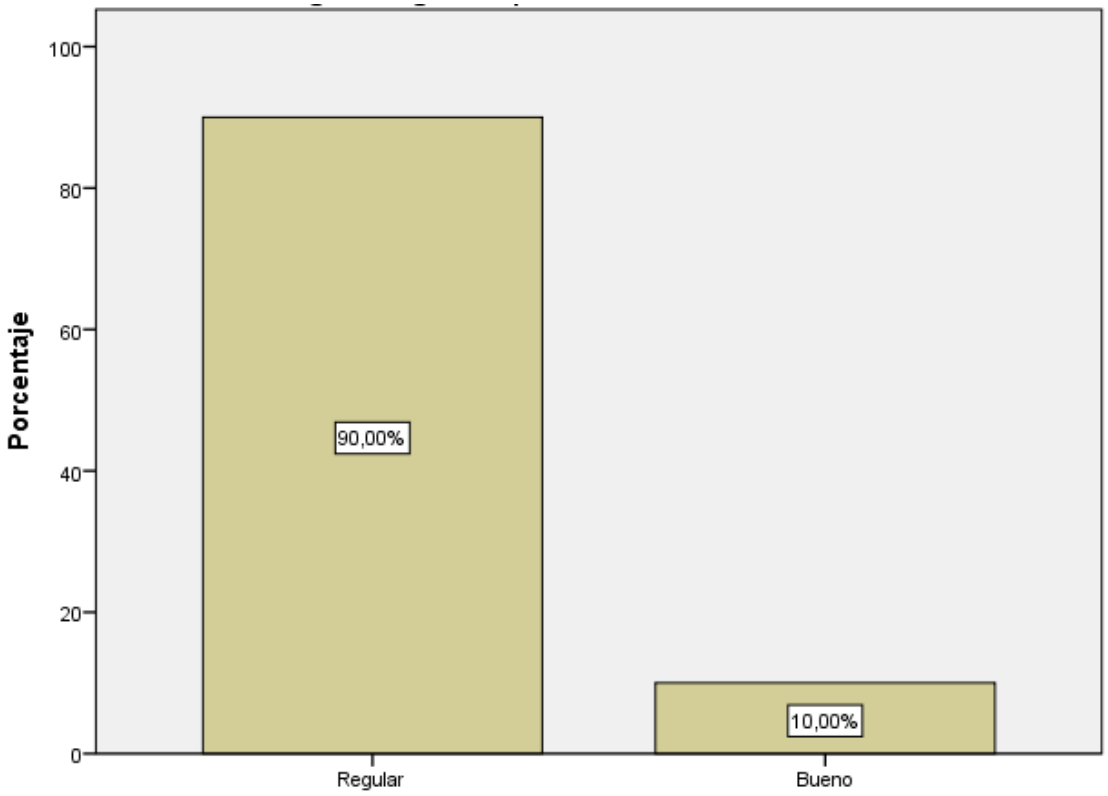


Figura 11. Descriptivo de la variable riesgos de seguridad.

Nota: Se observa que del total de usuarios encuestados considera que el 90% es Regular y el 10% es Bueno de los niveles de la variable minimizar riesgos de seguridad.

Tabla 10.
Descriptivo de la dimensión de identificación de riesgos.

Identificación de riesgos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	7	70,0	70,0	70,
	Bueno	3	30,0	30,0	100,
	Total	10	100,0	100,0	

Fuente: Elaboración propia

Gráfico de barras:

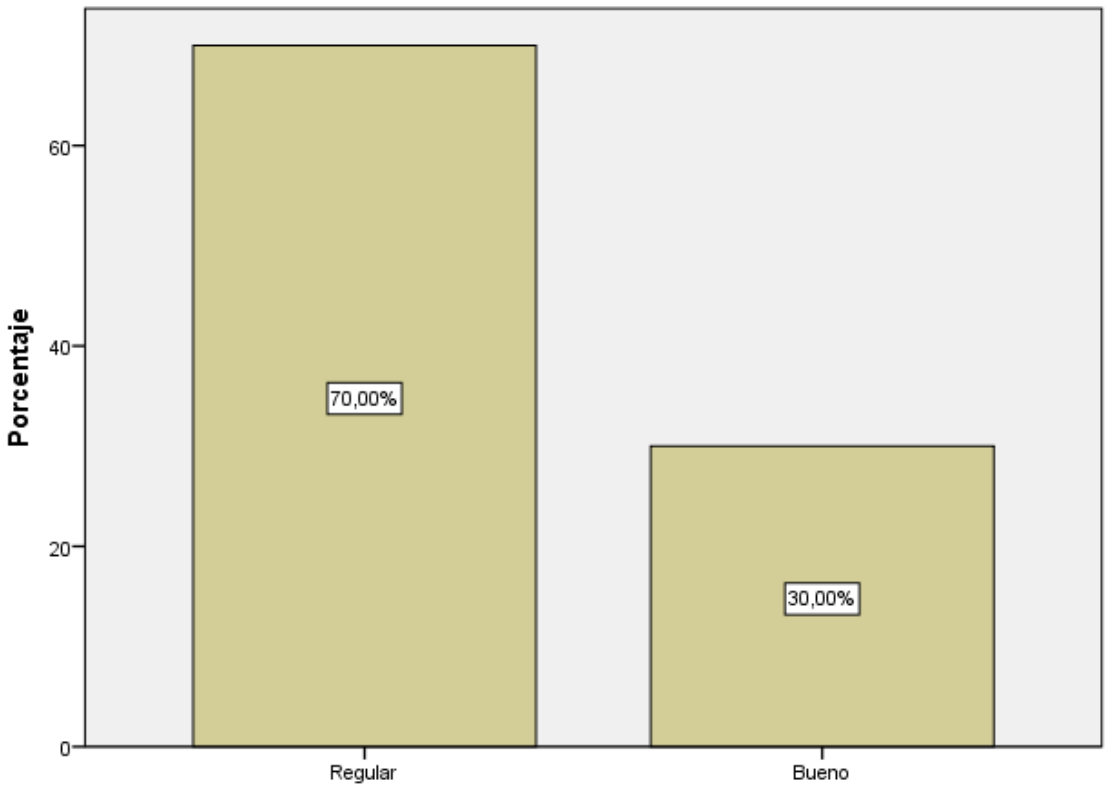


Figura 12. Descriptivo de los niveles de identificación de riesgos.

Nota: Se observa que del total de usuarios encuestados consideran que el 70% es Regular y el 30% es Bueno los niveles de identificación de riegos.

Tabla 11.
Descriptivo de la dimensión de análisis de riesgos.

Análisis riesgos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	3	30,0	30,0	
	Bueno	7	70,0	70,0	1
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico de barras:

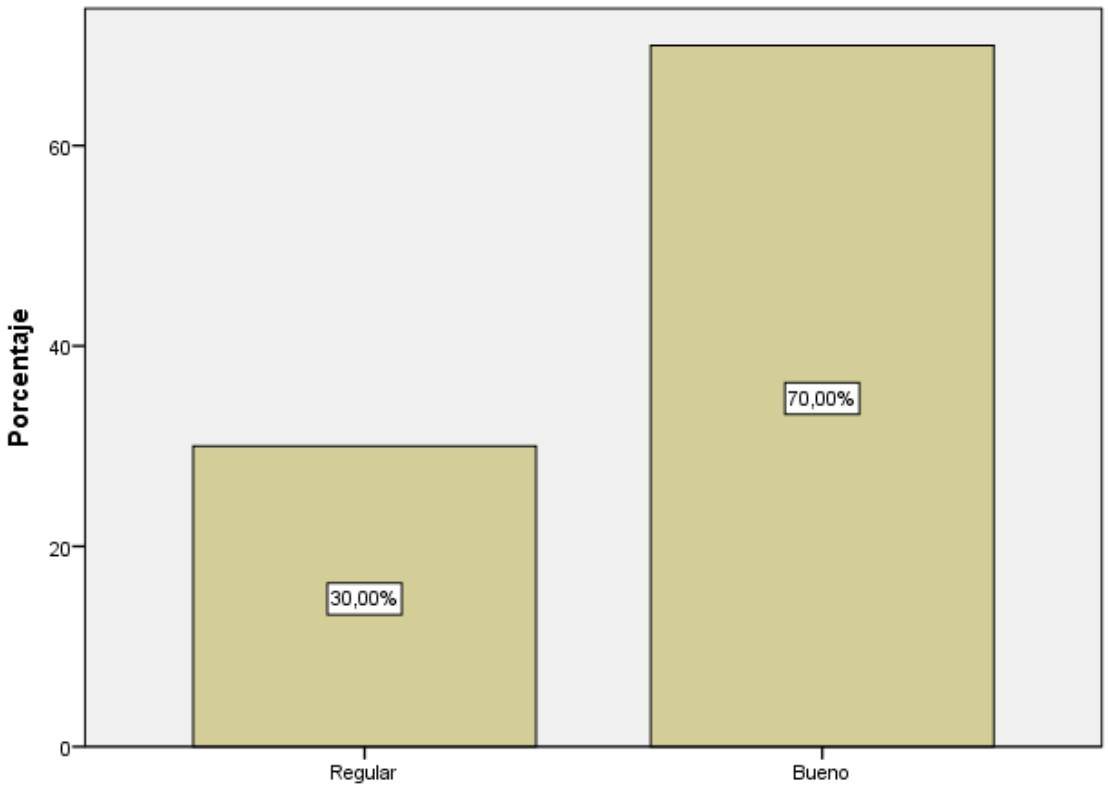


Figura 13. Descriptivo de la dimensión de análisis de riesgos.

