**UNIVERSIDAD NACIONAL FEDERICO VILLARREAL**

**FACULTAD INGENIERIA INDUSTRIAL Y DE SISTEMAS**

**ESPECIALIDAD INGENIERIA DE SISTEMAS**

**IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN (SGSI) PARA LA EMPRESA EMPORIUM COLOR SAC**

**PLAN DE TESIS**

**ALUMNO:**

**FREDY JOSE MAMANI MAMANI**

**PROFESOR:**

**ING. PEDRO MARTIN LEZAMA GONZALES**

**LIMA- PERÚ**

**2021**

[TÍTULO: 5](#_Toc435478154)

[AUTOR 5](#_Toc435478155)

[LUGAR DONDE SE VA A REALIZAR LA INVESTIGACIÓN: 5](#_Toc435478156)

[I. DESCRIPCIÓN DEL PROYECTO 5](#_Toc435478157)

**!Especificación de carácter no válida**

[I.2. PLANTEAMIENTO DEL PROBLEMA 28](#_Toc435478164)

[I.2.1. DESCRIPCIÓN DE LA PROBLEMÁTICA 28](#_Toc435478165)

[I.2.2. DESCRIPCIÓN DEL PROBLEMA 34](#_Toc435478166)

[I.2.3. FORMULACIÓN DEL PROBLEMA 35](#_Toc435478167)

[I.2.3.1. PROBLEMA GENERAL 35](#_Toc435478168)

[I.2.3.1. PROBLEMA ESPECÍFICO 36](#_Toc435478169)

[I.3. OBJETIVOS 36](#_Toc435478170)

[I.3.1. OBJETIVO GENERAL 36](#_Toc435478171)

[I.3.2. OBJETIVO ESPECÍFICOS 37](#_Toc435478172)

[I.4. JUSTIFICACIÓN E IMPORTANCIA 37](#_Toc435478173)

[I.4.1. JUSTIFICACIÓN 37](#_Toc435478174)

[I.4.2. IMPORTANCIA 38](#_Toc435478175)

[I.5. ALCANCES Y LIMITACIONES 38](#_Toc435478176)

[I.5.1. ALCANCE 38](#_Toc435478177)

[I.5.2. LIMITACIÓN 39](#_Toc435478178)

[I.5.2.1. DELIMITACION ESPACIAL 39](#_Toc435478179)

[I.5.2.2. DELIMITACION TEMPORAL 39](#_Toc435478180)

[II. MARCO TEÓRICO 41](#_Toc435478181)

[II.1. TEORÍAS GENERALES RELACIONADAS CON EL TEMA 41](#_Toc435478182)

[III. HIPÓTESIS Y OPERACIONALIZACIÓN DE LAS VARIABLES. 69](#_Toc435478198)

[III.1. HIPÓTESIS GENERAL 69](#_Toc435478199)

[III.2. HIPÓTESIS ESPECÍFICAS 69](#_Toc435478200)

[III.3. VARIABLES 69](#_Toc435478201)

[III.3.1. VARIABLES INDEPENDIENTE 69](#_Toc435478202)

[III.3.2. VARIABLES INTERVINIENTE 70](#_Toc435478203)

[III.3.3. VARIABLE DEPENDIENTE 70](#_Toc435478204)

[III.3.4. OPERACIONALIDAD DE LAS VARIABLES. 70](#_Toc435478205)

[III.4. TIPO 76](#_Toc435478206)

[III.5. POBLACIÓN: 76](#_Toc435478207)

[III.6. UNIVERSO SOCIAL: 76](#_Toc435478208)

[III.7. MUESTRA: 76](#_Toc435478209)

[IV. MÉTODO. 77](#_Toc435478210)

[IV.1. DISEÑO DE INVESTIGACIÓN 77](#_Toc435478211)

[IV.2. ESTRATEGIA DE PRUEBA DE HIPÓTESIS 78](#_Toc435478212)

[IV.3. TÉCNICAS DE RECOLECCIÓN DE DATOS 79](#_Toc435478213)

[IV.3.1. INSTRUMENTOS DE RECOLECCIÓN DE DATOS. 79](#_Toc435478214)

[V. CRONOGRAMA 83](#_Toc435478215)

[VI. PRESUPUESTO 85](#_Toc435478216)

[VII. REFERENCIAS BIBLIOGRÁFICAS 86](#_Toc435478217)

