UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

FACULTAD DE CIENCIAS E INGENIERÍA

CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS:

"Planificar la Implementación del Sistema de Gestión de Seguridad de la Información Basado en la Norma ISO/IEC 27001:2013 para la Integridad, Confidencialidad y Disponibilidad de su Información en la Empresa Automatisoft S.A.C."

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS E INFORMÁTICA

AUTOR:

Bach. Lucas Asencio, Jesús Lorenzo

ASESOR:

Mg. Hidalgo Palomino, Fernando Guillermo

ID ORCID: 0000-0002-9155-445X

DNI 06844769

LIMA- PERÚ

2023

UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

Facultad de Ciencias e Ingeniería

INFORME DE SIMILITUD Nº0021-2022-FCI-UPCI-T

A	:	**Decano(e) de la Facultad de Ciencias e Ingeniería**
DE	:	**Operador del Programa TURNITIN**
ASUNTO	:	Informe de Evaluación de Similitud de Tesis
FECHA	:	sábado, 17 de diciembre del 2022

Tengo el agrado de dirigirme a Ud. a fin de informar lo siguiente:

1. Mediante el uso del programa informático TURNITIN (con las configuraciones de excluir citas, excluir bibliografía y excluir oraciones con cadenas menores a 15 palabras) se ha analizado el trabajo de tesis titulado: **"PLANIFICAR LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA LA INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD DE SU INFORMACIÓN EN LA EMPRESA AUTOMATISOFT S.A.C."**, presentada por el(los) Br(s):

    - **Bach. Lucas Asencio, Jesús Lorenzo**

2. El resultado de la evaluación indica que el documento en mención tiene un INDICE DE SIMILITUD DE 17% (cumpliendo con el art. 35 del Reglamento de Grado de Bachiller y Titulo Profesional UPCI aprobado con Resolución N° 373-2019-UPCI-R de fecha 22/08/2019)

3. Al término del análisis, se concluye que PUEDE(N) CONTINUAR su trámite.

Sin otro particular quedo de usted.

Atentamente

Firma y Sello del Operador del Turnitin
Mg. Hidalgo Palomino Fernando Guillermo

PD:
Se adjunta:
- Resultado de similitud

DEDICATORIA

Esta presente tesis está hecha y dedicada a mi familia por creer siempre en mí e inculcarme buenos valores. En cada parte de mi vida profesional, todo el agradecimiento para ellos.

AGRADECIMIENTO

A mi familia y amigos muy cercanos por haberme facilitado ser la persona que soy actualmente; mis éxitos se los debo a ellos. Este nuevo logro es gran parte gracias a ustedes; he logrado concluir con éxito. Muchas gracias a aquellos seres queridos que siempre aguardo en mi alma.

A mi asesor, el Mg. Fernando Hidalgo, porque sin su guía no hubiese podido culminar con éxito esta investigación.

PRESENTACIÓN

Señores Miembros del Jurado:

De conformidad y en cumplimiento de los requisitos estipulados en el reglamento de grados y títulos de la Universidad Peruana de Ciencias e Informática y el reglamento interno de la Escuela profesional de Ciencias e Ingeniería, ponemos a vuestra disposición el presente Trabajo de Suficiencia Profesional titulado: "**Planificar la Implementación del Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para la Integridad, Confidencialidad y Disponibilidad de su información en la empresa Automatisoft S.A.C**" para obtener el Título Profesional de Ingeniero de Sistemas e Informática mediante la modalidad de Tesis.

El contenido de la presente tesis ha sido desarrollado tomando como marco de referencia los lineamientos establecidos y los conocimientos adquiridos durante nuestra formación profesional, consulta de fuentes bibliográficas e información obtenida de la Gerencia de la Empresa Automatisoft SAC.

Lucas Asencio, Jesús Lorenzo

ÍNDICE

INDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

La investigación está enfocada en la planificación de la “implementación de la seguridad basada en la norma ISO/IEC 27001:2013”, para proteger “la seguridad de la información” en la organización Automatisoft SAC. El recojo de datos e información fue con el diseñó de un instrumento en base al “análisis de brechas de la ISO 27001”; la cual luego de su análisis se pudo determinar la problemática de la empresa, calibrar sus defectos e incrementar la confianza en la “seguridad de la información”. Dichos resultados permitieron indicar que la planificación de la “implementación de la norma ISO/IEC 27001:2013” daría buenos resultados., Con los procesos de mejora de las “normativas de protección de datos se incrementó el control de la información”; el plan de proyecto de implementación, minimizará los “riesgos de la información”. Finalmente, con la implementación de herramientas tecnológicas se minimizarán las amenazas y vulnerabilidades, de esta manera se minimizará el peligro de la “confidencialidad, integridad y disponibilidad de la información”.

Palabras clave: Seguridad de la información, Confidencialidad, Integridad, Disponibilidad

ABSTRACT

The investigation is focused on planning the "implementation of security based on the ISO/IEC 27001:2013 standard", to protect "information security" in the Automatisoft SAC organization. The collection of data and information was with the design of an instrument based on the "gap analysis of ISO 27001"; which after its analysis it was possible to determine the problems of the company, calibrate its defects and increase confidence in the "information security". These results made it possible to indicate that the planning of the "implementation of the ISO/IEC 27001:2013 standard" would give good results. With the processes of improvement of the "data protection regulations, the control of information was increased"; the implementation project plan, will minimize “information risks”. Finally, with the implementation of technological tools, threats and vulnerabilities will be minimized, in this way the danger of "confidentiality, integrity and availability of information" will be minimized.

Keywords: Information security, Confidentiality, Integrity, Availability

I. INTRODUCCION

La presente investigación se realizó como una forma de aplicar a una “situación actual el manejo de la tecnología de la información y comunicación afín de superar las deficiencias presentadas en la empresa Automatisoft SAC. fruto de la fragilidad existente respecto a la “Seguridad de la Información”.

El principal problema es la insuficiencia de un “sistema de gestión de seguridad de la información” ya que actualmente se quiere avalar y/o “garantizar la confidencialidad, integridad y disponibilidad de su información”, afín de mantener la confianza de sus usuarios. Actualmente no hay soporte a sus procesos con el uso de tecnologías de la información y realizan mucho trabajo manual, se maneja datos personales de nuestros clientes y del personal administrativo y es de suma importancia “asegurar la confidencialidad, integridad y disponibilidad de la información”, ya que es indispensable minimizar los riesgos de información de la empresa y como finalidad de la empresa es “establecer políticas, procedimientos y controles” que relacionan a los servicios o productos de la empresa y planificar la “implementación de un sistema de gestión de seguridad de la información”.

Ante este problema nos propusimos “garantizar la integridad, confidencialidad y disponibilidad de su información, a través de la Planificación de un Sistema de Gestión de la Seguridad de la Información ISO/IEC 27001:2013”, para “garantizar la integridad, confidencialidad y disponibilidad de su información”. La población y la muestra seleccionada fueron las 22 personas asignados en las diferentes áreas de la empresa, se utilizó una encuesta para recopilar la información de los colaboradores, información

básicamente relacionada con la “tecnología de la información y comunicación”. Respecto a la delimitación fue situada en la ciudad de Lima en las instalaciones de la empresa y el estudio se aplicó el mes de abril del 2022, al concluir el análisis de la indagación fue victorioso ya que en esta planificación el principal objetivo es la meta para alcanzar los fines que se buscaban y cumplir los objetivos, existen buenos resultados de diferentes empresas reconocidas que utilizan esta metodología del SGSI donde establecen políticas y recursos en lista de metas de negocio, minimiza los riesgos, examina mediante un orden definido, documentado y prestigioso, que se revisa y mejora constantemente.

1.1. Realidad problemática

Durante muchos años pasados, las personas continuamente encontramos la forma de conservar información, ya sea como una simple actividad o por querer conservar perpetuamente el recuerdo de algún hecho o suceso valioso. Por todas las partes del mundo podemos hallar información que pasa de generación en generación distorsionándose hasta a veces que se pierde con el pasar del tiempo, pero no toda la información se considera como un simple recuerdo, podemos encontrar información rodeando en nuestro pasado que cuentan cómo era aquella vez o hasta información de mucha ayuda para todo aquel se encuentra en la sociedad. Sin duda alguna la información nos formemos como personas en esta sociedad, gracias a ella sabemos nuestro origen y de dónde venimos, de igual forma, toda formación de una organización ya sea pequeña necesita saber su situación actual el pasado y a donde ver a futuro en donde mejor se ocupe y desarrolle su talento a ser mejor.

> El 16 de septiembre de 2019, los ecuatorianos empezaron la semana con la noticia de que la información de casi toda la población estaba siendo filtrada. Se estima que la información estaba en un servidor en Miami que no tenía los requisitos de seguridad establecidos y que era administrado por Novaestrat, una empresa ecuatoriana de marketing y análisis digital. Fueron alrededor de 18 GB de datos, como nombres, información financiera, estado civil y números de identidad.
>
> El tema abrió el debate sobre la necesidad de una ley. Ecuador, Venezuela y Bolivia son los tres únicos países de la región que no tienen una

normativa al respecto, según dijo el ministro de Telecomunicaciones, Andrés Michelena. Días después, entregó una propuesta a la Asamblea Nacional, que incluye un sistema para mitigar riesgos, un régimen de sanciones, un Registro Nacional de Protección de Datos Personales, entidades certificadoras, entre otros temas. etc. (Publicay, 2019)

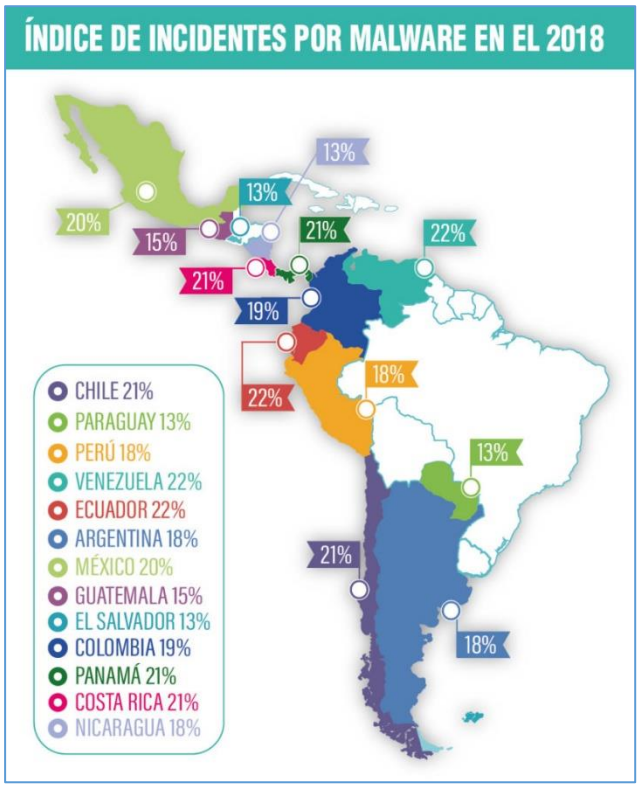


Figura 1 Índice de los incidentes por malware en el 2018

Fuente: Publicay

Como se puede apreciar en la figura anterior las personas maliciosas cibernéticas valen de cualquier falla que pueda encontrar en los sistemas para bloquear, dañar o acceder a la información y de esta forma aprovecharse de las vulnerabilidades del sistema.

Una en cuenta global de seguridad de la información en el país de argentina nos dice que más allá del costo es una necesidad de solución integral nos manifiesta lo siguiente:

Hoy en día, la mayoría de los negocios son digitales y el software se está convirtiendo en la columna vertebral de las operaciones, productos y servicios. En este escenario la mayoría de las organizaciones, ya sean digitales o tradicionales, están explorando nuevas oportunidades para

crear valor y ventajas competitivas, incorporando la ciberseguridad y privacidad con estrategias de negocios digitales. En este sentido, las empresas ofrecen servicios digitales complementarios a la venta de un producto o servicio. Los clientes en la actualidad esperan productos seguros y que protejan los datos sensibles. El 59% de los encuestados a nivel global manifestó, que la digitalización de sus ecosistemas empresariales ha impactado en el gasto en la ciberseguridad. Las empresas que integren la ciberseguridad con estrategias digitales estarán mejor preparadas para actuar en este nuevo paradigma de negocios. (PWC, 2017)

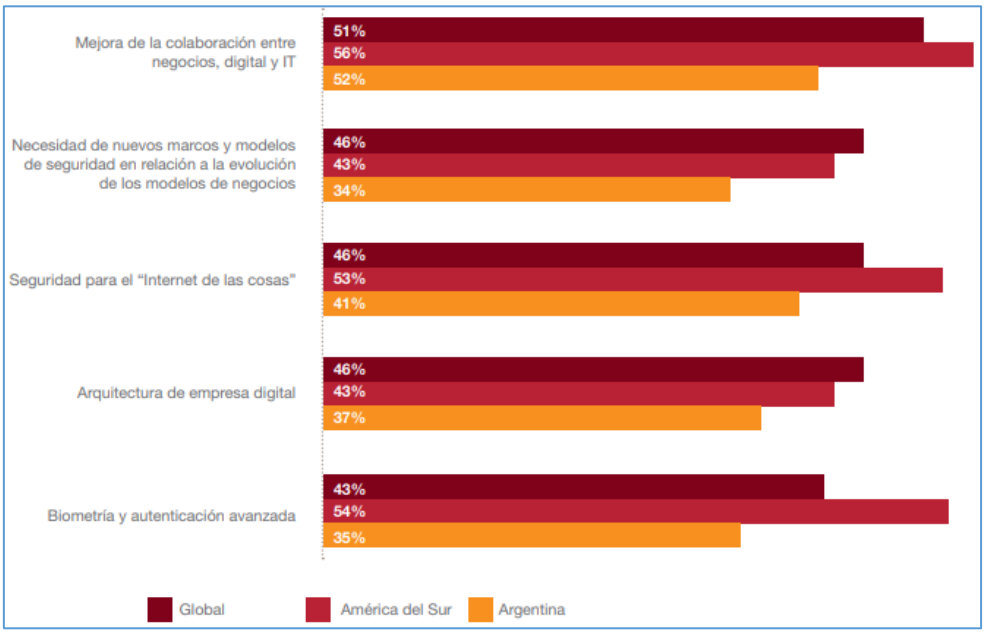


Figura 2 Encuesta Global de Seguridad de la Información 2017
Fuente: www.pwc.com/ar

En el Perú las empresas e instituciones públicas aun no planifican en su totalidad incorporar un ”Sistema de gestión de seguridad de la información la cual consistiría por un conjunto de políticas, procedimientos y líneas” junto a los actividades y buenos recursos asociados que serían administradas conjuntamente por una empresa, aseguraría proteger sus activos más importantes.