Nota: Se observa que del total de usuarios encuestados considera que el 70% es Bueno y el 30% es Regular el nivel de análisis riesgos.

Tabla 12.
Descriptivo de la dimensión de la evaluación de riesgos.

Evaluación riesgos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	9	90,0	90,0	9(
	Bueno	1	10,0	10,0	10(
	Total	10	100,0	100,0	

Fuente: Elaboración propia.

Gráfico de barras:

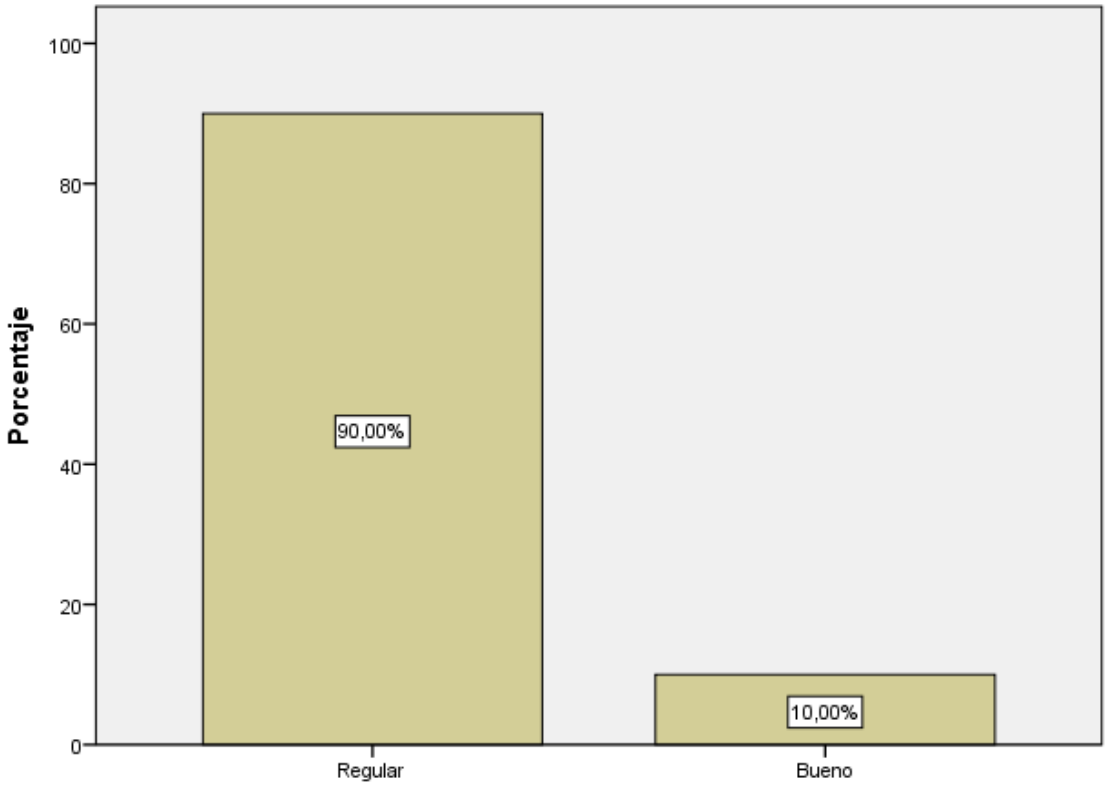


Figura 14. Descriptivo de los niveles de evaluación de riesgos.

Nota: Se observa que del total de usuarios encuestados considera que el 90% es Regular y el 10% es Bueno el nivel de evaluación de riesgos.

3.2. Prueba de normalidad

La prueba de normalidad aplicada fue con el método estadístico de Shapiro-Wilk por que el tamaño de la muestra es menor a 50.

Hipótesis:

H0: Los datos provienen de una distribución normal.

H1: Los datos no provienen de una distribución normal.

Decisión: Es significativa si $p > \alpha$, entonces aceptamos H0. ($\alpha = 0.05$).

Tabla 13.
Prueba de Shapiro-Wilk.

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
SGSI	,207	10	,200*	,921	10	,365
Riesgos_seduridad	,207	10	,200*	,921	10	,365

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia

Donde:

- Se observa la significancia de la variable "Sistema de Gestión de Seguridad de la Información" es de 0,365 cifra mayor a 0.05, se acepta la H0, por lo tanto, se infiere que los datos provienen de una distribución normal, por lo que se utilizará para la contrastación de las hipótesis el coeficiente de correlación de Pearson.
- Se observa la significancia de la variable "Riesgos de seguridad" es de 0,365 cifra mayor 0.05, se acepta la H0, por lo tanto, se infiere que los datos siguen una distribución normal, por lo que se utilizará para la contrastación de las hipótesis el coeficiente de correlación de Pearson.

3.3. Contrastación de hipótesis

Pruebas de hipótesis para la correlación de dos variables:

Pruebas de hipótesis:

$$\begin{cases} H_0: \text{Entre las variables } X \text{ e } Y \text{ No existe una relación significativa.} \\ H_1: \text{Entre las variables } X \text{ e } Y \text{ existe una relación significativa.} \end{cases}$$

Coeficientes de correlación por rangos de Pearson:

Para la prueba de hipótesis de la presente investigación se utilizó el coeficiente de correlación de Pearson ya que los datos presentaban una distribución normal.

La forma de calcular el coeficiente de correlación de Pearson entre dos variables es la siguiente:

$$r = \frac{S_{xy}}{S_x S_y}$$

Donde:

S_xy: Covarianza de X e Y.

S_x: Desviación estándar de X.

S_y: Desviación estándar de Y.

Hipótesis:

H0: p = 0 (Entre las variables X y Y no existe una relación significativa).

H1: p ≠ 0 (Entre las variables X y Y existe una relación significativa).

Decisión: Es significativa si p< α, entonces se rechaza H0. (α = 0.05).

Contrastación de hipótesis general

H0: No Existe relación entre el modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 para minimizar los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.

H1: Existe relación entre el modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 para minimizar los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.

Tabla 14.
Contrastación de hipótesis general.

Correlaciones

		SGSI	Riesgos_seguridad
SGSI	Correlación de Pearson	1	1,000**
	Sig. (bilateral)		,000
	N	10	10
Riesgos_seguridad	Correlación de Pearson	1,000**	1
	Sig. (bilateral)	,000	
	N	10	10

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Elaboración propia.

Se observa una correlación perfecta rho Spearman = 0.1, donde el P = 0.000 < 0.05, se rechaza la H0, por lo tanto, Si existe correlación perfecta entre el modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 para minimizar los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.

Contrastación de hipótesis específica 1

H0: No existe relación entre el modelo del sistema de gestión de seguridad de la información y la identificación de riesgos de la información en el área de sistemas de la empresa Quantify Agency.

H1: Existe relación entre el modelo del sistema de gestión de seguridad de la información y la identificación de riesgos de la información en el área de sistemas de la empresa Quantify Agency.

Tabla 15.
Contratación de hipótesis específica 1.

Correlaciones

		SGSI	Identificación_riesgos
SGSI	Correlación de Pearson	1	,807**
	Sig. (bilateral)		,005
	N	10	10
Identificación_riesgos	Correlación de Pearson	,807**	1
	Sig. (bilateral)	,005	
	N	10	10

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Elaboración propia.

Se observa una correlación alta rho Spearman = 0.080 , y el P = 0,005 < 0.05, se rechaza la H0, por lo tanto, Si existe correlación alta entre el sistema de gestión de seguridad de la información y la identificación de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.

Contrastación de hipótesis específica 2

H0: No Existe relación entre el sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y el análisis de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.

H1: Existe relación entre el sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y el análisis de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.

Tabla 16.
Contrastación de hipótesis específica 2.

Correlaciones

		SGSI	Análisis_riesgos
SGSI	Correlación de Pearson	1	,700*
	Sig. (bilateral)		,024
	N	10	10
Análisis_riesgos	Correlación de Pearson	,700*	1
	Sig. (bilateral)	,024	
	N	10	10

*. La correlación es significativa en el nivel 0,05 (bilateral).

Fuente: Elaboración propia.

Se observa que la correlación alta rho Spearman = 0.070, además el P=0.024 < 0.05, se rechaza la H0, por lo tanto, se puede inferir que si existe relación alta entre el sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y el análisis de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.

Contrastación de hipótesis específica 3

H0: No Existe relación del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y la evaluación de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.

H1: Existe relación del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y la evaluación de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.

Tabla 17.
Contrastación de hipótesis específica 3.