[I. DESCRIPCIÓN DEL PROYECTO](#_Toc435478157)

[I.1. ANTECEDENTES](#_Toc435478158)

### **I.1.2 ANTECEDENTES NACIONALES**

Rojas (2019) En la investigación “Implantación de la NTP-ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC ISO/IEC 27001:2014” La investigación, permitió gestionar la Confidencialidad, Integridad y Disponibilidad implementando mejores políticas en base a la Misión, Visión y Objetivos de la Organización. Este proyecto de investigación tiene un enfoque Cuantitativo, tipo Aplicada Experimental, diseño Pre-experimental, y un análisis de Pre-test y Post-test. Lo que intenta demostrar este proyecto de investigación, es cuanto contribuye la implantación de la NTP ISO/IEC 27001:2014 en la gestión de la Confidencialidad, de la Integridad y de la Disponibilidad de la base de datos del RENIEC. Las reuniones con las unidades orgánicas y con los especialistas de la Sub Gerencia de Gestión de Base de Datos, dieron como resultado la selección de los controles de la norma técnica necesarios para garantizar la seguridad de los datos, generar los indicadores y los documentos normativos, con la proyección de una posterior certificación en la ISO/IEC 27001:2013. Palabras claves: Seguridad de la Información, confidencialidad, integridad, disponibilidad

**Seclén (2016)** *Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001*: Identifica causas que restringen la implementación del sistema gestión de seguridad de la información SGSI en las entidades públicas. El estudio es de tipo cualitativo y haciendo uso de entrevistas a encargados de la implementación del SGSI en sus respectivas instituciones logró identificar las restricciones y facilidades que se encuentran en las entidades públicas al momento de implementar sistemas de seguridad de la información en el marco de la NTP-ISO/IEC 27001. Los resultados servirán para la mejora en la implementación, de las políticas de seguridad de información, de las entidades integrantes del Sistema Nacional de Informática. El estudio ayudó a encontrar un punto de equilibrio, entre el alineamiento del sistema con la estrategia de la organización, facilitando la evaluación de los factores que impiden la implementación efectiva de la NTP-ISO/IEC 27001.

**Vilca Mosquera (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*: El estudio tuvo como finalidad ~~de~~ implementar un sistema de gestión de la seguridad de la información en el marco de la norma ISO 27002, para mejorar la seguridad en cuanto al uso tecnologías de la información en la empresa Geosurvey de la ciudad de Lima en el año 2016. Se utilizó un enfoque cuantitativo, y un diseño pre experimental con una muestra no probabilística de 33 trabajadores, de las diferentes áreas de la empresa. Se aplicó un cuestionario para recoger información en las cuatro fases PDCA del ISO 27002, lo que permitió contar con un diagnóstico de la gestión de riesgos de la empresa, la elaboración de la política se seguridad y el sistema de gestión de incidentes para poder controlar y mejorar la seguridad de la información de la empresa.

### **I.1.3 ANTECEDENTES INTERNACIONALES**

**Yáñez (2017).** *Sistema de gestión de seguridad de la información para la Subsecretaría de Economía y Empresas de Menor Tamaño***.** El estudio secentra en ciclos de aprobación que permitan establecer consensos y conciliar visiones en torno a un fuerte sentimiento de trabajo en equipo para facilitar la implementación de las políticas y procedimientos de seguridad de la información. En el estudio la metodología de implementación se apoyó en el análisis y gestión de riesgos de acuerdo a la norma ISO31000. Los procesos estratégicos de la *Subsecretaría de Economía y Empresas de Menor Tamaño* fueron clasificados por prioridad según su exposición a los riesgos y su impacto. Se llegó determinar el estado actual de seguridad de la información en la entidad, la misma que es de nivel medio. La principal recomendación entregada por las auditorías fue profundizar la difusión de las políticas y procedimientos de seguridad de la información, continuar con la implementación de los restantes 70 objetivos de control de la norma ISO27001:2013 y realizar una nueva evaluación durante el 2017 del funcionamiento del SGSI, es decir se han implementado los restante objetivos de control y evaluar el grado de institucionalización de las políticas y procedimientos de seguridad de la información.