Según la encuesta de EY, solo el 36% de las compañías a nivel global incluye a la ciberseguridad en sus iniciativas empresariales desde la etapa de planificación, mientras que a nivel local este porcentaje es de 27%. De la misma manera, el 59% de los encuestados a nivel global y regional afirmó que la relación entre la ciberseguridad y las líneas de negocios en

> sus organizaciones es inexistente o neutral. Ello también ocurre en el Perú, donde dicha cifra corresponde al 51% de los encuestados. Paradójicamente, el 80% de las empresas encuestadas aseguran que la prevención de crisis y el manejo de riesgos en las organizaciones logran impulsar un aumento de presupuesto en el área. (Cama, 2020)

Por otro lado, la "importancia de la planificación de seguridad de la información" es muy importante ya que es la orientación sistemática para crear, implementar, manejar, monitorear, examinar, mantener y mejorar la seguridad de la información de una empresa pública y/o privada y poder lograr objetivos y servicios, es así donde nos preguntamos realmente el Perú está preparado para quizás los ciberataques el diario gestión dice lo siguiente:

> de acuerdo a la Encuesta Global de Seguridad de la Información 2019-2020 de EY, solo el 27% de empresas en el Perú incluye la ciberseguridad desde la etapa de planificación en sus nuevas iniciativas empresariales; mientras que un 51% sostiene que la relación entre la ciberseguridad y sus líneas de negocio es inexistente o neutral. (Gestion.pe, 2020)

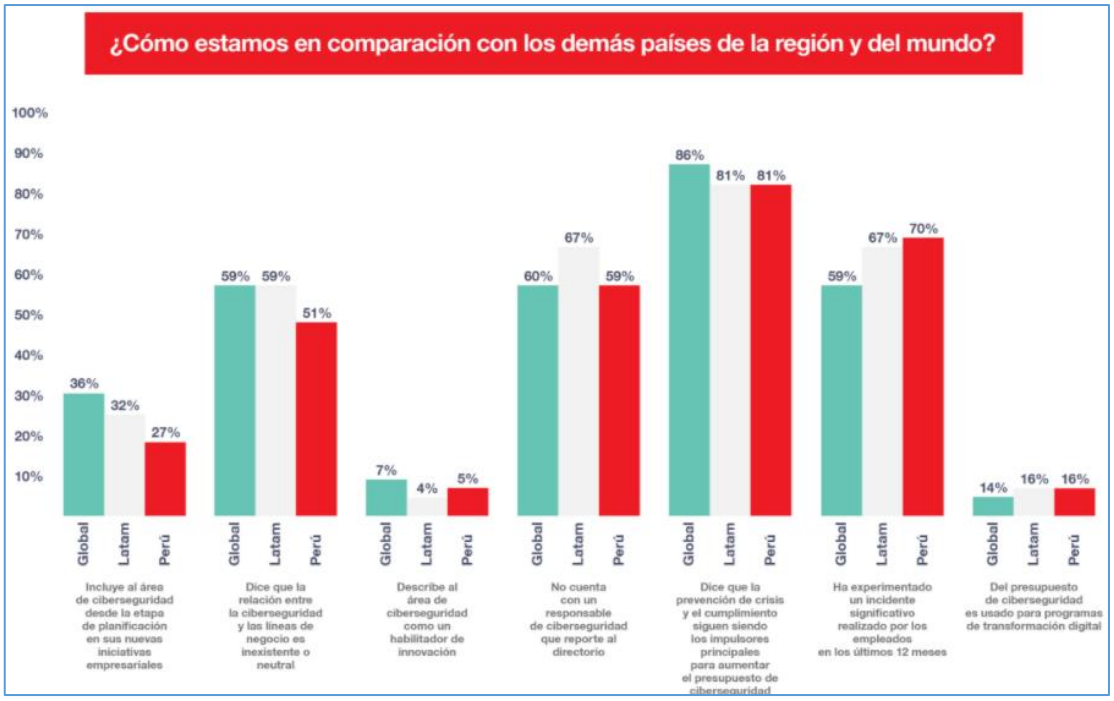


Figura 3 "Encuesta global de seguridad de la información 2019-2020 de EY"
Fuente: www.gestion.pe

Como podemos ver en el cuadro anterior según esta encuentra global de los riesgos que existen en un directorio es que el 48% cree que los ataques por los ciberdelincuentes y robo de información tendrán un impacto moderado en su empresa u organización, la cual es muy lamentable que en Perú las empresas u organizaciones solo el 27% tomen sus planes a futuro de sistema de gestión de seguridad de la información.

1.2. Planteamiento del problema

Delimitación del Problema

Espacial

La ubicación donde se realizó la investigación, recojo de datos y la planificación de "implementación de un Sistema de Gestión de la Seguridad de la Información" es en los ambientes de la empresa Automatisoft SAC, ubicada en Av. Canadá Urb. Parral, Comas-Lima.

Temporal

El recojo de la data para la investigación se realizó el mes de abril del año 2022 en la empresa Automatisoft SAC.

1.2.1. Problema General

¿En qué medida el SGSI ayudará a garantizar la "integridad, confidencialidad y disponibilidad de la información en la empresa"?

1.2.2. Problemas Específicos

a) ¿Cómo adecuar los procesos a las "normativas de protección de datos", para mejorar la "integridad de la información en la empresa"?
b) ¿Cómo implementar las políticas de "seguridad de la información" para mejorar la "confidencialidad de la información en la empresa"?
c) ¿Cómo implementar las "herramientas tecnológicas" para mejorar la "disponibilidad de la información en la empresa"?

1.3. Hipótesis de la investigación

1.3.1. Hipótesis General

Si se planifica un “Sistema de Gestión de la Seguridad de la Información ISO/IEC 27001:2013”, entonces garantizará la “integridad, confidencialidad y disponibilidad de su información”.

1.3.2. Hipótesis Específicas

a) Si se adecuar los procesos a las “normativas de protección de datos” entonces se mejora la “integridad de la información en la empresa”.
b) Si se implementan las “políticas de seguridad de la información” entonces se mejora la “confidencialidad de la información en la empresa”.
c) Si se implementan las “herramientas tecnológicas” entonces se mejora la “disponibilidad de la información en la empresa”.

1.4. Objetivos de la investigación

1.4.1. Objetivo General

Planificar un “Sistema de Gestión de la Seguridad de la Información ISO/IEC 27001:2013”, para garantizar la integridad, confidencialidad y disponibilidad de su información.

1.4.2. Objetivos Específicos

a) Adecuar los procesos a las “normativas de protección de datos”, para mejorar la “integridad de la información en la empresa”.
b) Implementar las “políticas de seguridad de la información” para mejorar la “confidencialidad de la información en la empresa”.
c) Implementar las “herramientas tecnológicas” para mejorar la “disponibilidad de la información en la empresa”.

1.5. Variables, dimensiones e indicadores

1.5.1. Variables Independientes

- ✓ Sistema de gestión de la seguridad de la información
- ✓ normativas de protección de datos
- ✓ políticas de seguridad de la información
- ✓ herramientas tecnológicas

1.5.2. Variables Dependientes

- ✓ Integridad
- ✓ Confidencialidad
- ✓ Disponibilidad

1.5.3. Dimensiones

- ✓ “normativas de protección de datos”
- ✓ “políticas de seguridad de la información”
- ✓ “herramientas tecnológicas”

1.5.4. Indicadores de las Variables Dependientes

- ✓ Nivel de integridad de datos
- ✓ Nivel de confidencialidad de la información
- ✓ Nivel de disponibilidad de la información

1.6. Justificación del estudio

Justificación Teórica

La planificación de desarrollo del documento del “Sistema de Gestión de la Seguridad de la Información (SGSI)” permitirá implementar las políticas de “seguridad de la información” para así poder minimizar los riesgos de perdida de información en la empresa.

Se identificarán eventuales amenazas y agresiones desfavorables para la empresa, podemos tomar buenas decisiones de protección de la información, para no perder ni dañar nuestros recursos de información.

Justificación Práctica

De acuerdo al presente estudio se podrá utilizar el "Sistema de Gestión de la seguridad de la información (SGSI)" como escenario para planificar las actividades relacionadas con el uso de "tecnologías de la información y comunicación en la Empresa".

Se describe una metodología de "Sistema de Gestión de la seguridad de la información (SGSI)" en la empresa para tener la "protección de la información para confidencialidad, integridad y disponibilidad", de esta manera se garantizará la confiabilidad de alcanzar y mantener los niveles de seguridad.

Justificación Legal

Se basa en estándares internacionales aceptados para la práctica de "norma ISI/IEC 27001 Sistema de gestión de Seguridad de la Información", es adecuada para pequeña, mediana o grande organización, en cualquier parte del mundo o sector. La norma esta basada en la protección de la información ya que es confidencial y puede ser en diferentes rubros como en finanzas, sanidad, sector público y tecnología de la información.

Justificación Económica

De acuerdo al presente estudio que da como resultado la justificación económica de la planificación del Sistema de Información, se establecieron los presentes recursos para desarrollar, implantar, y mantener en acción el sistema programado, donde se evaluará y se manifestará el equilibrio existente entre los costos específicos del sistema y los beneficios, se permitirá observar de una manera más precisa las facilidades de la planificación de "sistema de gestión de seguridad de la información".

Importancia del estudio

El "Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la norma ISO 27001" nos ofrece protección ante muchas amenazas en donde nos pueda poner en peligro nuestra empresa, en la actualidad todo tipo de empresa se enfrenta diariamente a una gran cantidad de riesgos e

inseguridad que proviene de medios diferentes y estos pueden afectar a un negocio y a las herramientas relacionadas con las TIC.

Contando con estos riesgos es de vital importancia aplicar el (SGSI) bajo los objetivos que tengan fijados la empresa garantizando de esta forma la "confidencialidad, integridad y disponibilidad", para así poder proteger la información; seguidamente tener cuidado y el progreso de las normas de seguridad y así aumente el prestigio y la imagen de la organización.

La planificación de "Seguridad de la Información" será de consideración para modernizar la seguridad y defender la "confidencialidad, integridad y disponibilidad de los activos de la información de la empresa", para de esta forma reducir los riesgos y perder información ante cualquier tipo de amenaza. Es necesario proteger la "información" sensible de la empresa, de no hacerlo, se generarían costos cuando se produzcan incidentes con el parque informático y por eso es muy importante que los riesgos de información sean gestionados.

La medición y control de los procesos de la información es una solución importante para tener un control seguido de lo que está pasando en la empresa y mejorar lo que no está yendo bien, "todos los datos que arrojan una medición es información valiosa y así poder tomar decisiones adecuadas en la empresa" y alcanzar sus objetivos, los resultados se obtienen en cualquier momento o actividad que se realiza.

Actualmente existen riesgos en el uso de las TI en las empresas por daños causados accidentalmente, por los empleados o debido a intentos intencionados de intrusos que quieren acceder a los datos de la empresa para sacar provecho de esta información, si sucede esto la empresa puede quedar seriamente dañada, ya que en la actualidad el valor de la información es grande, es por eso que es muy importante una estrategia y herramientas que permite evaluar y reconocer todos los riesgos asociados con el uso de las TI, con el único objetivo de poder minimizar inseguridades

Normalmente, el "activo más importante en la empresa es la información" y tiene que ser protegida, es un factor importante para su continuidad y logro de sus objetivos, para esto existen metodologías, prácticas y procedimientos que buscan proteger la información como activo valioso, que es conjunto de "estándares de la ISO/IEC 27000".

Actualmente no existe forma de reducir los riesgo a cero (0), sólo el equipo que se encuentra a cargo debe minimizar el riesgo, utilizando para ello un control interno, es muy importante tener las medidas de seguridad activas que son utilizadas para minimizar el riesgo tanto antes del incidente y durante el incidente, por esta razón es importante estar preparados para prevenir todo tipo de ataques o desastres, si se planifica la gestión de riesgos adecuadamente permitirá la continuidad del negocio tras sufrir alguna pérdida o daño.

La principal importancia de la norma ISO 27001 es analizar y gestionar dichos riesgos basados en los procesos, ya que se evalúa y controla nuestra empresa bajo este motivo se debe realizar un "análisis y gestión de riesgos en los sistemas de información" de forma realista orientada a los objetivos de nuestra empresa.

En la empresa es importante minimizar los riesgos empleando medidas de control, para eso es importante los certificados que amparan a una empresa por eso las empresas de bienes y servicios son cada vez más las empresas certificadas con la "norma ISO-27001", porque promueve la "protección de la información".

Automatisoft SAC. sabe lo importante que es "identificar y proteger sus activos de información", impidiendo su divulgación, deterioro, adulteración y el uso no autorizado de toda información relacionada con sus "empleados, clientes, precios de sus productos, manuales bases de conocimiento, códigos fuente, estrategia, gestión, y sobre todo mejorar continuamente el Sistema de Gestión de la Seguridad de la Información".

1.7. Antecedentes nacionales e internacionales

1.2.1 Antecedentes internacionales

Según (Ibáñez, 2015) “Diseño de un Sistema de Gestión de Seguridad de la Información en el área de Sistemas de la empresa RYMCOS S.A bajo la norma ISO/IEC 27001:2013” , indica que la “Integridad de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorías”. Las fallas de integridad pueden estar dadas por incoherencias en el “hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema”. (Ibáñez, 2015)

- “La Disponibilidad de la Información debe de estar siempre disponible para así poder ser procesada por el personal de la empresa”, pero debe de estar correctamente almacenada tanto como hardware o software y se deben respetar los formatos para su recuperación de información.
- La Integridad de la Información no debe ser modificado, salvo que sea realizada por personal autorizado, y “necesariamente sea registrada para posteriores controles o auditorías, una simple falla puede ser por el hardware, software, virus informáticos y/o modificación por personas que no son de la empresa”.
- El “Control sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso a la misma”. (Ibáñez, 2015)

Según (Gonzalez, 2016) “Diseño de un sistema de Gestión de Seguridad de la Información-SGSI bajo la norma ISO/IEC 27001:2013 para la empresa en línea financiera de la ciudad de Cali-Colombia, indica que se ha tratado de arrojar alguna luz sobre los tipos de motivaciones y los resultados que las empresas deben tratar a lo largo de las fases del diseño de un SGSI. Se coincide en que la identificación de “los activos de la empresa y la valoración de los riesgos” sobre ellos fue una de las tareas más complejas y demandantes, quizás uno de los aspectos que influyó fue la falta de experiencia del equipo. (Gonzalez, 2016)

- Se tiene que mejorar el nivel de seguridad en la empresa para así poder tener ventajas de competencias ya que indica que fue parte de su motivación, y así poder ver que la empresa expresa su satisfacción por los resultados, ver como el personal para reforzar las etapas de "seguridad de la información".
- Toda organización quiere garantizar la continuidad de su negocio y de esta manera identifica la información como activos y/o bienes más relevantes ya que es un factor determinante para lograr sus propósitos por lo tanto considera primordial establecer un ámbito para resguardar la información de una manera idónea.
- Al planificar un "sistema de gestión de seguridad de la información" se busca iniciar un proyecto de seguridad y posteriormente buscar la certificación con empresas top del país.

Asimismo, (Angarita Leiva & Bautista Bohorquez, 2014) en su tesis titulada "Diseño de un Sistema de Gestión de la Seguridad de la Información ISO27001 para la Alcaldía de Floridablanca Y", indica que:

> Hoy en día muchas empresas consideran la información como el activo más
>
> importante, es por esto que se buscan medios para su protección, la norma ISO 27001 da soporta para el proceso de gestión de la información. Debido a los grandes volúmenes de información que maneja una empresa, esta se encuentra expuesta a riesgos que pueden afectar la integridad, disponibilidad y confidencialidad de la información.
>
> La norma ISO 27001 presenta un modelo estándar para establecer, implementar, realizar seguimiento y revisión, mantenimiento y mejora de un sistema de gestión de seguridad de la información documentado en el contexto de los riesgos globales de cualquier organización, especificando la incorporación de "controles de seguridad de acuerdo a las características de la organización".
>
> En el desarrollo de este proyecto se realizó el "diseño de un SGSI para la Alcaldía de Floridablanca" fundamentado en los principales procesos de

la entidad, posteriormente se realiza el proceso de gestión del proyecto basado en la guía PMBOK.

1.2.2 Antecedentes nacionales

Según (Álvarez, 2015) "Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013"**,** indica que el "SGSI se encuentra estrechamente relacionado con la gestión de riesgos de una institución, el análisis que realiza no está sesgado a los activos o controles tecnológicos que la institución pueda tener o requiera". Es por este motivo que el equipo que tenga la responsabilidad de mantener el SGSI debería "trabajar en conjunto con el área de Control Interno apoyándose en el mismo durante el análisis de los riesgos de la institución dado que dicha área debería tener una visión holística de los riesgos que se presentan en la misma". (Álvarez, 2015)

- Es muy importante que se defina un personal en la empresa para resguardar y proteger la información, para que se encargue de la planificación de implementación del SGSI y por supuesto contar con el apoyo y comprensión del gerente general para puedan servir en bandeja toda la información posible de todas las áreas que pertenecen a la empresa.
- Cuando se culmine dicho proyecto el personal debe tener reuniones para la capacitación sobre lo importante que es la información con la cual ellos realizan su trabajo, a la vez deben tener en cuenta la ejecución de los procedimientos para asegurar la información.
- Existe falencias en la institución para que genere este proyecto de SGSI institucional, el cual debería ser gestionado para la mejora de la institución, ya que están en riesgo de amenazas y pérdida de información.

Según (Zacarias, 2017) "Modelo de la seguridad de la información basado en la ISO/IEC 27001:2013 para mitigar los riesgos de los activos de información en la central de operaciones policiales de la región policial Junín" Tesis para optar por el

Título de Ingeniero de Sistemas e informática de la Universidad Continental, Perú, indica que la implementación de un modelo de seguridad de la información basada en la norma ISO/IEC 27001:2013 influye positivamente en la mitigación de las amenazas de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, ya que el nivel de mitigación de amenazas pre implementación fue de 1,30 que representa el 26%, y el nivel de mitigación de amenazas después de la implementación fue de 4,94 que representa el 99%, lo que significa un aumento de 3,64 que representa el 75% en el nivel de mitigación de amenazas de los activos de información. (Zacarias, 2017)

- Se logró incrementar los conocimientos del personal policial, teniendo como resultado personal comprometido y no sólo involucrado con la seguridad de la información policial.