Correlaciones

		SGSI	Evaluación_riesgos
SGSI	Correlación de Pearson	1	,715*
	Sig. (bilateral)		,020
	N	10	10
Evaluación_riesgos	Correlación de Pearson	,715*	1
	Sig. (bilateral)	,020	
	N	10	10

*. La correlación es significativa en el nivel 0,05 (bilateral).

Fuente: Elaboración propia.

Se observa que la correlación alta rho Spearman = 0.071, además el P=0.020 < 0.05, se rechaza la H0, por lo tanto, Si existe relación alta del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y la evaluación de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.

IV. DISCUSIÓN

El objetivo general de esta investigación fue “determinar la relación del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y la minimización de los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency”, donde se ha podido observar que existe una correlación perfecta rho Spearman = 0.1 , además el P = 0.000 < 0.05, se rechaza la H0, por lo tanto, Existe relación perfecta entre el sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y la minimización de los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency, así como el 80%. que está de acuerdo con el sistema de gestión de seguridad de la información se relaciona con la mitigación de riesgos de la información en el área de sistemas de la empresa Quantify Agency. Para (Porras, 2019) quien desarrolló una tesis titulada “Sistema de gestión de seguridad de la información para la gestión de riesgos en activos de información”. Cuyo objetivo general de la investigación fue: “Determinar la influencia de la implementación del Sistema de Gestión de Seguridad de la Información en la gestión de riegos en activos de información en la Empresa de BPO Contac Center Digitex, Lima”. El resultado fue que la implementación del SGSI basado en controles de seguridad mejoró la madurez de la gestión de riesgos en los activos de información y el valor medio pasó de 3.65 a 5.22, se concluye que la implementación del SGSI genera resultados favorables en la gestión de Riesgos de los Activos de Información. Donde se puede corroborar si se aplica el SGSI, se reduce los riesgos en los activos de información.

Además de acuerdo con (Cruz & Fukusaki, 2017), en su tesis titulada “Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la clínica Medcam Perú SAC**”**. Cuyo

objetivo general de la investigación fue: **“**mitigar los riesgos a los que está expuesto los activos de información de la clínica MEDCAM Perú S.A.C.**”**. Obtuvo como resultado implementar un SGSI con el cual se logró minimizar los riesgos de amenazas y vulnerabilidades en los activos de información de MEDCAM Perú S.A.C. y de esta manera, lograr la confidencialidad, disponibilidad e integridad de la información. Donde concluye que el beneficio más importante fue asegurar los activos de información y con ello el cumplimiento de los objetivos de la empresa; así como que cada SGSI debe estar de acuerdo con el tamaño y madurez de los procesos de negocio.

V. CONCLUSIONES

A continuación, se describen los principales resultados obtenidos de la investigación:

1. Se concluye que existe una correlación perfecta entre el modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y minimizar los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency. Lo cual expresa que el modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 favorece en reducir los riesgos de seguridad.
2. Se concluye que existe una correlación alta entre el modelo del sistema de gestión de seguridad de la información y la identificación de riesgos de la información en el área de sistemas de la empresa Quantify Agency. Que expresa que el modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 favorece en la identificación de riesgos de seguridad.
3. Existe una correlación alta entre el modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y el análisis de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency, que expresa que el modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 favorece el análisis de riesgos de seguridad.
4. Existe una correlación alta entre el modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y la evaluación de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency. Que expresa que el modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 favorece la evaluación de riesgos de seguridad.

VI. RECOMENDACIONES

1. Recomendar desarrollar el modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 para minimizar los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.

2. Recomendar la implementación del modelo del sistema de gestión de seguridad de la información para la identificación de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.

3. Recomendar la implementación y mantenimiento del modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 en el análisis de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.
4. Recomendar la implementación y mantenimiento del modelo del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 para la evaluación de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency.

REFERENCIAS BIBLIOGRÁFICAS

Castillo, C. R. (2016). “Sistema de gestión de seguridad de la información en la municipalidad distrital de Pira aplicando la norma ISO/IEC 27001:2013. *Tesis para optar el Titulo Profesional de Ingenieria de Sistemas.* Universidad Catolica Los Angeles de Chimbote, Huaraz - Perú.

CONCYTEC. (2016). *I Censo Nacional de Investigación y Desarrollo a Centros de Investigación.* (T. e. Consejo Nacional de Ciencia, Ed.) Recuperado el 20 de Febrero de 2020, de https://portal.concytec.gob.pe/images/publicaciones/censo_2016/libro_censo_nacional.pdf

Crespo, M. P. (2016). Metodología de Seguridad de la Información para la Gestión del Riesgo Informático Aplicable a MPymes. *Tesis para optar el grado de Maestro en Gestion Estrategica de Tecnologias de Informacion.* Universidad de Cuenca, Cuenca - Ecuador.

Cruz, D. M., & Fukusaki, I. S. (2017). Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la clínica Medcam Perú SAC”. *Tesis para optar el Titulo Profesional de Ingeniero de Computacion y Sistemas.* Universidad San Martin de Porres, Lima - Perú.

Guerrero, S. d., Navarro, C. A., Lizcano, R. R., & Felizzola, C. L. (2019). Diseño del sistema de gestión de seguridad de la información SGSI basado en el estándar ISO 27001, en la Universidad Popular del Cesar, Seccional Aguachica. *Proyecto de grado para optar el Titulo de Especialista en Auditoria de Sistemas.* Universidad Francisco de Paula Santiago Ocaña, Ocaña - Colombia.

Hernández Sampieri, R., Fernádez Collado, C., & Baptista Lucio, P. (12 de 09 de 2014). *Metodología de la investigación* (Quinta ed.). (M. G. S.A., Ed.) Mexico, Mexico: McGraw Hill.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. d. (2014). *Metología de la investigación* (6 Edición ed.). México D.F, México. Obtenido de https://www.esup.edu.pe/wp-content/uploads/2020/12/2.%20Hernandez,%20Fernandez%20y%20Baptista-Metodolog%C3%ADa%20Investigacion%20Cientifica%206ta%20ed.pdf

Leon, C. J. (2019). Diseño de un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC27001 para entidades del estado. *Trabajo de grado para optar el Titulo de Especialista en Seguridad Informatica.* Universidad Nacional Abierta y a Distancia -UNAD, La Guajira - Colombia.

Molano, E. R. (2017). Estrategia para implementar un sistema de gestión de la seguridad de la información basada en la norma ISO 27001 en el área de ti para la empresa Market Mix. *Trabajo de grado para obtener el Titulo de especialistas en Auditoria de Sistemas.* Universidad Catolica de Colombia, Bogota - Colombia.

Ñaupas, H., Mejía, E., Novoa, E., & Villagómez, A. (2014). *Metodologìa de la Investigación.* Colombia: Ediciones de la U.

Ochoa, T. A. (2019). Sistema web de gestión de seguridad de la información asistida por computadora basada en el estándar ISO 27001 en la universidad nacional José María Arguedas. *Tesis para optar el Titulo de Ingeniero de Sistemas.* Universidad Nacional José María Arguedas, Andahuaylas - Perú.

Palella Stracuzzy, S., & Martins Pestana, F. (2017). Metodologia De La Investigacion Cuantitativa. Caracas, Venezuela.

Palella Stracuzzy, S., & Martins Pestana, F. (2017). *Metodologia De La Investigacion Cuantitativa* (4 ed.). (Fedupel, Ed.) Caracas, Venezuela.

Porras, R. M. (2019). Sistema de gestión de seguridad de la información para la gestión de riesgos en activos de información. *Tesis para optar el Titulo Profesional de Ingeniero de Sistemas y Computacón.* Universidad Peruana Los Andes, Huancayo - Perú.

Sabino, C. (1996). *El proceso de investigación.* Caracas: Editorial Panapo.

Santos, L. D. (2016). Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de software. *Tesis para optar el Titulo de Ingeniero Informático.* Pontificia Universidad Catolica del Perú, Lima - Perú.

Serna, V. M., Duran, P. A., & Sanchez, A. R. (2017). Diseño de un sistema de gestión de la seguridad de la información para la secretaria de hacienda de rio de oro-cesar, basado en la norma ISO/IEC 27001:2013. *Trabajo de grado para optar el Titulo de Especialista en Auditoria de Sistemas.* Universidad Francisco de Paula Santander, Ocaña - Colombia.

Vilca, M. E. (2017). Diseño e implementación de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos humanos de la empresa Geosurvey de la ciudad de Lima. *Tesis para optar el Titulo profesional de Ingeniero de Sistemas e Informática.* Universidad de Huánuco, Huánuco - Perú.

Zevallos, M. M. (2019). Modelo de gestión de riesgos de seguridad de la información. *Revista Peruana de Computacion y Sistemas.* Universidad Nacional Mayor de San Marcos, Lima - Perù.