**Calderón (2015)**. *Implementación del SGSI en el área de redes de COMPUSERVER basado en la norma ISO/IEC 27001:2013*. Se presenta el diseño del SGSI para para la Red de Datos de la empresa COMPUSERVER de la Ciudad de Saravena dedicada a la prestación de servicios informáticos ISP(Proveedor de Internet) entre otros con una red inalámbrica con alcance hasta de 2 Km., aplicando la norma ISO/IEC 27001:2013, con el fin de garantizar conexiones seguras y darle confianza a los clientes que hacen uso de la misma. La finalidad del estudio fue garantizar la disponibilidad, integridad y confiabilidad de la información tanto para los clientes como para la parte administrativa de la empresa.

**Felizzola, Navarro, Lizcano, Guerrero (2018).** *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*. El presente trabajo proporciona una guía para llevar a cabo una auditoria a un SGSI implementado de manera formal o no. La guía permitió identificar las actividades de verificación del grado de implementación del SGSI, de los controles detallados y de la madurez de los procesos del SGSI basado en la norma NTE INEN-ISO/IEC 27001:2011.

[I.2. PLANTEAMIENTO DEL PROBLEMA](#_Toc435478164)

[**I.2.1.** **DESCRIPCIÓN DE LA PROBLEMÁTICA**](#_Toc435478165)

Estamos en la era de información, y por ende el activo más valioso que hoy en día poseen las diferentes empresas, es la información (Miguel, 2015), y cada vez más esta información sufre grandes amenazas en cuanto a su confidencialidad, integridad y disponibilidad, lo que ha conducido a que uno de los principales objetivos de toda organización es el aseguramiento de dicha información, así como también de los sistemas que la procesan.

La emergencia de salud mundial por la que venimos atravesando ha conducido al uso intensivo de los sistemas de información y comunicación por los individuos y las organizaciones con fines de educación, esparcimiento, trabajo y las finanzas que si bien han facilitado las actividades humanas, incrementando a su vez su vulnerabilidad ~~les~~ a las ciber amenazas al ampliar el perímetro de seguridad de las empresas a las redes domésticas.

El desconocimiento del impacto que tienen los ciberataques sobre la empresa es alto, lo que lleva a que muchas de estas no implementen las acciones necesarias para protegerse de manera efectiva su información. Una pérdida de información puede ser muy grande y recuperarse puede demandar mucho tiempo.

Para que se pueda llevar a cabo una correcta gestión de la seguridad de la información dentro de las organizaciones, es necesario implantar un sistema de gestión de la seguridad de la información que aborde esta tarea de una forma metódica y lógica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización. El incremento en el uso de los sistemas informáticos en el mundo ha ido de la mano del establecimiento de mecanismos de gestión de la seguridad y las organizaciones han empezado a implementar sistemas en base a referentes internacionales como las Normas ISO 27000.

[**I.2.2.** **DESCRIPCIÓN DEL PROBLEMA**](#_Toc435478166)

La empresa Emporium Color SAC es una empresa del rubro grafico con mas de 20 años de servicios y tiene una facturación de 250,000 soles promedio anuales atendiendo las necesidades de la poblacion limeña, y en los ultimos seis años no ha sido ajena a ciberataques que ya han causado perdida de informacion, incluso que ha sido filtrada a la competencia.

La empresa no cuenta con mecanismos de seguridad de la informacion y menos con un SGSI, para el año 2021 ya ha perdido informacion valiosa y condidencial en varias oportunidades lo cual ha generado perdidas economicas en terminos economicos y equipos, que han afectado su continuidad.

Para lograr el relanzamiento de la empresa y el cumplimiento de sus objetivos, la empresa dispone de un conjunto de normas internacionales especialmente diseñadas para impulsar el resguardo y seguridad de la información, las normas internacionalmente reconocidas son las denominadas normas ISO 27001 y 27002.

[**I.2.3.** **FORMULACIÓN DEL PROBLEMA**](#_Toc435478167)

I.2.3.1. PROBLEMA GENERAL

¿Cuál será el grado de mejora de la seguridad de la información al implementar un SGSI basado en la norma ISO27001:2020 en la empresa Emporium Color SAC?

.

[I.2.3.1. PROBLEMA ESPECÍFICO](#_Toc435478169)

* ¿Cuál será el grado de mejora en la integridad al implementar un SGSI basado en la norma ISO27001:2020 en la empresa Emporium Color SAC?
* ¿Cuál será el grado de mejora en la disponibilidad al implementar un SGSI basado en la norma ISO27001:2020 en la empresa Emporium Color SAC?
* ¿Cuál será el grado de mejora en la confidencialidad al implementar un SGSI basado en la norma ISO27001:2020 en la empresa Emporium Color SAC?