- Se puso en compromiso al personal policial de las regiones en temas de seguridad de la información para que así no puedan generar pérdidas, también para su mayor control la mitigación de las amenazas.

Según (Salinas, 2015) "Diseño de un Sistema de Gestión de Seguridad de Información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013" Tesis para optar por el Título de Ingeniera informática de la Pontificia Universidad Católica, Perú, indica que la alta dirección tiene un papel muy importante en el Sistema de Gestión de Seguridad de Información, pues además de tomar las decisiones estratégicas más importantes de la organización, su compromiso será fundamental para llevar a cabo el SGSI e imprescindible para la implementación de los controles. (Salinas, 2015)

- Se debe tener en cuenta realizar políticas y procesos de seguridad de información para así poder tener una importante y efectiva administración de información en los sistemas que convenzan al pedido y necesidad del negocio para así poder preservar la integridad.
- Las empresas tienen fuga de información tanto externas como internas donde las amenazas a donde se ven descubiertas en estas

circunstancias es de vital importancia tener procedimientos de seguridad de información y de esta forma garantizar el complimiento de dichas políticas de la empresa para de esta forma monitorear la información.

- La empresa debe difundir estas políticas, para dar a todo el personal que está laborando como también estas personas son responsables de conocer y cumplir con todo lo que se especifica.

1.8. Marco teórico

1.8.1. Tecnología de Información y Comunicación:

La tecnología de información y comunicación (TIC) es muy importante en la organización ya que automatiza los procesos internos y externos de la empresa tanto así que es un punto importante para que el trabajo sea más productivo, por otro lado existen datos que se comparten en la red las cuales son privadas o de mucha importancia, una falta de seguridad puede llegar a tener pérdidas económicas, su imagen estaría dañada y perdería confianza de sus clientes por eso es de crucial relevancia para la seguridad de la información.

> Es indudable que las tecnologías de información y comunicación se han convertido en una herramienta indispensable para el desarrollo de las empresas, no obstante, a los grandes beneficios que aporta la tecnología a las empresas, existe una amenaza latente a la implantación de un equipamiento tecnológico en una empresa y son los ataques cibernéticos. (Palacios, 2015)

Por eso las empresas de hoy en día implementan herramientas que ayudan a alcanzar sus objetivos, al usar las TIC en las áreas de la empresa da un ahorro de costos y tiempo, ayudando a su vez a una mejor gestión de información.

Requerir de la tecnología de información y comunicación en los procesos de la empresa, pero se ha considerado ciertos factores importantes que viene a ser las amenazas, vulnerabilidad y riesgo.

> El incremento exponencial del uso de las nuevas tecnologías en las organizaciones, y la cada vez mayor dependencia de los sistemas de información, hacen que los procesos de negocio de una empresa dependen en gran medida de la disponibilidad de sus sistemas de información, y de la integridad y confidencialidad de los datos que éstos gestionan. (Pozo, Tecnologia de Informacion y Comunicacion, 2016)

1.8.2. La Seguridad De La Información

La seguridad de la información tiene la finalidad reunir técnicas y medidas para controlar la seguridad de la información de la empresa.

> La seguridad de la información tiene una finalidad que es asegurar los sistemas de información como los accesos, el uso, divulgación, interrupción y a la destrucción no autorizada.
>
> La Seguridad de la información es el conjunto de medidas preventivas y relativas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. (Orellana, Seguridad de la Informacion, 2014)

Importancia de la Seguridad de la Información

Toda información debe ser confidencial y protegida, en toda empresa esta agrupada con un alto valor que esta pueda tener en cada organización, es fundamental determinar que su uso está establecido en tecnología informática y puede ser vulnerada.

> Puede ser divulgada, mal utilizada, ser robada, borrada o saboteada. Esto afecta su disponibilidad y la pone en riesgo. La información es poder, y según las posibilidades estratégicas que ofrece tener acceso a cierta información, ésta se clasifica como:

Crítica: Es indispensable para la operación de la empresa.
Valiosa: Es un activo de la empresa y muy valioso.
Sensible: Debe de ser conocida por las personas autorizadas.

Existen dos palabras muy importantes que son riesgo y seguridad:
Riesgo: Es la materialización de vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el impacto negativo que ocasione a las operaciones de negocio.
Seguridad: Es una forma de protección contra los riesgos.
La seguridad de la información comprende diversos aspectos entre ellos la disponibilidad, comunicación, identificación de problemas, análisis de riesgos, la integridad, confidencialidad, recuperación de los riesgos. (Orellana, Seguridad de la Informacion)

"La seguridad de la información comprende diversos aspectos entre ellos la disponibilidad, comunicación, identificación de problemas, análisis de riesgos, la integridad, confidencialidad, recuperación de los riesgos." (Alvarez, 2008)

Objetivo de Seguridad de la Información

El objetivo primordial es implantar la administración de seguridad de información siendo la parte más fundamental en las actividades de la empresa, se debe gestionar diferentes tareas de poner en marcha la seguridad, exigencia de funciones y responsabilidades.

Los términos seguridad de la información, seguridad informática y garantía de la información son usados frecuentemente como sinónimos porque todos ellos persiguen una misma finalidad al proteger la confidencialidad, integridad y disponibilidad de la información.

Sin embargo, no son exactamente lo mismo existiendo algunas diferencias sutiles. Estas diferencias radican principalmente en el enfoque, las metodologías utilizadas, y las zonas de concentración.

> Además, la seguridad de la información involucra la implementación de estrategias que cubran los procesos en donde la información es el activo primordial. Estas estrategias deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.
>
> La seguridad de la información incumbe a gobiernos, entidades militares, instituciones financieras, los hospitales y las empresas privadas con información confidencial sobre sus empleados, clientes, productos, investigación y su situación financiera. (Alvarez, 2008)

Aspectos Fundamentales en la Seguridad de la Información.

La seguridad de la información se conforma por tres pilares que son:

Integridad:

"Propiedad de salvaguardar la exactitud y estado completo de los activos. La información solamente podrá ser modificada por el personal que se designe autorizado para realizarlo". (BETANCUR, 2016)

Confidencialidad:

"Propiedad que determina que la información no esté disponible ni se revelada a individuos, entidades o procesos no autorizados. Lo cual conlleva a determinar que la información sólo podrá ser consultada para el personal autorizado para esto." (BETANCUR, 2016)

Disponibilidad:

“Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada”. La consulta de información debe ser en tiempo real y al momento que ésta precisamente se necesite. (BETANCUR, 2016) (Ver Figura 01)

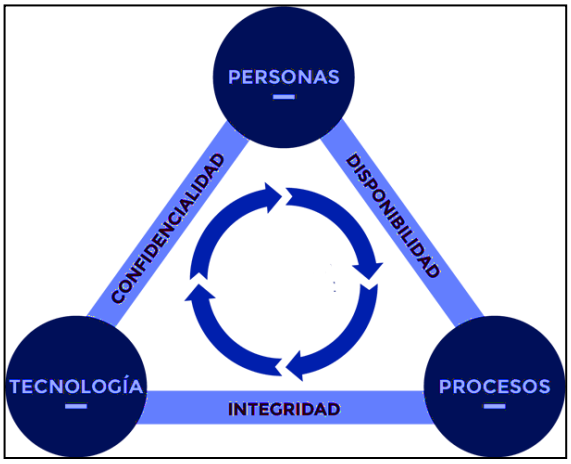


Figura 4 Seguridad de la información
Fuente: Elaboración propia

1.8.3. Sistema De Gestión De La Seguridad De La Información (SGSI)

El SGSI es una abreviatura de Sistema de Gestión de la Seguridad de la Información. En el inglés, las siglas es Información Security Management System.

> Información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración. (iso27000, 2012)

Es por eso que la información es importantes en todas las empresas y por eso se requiere ser protegida frente a amenazas que puedan poner en peligro la continuidad de negocio, las empresas almacenan su información en equipos informáticos que se conoce como sistemas de información pero estos sistemas están

en peligro de riesgos e inseguridades tanto dentro de la empresa como fuera por ejemplo riesgos físicos (accesos no autorizados a la información y catástrofes naturales, tales como fuego, inundaciones, terremotos, vandalismo, etc.) lógicos (virus, ataques de denegación de servicio, etc.).

Por otro lado, es de suma importancia actuar con procedimientos y políticas para tener una empresa segura y dar una mejor imagen a los clientes.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir (iso27000, 2012)(Ver Figura 5)

Figura 5 Esquema del Sistema de Gestión de Seguridad de Información ISO 27001
Fuente: Normas.ISO.com

¿Qué se entiende por SGSI?

La abreviatura significa Sistema de Gestión de la Seguridad de la Información donde mediante la implantación conoce dichos riesgos, los asume, minimiza, transfiere o controla mediante un sistema definido, documentado y sobre todo se revisa y actualiza continuamente.

> En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración. (Ver Figura 06)

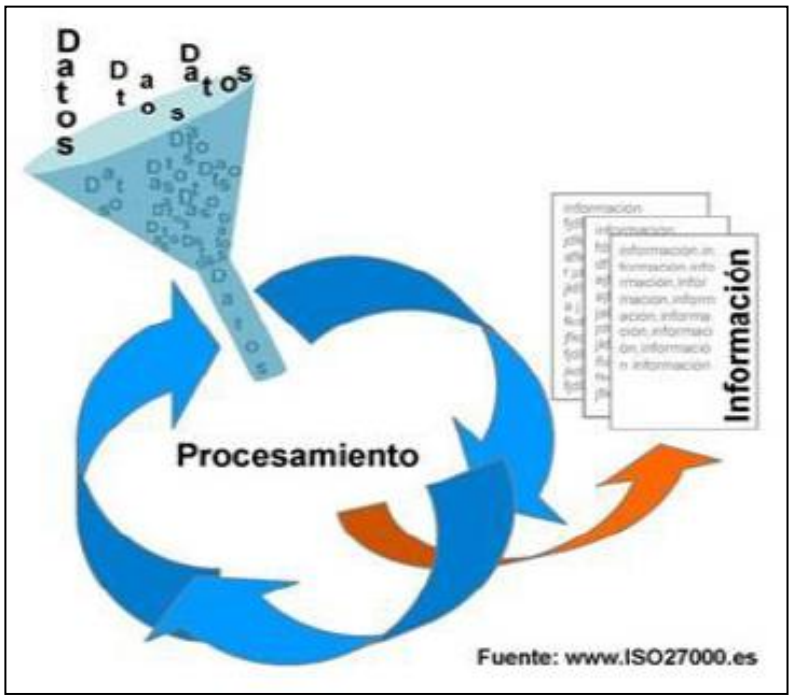


Figura 6 Estructura que referencia un SGSI
Fuente: Iso27000.es

Que Incluye un SGSI:

Tal y como se sabe de la gestión de la calidad de acuerdo con la ISO 9001, siempre se manifestó siempre se demostró la documentación del sistema como una pirámide de cuatro niveles, de acuerdo a esto es factible trasladar esta referencia a un sistema de gestión de la seguridad de la información de acuerdo a la ISO 27001 de la siguiente: (Ver Figura 7)

Figura 7 Pirámide de los niveles de un SGSI
Fuente: Iso27000.es

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. (iso27000, 2012)

Gestión de la Seguridad de la Información:

ISO/IEC 27001 adopta además el modelo PDCS (o de Demming). PDCA son siglas de (Plan-Do-Check-Act) y el modelo se aplica para estructurar todos los procesos del SGSI, así como en muchos otros entornos y marcos generales al modelo PDCS aplicadas al SGSI son:

- Planificar: Establecer políticas, objetivos, procesos y procedimientos que se relevante para la gestión de riesgos y para la mejorar la seguridad de la información, con el objetivo de conseguir resultados satisfactorios con respecto a los objetivos.
- Hacer: implementar y operar los elementos del SGSI: política, controles, procesos y procedimientos.
- Controlar: medir el rendimiento de los procesos contra los objetivos del SGSI, notificando los resultados a la dirección para su revisión.
- Actuar: basándose en las revisiones, realizar acciones preventivas y correctivas para alcanzar la mejora continua del SGSI.

El ciclo de estas cuatro fases nunca termina, todas las actividades deben ser implementadas cíclicamente para mantener la eficacia del SGSI. (Orueta, 2014)

Especificando a lo anterior (Ver Figura 8).

Figura 8 Plan do check act 27001
Fuente: djekova.info

Fase de planificación:

Implementación de gestión de servicios.

Facilitar los procesos de gestión de servicios.

Los cambios en los procesos de gestión de servicios.

Las mejoras en los procesos de gestión de servicios.

Nuevos servicios.

Fase de Hacer:

La asignación de fondos y presupuestos.

Asignación de funciones y responsabilidades.

Documentación y mantenimiento de políticas, procedimientos y definiciones para cada proceso.

Identificar y gestionar los riesgos para el servicio.

Gestionar equipos.

Servicio de atención al cliente y operaciones.

Informe de progreso y coordinación de procesos de gestión de servicios.

Fase de Verificar:

Los logros respecto de los objetivos del servicio definido.

La satisfacción de los clientes.

La utilización de recursos.

Las tendencias.

Las no conformidades.

Todos los resultados de los análisis que pueden generar una mejora.

Fase de Actuar:

El objetivo que persigue esta fase es mejorar la eficacia de las prestaciones y la gestión de los servicios. Se debe realizar una política, que sea pública, para mejorar el servicio. Cualquier falta de conformidad con la norma ISO 27001 tiene que ser remediada. Todas las funciones y las responsabilidades que sean necesarias para realizar las actividades de mejora del servicio se tienen que definir de forma clara. Todas las mejoras de los servicios que propone la organización deben pasar por ser revisadas, registradas, priorizadas y autorizadas. Se puede utilizar un plan de mejora del servicio para poder controlar la actividad. (Iso27001:2013, 2015)

Lista de Verificación de la Norma ISO 27001:

La ISO Organización Internacional de Normalización publicó la norma ISO 27001 para establecer, supervisar y mejorar la gestión de seguridad de la información en las organizaciones. La lista de verificación la norma ISO 27001 ayuda a las empresas desarrollar y mantener un programa de seguridad que impida las fugas de información y otras violaciones de seguridad de la información. La lista cubre una amplia gama de medidas de control legales, físicas y técnicas que van desde la clasificación sensitiva de los datos a la entrada de restricción de las personas con malas intenciones.

Política de seguridad:

La lista de verificación de la norma ISO 27001 debe analizar si una empresa tiene un sistema de información del programa de seguridad que está aprobado por la dirección y se comunica a todos los empleados de la compañía. La administración debe manifestar su compromiso con la seguridad y el enfoque de la organización para la gestión de seguridad de la información. La política debe revisarse a intervalos. Esto es para asegurar la continua estabilidad, suficiencia y efectividad de la tecnología de la información del sistema. Todas estas cuestiones deben abordarse en la lista.

Coordinación de seguridad:

Las actividades de seguridad de la información deben ser coordinadas por representantes de diversos departamentos de la empresa. La necesidad de la organización de acuerdos de confidencialidad o no divulgación debe estar claramente definida y revisada con regularidad. Los empleados deben entender que la violación del acuerdo de no divulgación tiene sus consecuencias. Por ejemplo, un analista de inteligencia de EE.UU. fue detenido en Irak en junio de 2010 por filtrar un video clasificado de las tropas disparando contra civiles. Bradley Manning filtró el vídeo a los denunciantes del sitio web Wikileaks. El liderazgo organizacional también debe identificar los riesgos a los servicios de información antes de conceder acceso a terceros. Las medidas de control deben ser implementadas antes de concederse el acceso. La información debe ser clasificada también en términos de su valor y la sensibilidad de la empresa.