ANEXOS

Anexo 1: Matriz de Consistencia

Tabla 18:
Matriz de Consistencia

Problemas General	**Objetivos General**	**Hipótesis General**	**Variable Independiente**	**Indicador V.I.**	**Variable Dependiente**	**Indicador V.D.**
¿Cómo se relaciona el sistema de gestión de seguridad de la información basado en la ISO 27001:2013 para minimizar los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency?	Determinar la relación del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 para minimizar de los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency	Existe relación entre el sistema de gestión de seguridad de la información basado en la ISO 27001:2013 para m minimizar de los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency	***Sistema de Gestión de Seguridad de la Información***	--.--	***Riesgos de seguridad***	--.--
Problemas Especifico	**Objetivos Específicos**	**Hipótesis Especificas**				
¿Cómo se relaciona el sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y la identificación de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency?	Determinar la relación del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y la identificación de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency	Existe relación entre el sistema de gestión de seguridad de la información y la identificación de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency	Requisitos del SGSI	% de cumplimiento del SGSI	Identificación de riesgos	Nivel identificación de riesgos
¿Cómo se relaciona el sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y el análisis de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency?	Determinar la relación del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y el análisis de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency	Existe relación entre el sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y el análisis de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency	Análisis de brechas	Nivel de brechas	Análisis riesgos	Nivel de análisis riesgos
¿Cómo se relaciona el sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y la evaluación de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency?	Determinar la relación del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y la evaluación de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency	Existe relación del sistema de gestión de seguridad de la información basado en la ISO 27001:2013 y la evaluación de riesgos de seguridad en el área de sistemas de la empresa Quantify Agency	Controles de seguridad	% de activos vulnerables	Evaluación riesgos	Nivel de evaluación riesgos

Elaboración propia

Anexo 2: Instrumento de recolección de datos

"Modelo del Sistema de Gestión de Seguridad de la Información para minimizar los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency"

La presente encuesta tiene como objetivo: **Determinar en qué medida el modelo del sistema de gestión de seguridad de la información para minimizar los riesgos de la seguridad en el área de sistemas de la empresa Quantify Agency.**

Edad: _____ Sexo: _____

ESCALA VALORATIVA

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

CUESTIONARIO	ESCALA VALORATIVA				
Sistema de Gestión de Seguridad de la Información	1	2	3	4	5
Requisitos del SGSI					
1. ¿Sabe Ud. que la empresa viene cumpliendo los requisitos del sistema de gestión de la seguridad de la información?					
2. ¿Estaría de acuerdo con la implementación del sistema de gestión de la seguridad de la información en la empresa?					
3. ¿Cree usted que es importante la seguridad de los activos de información?					
4. ¿El diseño de un Sistema de Seguridad de Información para la empresa Quantify Agency mejorara la protección de los activos de información?					
5. ¿Está de acuerdo que se debe cumplir los requisitos del SGSI ?					
Análisis de brechas					
6. ¿El diseño y la implementación de controles de seguridad de la información permitirá reducir los riesgos a los activos de					

información?					
7. ¿Para Ud. el no contar con controles de Seguridad de la Información representa una desventaja considerable frente a otras empresas?					
8. ¿Para Ud. El diseño y la implementación de controles de seguridad reducirá los riesgos de seguridad de la información.?					
9. ¿Sabe Ud, si existen controles para evitar la manipulación, pirateo, de un sistema de información en la empresa?					
10. ¿Existe controles de las vulnerabilidades de los sistemas de información en la empresa?					
Controles de seguridad					
11.- ¿Tiene conocimiento Ud. de la aplicación de los controles de seguridad de la información?					
12.- Para Ud. el Plan del SGSI será la herramienta adecuada para mejorar los controles de seguridad?					
13.- ¿Para Ud. ¿El plan del SGSI permitirá establecer los lineamientos para mitigar los riesgos?					
14.- ¿La implementación del plan del SGSI permitirá mitigar los riesgos a los activos de información?					
15.- ¿Para Ud. el no contar con un plan de Sistema de Gestión de Seguridad de la Información representa una desventaja considerable frente a otras empresas?					
Riesgos de seguridad					
Identificación de riesgos					
16.- ¿Cree Ud. que la empresa brinda una protección adecuada a la información crítica de los clientes?					
17.- ¿Para Ud. los sistemas de información cumplen con garantizar la confidencialidad de la información de los clientes?					
18.- Sabe Ud. ¿Si la empresa ha implementado algún control para evitar el acceso no autorizado en los sistemas de información?					
19. ¿Tiene conocimiento si en su contrato de trabajo contemplan algún ítem de confidencialidad en relación con la información que haya tenido acceso en el desempeño de sus funciones?					

20.- Sabe Ud. ¿Si se ha implementado algún control para mitigar los riesgos de la confidencialidad de los datos personales de los empleados, proveedores y clientes?					
Análisis de riesgos					
21.- ¿Considera Ud. que en su área de trabajo existe información valiosa que debe ser protegida de manera íntegra?					
22.- Cuando su computador está en estado inactivo ¿Se activa el bloqueo de pantalla con contraseña para proteger la información?					
23.- ¿En lo que va del año ha sufrido alguna modificación o pérdida de información por virus o acceso de personas no autorizadas?					
24. ¿En su área de trabajo se han realizado evaluación de riesgos relacionados a la integridad de la información de la empresa?					
25. ¿Considera que la empresa se protege de amenazas externas o ambientales que ocasionen pérdidas de la integridad de la información?					
Evaluación de riesgos					
26 ¿Estás de acuerdo que la empresa pueda transferir algunos riegos a terceros?					
27.- ¿Tienes conocimiento si la información de los clientes, han sido guardados en la nube?					
28.- ¿Sabe Ud. si la empresa recurre a terceros para reducir los riegos de la información de los clientes y proveedores?					
29.-Sabe Ud. ¿Si existe un plan de contingencias en la empresa para afrontar un evento de disponibilidad de información de los clientes y proveedores?					
30.- Sabe Ud. ¿Si existe un plan de continuidad de negocio en la empresa para garantizar la disponibilidad de los sistemas de información?					

Juicio de expertos

UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA
FACULTAD DE CIENCIAS E INGENIERÍA
INGENIERÍA DE SISTEMAS E INFORMATICA

VALIDACIÓN DE INSTRUMENTO

TÍTULO DE LA TESIS: "Modelo del Sistema de Gestión de Seguridad de la Información basado en la ISO 27001:2013 para minimizar los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency".

PRESENTADO POR (Tesistas): Bach. Córdova Salinas, José María
Bach. Remicio Canales, Wilian Eusebio

I. DATOS GENERALES DEL EXPERTO N°: 01

1.1. Apellidos y Nombres : Saravia Aguilar, Karina
1.2. Grado Académico : Ingeniero de Sistemas y Computo
1.3. Cargo e Institución donde Labora: Jefe de la Unidad de Encuestas y Registros – OTIN - INEI
1.4. Tipo de Instrumento de Evaluación: **ENCUESTA**

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 40%	BUENO 41 – 60%	MUY BUENO 61 – 80%	EXCELENTE 81 – 100%
1. CLARIDAD	Está formulado con lenguaje apropiado				X	
2. OBJETIVIDAD	Está expresado en conducta observable					X
3. ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología				X	
4. ORGANIZACIÓN	Existe organización Lógica				X	
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad					X
6. INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico				X	
7. CONSISTENCIA	Se basa en aspectos teóricos, científicos acordes a la tecnología					X
8. COHERENCIA	Entre índices, indicadores y dimensiones					X
9. METODOLOGÍA	Responde al propósito del trabajo bajo los objetivos a lograr.					X

II. OPCIÓN DE APLICABILIDAD : .....Se puede aplicar.....

III. PROMEDIO DE VALORACIÓN : .....85%.....

IV. RECOMENDACIONES : .....Ninguno.....

Firmado digitalmente por SARAVIA AGUILAR Karina Helga FAU 20131369981 soft
Motivo: Soy el autor del documento
Fecha: 12.01.2022 01:49:29 -05:00

Firma del experto:

Fecha: 12/01/2022 DNI : 40050032

UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA
FACULTAD DE CIENCIAS E INGENIERÍA
INGENIERÍA DE SISTEMAS E INFORMATICA

VALIDACIÓN DE INSTRUMENTO

TÍTULO DE LA TESIS: "Modelo del Sistema de Gestión de Seguridad de la Información basado en la ISO 27001:2013 para minimizar los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency".

PRESENTADO POR (Tesistas): Bach. Córdova Salinas, José María
Bach. Remicio Canales, Wilian Eusebio

I. DATOS GENERALES DEL EXPERTO N°: 02

1.1. Apellidos y Nombres : Acosta Salvador Sabina Gualvertina
1.2. Grado Académico : Mg. En Educación con Mención en Docencia y Gestión Educativa
1.3. Cargo e Institución donde Labora: Docente en la facultad de Humanidades Universidad Cesar Vallejo
1.4. Tipo de Instrumento de Evaluación: **ENCUESTA**

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 40%	BUENO 41 – 60%	MUY BUENO 61 – 80%	EXCELENTE 81 – 100%
1. CLARIDAD	Está formulado con lenguaje apropiado					X
2. OBJETIVIDAD	Está expresado en conducta observable					X
3. ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología					
4. ORGANIZACIÓN	Existe organización Lógica				X	X
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad					X
6. INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico				X	
7. CONSISTENCIA	Se basa en aspectos teóricos, científicos acordes a la tecnología					X
8. COHERENCIA	Entre índices, indicadores y dimensiones				X	
9. METODOLOGÍA	Responde al propósito del trabajo bajo los objetivos a lograr.					X

II. OPCIÓN DE APLICABILIDAD : .....Se puede aplicar.....

III. PROMEDIO DE VALORACIÓN : .....86%.....

IV. RECOMENDACIONES : .....Ninguno.....

Firma del experto:

Fecha: 31/03/2022 DNI : 40399889

UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA
FACULTAD DE CIENCIAS E INGENIERÍA
INGENIERÍA DE SISTEMAS E INFORMATICA

VALIDACIÓN DE INSTRUMENTO

TÍTULO DE LA TESIS: "Modelo del Sistema de Gestión de Seguridad de la Información basado en la ISO 27001:2013 para minimizar los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency".