[I.3. OBJETIVOS](#_Toc435478170)

[I.3.1. OBJETIVO GENERAL](#_Toc435478171)

* Determinar el grado de mejora en la seguridad de la información al implementar un SGSI basado en la norma ISO27001 en la empresa Emporium Color SAC.

[I.3.2. OBJETIVO ESPECÍFICOS](#_Toc435478172)

* Determinar el grado de mejora en la integridad al implementar un SGSI basado en la norma ISO27001:2020 en la empresa Emporium Color SAC.
* Determinar el grado de mejora en la disponibilidad al implementar un SGSI basado en la norma ISO27001:2020 en la empresa Emporium Color SAC.
* Determinar el grado de mejora en la confidencialidad al implementar un SGSI basado en la norma ISO27001:2020 en la empresa Emporium Color SAC.

[I.4. JUSTIFICACIÓN E IMPORTANCIA](#_Toc435478173)

[I.4.1. JUSTIFICACIÓN](#_Toc435478174)

La implementación de un sistema de gestión de la seguridad de la información (SGSI) permitirá que la empresa Emporium Color SAC cuente con las políticas adecuadas sobre confidencialidad, disponibilidad e integridad de la información, de esta forma estará protegiendo su activo más valioso, la información, y además estará cumpliendo con la norma ISO 27001:2020, la cual permitirá demostrar a sus clientes que es una empresa segura y que cumple con los niveles de protección que se requiere para el manejo de la información.

[I.4.2. IMPORTANCIA](#_Toc435478175)

La importancia del presente estudio de investigación radica en la necesidad que tiene la empresa Emporium Color SAC, de proteger la información adecuadamente, cumpliendo con que la información esté disponible, sea confidencial e integra.

Los resultados del presente estudio permitirán a la empresa a tener en cuenta la importancia que se debe dar al resguardo de su información, ya que si sufriera un ataque o robo de información o manipulación de la información por personas ajenas a la empresa conllevaría a resultados adversos para la empresa misma, a tal punto de quebrar.

Se logrará mejorar las áreas relacionadas con la información en la empresa Emporium Color SAC, lo cual le permitirá que sus procesos sean más rápidos y seguros.

[I.5. ALCANCES Y LIMITACIONES](#_Toc435478176)

[I.5.1. ALCANCE](#_Toc435478177)

La investigación por su naturaleza tiene alcance aplicativo ya que la implementación del sistema se realizará en las áreas de informática, logística y administración de personal, y cubrirá todos los procesos involucrados en cada una de estas áreas en la empresa Emporium Color SA.C.

El estudio cubrirá la implementación de todos (las normas ISO 27000 tienen hasta a veces 114 objetivos de control de la norma, ejm. la ISO27001), pero cierra las principales brechas de seguridad de la información existentes en la empresa al cubrir en forma completa el primer ciclo PHCA del SGSI.

[I.5.2. LIMITACIÓN](#_Toc435478178)

Para la implementación se requiere el apoyo de gerencia, área informática, personal de logística y administración, para involucrar a todo el personal para que este disponible en los procesos de recopilación de la información, con los métodos disponibles como entrevistas, reuniones virtuales de trabajo, y procesos de aprobación de políticas, directivas y procedimientos, entre otros.

[I.5.2.1. DELIMITACION ESPACIAL](#_Toc435478179)

El SGSI se implementará en la Empresa Emporium Color SAC ubicado en la av. Garcilazo de la Vega 1282 Of 329 Cercado de Lima.

[I.5.2.2. DELIMITACION TEMPORAL](#_Toc435478180)

El tiempo estimado para la implementación de un SGSI basado en la Norma ISO 27001:2020 será en un plazo de seis meses.

II. MARCO TEÓRICO

II.1. TEORÍAS GENERALES RELACIONADAS CON EL TEMA (lo he ordenado para que luego lo pongas indice automtico)

En esta sección se presenta la teoría, que nos permite conocer la importancia de la seguridad información en las organizaciones y otros conceptos relacionados con la investigación.