Protección contra la entrada maliciosa:

Necesitas tener la capacidad para detectar y prevenir intentos maliciosos internos o externos para acceder a tu información. Si se trata de un negocio en línea, por ejemplo, los clientes deben ser capaces de comprar de forma segura la mercancía. El programa que transfiere datos de un ordenador a otro debe ser capaz de funcionar efectivamente por su cuenta. Con el fin de evitar poner en peligro información valiosa, la red de una organización debe ser

adecuadamente gestionada y controlada para evitar cualquier amenaza y mantener la seguridad de los sistemas y aplicaciones en toda la red de la organización. Sin ese mecanismo, la información de la organización está en riesgo de abuso por parte de delincuentes que se benefician con datos en línea. (Kosutic, 2013)

Como Implementar la ISO 27001:

La ISO 27001 es un estándar de calidad general desarrollado por ISO (International Standards Organization - Organización Internacional de Estándares) enfocado en la seguridad de la información. La seguridad de la información varía por organización; sin embargo, en general incluye todas las formas de datos, comunicaciones, conversaciones, grabaciones, documentos e incluso fotografías. Incluye todo desde correos electrónicos a faxes y conversaciones telefónicas. La implementación del ISO 27001 es utilizada específicamente para obtener certificación para el sistema de administración de seguridad de la información (ISMS o Information Security Management System) de una organización. El ISMS define el estándar para toda la organización, proveyendo objetivos marcados por un plan accionable para lograr y mejorar sobre ellos de acuerdo al estándar de la administración.

Instrucciones:

Establece objetivos: Cada sistema de administración de seguridad de la información debería tener un conjunto de ISMS hacia el cual trabajar. Los objetivos exactos dependen de la organización y el entorno regulador de la industria en la que la industria trabaja. Por ejemplo, un banco que trabaje con clientes con un alto patrimonio neto necesitará establecer objetivos más rigurosos en relación a la seguridad de la información que una compañía de ganado.

Define el alcance y los límites de los objetivos de tu ISMS: Para cada objetivo, asigna un valor que te ayude a medir el alcance de su éxito. Por ejemplo, si quieres reducir el fraude en relación a la seguridad de la

información, puedes establecer un objetivo que incluya una reducción del fraude de un 5 al 10 por ciento por año. Además, puede que quieras establecer diferentes objetivos para diferentes departamentos dentro de la organización. Por ejemplo, el personal de ventas puede tener una tasa más alta de fraudes que otras funciones como administración o soporte. Definir el alcance y establecer los límites mejorará el éxito de la implementación.

Identifica la mejor manera de abordar la evaluación de riesgos: Los riesgos para el ISO 27001 son eventos que pueden comprometer la seguridad de la información de una organización. Por ejemplo, tu compañía puede querer realizar una auditoría o contabilización interna para evaluar riesgos regularmente en conjunto con sus tareas normales. Estos grupos tienden a trabajar objetivamente con toda la organización y usualmente ayudan a establecer y monitorear controles internos.

Identifica los mayores riesgos de seguridad en tu organización: Luego de evaluar los riesgos, tendrás una lista de eventos de seguridad. Prioriza estos riesgos para el equipo de implementación.

Evalúa tu entorno de seguridad de la información actual y mide la amenaza de cada riesgo de seguridad: Cada riesgo de seguridad también debe estar conectado a un objetivo específico para medir el desempeño a lo largo del tiempo.

Crea un plan para tratar y mejorar sobre estos riesgos: Cada riesgo debe tener una lista de acciones y opciones que pueda ser seguida por el equipo de evaluación de riesgos. Las acciones deben proveer una forma clara de alcanzar los objetivos, y también controles definidos para poder monitorear los riesgos. Para una organización grande, separa el plan en diferentes secciones. Por ejemplo, puede que quieras empezar con un piloto y luego desplegar el plan a la organización.

Obtén aprobación de la gerencia: La gerencia debe formalmente ratificar el plan antes de implementarlo. Pide hacer un anuncio general del plan a la

> organización. También provee una línea de tiempo para que la implementación se apruebe y disemine a lo largo de la organización.
>
> **Comienza la implementación:** Realiza auditorías internas con regularidad y reporta los resultados a la gerencia con la misma regularidad. Actualiza tus objetivos y planes de seguridad de manera apropiada. (Alvarez S. c., 2013)

BMIS (Business Model for Information Security)

Este es considerado como un enfoque integral y orientado a negocios de gestión de seguridad de la información. Implica en un lenguaje sumamente común para la protección de la información en una empresa permitiendo a los profesionales investigar la seguridad minuciosamente de los sistemas, de esta forma se verá que la seguridad se puede gestionar de manera integral.

"El BMIS usa un enfoque orientado al negocio para gestionar la seguridad de la información, basándose en conceptos fundamentales desarrollados por el Instituto." (Isaca, Modelo de Negocios para la Seguridad de la Información., 2013)

> El modelo utiliza el pensamiento sistémico con el propósito de aclarar relaciones complejas dentro de la empresa y, por ende, gestionar la seguridad más efectivamente. Los elementos y las interconexiones dinámicas que conforman la base del modelo establecen los límites de un programa de seguridad de la información y configuran cómo funciona y reacciona al cambio interno y externo. (Isaca, Modelo de Negocios para la Seguridad de la Información., 2013)

De las cuales tenemos 4 modelos y 6 interconexiones: (Ver figura 06)

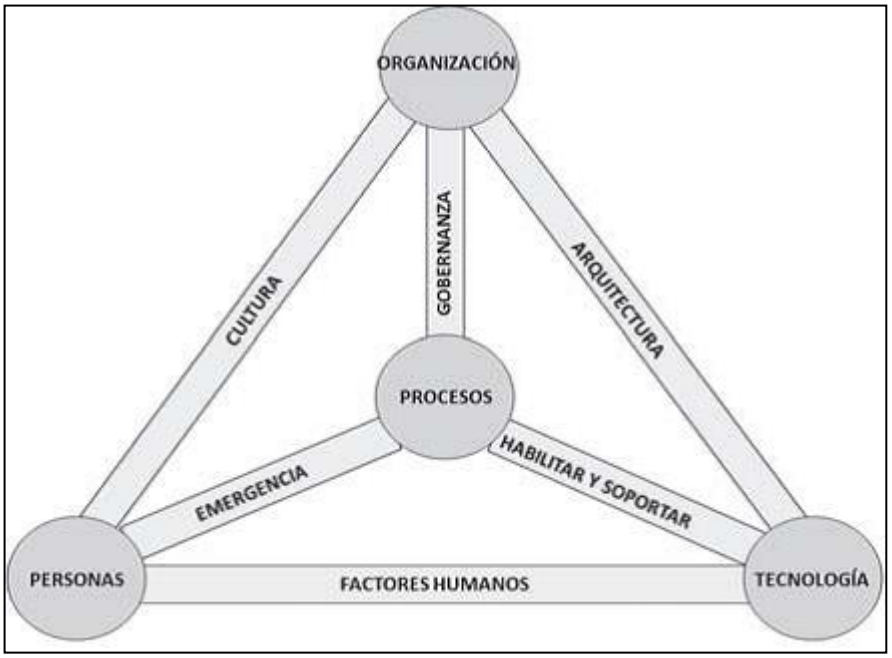


Figura 9 Esquema del Modelo de negocio para la Seguridad de Información.
Fuente: Isaca 2013

Modelos:

- Organización
- Personas
- Procesos
- Tecnología

Interconexiones:

- Gobierno
- Arquitectura
- Cultura
- Surgimiento
- Habilitación y soporte
- Factores humanos

1.8.4. Planificación De Seguridad De La Información:

Lo primero que se debe hacer es saber los objetivos de la empresa en la seguridad de la información para poder así alcanzarlos, la empresa deberá conservar esta información documentada sobre estos objetivos.

¿Qué se debe considerar para la planificación del SGSI?

Existe un procedimiento que detalla paso a paso de cómo implementar y son factores que resultan importantes:

*** Respaldo y patrocinio**

El principal elemento que se debe tener en cuenta antes de la implementación es el respaldo de la alta dirección con relación a las actividades de seguridad de la información, de manera específica con la iniciativa de comenzar a operar con un SGSI.

La idea puede surgir en cualquier nivel dentro de la organización, pero requiere del patrocinio de los **niveles jerárquicos más elevados.**

El soporte y compromiso de la alta dirección refleja un esfuerzo compuesto, no solo un proyecto aislado y administrado por un subordinado. Del mismo modo, resulta útil la formación de estructuras dentro de las organizaciones, que permitan la **colaboración y cooperación** de los representantes de las diferentes partes con roles y funciones relevantes.

En este sentido, una buena práctica consiste en desarrollar la estructura adecuada para la toma de decisiones en torno al sistema de gestión, a través de la conformación de un **foro o comité** de seguridad, que permita llevar a la práctica lo que se ha denominado gobierno de seguridad de la información, es decir, todas aquellas responsabilidades y acciones que ejerce la alta dirección en cuanto a la seguridad.

*** Estructura para la toma de decisiones**

Para fines de las actividades de gestión de la seguridad, el comité es un **grupo interdisciplinario** encargado de tomar decisiones referentes a la implementación y operación del sistema de gestión, así como mantener el control administrativo del marco de trabajo de seguridad.

El objetivo es integrar a miembros de la dirección (incluyendo al CEO), para proporcionar una visión de negocio a las decisiones que competen a este comité, así como la generación de consensos en torno a las necesidades e iniciativas de seguridad, **alineadas con los objetivos de la organización.**

De manera general, puede agrupar las necesidades y puntos de vista de los integrantes de la organización como usuarios, administradores, auditores, especialistas en seguridad y de otras áreas como la parte jurídica, recursos humanos, TI o de gestión de riesgos.

Otros miembros que pueden conformar este foro son el responsable del sistema de gestión, jefes de áreas funcionales de la organización y un rol de auditor para una evaluación objetiva e imparcial del SGSI.

*** Análisis de brecha (GAP)**

El análisis de brechas o GAP Analysis es un **estudio preliminar** que permite conocer la forma en la que se desempeña una organización en materia de seguridad de la información, con relación a las mejores prácticas reconocidas en la industria; para ello se utilizan criterios establecidos en **normas o estándares.**

El análisis establece la diferencia entre el desempeño actual y el deseado. Aunque este análisis es aplicable a cualquier estándar certificable, normalmente se lleva a cabo para nuevos esquemas de certificación, que son los que más dudas generan en las organizaciones, debido a su novedad.

*** Análisis de Impacto al Negocio (BIA)**

El análisis de impacto al negocio (BIA por las siglas en inglés) es un elemento utilizado para estimar la afectación que podría padecer una organización como resultado de la ocurrencia de algún incidente o un desastre.

Tiene dos objetivos principales, el primero de ellos consiste en proveer una base para **identificar los procesos críticos** para la operación de una organización y la priorización de ese conjunto de procesos, siguiendo el criterio de cuanto mayor sea el impacto, mayor será la prioridad.

El BIA está directamente relacionado con los aquellos procesos que poseen un tiempo crítico para su operación, porque si bien, todos los procesos sujetos a un tiempo crítico son de misión crítica, no todos los procesos de misión crítica están relacionados con un tiempo crítico para su ejecución.

*** Recursos: tiempo, dinero y personal**

Con base en los resultados del análisis de brecha y del impacto al negocio, es posible estimar elementos necesarios para la implementación de ISO/IEC 27001. En caso de tratarse del primer ciclo de operación, el momento sugerido para la implementación de la norma es un periodo con una carga de trabajo menor, que permita una planificación adecuada o, en caso de ser necesario, contratar nuevo personal enfocado a esta tarea.

Es recomendable que el tiempo dedicado al sistema de gestión no exceda un periodo mayor a un año antes de que se cumpla su primer ciclo, esto debido a distintas razones como los continuos cambios en los riesgos, cambio en las prioridades de la dirección con respecto a la protección de activos, aparición de nuevas amenazas, entre otras.

El análisis también permite **estimar los recursos financieros** necesarios para alcanzar el estado deseado en materia de seguridad de la información, conforme a ISO 27001. Se debe tener en mente que durante la implementación se deberán destinar recursos para implementar controles técnicos, físicos o administrativos, conforme a los resultados de una evaluación de riesgos.

Por otro lado, la organización debe contar con **personal idóneo** para llevar a cabo las actividades técnicas y administrativas relacionadas con el sistema de gestión, por lo que puede optar por capacitar a miembros de la organización o contratar los servicios de personal externo que colabore para los objetivos planteados en el SGSI.

*** Revisión de los estándares de seguridad**

Otra actividad útil previa de la implementación del SGSI está relacionada con conocer el contenido y la estructura del estándar ISO/IEC 27001, así como de los estándares que conforman la serie 27000. De manera específica, una tarea necesaria consiste en conocer ISO/IEC 27000, que permite conocer los principios en los cuales se fundamenta la implementación de un SGSI.

ISO/IEC 27000 contiene el glosario de todos los términos utilizados en la serie 27000, un resumen general de esta familia de estándares, así como una introducción al SGSI. Este estándar adquiere mayor relevancia, ya que se convierte en la única referencia normativa de la nueva versión de ISO/IEC 27001. (Mendoza, Consideraciones previas a la implementación del SGSI, 2017)

1.8.5. El Gobierno de la Seguridad de la Información:

Es un término genérico que trata de agrupar todas las actividades que el responsable de TI debe llevar a cabo para cumplir el objetivo fundamental de las Tecnologías de la Información, que es la generación de valor para el negocio.

” Así, se han desarrollado en el mercado guías de buenas prácticas, marcos de trabajo, estándares y directrices que pueden ayudar al responsable IT a establecer procesos de Gobierno IT acordes con la organización”. (SecureIT, 2016)

La presente investigación es para planificar la implementación, desarrollo y gestión en la seguridad de la información para la cual existen los dominios siguientes:

- ✓ Alineamiento de TI con el negocio: En esta fase se creó la base para promover la alineación estratégica, para lo cual se empezó conociendo el contexto actual de la organización e identificando y definiendo los objetivos 26 de TI, los cuales se van a alinear con los objetivos del negocio. (Bermejo, 2012)
- ✓ Evaluación del rendimiento y la capacidad: En esta fase se verificó la capacidad actual del área de TI, para lo que se identifica y evalúa la madurez de los procesos críticos de TI en base a los objetivos de negocio propuesto para TI, además se realizó un análisis FODA de los recursos de TI (información, personal, aplicaciones e infraestructura) y por último se encuesto y analizó la matriz de acordada del gobierno de TI. (Bermejo, 2012)
- ✓ Planificación estratégica de TI: En esta fase se propuso los indicadores para medir el cumplimiento de los objetivos definidos y la eficiencia de los procesos críticos, también se definieron las acciones estratégicas que deben de cubrir la eliminación o reducción de brechas identificadas en la fase 2, y el desarrollo de mando de control integral para. (Bermejo, 2012)
- ✓ Planificación táctica de TI: En esta fase se formularon los planes de acción para alcanzar las estrategias del negocio y de TI, por lo se crearon: proyectos estratégicos, estrategias para la adquisición de los recursos de TI, para la capacitación del personal y para el outsourcing de los servicios de TI. (Bermejo, 2012)
- ✓ Socialización y cierre: En esta fase el resultado del planeamiento es validado, por lo que se revisa y valida los resultados que se acordaron para el gobierno de TI, para luego comunicar los resultados a todos los interesados de la organización y poder seguir con el compromiso de los involucrados para seguir con la ejecución del proyecto. (Bermejo, 2012) (Ver Figura 10)

Figura 10 Áreas de enfoque del gobierno TI.
Fuente: Isaca - Cobit

1.8.6. COBIT 5.0

COBIT (Control Objectives Control Objectives for Information and related Technology) son buenas prácticas para el control de la información.