PRESENTADO POR (Tesistas): Bach. Córdova Salinas, José María
Bach. Remicio Canales, Wilian Eusebio

I. DATOS GENERALES DEL EXPERTO N°: 03
1.1. Apellidos y Nombres : Gonzales Calderón José Ramos
1.2. Grado Académico : Magister en Gestión Tecnologica de la Información
1.3. Cargo e Institución donde Labora: Docente Universidad Peruana de Ciencias e Informática
1.4. Tipo de Instrumento de Evaluación: **ENCUESTA**

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 40%	BUENO 41 – 60%	MUY BUENO 61 – 80%	EXCELENTE 81 – 100%
1. CLARIDAD	Está formulado con lenguaje apropiado					X
2. OBJETIVIDAD	Está expresado en conducta observable					X
3. ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología					
4. ORGANIZACIÓN	Existe organización Lógica				X	X
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad					X
6. INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico				X	
7. CONSISTENCIA	Se basa en aspectos teóricos, científicos acordes a la tecnología					X
8. COHERENCIA	Entre índices, indicadores y dimensiones				X	
9. METODOLOGÍA	Responde al propósito del trabajo bajo los objetivos a lograr.					X

II. OPCIÓN DE APLICABILIDAD : ……Se puede aplicar……

III. PROMEDIO DE VALORACIÓN : ……86%……

IV. RECOMENDACIONES : ……Ninguno……

Firma del experto:

Fecha: 30/03/2022 DNI : 17541317

Anexo 3: Base de datos

	Sistema de Gestión de Seguridad de la Información															Minimizar riesgo de seguridad												
	Requisitos del SGSI					Análisis de brechas					Controles de seguridad					Identificacion riesgos					Analisis de riesgos					Evalaucion de riesgos				
N°	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30
1	4	5	5	5	5	4	4	4	3	2	3	4	4	4	5	3	4	3	3	3	5	2	4	3	2	4	4	3	3	3
2	3	5	4	4	3	4	3	4	3	3	3	4	4	4	4	4	4	2	3	3	5	4	3	3	3	3	5	3	3	3
3	3	5	5	5	5	5	5	4	4	3	4	4	5	4	5	4	4	3	3	3	5	4	2	3	3	5	4	3	3	3
4	3	5	5	4	4	4	2	4	3	3	3	4	5	5	5	4	4	3	3	3	5	4	3	3	3	5	5	3	3	3
5	5	4	4	4	4	5	5	5	3	3	3	3	3	3	3	4	4	3	2	3	4	4	2	3	3	3	4	3	3	3
6	5	5	5	5	5	5	5	5	4	4	3	5	5	5	5	4	4	4	4	3	5	4	1	3	4	5	5	3	4	3
7	3	5	5	5	5	5	5	5	3	3	3	5	5	5	5	4	4	3	3	3	5	4	1	3	2	5	4	3	3	3
8	3	4	4	4	4	4	4	4	3	3	3	4	4	4	3	4	4	3	3	3	5	5	1	3	2	4	4	3	4	3
9	4	5	5	5	5	4	4	4	3	2	3	4	4	4	5	3	4	3	2	3	5	5	4	3	2	4	4	4	3	3
10	3	4	4	4	4	4	4	4	4	2	3	4	5	5	5	3	4	3	4	3	5	2	3	2	4	4	4	4	4	4

Anexo 4: Evidencia de similitud digital

“Modelo del Sistema de Gestión de Seguridad de la Información basado en la ISO 27001:2013 para minimizar los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency”

por José María, Wilian Eusebio Córdova Salinas, Remicio Canales

Fecha de entrega: 30-abr-2022 02:58a.m. (UTC-0500)
Identificador de la entrega: 1824586922
Nombre del archivo: Tesis_REMICIO_CORDOVA_29_04_22.docx (3.51M)
Total de palabras: 16820
Total de caracteres: 89763

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

INFORME DE ORIGINALIDAD

25%	25%	8%	8%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.upci.edu.pe Fuente de Internet	8%
2	repositorio.ucv.edu.pe Fuente de Internet	3%
3	www.redalyc.org Fuente de Internet	3%
4	repositorioacademico.upc.edu.pe Fuente de Internet	2%
5	hdl.handle.net Fuente de Internet	1%
6	www.repositorioacademico.usmp.edu.pe Fuente de Internet	1%
7	repositorio.uns.edu.pe Fuente de Internet	1%
8	openaccess.uoc.edu Fuente de Internet	1%

9	tesis.pucp.edu.pe Fuente de Internet	1 %
10	ri.ues.edu.sv Fuente de Internet	<1 %
11	Esteban Crespo Martínez. "Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMEs", Enfoque UTE, 2017 Publicación	<1 %
12	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	<1 %
13	www.tdx.cat Fuente de Internet	<1 %
14	dspace.ucuenca.edu.ec Fuente de Internet	<1 %
15	repositorio.uladech.edu.pe Fuente de Internet	<1 %
16	Submitted to Universidad del Valle, Colombia Trabajo del estudiante	<1 %
17	Nohora Nubia Mercado Caruso. "Determinantes de eco-innovación en clústers industriales. Una aplicación empírica en el departamento del Atlántico", Universitat Politecnica de Valencia, 2022 Publicación	<1 %

18	tesis.luz.edu.ve Fuente de Internet	<1 %
19	repositorio.udh.edu.pe Fuente de Internet	<1 %
20	upc.aws.openrepository.com Fuente de Internet	<1 %
21	www.theibfr.com Fuente de Internet	<1 %
22	Submitted to Universidad Señor de Sipan Trabajo del estudiante	<1 %
23	apuntesperuanos.com Fuente de Internet	<1 %
24	repositorio.uss.edu.pe Fuente de Internet	<1 %
25	www.newsletter.iqnet-certification.com Fuente de Internet	<1 %
26	Submitted to Cranfield University Trabajo del estudiante	<1 %
27	www.ofspuebla.gob.mx Fuente de Internet	<1 %

Excluir citas	Activo	Excluir coincidencias	< 15 words
Excluir bibliografía	Activo		

Anexo 5: Autorización de publicación en repositorio

UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA
La Universidad del futuro, hoy

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJO DE INVESTIGACIÓN O TESIS EN EL REPOSITORIO INSTITUCIONAL UPCI

1.- DATOS DEL AUTOR

Apellidos y Nombres: CÓRDOVA SALINAS JOSÉ MARÍA

DNI: 44463851 Correo electrónico: JOSE.CORDOVAS@OUTLOOK.COM

Domicilio: AV. MICAELA BASTIDAS 1084-1088

Teléfono fijo: 5968436 Teléfono celular: 902718505

2.- IDENTIFICACIÓN DEL TRABAJO Ó TESIS

Facultad/Escuela: INGENIERÍA DE SISTEMAS

Tipo: Trabajo de Investigación Bachiller ( ) Tesis (X)

Título del Trabajo de Investigación / Tesis:

MODELO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA ISO 27001:2013 PARA MINIMIZAR LOS RIESGOS DE SEGURIDAD EN EL AREA DE SISTEMAS DE LA EMPRESA QUANTIFY AGENCY

3.- OBTENER:

Bachiller ( ) Título (X) Mg. ( ) Dr. ( ) PhD. ( )

4. AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

Por la presente declaro que el documento indicado en el ítem 2 es de mi autoría y exclusiva titularidad, ante tal razón autorizo a la Universidad Peruana Ciencias e Informática para publicar la versión electrónica en su Repositorio Institucional (http://repositorio.upci.edu.pe), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art23 y Art.33.

Autorizo la publicación de mi tesis (marque con una X):
(X) Sí, autorizo el depósito y publicación total.
( ) No, autorizo el depósito ni su publicación.

Como constancia firmo el presente documento en la ciudad de Lima, a los ____ días del mes de MAYO de 2022.