**A- Riesgo**

Es el efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación respecto a lo previsto. Puede ser positivo, negativo o ambos, y puede abordar, crear o resultar en oportunidades y amenazas. Los objetivos pueden tener diferentes aspectos y categorías, y se pueden aplicar a diferentes niveles.

Con frecuencia, el riesgo se expresa en términos de fuentes de riesgo, eventos potenciales, sus consecuencias, sus [consecuencias](https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es:term:3.6)y sus probabilidades.

B. **Gestión de Riesgos.**

Las organizaciones de todos los tipos y tamaños se enfrentan a factores e influencias externas e internas que hacen incierto si lograrán sus objetivos. La gestión de riesgos comprende todas las actividades coordinadas para dirigir y controlar la organización con relación al riesgo**.**

La gestión del riesgo es iterativa y asiste a las organizaciones a establecer su estrategia, lograr sus objetivos y tomar decisiones informadas, es parte de la gobernanza y el liderazgo y es fundamental en la manera en que se gestiona la organización en todos sus niveles. Esto contribuye a la mejora de los sistemas de gestión. Considera los contextos externos e interno de la organización, incluido el comportamiento humano y los factores culturales.

Gestionar riesgo tiene como base un conjunto de principios, La organización Internacional de Normalización (ISO) ha establecido la Norma ISO 31000 en la que se descríbelos procesos para gestionar los riesgos en toda o parte de la organización, y orientan al establecimiento de sistemas de gestión de diversos tipos de riesgos como los de pérdida de seguridad en aspectos de manejo de la información.

C. definiciones básicas de la gestión de riesgos.

**C.1 Evento**

Es una ocurrencia o cambio de un conjunto particular de circunstancias. Un evento puede tener una o más ocurrencias y puede tener varias causas y varias [***consecuencias***](https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es:term:3.6).

Un evento también puede ser algo previsto que no llega a ocurrir, o algo no previsto que ocurre. Un evento puede ser una fuente de riesgo.

**C.2 Consecuencia**

Es el resultado de un [***evento***](https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es:term:3.5)que afecta a los objetivos. Una consecuencia puede ser cierta o incierta y puede tener efectos positivos o negativos, directos o indirectos sobre los objetivos.

Las consecuencias se pueden expresar de manera cualitativa o cuantitativa. Cualquier consecuencia puede incrementarse por efectos en cascada y efectos acumulativos.

**C.3 Probabilidad**

Es la posibilidad de que algo suceda. En la terminología de ***gestión del riesgo***, la palabra “probabilidad” se utiliza para indicar la posibilidad de que algo suceda, esté definida, medida o determinada objetiva o subjetivamente, cualitativa o cuantitativamente, y descrita utilizando términos generales o matemáticos (como una probabilidad matemática o una frecuencia en un periodo de tiempo determinado).

**C.4 Control**

Es la medida que mantiene y/o modifica un riesgo. Los controles incluyen, pero no se limitan a cualquier proceso, política, dispositivo, práctica u otras condiciones y/o acciones que mantengan y/o modifiquen un riesgo. Los controles no siempre pueden producir el efecto de modificación previsto o asumido.

**D. Ciberseguridad** La ciberseguridad es un término amplio que se usa de manera diferente en todo el mundo. Sin embargo, se refiere a la gestión de los riesgos de seguridad de la información cuando la información está en forma digital en computadoras, almacenamiento y redes. Muchos de los controles, métodos y técnicas de seguridad de la información se pueden aplicar para gestionar los riesgos cibernéticos.

La norma ISO / IEC 27001 proporciona requisitos para los sistemas de gestión de seguridad de la información. El enfoque de ISO / IEC 27001 está en la seguridad de la información y los riesgos asociados, dentro de entornos predominantemente bajo el control de una organización en particular. La ciberseguridad se centra en los riesgos en el ciberespacio, un entorno digital interconectado que puede extenderse más allá de los límites organizacionales y en el que las entidades comparten información, interactúan digitalmente y tienen la responsabilidad de responder a los incidentes de ciberseguridad.

**E. Sistema de Gestión de Seguridad de Información (SGSI)**

SGSI es la abreviatura que se usa para referirse al Sistema de Gestión de la Seguridad de la Información e ISMS son las siglas equivalentes en ingles a Information Security Management System. SGSI según la norma ISO 27001 consiste en preservar la confidencialidad, integridad y disponibilidad, de la información minimizando a la vez los riesgos de seguridad.