> La información es actualmente uno de los recursos más valiosos dentro de una organización ya que se crea, usa, retiene, distribuye y destruye, todo con el fin de alcanzar las metas establecidas, es aquí donde el marco de los objetivos de control para la información y Tecnologías relacionadas. (Medina, 2017)

Familia de productos Cobit 5 (Ver figura 11)

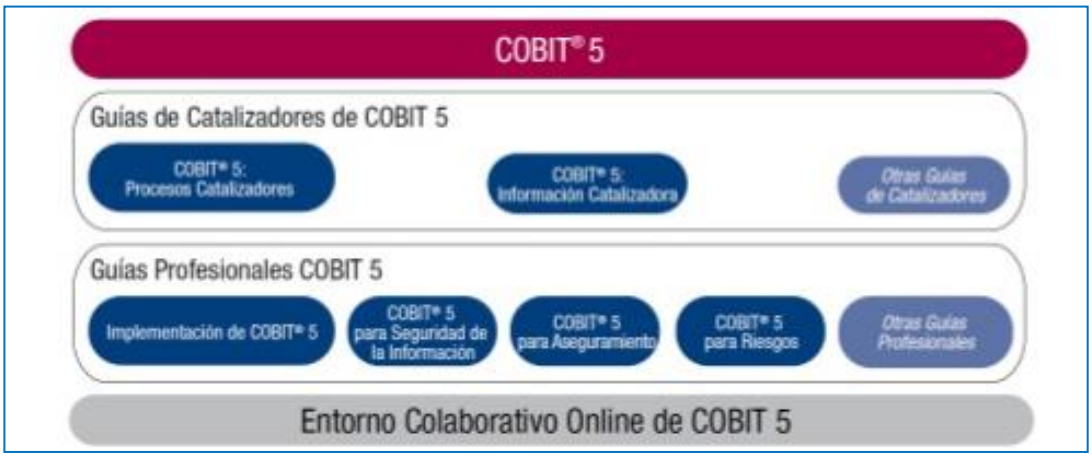


Figura 11 Familia de productos Cobit 5
Fuente: COBIT 5

1.8.7. COBIT 5 for Information Security

En el grupo de COBIT existe en una última versión uno específicamente enfocado en la seguridad de la información llamada COBIT 5 for Information Security, la cual tiene un marco de referencia (framework) con mejoras prácticas y también agrega una guia de prácticas detalladas para la protección de la información en todos los niveles de la organización. (Ver figura 06)

En el documento se plantea la idea de que la seguridad de la información es una disciplina transversal, por lo que considera aspectos de protección de datos en cada actividad y proceso desempeñado.

Además, sirve como un complemento de COBIT 5, ya que este último considera algunos procesos que brindan una guía básica para definir, operar y monitorear un sistema para gestión de la seguridad, como son:

- ✓ APO13 Gestión de la seguridad (treceavo proceso del dominio Alineación, Planeación y Organización).
- ✓ DSS04 Gestión de la continuidad (cuarto proceso del dominio Entrega, Soporte y Servicio).
- ✓ DSS05 Gestión de servicios de seguridad (quinto proceso del mismo dominio).

Por lo que además de revisar con más detalle estos procesos, se agregan metas y métricas específicas de seguridad para cada proceso definido en los dominios de COBIT 5. Del mismo modo, se establecen prácticas, actividades, entradas y salidas entre procesos, para cada uno de los que conforman el modelo de referencia descrito en esta versión. (Mendoza, COBIT para la seguridad en las organizaciones, 2015) (Ver figura 12)

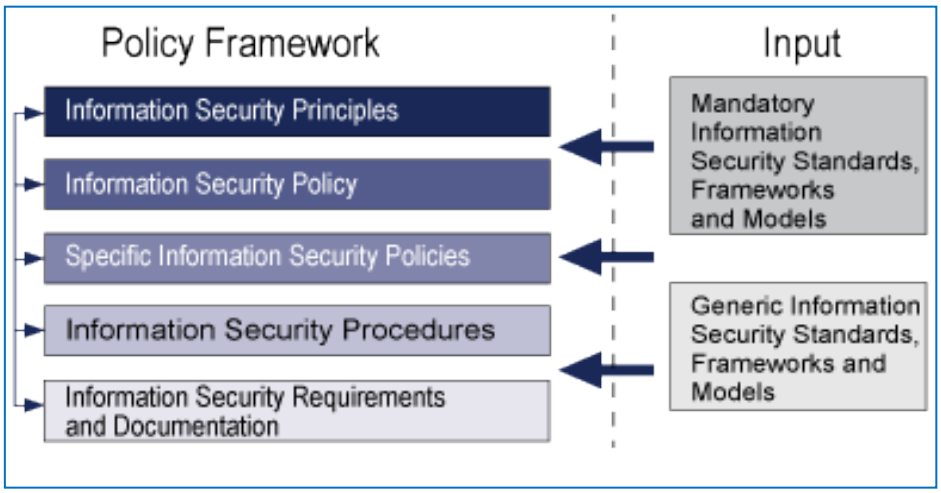


Figura 12 COBIT 5 for Information Security
Fuente: Isaca.Org

ISACA (por su nombre en inglés Information Systems Audit and Control Association) Information Systems Audit and Control Association, define que la Seguridad de la Información es lo que se asegura dentro de la empresa, la información está protegida contra la divulgación a los usuarios no autorizados (Confidencialidad), la modificación indebida (Integridad) y el no acceso cuando sea necesario (Disponibilidad).

Confidencialidad: significa preservar las restricciones autorizadas en materia de acceso a la información y su divulgación, incluidos los medios para la protección de la privacidad y la propiedad de la información. Integridad: significa protección contra la incorrecta modificación o destrucción de información, y comprende la garantía de no repudio y autenticidad de la información. Disponibilidad: significa garantizar el acceso oportuno y confiable, y el uso de información. (Isaca, Modelo de Negocios para la Seguridad de la Información., 2013)

1.8.8. Gestión De Riesgos En La Seguridad Informática

La Gestión de riesgo es una metodología para analizar, determinar, clasificar y valorar y el riesgo, para poder así implementar procesos que permitan controlar, para eso debemos seguir dichos pasos:

Análisis del Riesgo: Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.
Clasificación: Determina si los riesgos encontrados y los riesgos restantes son aceptables.
Reducción: Define e implementa las medidas de protección. Además sensibiliza y capacita los usuarios conforme a las medidas.
Control: Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sancionar el incumplimiento.

Todo el proceso está basado en las llamadas políticas de seguridad, normas y reglas institucionales, que forman el marco operativo del proceso, con el propósito de:

Potenciar las capacidades institucionales, reduciendo la vulnerabilidad y limitando las amenazas con el resultado de reducir el riesgo.
Orientar el funcionamiento organizativo y funcional.
Garantizar comportamiento homogéneo.
Garantizar corrección de conductas o prácticas que nos hacen vulnerables.
Conducir a la coherencia entre lo que pensamos, decimos y hacemos.

Mantener la seguridad de la información en nuestra actualidad es dirigirse a un punto muy importante que corresponde a la identificación, análisis y tratamiento de riesgo en la organización, después de haber determinado los riesgos en la empresa se toman medidas adecuadas para poder resolverlos.

> Para tratar de minimizar los efectos de un problema de seguridad, se realiza el denominado análisis de riesgo, término que hace referencia al proceso necesario para responder a tres cuestiones básicas de la seguridad de una organización, que es saber qué queremos proteger, contra quien o que se requiere proteger y cómo lo vamos a hacer. (Airitio, 2008)

Sabiendo esto es fundamental un proceso para identificar los peligros que afecten a la seguridad para poder así salvaguardar información.

1.8.9. Ley De Protección De Datos Personales

Todos los empleados deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo de proteger dichos datos personales tanto de los clientes como del personal que trabajan en la empresa, el reglamento de ley dice:

> El presente reglamento tiene por objeto desarrollar la Ley N° 29733, la protección de Datos Personales, a fin de garantizar el derecho fundamental a la protección de datos personales, regulando un adecuado tratamiento, tanto por las entidades públicas, como las instituciones pertenecientes al sector privado. Sus disposiciones constituyen normas de orden público y de cumplimiento obligatorio. (Peruano, 2012)

Es así donde la empresa buscara el proceso de protección de datos para la mejor calidad de confianza ante sus clientes.

Este nueva ley impone una compromiso con las personas y empresas en el desarrollo de sus actividades trabajan administrando datos personales de sus clientes, de sus trabajadores o de otras personas naturales.

En el artículo 79 de la Ley 29733, Protección de datos personales indica los requisitos de procedimiento de inscripción donde nos dice lo siguiente:

> Los titulares de los bandos de datos personales deberán inscribirlos en el Registro de Protección de Datos Personales proporcionando la siguiente información:

1. La denominación y ubicación del banco de datos personales, sus finalidades y los usos previstos.
2. La identificación de datos personales sometidos a tratamiento en dicho banco.
3. Procedimientos de obtención y el sistema de tratamiento de los datos personales
4. La descripción técnica de las medidas de seguridad.
5. Los destinarios de transferencia de datos. (Peruano, 2012)

1.8.10. Herramientas Tecnológicas De Seguridad

Existen herramientas tecnológicas para la seguridad de la información y la seguridad informática, es muy importante tenerlas en las empresas para poder evitar riesgos y amenazas para no tener problemas a futuro.

> Acerca de la seguridad de la información y la seguridad en redes de telecomunicación. Se introducen brevemente los mecanismos y herramientas para la protección de los datos que o bien están almacenadas en un ordenador personal, o bien son transmitidos a través de una red. Asimismo, se indican algunas pinceladas sobre los procedimientos para mitigar los diferentes tipos de amenazas de seguridad. También incluye una breve descripción de la criptografía de clave pública, de clave simétrica y algoritmos. Por último, se comentan algunos conceptos básicos sobre la seguridad perimetral de la red incluyendo cortafuegos y sistemas de detección de intrusión, así como los protocolos habituales de seguridad en redes inalámbricas. (Soriano, 2013)

Las herramientas tecnológicas de seguridad para vulnerabilidades y amenazas existe muchas tanto como hardware y software de código abierto, a continuación alguna de las herramientas de seguridad.

El monitoreo de la red

Es fundamental realizar observaciones periódicas, ya sea que un administrador de red ingrese al equipo y supervise cada cierto tiempo; o lo recomendable es que una herramienta haga el trabajo por él, sostiene el especialista. “La herramienta tiene que obtener data sobre el consumo del servidor, graficarla de un modo amigable y guardarla de tal forma que uno pueda ver el patrón en el tiempo, y de acuerdo a ello establecer una referencia de funcionamiento. Ahora la pregunta es ¿qué monitoreo?, lo clásico: disponibilidad de la red, router, fireware, servidores, CPU, espacio de disco. Por experiencia, sucede muy a menudo que la red se queda colgada, no levanta el servicio de web. El problema es que el disco duro está lleno. Las herramientas nos van a permitir -aparte de obtener, graficar y guardar en un histórico- generar una alerta de manera que cuando el disco llegue por ejemplo a un 80% de capacidad, envíe un aviso al administrador o a todos los empleados si se desea”. (Rojas, 2010)

Herramienta de Auditoria

Las principales herramientas internas para ellos son los sistemas de autoevaluación y una función de auditoría interna realmente eficiente y eficaz.

Los sistemas de autoevaluación

Son una herramienta muy usada en sistemas completos de control interno. Primero se elabora un cuestionario con una lista de puntos de control agrupados por temas, que en general van a ser los principales procesos. Para una empresa industrial y comercial, por ejemplo, se van a incluir puntos que tienen que ver con el control de calidad en cada etapa del proceso de producción o con la confiabilidad y seguridad del proceso de facturación. También existen en las entidades del sistema financiero, pero cabe mencionar que la SBS los diseña cada vez más para los supervisados, para diferentes temas, como para la gestión del riesgo operacional o la del riesgo de mercado.

Es necesario designar responsables claros del llenado de ese cuestionario, de otra manera, podría haber ciertas incongruencias al hacerlo, sea por diferencias de interpretación sea por el recurso a personas poco preparadas para hacerlo.

Las respuestas son de 3,4 o 5 tipos, según el grado de cumplimiento auto-estimado del punto de control (la SBS suele utilizar 3 o 4): son respuestas de tipo" cumple", "cumple parcialmente", "no cumple". (Belaunde, 2012)

Criptografía

Los controles criptográficos deben utilizarse de forma que no sea necesario utilizar la información confidencial para protegerla contra cualquier acceso no deseado. La criptografía es la ciencia de la escritura en código secreto, mientras que el cifrado es un mecanismo específico para poder convertir la información en un código diferente que pueda ser descifrado sólo por las personas autorizadas. Algunos ejemplos en los que podemos utilizar controles criptográficos son:

Contar con un dispositivo con información confidencial que se encuentre fuera de la organización.

Tiene que enviar un correo electrónico con información confidencial.

Tiene un servidor de archivos con una carpeta en la que todos los trabajadores tienen acceso, pero uno o varios archivos contienen información confidencial.

Contar con un sitio web público en el que todos los usuarios puedan acceder mediante la introducción de nombre de usuario y contraseña.

Contar con un sitio web desde el que se pueda ofrecer un comercio electrónico y que tenga una pasarela de pago.

Los trabajadores conectan con la red corporativa desde casa para acceder a los recursos corporativos. (ISOTools, 2015)

Herramienta de filtrado

Permite ver y controlar fácilmente los sitios web que los usuarios visitan. El servicio funciona a través de unos cortafuegos que permite bloquear

> descargas de malware y virus, así como bloquear el acceso a otros recursos que puedan poner en riesgo la seguridad de la conexión.
>
> Muchas veces escuchamos del robo de claves mediante páginas que aparentan ser de entidades bancarias (phishing) pero que en realidad son páginas web falsas diseñadas igual que la original para hacernos creer que estamos en la web de nuestro banco para capturar nuestros datos de acceso**.** (OpticalNews, 2013)

1.8.11. Octave

Es una metodología desarrollada por Computer Emergency Response Team (CERT), que tiene como objetivo facilitar la evaluación de riesgos en una organización. De esta forma, OCTAVE estudia la infraestructura de información y, más importante aún, la manera como dicha infraestructura se usa. Se considera que, con el fin de que una organización pueda cumplir su misión, los empleados de todos los niveles necesitan entender qué activos relacionados con la información son importantes y cómo deben protegerlos.

> La metodología OCTAVE es la conformación de un equipo mixto, ocupado por personas en las áreas de negocios y de TI. Esta configuración explica el hecho de que los empleados del negocio son los más indicados para identificar qué información es importante en los procesos y cómo se usa dicha información. (Campo, 2012)

Por otro lado, el equipo de TI, es el que conoce la configuración de la infraestructura y las debilidades que pueden tener, estos dos puntos de vista son importantes para tener una visión global de los riesgos de seguridad de los servicios de TI.

En conclusión, Octave es un método operativo, orientado a resultados. Después de la primera iteración (2-3 meses) se obtiene un plan a corto plazo y un plan estratégico a largo plazo para mitigar los riesgos detectados.

En la siguiente iteración (después de 6 meses o un año) se parte de los resultados de la implantación de las acciones anteriores; propone una metodología muy bien detallada, con unos pasos muy claros y definidos, proporcionando el suficiente material de soporte (plantillas, ejemplos, etc.) y asumiendo todas las buenas prácticas de las normas y estándares actuales. (Ver Figura 13)

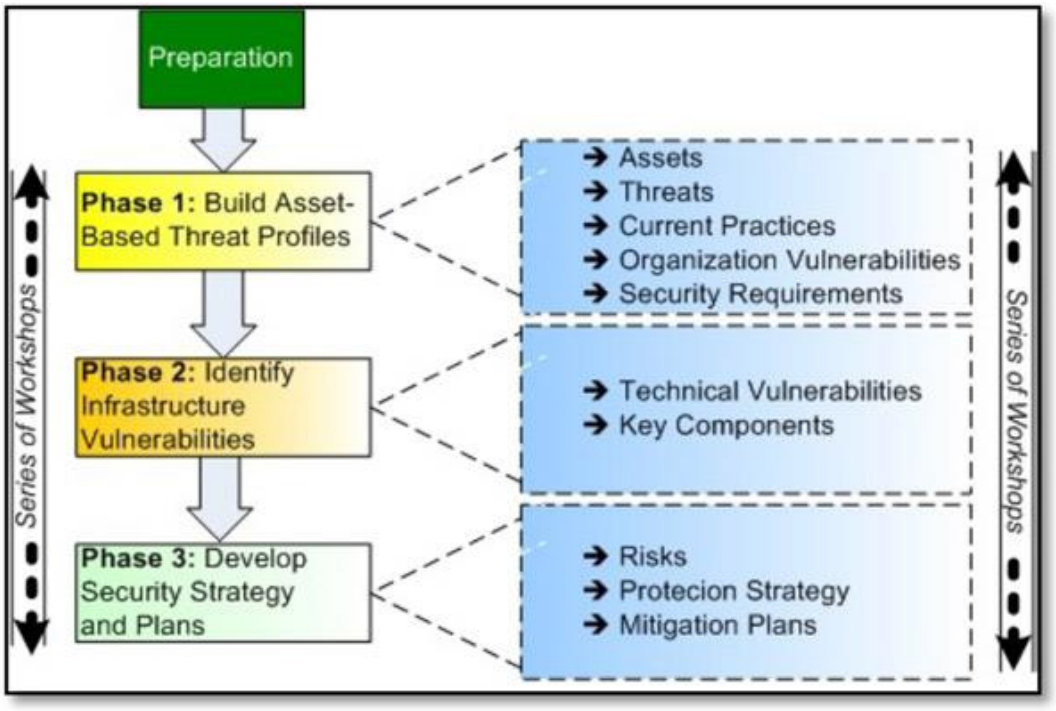


Figura 13 Procesos y subprocesos de OCTAVE
Fuente: Octave

1.8.12. Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)

Estudia los riesgos que soporta un sistema de información y el entorno asociado a este, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio, en una primera aproximación que se atiene a la aceptación habitual del término, y otro relacionado con recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir impedir, reducir o controlar los riesgos investigados.