J. Córdova S.

Firma

UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJO DE INVESTIGACIÓN O TESIS EN EL REPOSITORIO INSTITUCIONAL UPCI

1.- DATOS DEL AUTOR

Apellidos y Nombres: REmicio canales, wilian Eusebio

DNI: 44615604 Correo electrónico: WRcanales@gmail.com

Domicilio: Mz. F2 Lt. 05 A.H. Municipal III Sector Balcon del Rimac

Teléfono fijo: 573 7147 Teléfono celular: 949310622

2.- IDENTIFICACIÓN DEL TRABAJO Ó TESIS

Facultad/Escuela: Ciencias e Ingeniería

Tipo: Trabajo de Investigación Bachiller ( ) Tesis (X)

Título del Trabajo de Investigación / Tesis:

"Modelo del Sistema de gestión de seguridad de la información basado en la ISO 27001:2013 para minimizar los riesgos de seguridad en el área de sistemas de la Empresa Quantify Agency"

3.- OBTENER:

Bachiller ( ) Título (X) Mg. ( ) Dr. ( ) PhD. ( )

4. AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

Por la presente declaro que el documento indicado en el ítem 2 es de mi autoría y exclusiva titularidad, ante tal razón autorizo a la Universidad Peruana Ciencias e Informática para publicar la versión electrónica en su Repositorio Institucional (http://repositorio.upci.edu.pe), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art23 y Art.33.

Autorizo la publicación de mi tesis (marque con una X):
(X) Sí, autorizo el depósito y publicación total.
( ) No, autorizo el depósito ni su publicación.

Como constancia firmo el presente documento en la ciudad de Lima, a los 16 días del mes de Junio de 2022.

Firma

Anexo 6: Modelo del Sistema de Gestión de Seguridad de la Información

1. Descripción de la empresa.

Quantify Agency E.I.R.L. es una empresa peruana dedicada al asesoramiento de empresas en Marketing que inicia sus actividades el 10 de Setiembre del 2019.

La sede de su oficina está ubicada en el distrito de Miraflores, en Lima. Al ser una empresa relativamente nueva, cuenta con diez colaboradores, los cuales trabajan en planilla de la misma. Cuenta con clientes de diferentes rubros como la consultoría, medicina, producción de alimentos y demás.

Misión

Que nuestros clientes transformen y mejoren sus empresas y dispongan de una comunicación ágil, eficaz y tecnológicamente avanzada hacia todos sus públicos.

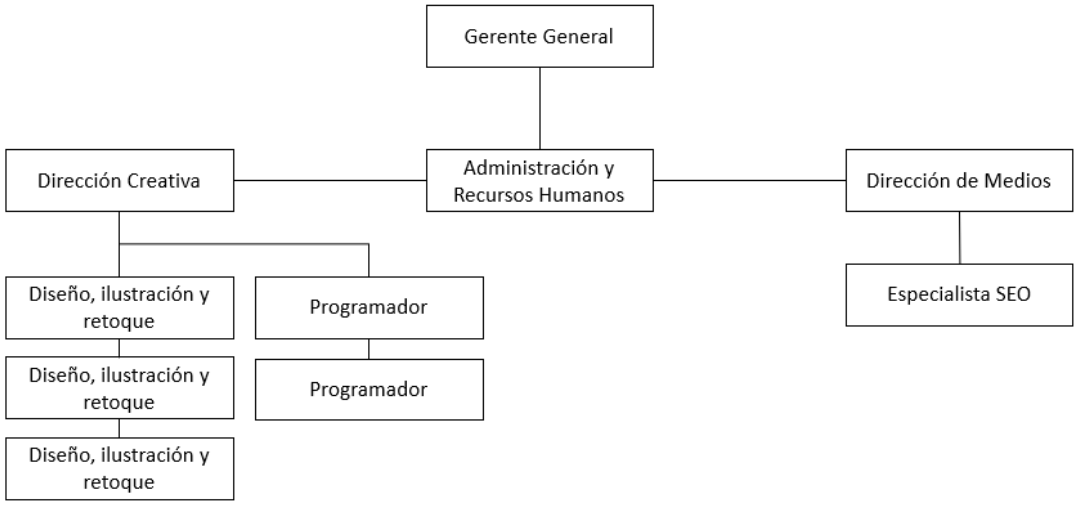
Visión

Ser la mejor consultora de marcas en base a la confianza y satisfacción de nuestros clientes. Convertirnos en la consultora de marcas más atractiva para las empresas que quieran transformarse para mejorar y optimizar sus negocios.

Valores

- Puntualidad.
- Ética.
- Calidad.
- Innovación.
- Lealtad.
- Honestidad.
- Identidad.
- Responsabilidad social.

Organigrama



a. Alcance

Se aplica a todas las actividades que serán en el área de sistemas de la empresa Quantify Agency.

b. Usuarios que áreas de la empresa

- Miembros del directorio.
- Miembros del equipo del proyecto SGSI.
- Oficial de Seguridad de la Información.

2. Documentos de referencia.

- NTP ISO/IEC 27001:2014: Sistema de Gestión de la Seguridad de la Información, su implementación es obligatoria en el Estado, en tal sentido el PCM (Secretaria de gobierno digital brindará la asistencia técnica a las entidades que lo requieran.
- ISO/IEC 27001:2013.
- ISO/IEC 27002:2013.

Especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. También incluye requisitos para la evaluación y el tratamiento de riesgos de seguridad de la información adaptados a las necesidades de la organización.

Modelo Propuesto del SGSI

1. OBJETIVO DEL PLAN

Definir el proyecto de implementación del Sistema de Gestión de Seguridad de la Información (SGSI), los documentos que se redactarán, los plazos, las funciones y responsabilidades del proyecto.

2. ALCANCE

Se aplica a todas las actividades que serán realizadas dentro del proyecto de implementación del SGSI.

3. USUARIOS DEL PROYECTO

- Miembros de la Alta Dirección.
- Miembros del Comité de Gestión de Seguridad de la Información (CGSI).
- Oficial de Seguridad de la Información.

4. DOCUMENTOS DE REFERENCIA

- Ley 27658 - Ley Marco de Modernización de la Gestión del Estado.
- Ley 29733 - Protección de datos personales.
- RM 129-2012-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos".
- R. M N°004-2016-PCM, que aprueba el uso obligatorio de la NTP ISO/IEC.
- 27001:2014 "Tecnología de la Información. Técnicas de Seguridad, Sistemas de
- Gestión de Seguridad de la Información. Requisitos".
- Resolución Directoral N°056-2017-INACAL/DN, que aprueba la Norma Técnica Peruana "NTP-ISO/IEC 27002:2017 Tecnología de la información. Técnicas de Seguridad. Código de buenas prácticas para controles de seguridad de la información. 1a Edición".

- ISO/IEC 27001:2013 "Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de Seguridad de la Información. Requisitos".
- ISO/IEC 27002:2013 "Tecnología de la Información - Técnicas de Seguridad- Código de Conducta para los Controles de Seguridad de la Información".
- RM 166-2017-PCM- Modifican el artículo 5 de la R.M. W 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información.

5. PROYECTO DE IMPLEMENTACIÓN DEL SGSI

5.1. Objetivo del proyecto

Administrar la seguridad de la información, implementando controles adecuados que permitan medir la confidencialidad, integridad y disponibilidad de la información gestionada en la institución en conformidad con la norma ISO/IEC 27001:2013.

5.2. Entregables del proyecto

Los entregables del proyecto son los siguientes:

1) **Acta de constitución del Proyecto. -** Documento en el que se define el alcance, los objetivos y los participantes del proyecto.

2) **Procedimiento para el control de documentos y registros**.- Documento que detalla la forma de redactar, aprobar, distribuir y actualizar los documentos y registros.

3) **Alcance del SGSI**.- Es un documento o puede ser un capítulo dentro de otro documento que define los activos, ubicaciones, tecnología, etc... que forman **parte del SGSI.**

4) **Política General de Seguridad de la Información**. - Es un documento o puede ser un capítulo dentro de otro documento que define la forma en que la dirección controla la gestión de la seguridad de la información.

5) **Informe de Análisis de Brechas o GAP**.- Documento que permite identificar el nivel de cumplimiento en relación a la ISO 27001.

6) **Metodología para la evaluación de riesgos.-** Describe los métodos, procedimientos y parámetros para gestionar los riesgos de la información.

7) **Declaración de Aplicabilidad.-** Documento que determina los objetivos y la aplicabilidad de cada control establecido en el Anexo A de la norma ISO/IEC 27001:2013.

8) **Inventario de Activos de Información. -** Documento que detalla la verificación, identificación y ubicación de cada uno de los bienes que la institución posee en el marco del alcance del SGSI.

9) **Matriz de evaluación de riesgos. -** Es el resultado de la evaluación del valor, de amenazas y vulnerabilidades de los activos.

10) **Informe de la evaluación y tratamiento de riesgos.-** Documento resultante del proceso de evaluación de riesgos. Describe la base establecida para la toma de decisiones y la planificación del tratamiento de los riesgos que están expuestos.

11) **Plan de tratamiento del riesgo.-** Documento donde se detallan los controles de seguridad adecuados para cada riesgo inaceptable de tal forma que se evidencia su tratamiento.

12) **Plan de sensibilización de Seguridad de la Información. -** Documento que establece los propósitos, estrategias, actividades, variables, y lineamientos a seguir para lograr que las personas entiendan y se comprometan con todos los aspectos relacionados con la seguridad de la información.

13) **Plan de auditoría interna**.- Documento que establece las actividades y plazos para la ejecución de una auditoría interna.