Estos pilares de la seguridad se definen como:

**Confidencialidad:** Se refiere al atributo que deben tener los datos y/o información, al encontrarse únicamente al alcance de las personas y/o entidades autorizadas, en el momento autorizado.

**Integridad:** Por medio de esta propiedad se garantiza que los datos no han sido alterados y/o destruidos de modo no autorizado, es decir se garantiza la autenticidad de la información sin importar el momento.

**Disponibilidad:** Se debe garantizar que la información se encuentra disponible para los usuarios siempre que la necesiten, en caso contrario se provocan interrupciones de servicio y con ello problemas de calidad.

**F. Estándares de Seguridad de la Información**

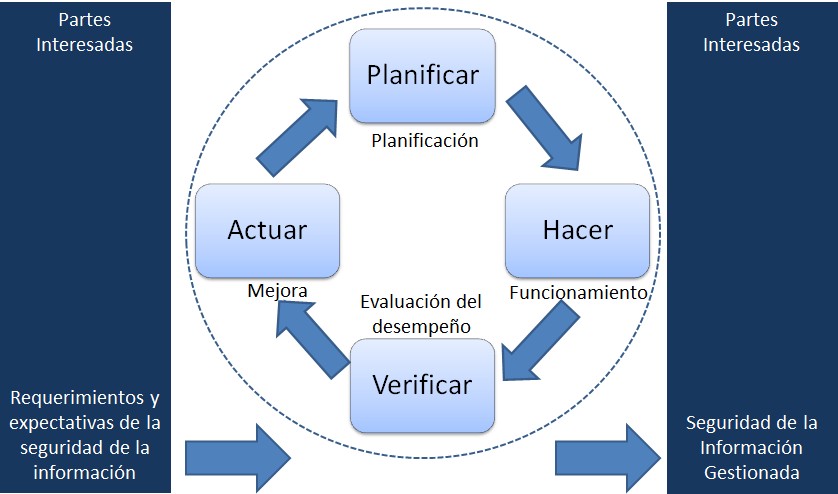
La Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) proveen una gama de estándares orientados a garantizar la conservación de la información, siendo una fuente útil sobre buenas prácticas, para distintos modelos de organización, sea grande o pequeña, privada o pública.

**ISO 27001:2013**. Este estándar fue preparado por el comité técnico conjunto ISO/IEC JTC1, Tecnología de Información, Subcomité SC 27, Técnicas de seguridad de TI. Esta norma en su segunda edición, cancela y reemplaza a la primera (ISO/IEC 27001:2005) la cuál ha sido revisada. La norma ha sido preparada para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. [ISO 27001, 2013]

**G. Ciclo PHVA**

La implementación de un sistema de gestión de acuerdo a las Normas internacionales ISO siguen el modelo de mejora comtinua de Deming (1986) la misma que contempla un proceso de cuatro etapas: "Planificar-Hacer- Verificar-Actuar'' (PHVA) también conocido como "Ciclo de Deming", que se aplica a la estructura de todos los procesos de un sistema de gestión. La figura 1 muestra el modelo, destacando a las partes interesadas y los procesos , y los resultados de seguridad de la información esperados.

Figura 1. Modelo Ciclo de Deming



**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.

**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.

**H. Documentación del sistema de gestión de seguridad de la información.**

El SGSI como mecanismo de gestión de la calidad de los procesos comprende la documentación de los procesos de control. La documentación es de diferente nivel.

Documentos de Nivel 1.- Manual de seguridad: por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

Documentos de Nivel 2.- Procedimientos: documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

Documentos de Nivel 3.- Instrucciones, checklists y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

Documentos de Nivel 4.- Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

Para la presente investigación, se diseñará un sistema de Gestión en el marco de los componentes de la Norma ISO 27001:2020 para implementar el Sistema de Gestión de Seguridad de información, en la empresa peruana Emporium Color SAC.