> Es un método formal para investigar los riesgos que soportan los Sistemas de información para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos, Magerit ha sido elaborada por un

equipo interdisciplinar del comité de seguridad de los sistemas de información y tratamiento automático de datos Personales. (Desongles, 2005)

El análisis de riesgos es una tarea que sirve para determinar el riesgo a través de unos pasos secuenciales:

1. Identificar los activos importantes para la compañía, su interrelación y su valor, en el sentido en que afectaría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos
3. Establecer qué medidas preventivas hay dispuestas y que tan eficaces son respecto al riesgo
4. Medir el impacto, definido como la afectación causada sobre el activo generado por la materialización de la amenaza
5. Medir el riesgo, reconocido como el impacto ponderado con la probabilidad de materialización de la amenaza (Ver Figura 14)

Figura 14 Flujo descriptivo de pasos
Fuente: ccn-cert.cni.es

Objetivos de Magerit:

- Estudiar los riesgos que soportan un sistema de información y el entorno asociado a él.

- Propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización.
- Señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenas, obteniendo unos resultados.
- Permite recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o posibles perjuicios. (Corrales, 2005)

Con esta aplicación se permitirá: (Ver Figura 12)

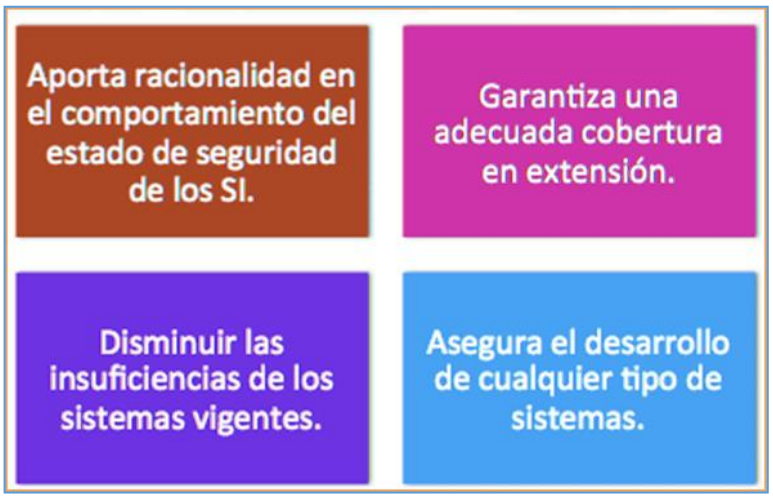


Figura 15 Aplicación Magerit
Fuente: Elaboración propia

Tipos De Proyectos:

MAGERIT se enfoca a cada empresa u organización en los sistemas de seguridad de Información, las cuales son:

- Situación dentro del "ciclo de estudio": Marco estratégico, planes globales, análisis de grupos múltiples activos, gestión de riesgos de activos concretos, determinación de mecanismos específicos de salvaguarda.
- Envergadura: Complejidad e incertidumbre relativas del sistema estudiado, tipo de estudio más adecuado a la situación: corto, simplificado, etc.

- Problemas específicos a solventar: Seguridad lógica, Seguridad de Redes y Comunicaciones, Planes de Emergencia y Contingencia, Estudios técnicos para lo homologación de sistemas o productos, Auditorías de seguridad. (Corrales, 2005)

Elementos Magerit:

Análisis de Riegos para identificar las amenazas que acechan a los distintos componentes pertenecientes o relacionados al Sistema de Información (activos); para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener en la organización, obteniendo cierto conocimiento del riesgo que se corre. (Corrales, 2005)

Gestión de Riesgos basada en los resultados obtenidos en el análisis anterior, que permite seleccionar e implantar las medidas o "salvaguardas" de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. (Corrales, 2005)

Modelo de Magerit:

El modelo margerit se divide en tres partes las cuales podemos observar a continuación: (Ver Figura 13)

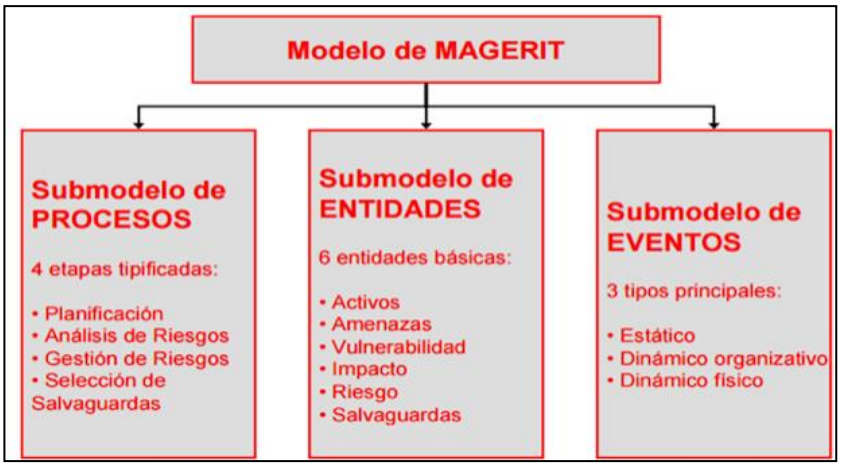


Figura 13: Modelo Margerit
Fuente: Magerit

Tipo De Técnicas:

Magerit consta de siete técnicas las cuales son:

- Guía de aproximación
- Guía de procedimientos
- Guía de técnicas
- Guía para responsables del dominio
- Guía para desarrolladores de aplicaciones
- Arquitectura de información y especificaciones de interfaz para el intercambio de datos
- Referencia normativa (Corrales, 2005)

Un pequeño ejemplo metodología magerit de toma de datos y procesos de información (Ver Figura 16)

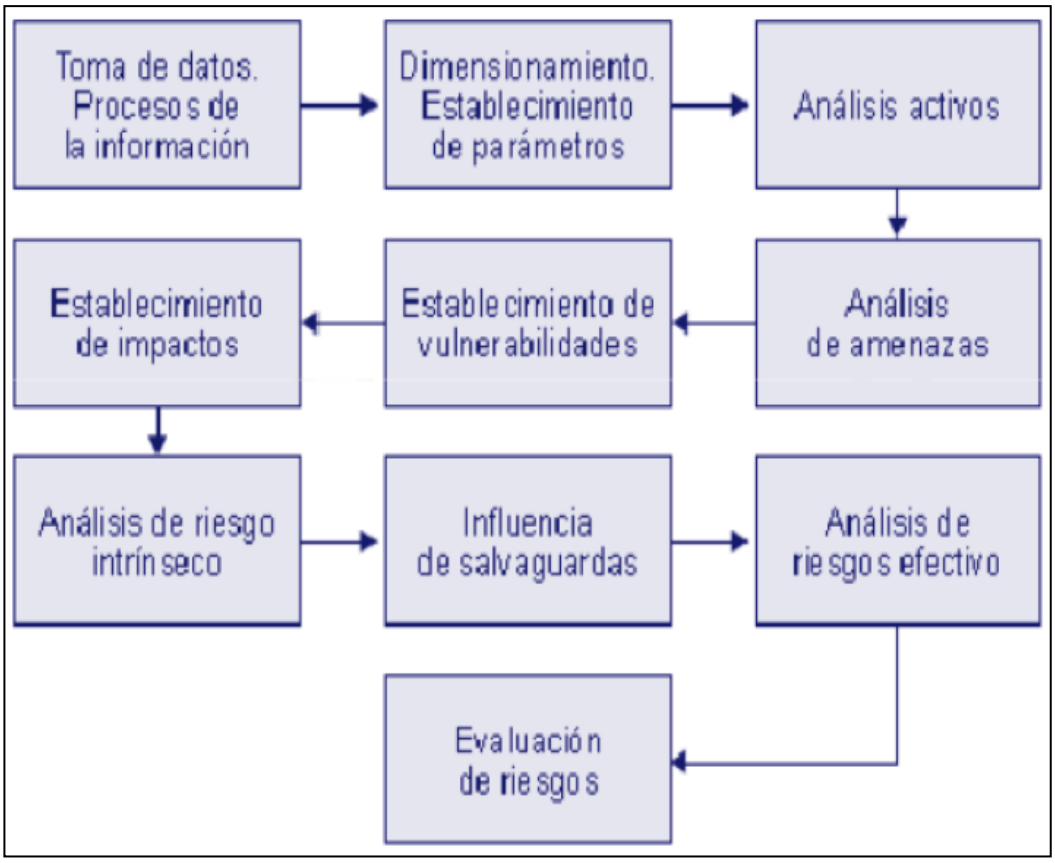


Figura 16 ejemplo de margerit
Fuente: Magerit

ISO 31000:2009

Es un documento práctico que pretende ayudar a las organizaciones en el desarrollo de su propio enfoque a la gestión del riesgo. Pero esto no es un estándar donde las organizaciones pueden solicitar la certificación.

Mediante la implementación de la norma ISO 31000, las organizaciones pueden comparar sus prácticas de gestión de riesgos con un punto de referencia reconocido internacionalmente, proporcionando sólidos principios para una gestión eficaz. (Ver Figura 17)

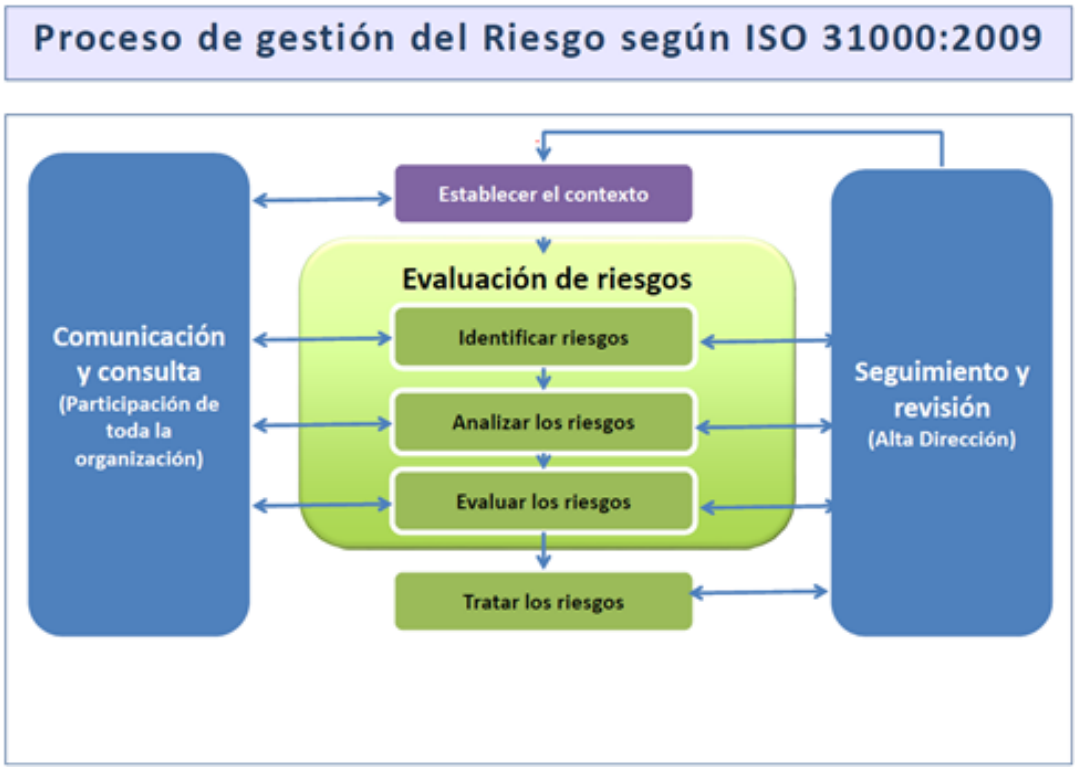


Figura 17 proceso de gestión de riesgo iso 31000:2009
Fuente: ISO 31000: 2009

A continuación, los Principios Básicos Proceso Gestión Riesgos Norma ISO 31000:

"Los auditores internos tienen que obtener evidencia suficiente y apropiada para determinar que los objetivos clave de los procesos de gestión de riesgos se hayan cumplido, con el fin de formarse una opinión sobre la adecuación de dichos procesos". (Frett, 2013)

Un sistema efectivo de gestión de riegos permite entre otras cosas:

1. Aumentar la probabilidad de alcanzar objetivos;
2. Motivar una dirección proactiva;
3. Ser consciente de la necesidad de identificar y tratar el riesgo en todas partes de la organización;
4. Mejorar la identificación de oportunidades y amenazas;
5. Cumplir con exigencias legales y requerimientos de regulación y normas internacionales;
6. Mejorar la gobernabilidad;

7. Mejorar la confidencialidad y confianza en las partes interesadas.
8. Establecer una base confiable para la toma de decisiones y la planificación;
9. Mejorar controles;
10. Asignar con eficacia el uso de los recursos para el tratamiento de riesgo;
11. Mejorar la eficacia y eficiencia operacional;
12. Mejorar la prevención de pérdidas y manejo de incidentes;
13. Minimizar pérdidas;
14. Mejorar el conocimiento de la organización;
15. Mejorar la capacidad de recuperación de la organización. (Frett, 2013)

1.8.13. Risk It (Riesgos De Tecnología De Información)

El Riesgo de TI (Risk TI) es el riesgo de negocio asociado con el uso, propiedad, operación, involucramiento, influencia y adopción de la TI dentro de la empresa.

Este riesgo consiste en los eventos relacionados con la TI que pueden potencialmente impactar al negocio.

Cada evento puede ser visto como riesgo y oportunidad. (Isaca, Risk IT Framework, 2009)

Risk IT pretende ser una herramienta práctica para la gestión de riesgos basado en los conceptos de valor y beneficios que la organización obtiene a través de sus iniciativas de TI. Al igual que CobIT y Val IT, Risk IT se concentra en el cumplimiento de los objetivos de la organización.