14) **Informe de acciones correctivas y preventivas**.- Descripción detallada de las actividades que deben realizarse como parte de las acciones correctivas y preventivas.

15) **Estándares, procedimientos, políticas y controles específicos.-** Documentos de apoyo que se emplean para asegurar que las actividades operativas sean correctas y seguras.

5.3. Fases, Actividades y Plazos

La empresa Quantify Agency ha establecido un Plan de Implementación iterativo e incremental de la ISO/IEC 27001:2013, desarrollando actividades y entregables.

Las fases son las siguientes:

FASE	DESCRIPCIÓN	TIEMPO DE LA IMPLEMENTACIÓN
FASE I PLANIFICAR (P) Establecer el Sistema de Gestión de Seguridad de la Información (SGSI)	Se define la estructura del SGSI, se valida el alcance, los objetivos y se identifican los criterios para la evaluación de riesgos de seguridad de la información	3 meses (65 días hábiles)
FASE II HACER (H)	Se desarrollan los controles que integran la Declaración de	

Implantación Operación del SGSI	Aplicabilidad, asimismo, se lleva a cabo la ejecución del programa de concientización de los usuarios y el equipo de administración, y se inicia la operación del SGSI.	3 meses (73 días hábiles)
FASE III VERIFICAR (V) Monitoreo y Revisión del SGSI	Se realizan revisiones y auditorías al SGSI para detectar áreas de oportunidad en la eficiencia de implantación de controles de seguridad, y se determina el grado de apego del SGSI a los objetivos institucionales.	1 mes (26 días hábiles)
FASE IV ACTUAR (A Mantenimiento y Mejora con base a las del SGSI)	Se realizan las correcciones necesarias observaciones de la Etapa anterior.	2 meses (33 días hábiles)

Los detalles de la ejecución de las tareas se indican en el ANEXO 01: PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - QUANTIFY AGENCY.

El tiempo de implementación variará de acuerdo con la asignación de recursos humanos. Para la función de seguridad de la información. La empresa Quantify Agency cuenta con el Oficial de Seguridad de la Información (IN HOUSE) y, dentro de la Gerencia de Informática. Otra opción es tercerizar una o más fases de la implementación con lo que los tiempos se acortarían.

El presente documento es susceptible de mejoras durante su desarrollo, dado que este tipo de proyectos no han sido desarrollados anteriormente en la institución además es de esperar que durante el avance se presenten variables que pueden ser consideradas desde el inicio, tales como la cultura organizacional, disponibilidad presupuestal y cumplimiento de disposiciones urgentes. Se ha desarrollado en función de la aplicación del ciclo de Deming (metodología PHVA) descrita en el literal 7 METODOLOGIA del presente documento.

5.4. Organización del proyecto

El proyecto estará organizado de la siguiente manera:

- Comité de Gestión de Seguridad de la Información (CGSI), deberá cumplir las funciones establecidas por la Resolución Ministerial N°166-2017- PCM.
- Comité Operativo de Seguridad de la Información, comité que se forma con los representantes directos de cada área involucrada en el alcance del proyecto, para poder coordinar la implementación del SGSI.
- Oficial de Seguridad de la Información (CISO), quien brinda la dirección metodológica para la implementación del SGSI-QA además de coordinar la implementación del Sistema de Gestión de Seguridad de la Información en la institución.

5.5. Riesgos del proyecto

La implementación de un Sistema de Gestión de Seguridad de la Información, es un proyecto que conlleva a un cambio en la cultura organizacional en todos los niveles de la institución.

Los principales riesgos en la implementación del proyecto son los siguientes:

- Falta de respaldo de la Alta Dirección
- Falta de compromiso del equipo del proyecto
- Falta de recursos asignados al proyecto
- Ampliación de los plazos en los entregables
- Cambios en los integrantes del equipo del proyecto
- Inadecuada definición del alcance
- Selección de demasiados controles y/o muy caros.3
- Posibilidad que las políticas de información no se cumplan por falta de difusión o porque los controles no están efectivamente implementados.

5.6. Herramientas utilizadas en el proyecto

Se utilizará las herramientas ofimáticas.

6. GESTIÓN DE REGISTROS

Se definirán procedimientos y registros con codificaciones estándar para la elaboración de los documentos de gestión, lineamientos y directivas como resultado de la implementación del proyecto.

- La mejora continua de este documento es consignada en la tercera página de este en la tabla Mejora Continua.
- Deberán elaborarse informes parciales de la implementación del proyecto, la periodicidad será establecida por el CGSI.
- Toda incidencia producto de cambios o mejoras al proyecto también serán reportadas al CGSI.

7. GESTIÓN DE REGISTROS

Se definirán procedimientos y registros con codificaciones estándar para la elaboración de los documentos de gestión, lineamientos y directivas como resultado de la implementación del proyecto.

- La mejora continua de este documento es consignada en la tercera página de este en la tabla Mejora Continua.
- Deberán elaborarse informes parciales de la implementación del proyecto, la periodicidad será establecida por el CGSI.
- Toda incidencia producto de cambios o mejoras al proyecto también serán reportadas al CGSI.

7. METODOLOGIA

Para la implementación del Proyecto, se empleará la metodología denominada Ciclo de Deming, basado en un enfoque iterativo e incremental de procesos, generando que la cobertura del sistema se extienda con cada ciclo de mejora. Consiste en los siguientes pasos:

- Planificar (P).- Se establecen objetivos y se identifican los procesos.
- Hacer (H).- Se implementan los cambios o acciones necesarias para lograr las mejoras planteadas.
- Verificar (V).- Se realizan pruebas para medir y valorar la efectividad de los cambios.
- Actuar (A).- Se ejecutan correcciones y modificaciones necesarias.

Matriz de Inventario de activo y tipo de activo

ID	Inventario de activo de información	Tipo de activo	Propietario del activo
1	Correo Electrónico	Aplicaciones de software	Gerencia General
2	Contratos con los proveedores	Aplicaciones de software	Gerencia General
3	Equipos de Cómputo	Equipamiento informático	Gerencia General
4	Internet	Aplicaciones de software	Gerencia General
5	Impresora	Equipamiento informático	Gerencia General
6	Teléfono IP	Redes y comunicaciones	Gerencia General
7	Directorio Activo	Equipamiento informático	Gerencia General
8	Software Ofimática	Aplicaciones de software	Gerencia General
9	Smartphone	Redes y comunicaciones	Gerencia General
10	Sistema de Inventario TI Personal operativo	Aplicaciones de software	Gerencia General
11	Servidor de Archivos	Equipamiento informático	Gerencia General
12	Red Interna	Redes y comunicaciones	Gerencia General
13	Responsable de TI	Personal	Gerencia General
14	Personal de mando medio	Personal	Gerencia General
15	Personal operativo	Personal	Gerencia General

Aplicabilidad de controles de seguridad de la información

CONTROLES DE SEGURIDAD DE LA INFORMACION				
1.1 A.5 Política de Seguridad.				
A.5.1 Política de seguridad de información				
Controles		Aplica		Estado
		SI	NO	
A.5.1.1	Documento de Política de Seguridad de Información.	X		Aplicable
A.5.1.2	Revisión de la Política de Seguridad de la Información		X	Inaplicable
A.6 Organización de la seguridad de la información				
A.6.1 Organización interna				
Controles		Aplica		Estado
		SI	NO	
A.6.1.1	Roles y responsabilidades para la seguridad de la información	X		Aplicable
A.6.1.2	Segregación de funciones	X		Aplicable
A.6.1.3	Contacto con autoridades		X	Inaplicable
A.6.1.4	Contacto con grupos especiales de interés	X		Aplicable
A.6.1.5	Seguridad de la información en la gestión de proyectos	X		Aplicable
A.6.2 Dispositivos móviles y teletrabajo				
A.6.2.1	Política de dispositivos móviles		X	Inaplicable
A.6.2.2	Teletrabajo	X		Aplicable
A.7 Seguridad de los recursos humanos				
A.7.1 Antes del empleo				
Controles		Aplica		Estado
		SI	NO	
A.7.1.1	Selección	X		Aplicable
A.7.1.2	Términos y condiciones del empleo	X		Aplicable
A.7.2 Durante el empleo				
A.7.2.1	Responsabilidades de la gerencia	X		Aplicable

A.7.2.2	Conciencia, educación y capacitación sobre la seguridad de la información		X	Inaplicable
A.7.2.3	Proceso disciplinario	X		Aplicable
A.7.3 Terminación y cambio de empleo				
A.7.3.1	Terminación o cambio de responsabilidades del empleo.	X		Aplicable.
A.8 Gestión de activos				
A.8.1 Responsabilidad por los activos				
Controles		Aplica		
		SI	NO	
A.8.1.1	Inventario de activos	X		Aplicable
A.8.1.2	Propiedad de los activos	X		Aplicable
A.8.1.3	Uso aceptable de los activos	X		Aplicable
A.8.1.4	Retorno de activos	X		Aplicable
A.8.2 Clasificación de la información				
A.8.2.1	Clasificación de la información	X		Aplicable
A.8.2.2	Etiquetado de la información	X		Aplicable
A.8.2.3	Manejo de activos	X		Aplicable
A.8.3 Manejo de los medios				
A.8.3.1	Gestión de medios removibles		X	Inaplicable
A.8.3.2	Disposición de medios		X	Inaplicable