**Norma ISO/IEC 27001:**

III. HIPÓTESIS Y OPERACIONALIZACIÓN DE LAS VARIABLES

III.1. HIPÓTESIS GENERAL

La implementación de un SGSI basado en la norma ISO27001:2020 mejorará significativamente la seguridad de la información en el area de recursos humanos de la empresa Emporium Color SAC

III.2. HIPÓTESIS ESPECÍFICAS

H1: La implementación de un SGSI basado en la norma ISO27001:2020 mejorará significativamente la integridad de la seguridad de la informacion en la empresa Emporium Color SAC

H2: La implementación de un SGSI basado en la norma ISO27001:2020 mejorará significativamente la disponibilidad de la seguridad de la informacion en la empresa Emporium Color SAC

H3: La implementación de un SGSI basado en la norma ISO27001:2020 mejorará significativamente la confidencialidad de la seguridad de la informacion en la empresa Emporium Color SAC

III.3. VARIABLES

III.3.1. VARIABLES INDEPENDIENTE

**X:** Sistema de Gestión de la Seguridad de la Información.

III.3.3. VARIABLE DEPENDIENTE

**Y:** Seguridad en la empresa Emporium Color SAC.

**III.3.4** **OPERACIONALIDAD DE LAS VARIABLES**

|  |  |  |
| --- | --- | --- |
| VARIABLE | DIMENSIONES | INDICADORES |
| Seguridad de la Información |  |  |
| Mejora de la integridad de la información. | Número o porcentaje de accesos y/o cambios no autorizados a los datos de producción |
| Mejora de la disponibilidad de la información. | Porcentaje de tiempo durante el cual un sistema está disponible para el usuario  Registro de incidentes |
| Mejora de la confidencialidad de la información | Número de información confidencial divulgada  Control de préstamos de equipos.  Control de ingreso a la red.  Cifrado de información. |

**III.4. TIPO**

La investigación es de tipo cuantitativa (Hernández et al, 2010).

**III.5. POBLACIÓN**

Con respeto a la población que comprende el estudio se considera al número de personas y procesos informáticos administrativo y operativo de la empresa.

El cuadro 1 muestra al personal involucrado en procesos informativos en situación de vulnerabilidad.

|  |  |
| --- | --- |
| Área | Cantidad |
| Gerencia General | 1 |
| Recursos Humanos | 2 |
| Colaboradores | 20 |

**III.6. UNIVERSO SOCIAL**

**III.7. MUESTRA**

El estudio considera una sola empresa con sus procesos administrativos que generan y producen información para fines internos y externos.

**IV. MÉTODO**

**IV.1. DISEÑO DE INVESTIGACIÓN**

El estudio seguirá el proceso cíclico PHVA, mediante el cual la organización

puede implementar y gestionar un Sistema de Gestión de Seguridad de la

Información.

**IV.2. ESTRATEGIA DE PRUEBA DE HIPÓTESIS**

La prueba de hipótesis se realizará analizando los cuadros de control

estadísticos de procesos que se controlan con el sistema. Se utilizarán

herramientas estadísticas para los análisis comparativos de las variables e

indicadores controlados.

**IV.3. TÉCNICAS DE RECOLECCIÓN DE DATOS**

La técnica de recolección de datos es el Cuestionario (Muños, 2003).

**IV.3.1. INSTRUMENTOS DE RECOLECCIÓN DE DATOS**

En este estudio de investigación se utilizará la encuesta para la cual se elaborará un cuestionario como principal técnica de recolección de datos, con el propósito de recolectar toda la información de los trabajadores de las diferentes áreas de la empresa EMPORIUN COLOR SAC, relevante con respecto a la seguridad de la información de dicha empresa.

**V. CRONOGRAMA**

El cronograma del estudio está orientado por las etapas de la metodología de implantación de SGSI proporcionado por Deming (1,986) como estrategia de mejora continua en las organizaciones.

Gráfico

Descripción generada automáticamente

**VI. PRESUPUESTO**

|  |  |  |  |
| --- | --- | --- | --- |
| ***COSTO DEL PROYECTO*** |  |  |  |
| |  | | --- | |  | | ***CONCEPTO*** | |  | MONTO S/. |  |
| ***1. Personal*** | Consultor | 3500.00 |  |
| ***2. Materiales*** | Útiles de Oficina | 1100.00 |  |
| ***3. Equipos de Computo*** | Pcs | 2000.00 |  |
| ***4. Servicios*** | Internet, Luz, Agua, Copias | 900.00 |  |
| ***5. Otros Costos*** |  | 350.00 |  |
| ***6. Reserva de contingencia*** |  | 600.00 |  |
| ***7. Reserva de Gestión*** |  | 500.00 |  |
| ***TOTAL PRESUPUESTO*** |  | 7960.00 |  |