Risk IT tiene como fin gestionar los riesgos relacionados con la no obtención de ese valor / beneficios, así como los riesgos de no aprovechar las oportunidades y beneficios que una iniciativa de TI podría proporcionar a la organización. Es decir, el riesgo de no tomar ventaja de TI. (Isaca, Risk IT Framework, 2009)

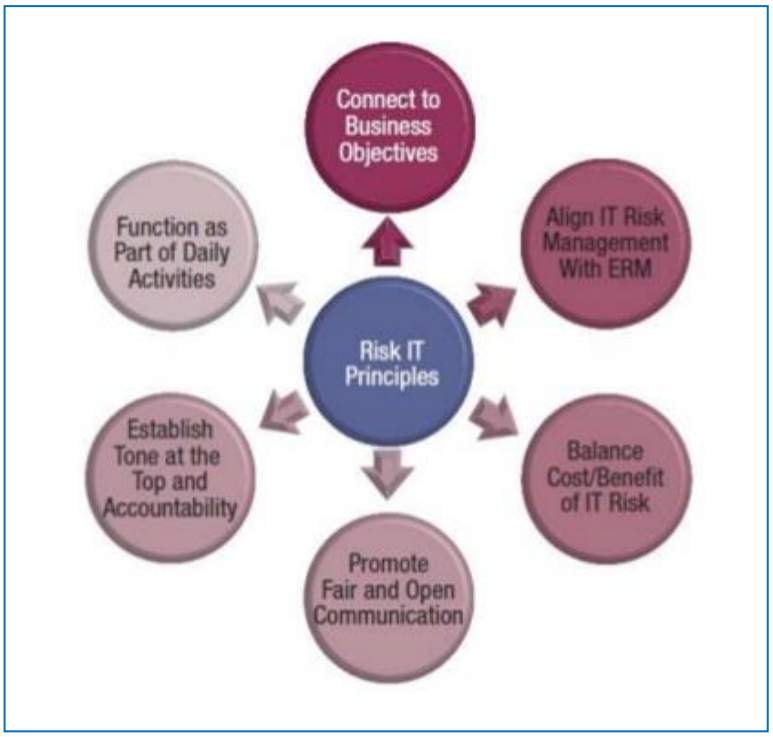


Figura 18 Risk principios
Fuente: Risk IT Rinciples

1.9. Definición de términos básicos

1.9.1. ACTIVO DE SERVICIO: Es un componente esencial para el suministro del servicio o que suponga un elevado coste para la organización. Esta noción es un poco diferente de activo en sentido financiero del término (gestión de configuración), porque no solo interviene el valor del componente, sino también la noción del que el componente es indispensable para el funcionamiento del servicio informático. **(Baud, 2016)**

1.9.2. AMENAZA: Una amenaza es una acción, una situación o un hecho que puede comprometer el buen funcionamiento de un activo de servicio o de un conjunto de activos de servicio. Las amenazas se recogen y clasifican: error grave natural (incendio, inundación, temblor de tierra, etc.), terrorismo, ataque viral, conflicto social, etc. **(Baud, 2016)**

1.9.3. ATAQUE INFORMÁTICO: Existen diferentes métodos para interceptar, atacar y descubrir una red. Estos ataques están divididos en dos grandes grupos: pasivos y activos. **(Miranda, Informática Industrial, 2017)**

1.9.4. CONTROL DE SEGURIDAD: "La seguridad computacional a menudo se divide en tres categorías maestras distintas, llamadas controles: Físico, Técnico, Administrativo. Estas tres categorías definen los objetivos principales de una implementación de seguridad apropiada. Dentro de estos controles hay sub-categorías que detallan aún más los controles y cómo estos se implementan". **(MitEdu, 2013)**

1.9.5. EVENTO: "Es una situación que es posible pero no certera; es siempre un evento futuro y tiene influencia directa o indirecta sobre el resultado. Un evento se trata como un suceso negativo y representa algo indeseado". **(Corcho, 2014)**

1.9.6. IMPACTO: "Es la cantidad de daño que puede causar una amenaza que explote una vulnerabilidad". **(Miranda, Informática Industrial, 2017)**

1.9.7. POLÍTICAS DE SEGURIDAD: "La política de seguridad define qué es lo que desea proteger y qué espera de los usuarios del sistema. Proporciona una base para la planificación de la seguridad al diseñar nuevas aplicaciones o ampliar la red actual. Describe responsabilidades del usuario como las de proteger información confidencial y crear contraseñas no triviales". **(IBM, 2014)**

1.9.8. RIESGO INFORMÁTICO: "Es el proceso que permite asignar valores para determinar la probabilidad y las consecuencias de un riesgo sobre un activo". **(Bolaños, 2013)**

1.9.9. VULNERABILIDAD: Una vulnerabilidad es un punto débil en la seguridad de un sistema informático. A través de ésta se pueden presentar amenazas que pongan en peligro la confidencialidad e integridad de la información; haz un análisis para identificar el tipo y el nivel de cada vulnerabilidad. **(Him, 2012)**

1.9.10. ACCESO: Consecuencia de una identificación positiva. Tomemos el caso de una persona que pretende acceder a su cuenta bancaria a través del sitio web de su banco, con la intención de realizar una transferencia de dinero. Para ingresar a su cuenta, debe especificar su nombre de usuario y su clave. **(Definicion.de, 2008)**

1.9.11. ACTIVOS: Los activos son los componentes indispensables para el funcionamiento de un sistema informático. Se clasifican en: Hardware, Software y datos e información. **(Him, 2012)**

1.9.12. CONTROL: Control de acceso es un término genérico que se utiliza para designar el proceso por el que un sistema de computación o un monitor de referencia controlan la interacción entre los usuarios y los recursos del sistema de tal forma que los primeros accedan a los recursos deseados. **(Airitio, 2008)**

1.9.13. DATOS: Un dato es un conjunto discreto de factores objetivos sobre un hecho real, dentro de un contexto empresarial el concepto el dato es definido como un registro de transacciones. **(Vidal, 2004)**

1.9.14. GOLPE (BREACH): Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc. **(MuniMolina, 2003)**

1.9.15. INTEGRIDAD DE DATOS: La integridad de un dato alude a ese atributo o cualidad que es inherente a la información cuando se considera exacta, completa, homogénea, sólida y coherente con la intención de los creadores de los datos que la conforman. **(Rizzuti, 2013)**

1.9.16. PLAN DE SEGURIDAD: El Plan de Seguridad Informática constituye el documento fundamental para el control y la seguridad en la explotación de las tecnologías informáticas de la Organización. **(Ayala, 2011)**

1.9.17. SEGURIDAD LÓGICA: La seguridad lógica hace referencia a la aplicación de mecanismos y barreras para mantener el resguardo y la integridad de la información dentro de un sistema informático. La seguridad lógica se complementa con la seguridad física. **(Tecnologia, 2017)**

1.9.18. SEGURIDAD FÍSICA: La seguridad física hace referencia a las barreras físicas y mecanismos de control en el entorno de un sistema informativo, para proteger el hardware de amenazas físicas. Esta también se complementa con la seguridad lógica. **(Tecnologia, 2017)**

II. METODO

2.1. Tipo y diseño de la investigación

Tipo de investigación

Investigación Tecnológica:

Responde a problemas técnicos, está orientada a demostrar la validez de ciertas técnicas bajo las cuales se aplican principios científicos que se demuestren su eficacia en la modificación o trasformación de un hecho o fenómeno. La investigación tecnológica aprovecha del conocimiento teórico científico producto de la investigación básica o sustantiva y organiza reglas técnicas cuya aplicación posibilita cambios en la realidad. (Carlessi, 2006) (Ver Figura 19)

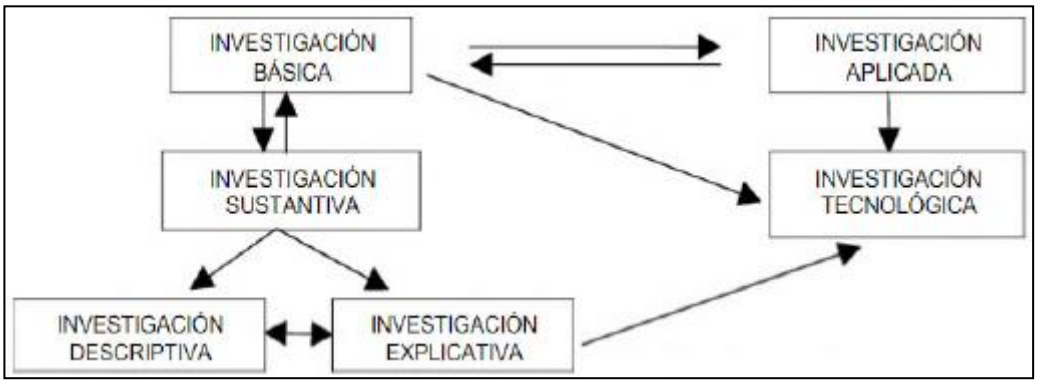


Figura 19 Esquema relación entre los tipos de investigación según su finalidad.
Fuente: Libro diseño metodológico

Diseño de la investigación

Diseño Cuasi Experimental:

Es una investigación que posee todos los elementos de experimento, excepto que los sujetos no se asignan aleatoriamente a los grupos. En ausencia de aleatorización, el investigador se enfrenta con las tareas de identificar y separar los efectos de los tratamientos del resto de los factores que afectan a la variable dependiente. (Peshazur, 1991)

Diseño Experimental:

Una aceptación particular del experimento, más armónica con un sentido científico del término, se refiere a un estudio en el que se manipulan intencionalmente una o más variables independientes (supuestas causas-antecedentes), para analizar las consecuencias que la manipulación tiene sobre una o más variables dependientes (supuestos afectos-consecuentes), dentro de una situación de control para el investigador. Esta definición quizá parezca compleja; sin embargo, conforme a se analicen sus componentes se aclara el sentido de la misma. (Hernández, 2010)

(Ver Figura 19)

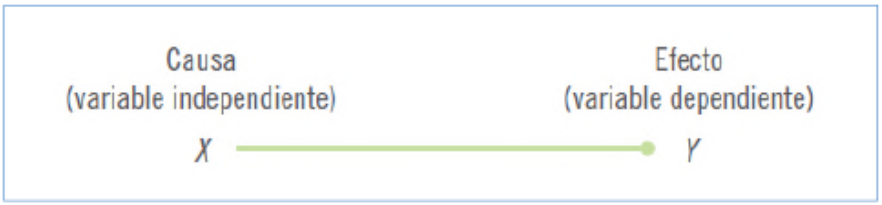


Figura 20 Causa y efecto de variables
Fuente: Libro metodología de la investigación, Quinta edición

Para la investigación se ha decidido un diseño de investigación:

Experimental – Cuasi Experimental.

X

G: O_1 --> O_2

Grupo Asignación	Pre Prueba	Estimulo	Post Prueba	Hipótesis
G	O_1	X	O_2	$O_1 < O_2$

- ✓ 1ro. Medición previa de la variable dependiente a ser estudiada (Pretest).
- ✓ 2do. Aplicación de la variable independiente o experimental X a los sujetos Y.
- ✓ 3ro. Una nueva medición de la variable dependiente en los sujetos Y (Postest).

Dónde:

GE: grupo experimental

O_1: primera observación, Pretest

X: aplicación o tratamiento de la variable independiente.

O_2: segunda observación, Postest

Hipótesis:

- ✓ Si $O_1 < O_2$ se acepta la hipótesis.

- ✓ Si $O_1 > O_2$ se rechaza la hipótesis y se acepta la hipótesis nula.

Nivel de la investigación

Investigación descriptiva:

Tiene como objetivo la descripción de los fenómenos o investigar, tal como es y cómo se manifiesta en el momento (presente) de realizarse el estudio y utiliza la observación como método descriptivo, buscando especificar las propiedades importantes para medir y evaluar aspectos, dimensiones o componentes. Pueden ofrecer la posibilidad de predicciones aunque rudimentarias. Se sitúa en el primer nivel de conocimiento científico. Se incluye en esta modalidad gran variedad de estudios (estudios correlaciónales, de casos, de desarrollo, etc.) Ejemplo: Investigación sobre la estructura socio económica y rendimiento académico de los estudiantes del IESPP “Indoamérica”. (Carlessi, 2006)

Investigación explicativa o de comprobación de hipótesis casuales:

Su objetivo es la explicación de los fenómenos y el estudio de sus relaciones para conocer su estructura y los aspectos que se intervienen en la dinámica de aquellos. Son estudios de alto nivel que se generan teorías, leyes o enunciados totalmente novedosos. Son de gran complejidad y por lo general sus resultados pasan a ser revisión obligatoria para los profesionales de ese campo.

Está dirigida a responder a las causas de eventos físicos o sociales y su interés es centra en explicar por qué y en qué condiciones ocurre un fenómeno o porque dos o más variables se relacionan. Hay predominio de explicación, descripción y correlación.

Es aquella que tiene relación causal, no solo persigue describir o acercarse a un problema, sino que intenta encontrar las causas del mismo. Son aquellas que por parten de una situación problema o conocimiento presente para luego indagar posibles causas o factores asociados que permiten interpretarla. En este caso la dirección es de V.D → V.I (Carlessi, 2006)(Ver Figura 21)

Figura 21 Esquema niveles de investigación científica.
Fuente: Libro diseño metodológico

Enfoque de la investigación

Enfoque cuantitativo:

El enfoque cuantitativo (que representa, un conjunto de procesos) es secuencial y probatorio. Cada etapa precede a la siguiente y no podemos "brincar o eludir" pasos, el orden es riguroso, aunque, desde luego, podemos redefinir alguna fase.

Parte de una idea, que va acotándose y, una vez delimitada, se derivan objetivos y preguntas de investigación, se revisa la literatura y construye un marco o una perspectiva teórica.

De las preguntas se establecen hipótesis y determinan variables; se desarrolla un plan probarlas (diseño); se miden las variables en un determinado contexto; analizan las mediciones obtenidas (con frecuencia utilizando métodos estáticos), y se establece una serie de conclusiones respecto de la(s) hipótesis. (Hernández, 2010).

Este proceso se representa en la siguiente figura (Ver Figura 22)

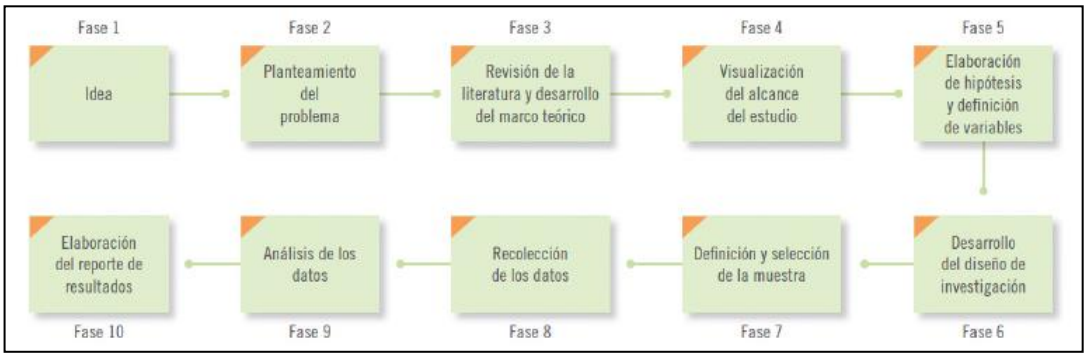


Figura 22 Definición de los enfoques cuantitativo y cualitativo
Fuente: Libro metodología de la investigación, Quinta edición

Enfoque

Investigación Cuantitativa: El esquema metodológico asume el positivismo lógico, en tal sentido busca que la medición sea objetiva y controlada. Supone procedimientos cuantitativos de procesamiento de datos, hace uso de la estadística descriptiva y/o inferencial.

Las inferencias son derivadas del análisis estadístico, que van más allá de los datos, es decir trasciende, explica y generaliza al trabajar sobre planteamientos hipotéticos deductivos. (Carlessi, 2006)

2.2. Población y muestra

- ✓ **Población**

  En la presente investigación, la población está conformada por el órgano administrativo y operativo de la empresa y responsables de área que accederían al manejo de la información siendo una cantidad de 22 personas.

- ✓ **Muestra**

  Debido a que la muestra del sector administrativo y operativo que laboran en las diferentes áreas es muy pequeña se vio por conveniente aplicar la técnica de muestreo censal, es decir se aplicó el instrumento al total de la población identificada.

2.3. Técnicas para la recolección de datos

- ✓ **Técnicas**

  En este estudio de investigación se utilizará un cuestionario de encuesta como principal técnica de recolección de datos, que su finalidad será recolectar toda información de los trabajadores de las diferentes áreas de la empresa Automatisoft SAC, la cual será de suma importancia con respecto a la seguridad de la información de la empresa.

- ✓ **Instrumentos**

  La vía de investigación que se utilizará será el cuestionario de preguntas.

2.4. Validez y confiabilidad de instrumentos

Validez del instrumento

Para la validación de la encuesta, se ha utilizado el Juicio de tres expertos

Criterio de confiabilidad de instrumento

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

$$\alpha = \frac{k}{(k-1)}\left(1 - \frac{\sum \sigma_i^2}{\sigma_X^2}\right)$$

Donde

k = es el número de ítems

$(\sigma_i)^2$ = varianza de cada ítem

$(\sigma_x)^2$ = varianza del cuestionario total

Según lo mencionado por (Ñaupas, Mejia, Novoa, & Villagomez, 2014, pág 217) se dice que 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

Confidencialidad

Estadísticos de fiabilidad

Alfa de Cronbach[a]	N de elementos
,602	7

El valor del Alfa de Cronbach esta dando un valor de cuestionable en cuanto a la variable Confidencialidad, sin embargo, esto se puede dar porque los encuestados no dominan el tema que se les ha preguntado.