A.8.3.3	Transferencia de medios físicos	X		Aplicable
A.9 Control de acceso				
A.9.1 Requisitos de la empresa para el control de acceso				
Controles		Aplica		
		SI	NO	
A.9.1.1	Política de control de acceso	X		Aplicable
A.9.1.2	Acceso a redes y servicios de red	X		Aplicable
A.9.2 Gestión de acceso de usuario				
A.9.2.1	Registro y baja de usuarios	X		Aplicable
A.9.2.2	Aprovisionamiento de acceso a usuario	X		Aplicable
A.9.2.3	Gestión de derechos de acceso privilegiados	X		Aplicable
A.9.2.4	Gestión de información de autentificación secreta de usuarios	X		Aplicable
A.9.2.5	Revisión de derechos de acceso de usuarios	X		Aplicable
A.9.2.6	Remoción o ajuste de derechos de acceso	X		Aplicable
A.9.3 Responsabilidades de los usuarios				
Controles		Aplica		
		SI	NO	
A9.3.1	Uso de información de autentificación secreta.	X		Aplicable
A.9.4 Control de acceso a sistemas y aplicación.				

A.9.4.1	Restricción de acceso a la información	X		Aplicable
A.9.4.2	Procedimientos de ingreso seguro	X		Aplicable
A.9.4.3	Sistema de gestión de contraseñas		X	Inaplicable
A.9.4.4	Uso de programas utilitarios privilegiados	X		Aplicable
A.9.4.5	Control de acceso al código fuente de los programas	X		Aplicable
A.10 Criptografía				
A.10.1 Controles criptográficos				
Controles		Aplica		
		SI	NO	
A.10.1.1	Política sobre el uso de controles criptográficos		X	Inaplicable
A.10.1.2	Gestión de claves		X	Inaplicable
A.11 Seguridad física y ambiental				
A.11.1 Áreas seguras				
Controles		Aplica		
		SI	NO	
A.11.1.1	Perímetro de seguridad física	X		Aplicable
A.11.1.2	Controles de ingreso físico	X		Aplicable
A.11.1.3	Asegurar oficinas, áreas e instalaciones	X		Aplicable
A.11.1.4	Protección contra amenazas externas y ambientales	X		Aplicable

A.11.1.5	Trabajo en áreas seguras	x		Aplicable
A.11.1.6	Áreas de despacho y carga	x		Aplicable
A.11.2 Equipos				
Controles		Aplica		
		SI	NO	
A.11.2.1	Emplazamiento y protección de los equipos	X		Aplicable
A.11.2.2	Servicios de suministro	X		Aplicable
A.11.2.3	Seguridad del cableado	X		Aplicable
A.11.2.4	Mantenimiento de equipos	X		Aplicable
A.11.2.5	Remoción de activos	X		Aplicable
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones		X	Inaplicable
A.11.2.7	Disposición o reutilización segura de equipos	X		Aplicable
A.11.2.8	Equipos de usuario desatendidos		X	Inaplicable
A.11.2.9	Política de escritorio limpio y pantalla limpia		X	Inaplicable
A.12 Seguridad de las operaciones				
A.12.1 Procedimientos y responsabilidades operativas				
Controles		Aplica		
		SI	NO	
A.12.1.1	Procedimientos operativos documentados		X	Inaplicable

A.12.1.2	Gestión del cambio		X	Inaplicable
A.12.1.3	Gestión de la capacidad	X		Aplicable
A.12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	X		Aplicable
A.12.2 Protección contra códigos maliciosos				
A.12.2.1	Controles contra códigos maliciosos	X		Inaplicable
A.12.3 Respaldo				
A.12.3.1	Respaldo de la información	X		Inaplicable
A.12.4 Registros y monitoreo				
A.12.4.1	Registro de eventos		X	Inaplicable
A.12.4.2	Protección de información de Registros.	X		Aplicable
A.12.4.3	Registros del administrador y del operador	X		Aplicable
A.12.4.4	Sincronización de reloj	X		Aplicable
A.12.5 Control del software operacional				
A.12.5.1	Instalación de software en sistemas operacionales	X		Aplicable.
A.12.6 Gestión de vulnerabilidad técnica				
A.12.6.1	Gestión de vulnerabilidades técnicas		X	Inaplicable
A.12.6.2	Restricciones sobre la instalación de software		X	Inaplicable
A.12.7 Consideraciones para la auditoría de los sistemas de información				
Controles		Aplica		

		SI	NO	
A.12.7.1	Controles de auditoría de sistemas de información	X		Aplicable.
A.13 Seguridad de las comunicaciones				
A.13.1 Gestión de seguridad de la red				
Controles		Aplica		
		SI	NO	
A.13.1.1	Controles de la red	X		Aplicable.
A.13.1.2	Seguridad de servicios de red	X		Aplicable.
A.13.1.3	Segregación en redes	X		Aplicable.
A.13.2 Transferencia de información				
A.13.2.1	Políticas y procedimientos de transferencia de la información	X		Aplicable.
A.13.2.2	Acuerdo sobre transferencia de información	X		Aplicable.
A.13.2.3	Mensajes electrónicos	X		Aplicable.
A.13.2.4	Acuerdos de confidencialidad o no divulgación	X		Aplicable.
A.14 Adquisición, desarrollo y mantenimiento de sistemas				
A.14.1 Requisitos de seguridad de los sistemas de información				
Controles		Aplica		
		SI	NO	
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	X		Aplicable.
A.14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas		X	Inaplicable
A.14.1.3	Protección de transacciones en servicios de aplicación		X	Inaplicable
A.14.2 Seguridad en los procesos de desarrollo y soporte				

A.14.2.1	Política de desarrollo seguro		X	Inaplicable
A.14.2.2	Procedimientos de control de cambio del sistema		X	Inaplicable
A.14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa		X	Inaplicable
A.14.2.4	Restricciones sobre cambios a los paquetes de software		X	Inaplicable
A.14.2.5	Principios de ingeniería de sistemas seguros		X	Inaplicable
A.14.2.6	Ambiente de desarrollo seguro		X	Inaplicable
A.14.2.7	Desarrollo contratado externamente		X	Inaplicable
A.14.2.8	Pruebas de seguridad del sistema		X	Inaplicable
A.14.2.9	Pruebas de aceptación del sistema		X	Inaplicable
A.14.3 Datos de prueba				
A.14.3.1	Protección de datos de prueba		X	Inaplicable
A.15 Relaciones con los proveedores				
A.15.1 Seguridad de la información en las relaciones con los proveedores				
Controles		Aplica		
		SI	NO	
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores	X		Aplicable
A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	X		Aplicable
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	X		Aplicable.

A.15.2 Gestión de entrega de servicios del proveedor				
Controles		Aplica		
		SI	NO	
A.15.2.1	Monitoreo y revisión de servicios de los proveedores	X		Aplicable
A.15.2.2	Gestión de cambios a los servicios de proveedores	X		Aplicable
A.16 Gestión de incidentes de seguridad de la información				
A.16.1 Gestión de incidentes de seguridad de la información y mejoras				
Controles		Aplica		
		SI	NO	
A.16.1.1	Responsabilidades y procedimientos	X		Aplicable
A.16.1.2	Reporte de eventos de seguridad de la información	X		Aplicable
A.16.1.3	Reporte de debilidades de seguridad de la información		X	Inaplicable
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	X		Aplicable
A.16.1.5	Respuesta a incidentes de seguridad de la información	X		Aplicable
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	X		Aplicable
A.16.1.7	Recolección de evidencia	X		Aplicable
A.17 Aspectos de seguridad de la información en la gestión de continuidad del negocio				
A.17.1 Continuidad de seguridad de la información				
Controles		Aplica		
		SI	NO	
A.17.1.1		X		Aplicable

	Planificación de continuidad de seguridad de la información			
A.17.1.2	Implementación de continuidad de seguridad de la información	X		Aplicable
A.17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información	X		Aplicable
A.17.2 Redundancias				
A.17.2.1	Instalaciones de procesamiento de la información	X		Aplicable
A.18 Cumplimiento				
A.18.1 Cumplimiento con requisitos legales y contractuales				
Controles		Aplica		
		SI	NO	
A.18.1.1	Identificación de requisitos contractuales y de legislación aplicables	X		Aplicable
A.18.1.2	Derechos de propiedad intelectual	X		Aplicable
A.18.1.3	Protección de registros	X		Aplicable
A.18.1.4	Privacidad y protección de Datos personales.	X		Aplicable
A.18.1.5	Regulación de controles criptográficos	X		Aplicable
A.18.2 Revisiones de seguridad de la información				
A.18.2.1	Revisión independiente de la seguridad de la información	X		Aplicable
A.18.2.2	Cumplimiento de políticas y normas de seguridad	X		Aplicable

A.18.2.3	Revisión del cumplimiento técnico	X		Aplicable