**División de los Costos**

|  |  |  |
| --- | --- | --- |
| ***COSTOS VARIABLES*** |  |  |
| ***CONCEPTO*** |  | MONTO S/. |
| ***1. Personal*** | Consultor  Y Personal de Apoyo | 4500.00 |
| ***TOTAL COSTO VARIABLE*** |  | 4500.00 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Costos Fijos** | | | |
| Concepto | | S/. |  |
| **2. Materiales** | Utiles de Oficina | 1100 |  |
| **3. Equipos de computo** | Servidor, PC | 2000 |  |
| **4. Servicios** | Luz, Agua, Internet, Copias | 900 |  |
| **5. Otros costos** | Refrigerio, transporte | 700 |  |
| **6. Reserva de contingencia** |  | 600 |  |
| **7. Reserva de gestion** |  | 500 |  |
| **Costos Fijo** | | 5800 |  |

**VII. REFERENCIAS BIBLIOGRÁFICAS**

Calderón Sanchez, (2015)Implementación del SGSI en el área de redes de COMPUSERVER basado en la norma ISO/IEC 27001:2013

Miguel Pérez, (2015) Protección de datos y seguridad de la información. Cuarta ed. España: Ra-Ma .

Hernández et al, (2010). Metodología de la investigación. Sexta ed. España: McGraw-Hill Interamericana; 2014.

IEC 31010, *Risk management — Risk assessment techniques Standard.*

ISO (2020). Standard ISO 27001:2020.

Seclén A. Javier A. (2016) Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001:

Vilca M. Ehitel C. (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*.

Yáñez C. Nelson A. (2017). *Sistema de gestión de seguridad de la información para la Subsecretaría de Economía y Empresas de Menor Tamaño*.

Muñoz A., T.G.(2003) El Cuestionario como instrumento de investigación /evaluación. Tesis. España: Universitario Santa Ana, Sociología.

**ANEXOS**

**VII.1 ANEXO A: MATRIZ DE CONSISTENCIA**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Problemas** | **Objetivos** | **Hipótesis** | **Variables** | **Metodología** |
| **Problema Principal** | **Objetivo General** | **Hipótesis General** |  |  |
| ¿Cuál será el grado de mejora de la seguridad al implementar un SGSI basado en la norma ISO27001:2020 en la empresa Emporium Color SAC? | Determinar el grado de mejora en la seguridad de la información al implementar un SGSI basado en la norma ISO27001:2020 en la empresa Emporium Color SAC | La implementación de un SGSI basado en la norma ISO27001:2020 mejorará significativamente la seguridad de la información en el area de recursos humanos de la empresa Emporium Color SAC | VARIABLES INDEPENDIENTE  **X:** Sistema de Gestión de la Seguridad de la Información  VARIABLE DEPENDIENTE  **Y:** Seguridad en la empresa Emporium Color SAC. | Ciclo de mejora continua  PHVA |



**VII.2. ANEXO B: DEFINICIÓN DE TERMINOS**

**Activo de información:** Aquello que es de mucho valor y que contiene información vital de la empresa que debe ser protegida.

**Amenaza:** Es la causa potencial de un daño a un activo de información.

**Análisis de riesgos:** Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

**Causa:** Razón por la cual el riesgo sucede.

**Ciclo de Deming:** Modelo mejora continua para la implementación de un sistema de mejora continua.

**Confidencialidad:** Propiedad que determina que la información no esté disponible a personas no autorizados

**Controles:** Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.

**Control:** Es lo que permite garantizar que cada aspecto, que se valoró con un cierto riesgo, queda cubierto y auditable.

**Disponibilidad**: Propiedad de determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas.

**Impacto:** Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.

**Indicadores**: Unidad de medida, que permite evaluar el rendimiento de los procesos internos de la organización

**Incidente de seguridad de la información:** Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.

**Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.

**Probabilidad de ocurrencia:** Posibilidad de que se presente una situación o evento específico.

PHVA:

**Riesgo:** Grado de exposición de un activo que permite la materialización de una amenaza.

**SGSI:** Siglas del Sistema de Gestión de Seguridad de la Información.

**Sistema de Gestión de Seguridad de la información SGSI:** Permite establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001.

**Vulnerabilidad:** Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. Se caracteriza por ausencia en controles de seguridad que permite ser explotada.