Integridad

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,709	20

El valor del Alfa de Cronbach está dando un valor de aceptable en cuanto a la variable Integridad

Disponibilidad

Estadísticos de fiabilidad

Alfa de Cronbach[a]	N de elementos
,761	8

El valor del Alfa de Cronbach está dando un valor de aceptable en cuanto a la variable Disponibilidad

2.5. Procesamiento y análisis de datos

El procesamiento de la información se ha realizado usando el IBM SPSS versión 25, previamente toda la información de la encuesta fue digitada en una base de datos en MS Excel, para posteriormente importarla desde el SPSS y así poder trabajar las estadísticas y pruebas no paramétricas, dada que, por el poco volumen de datos, se ha realizado un análisis no paramétrico.

2.6. Aspectos éticos

El estudio velará por las siguientes razones éticas:

- Se acepta en totalidad informar de la investigación.
- Se respetará la sinceridad de los resultados y de los datos proporcionados por los usuarios de las empresas implicadas.
- Se hará uso de las normas APA para citar a los autores que fueron usados para amparar la actual investigación, mencionándolos en las referencias bibliográficas.
- Se mantendrá en discreción la información privada a la que se ha podido poseer acceso en la organización.
- Se mantendrá en absoluta discreción la identidad del nombre de la organización en la cual se realizan las practicas, debido a la estrictica y rigurosa confidencialidad que se maneja en dicha organización lo cual puede quebrantar sus políticas de seguridad.

III. RESULTADOS

3.1. Resultados descriptivos

Tabla 1 P1

La gerencia apoya activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explicita y reconocimiento de las responsabilidades de la seguridad de información.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	3 Parcialmente	11	50,0	50,0	50,0
	4 De acuerdo	8	36,4	36,4	86,4
	5 Totalmente de acuerdo	3	13,6	13,6	100,0
	Total	22	100,0	100,0	

Fuente: Elaboración propia

Tabla 2 P2

Las actividades de seguridad de la información son coordinadas por representantes de diferentes partes de la organización con funciones y roles laborales relevantes.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1 Totalmente en desacuerdo	3	13,6	13,6	13,6
	2 En desacuerdo	8	36,4	36,4	50,0
	3 Parcialmente	11	50,0	50,0	100,0
	Total	22	100,0	100,0	

Fuente: Elaboración propia

Tabla 3 P3

Se definen claramente las responsabilidades de la seguridad de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	2 En desacuerdo	3	13,6	13,6	13,6
	3 Parcialmente	12	54,5	54,5	68,2
	4 De acuerdo	7	31,8	31,8	100,0
	Total	22	100,0	100,0	

Fuente: Elaboración propia

Tabla 4 P4

Se define e implementa un proceso de autorización gerencial para los nuevos medios de procesamiento de información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	3 Parcialmente	13	59,1	59,1	59,1
	4 De acuerdo	9	40,9	40,9	100,0
	Total	22	100,0	100,0	

Fuente: Elaboración propia

Tabla 5 P5

Se identifica y revisa regularmente los requerimientos de confidencialidad de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	2 En desacuerdo	5	22,7	22,7	22,7
	3 Parcialmente	14	63,6	63,6	86,4
	4 De acuerdo	3	13,6	13,6	100,0
	Total	22	100,0	100,0	

Fuente: Elaboración propia

Tabla 6 P6

Se revisa independientemente a intervalos planeados, o cuando ocurran cambios significativos la seguridad de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1 Totalmente en desacuerdo	4	18,2	18,2	18,2
	2 En desacuerdo	13	59,1	59,1	77,3
	3 Parcialmente	5	22,7	22,7	100,0
	Total	22	100,0	100,0	

Fuente: Elaboración propia

Tabla 7 P7

Han firmado un documento de confidencialidad de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1 Totalmente en desacuerdo	8	36,4	36,4	36,4
	2 En desacuerdo	4	18,2	18,2	54,5
	3 Parcialmente	10	45,5	45,5	100,0
	Total	22	100,0	100,0	

Fuente: Elaboración propia

Tabla 8 P8

Se identifican los riesgos que corren la información y los medios de procesamiento de información de la organización y se implementan los controles apropiados antes de otorgar acceso.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1 Totalmente en desacuerdo	2	9,1	9,1	9,1
	2 En desacuerdo	3	13,6	13,6	22,7
	3 Parcialmente	5	22,7	22,7	45,5
	4 De acuerdo	10	45,5	45,5	90,9
	5 Totalmente de acuerdo	2	9,1	9,1	100,0
	Total	22	100,0	100,0	

Fuente: Elaboración propia

Tabla 9 P9

Se tratan todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o activos de la organización

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	2 En desacuerdo	1	4,5	4,5	4,5
	3 Parcialmente	8	36,4	36,4	40,9
	4 De acuerdo	10	45,5	45,5	86,4
	5 Totalmente de acuerdo	3	13,6	13,6	100,0
	Total	22	100,0	100,0	

Fuente: Elaboración propia

Tabla 10 P10

Los acuerdos que involucran acceso, procesamiento, comunicación o manejo por parte de terceras personas a la información de la organización abarcan los requerimientos de seguridad necesarios relevantes

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	3 Parcialmente	3	13,6	13,6	13,6
	4 De acuerdo	9	40,9	40,9	54,5
	5 Totalmente de acuerdo	10	45,5	45,5	100,0
	Total	22	100,0	100,0	

Fuente: Elaboración propia

Tabla 11 P11

Se requiere que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	5 Totalmente de acuerdo	21	95,5	95,5	95,5
	55	1	4,5	4,5	100,0
	Total	22	100,0	100,0	

Fuente: Elaboración propia

Tabla 12 P12

Se adopta una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de información.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	5 Totalmente de acuerdo	22	100,0	100,0	100,0

Fuente: Elaboración propia

Tabla 13 P13

Los usuarios sólo tienen acceso a los servicios para los cuales han sido específicamente autorizados.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	5 Totalmente de acuerdo	22	100,0	100,0	100,0

Fuente: Elaboración propia

Tabla 14 P14

Se utilizan métodos de autenticación para controlar el acceso de usuarios remotos.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	3 Parcialmente	5	22,7	22,7	22,7
	4 De acuerdo	3	13,6	13,6	36,4
	5 Totalmente de acuerdo	14	63,6	63,6	100,0

Se utilizan métodos de autenticación para controlar el acceso de usuarios remotos.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	3 Parcialmente	5	22,7	22,7	22,7
	4 De acuerdo	3	13,6	13,6	36,4
	5 Totalmente de acuerdo	14	63,6	63,6	100,0
	Total	22	100,0	100,0	

Fuente: Elaboración propia

Tabla 15 P15

Se considera la identificación automática del equipo como un medio para autenticar las conexiones desde equipos y ubicaciones específicas

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	5 Totalmente de acuerdo	22	100,0	100,0	100,0

Fuente: Elaboración propia

Tabla 16 P16

Se controla el acceso físico y lógico a los puertos de diagnóstico y configuración

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	5 Totalmente de acuerdo	22	100,0	100,0	100,0

Fuente: Elaboración propia

Tabla 17 P17

Los servicios de información, usuarios y sistemas de información están desagregados en las redes

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	5 Totalmente de acuerdo	22	100,0	100,0	100,0

Fuente: Elaboración propia

Tabla 18 P18

Se restringe la capacidad de conexión de los usuarios en las redes compartidas

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	3 Parcialmente	1	4,5	4,5	4,5
	4 De acuerdo	6	27,3	27,3	31,8
	5 Totalmente de acuerdo	15	68,2	68,2	100,0
	Total	22	100,0	100,0	

Fuente: Elaboración propia

Tabla 19 P19

Se controla el acceso a los servicios operativos mediante un procedimiento de registro seguro

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	5 Totalmente de acuerdo	22	100,0	100,0	100,0

Fuente: Elaboración propia

Tabla 20 P20

Todos los usuarios tienen un identificador singular (ID de usuario) para su uso personal y exclusivo

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	5 Totalmente de acuerdo	22	100,0	100,0	100,0

Fuente: Elaboración propia

Tabla 21 P21

Los sistemas de manejo de claves son interactivos y aseguran la calidad de las claves.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	3 Parcialmente	1	4,5	4,5	4,5
	4 De acuerdo	5	22,7	22,7	27,3
	5 Totalmente de acuerdo	16	72,7	72,7	100,0
	Total	22	100,0	100,0	

Fuente: Elaboración propia

Tabla 22 P22

Se restringe y controla estrictamente el uso de los programas de utilidad que podrían superar al sistema y los controles de aplicación

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	5 Totalmente de acuerdo	22	100,0	100,0	100,0

Fuente: Elaboración propia

Tabla 23 P23

Las sesiones inactivas se cierran después de un periodo de inactividad definido.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	5 Totalmente de acuerdo	22	100,0	100,0	100,0

Fuente: Elaboración propia

Tabla 24 P24

Se utilizan restricciones sobre los tiempos de conexión para proporcionar seguridad adicional a las aplicaciones de alto riesgo

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	5 Totalmente de acuerdo	22	100,0	100,0	100,0

Fuente: Elaboración propia

Tabla 25 P25

Se restringe el acceso de los usuarios y personal de soporte al sistema de información y aplicación en concordancia con la política de control de acceso definida.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	5 Totalmente de acuerdo	22	100,0	100,0	100,0

Fuente: Elaboración propia

Tabla 26 P26

Los sistemas sensibles tienen un ambiente de cómputo dedicado

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	3 Parcialmente	16	72,7	72,7	72,7
	4 De acuerdo	5	22,7	22,7	95,5
	5 Totalmente de acuerdo	1	4,5	4,5	100,0
	Total	22	100,0	100,0	

Fuente: Elaboración propia

Tabla 27 P27

Todos los ítems de equipo que contengan medios de almacenaje son chequeados para asegurar que se haya removido o sobre escrito de manera segura cualquier data confidencial y software con licencia antes de su eliminación.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	4 De acuerdo	7	31,8	31,8	31,8
	5 Totalmente de acuerdo	15	68,2	68,2	100,0
	Total	22	100,0	100,0	

Fuente: Elaboración propia

Tabla 28 P28

Los equipos están protegidos para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	5 Totalmente de acuerdo	22	100,0	100,0	100,0

Fuente: Elaboración propia

Tabla 29 P29

Los equipos están protegidos de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	3 Parcialmente	5	22,7	22,7	22,7
	5 Totalmente de acuerdo	17	77,3	77,3	100,0
	Total	22	100,0	100,0	

Fuente: Elaboración propia

Tabla 30 P30

El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información están protegidos de la intercepción o daño.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	5 Totalmente de acuerdo	22	100,0	100,0	100,0

Fuente: Elaboración propia

Tabla 31 P31

Los equipos son mantenidos correctamente para permitir su continua disponibilidad e integridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	1 Totalmente en desacuerdo	2	9,1	9,1	9,1
	2 En desacuerdo	6	27,3	27,3	36,4
	3 Parcialmente	8	36,4	36,4	72,7
	5 Totalmente de acuerdo	6	27,3	27,3	100,0
	Total	22	100,0	100,0	

Fuente: Elaboración propia

Tabla 32 P32

Los equipos, información o software no son sacados fuera de la propiedad sin previa autorización.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	4 De acuerdo	10	45,5	45,5	45,5
	5 Totalmente de acuerdo	12	54,5	54,5	100,0
	Total	22	100,0	100,0	

Fuente: Elaboración propia

Tabla 33 P33

Se realizan copias de back up o respaldo de la información comercial y software esencial y se prueban regularmente de acuerdo a la política

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	5 Totalmente de acuerdo	22	100,0	100,0	100,0

Fuente: Elaboración propia

Tabla 34 P34

Las redes son manejadas y controladas adecuadamente para poderlas proteger de amenazas y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo información en tránsito.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	5 Totalmente de acuerdo	22	100,0	100,0	100,0

Fuente: Elaboración propia

Tabla 35 P35

Se identifican los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red, ya sea que estos servicios sean provistos en casa o sean abastecidos externamente

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	4 De acuerdo	7	31,8	31,8	31,8
	5 Totalmente de acuerdo	15	68,2	68,2	100,0
	Total	22	100,0	100,0	

Fuente: Elaboración propia

Gráficos de los indicadores más relevantes

Tabla 36 Estadísticos de la Confidencialidad, Integridad y Disponibilidad

Estadísticos

		Confidencialidad	Integridad	Disponibilidad
N	Válidos	22	22	22
	Perdidos	0	0	0
Media		2,8052	4,6500	4,6080
Desv. típ.		,22714	,57982	,17802
Varianza		,052	,336	,032

Fuente: Elaboración propia

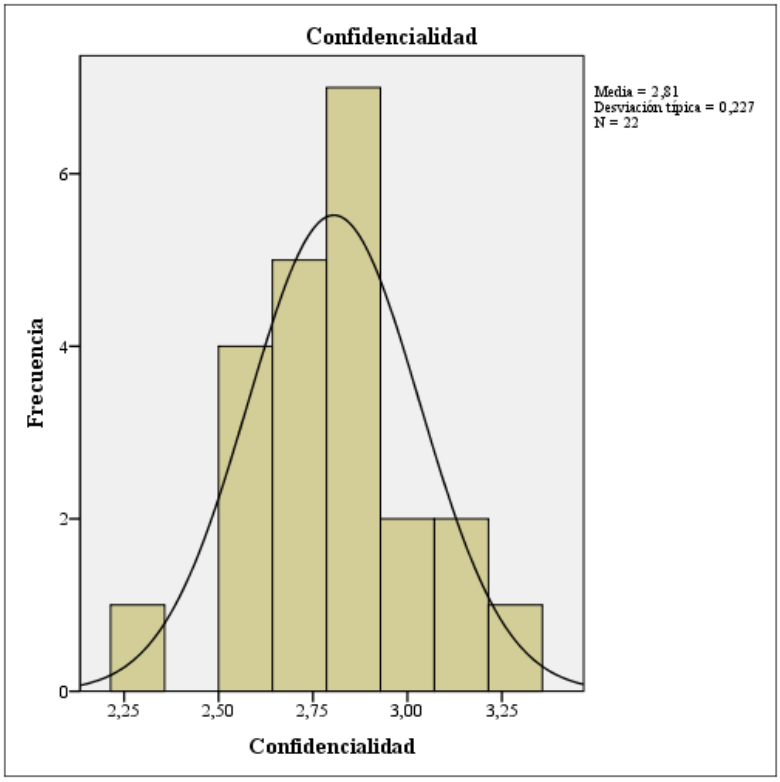


Figura 23 Confidencialidad de la información
Fuente: Elaboración propia

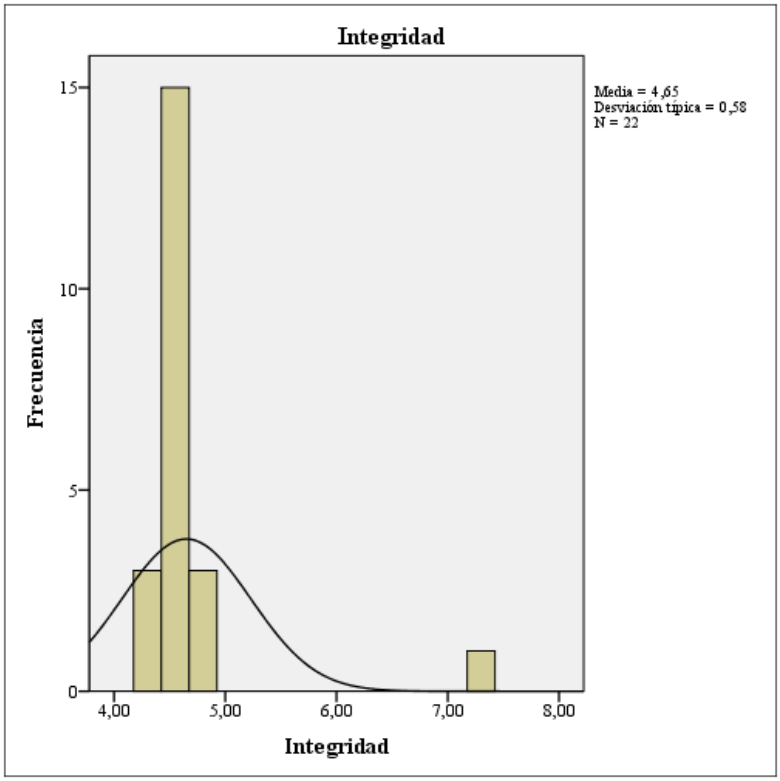


Figura 24 Integridad de la información
Fuente: Elaboración propia

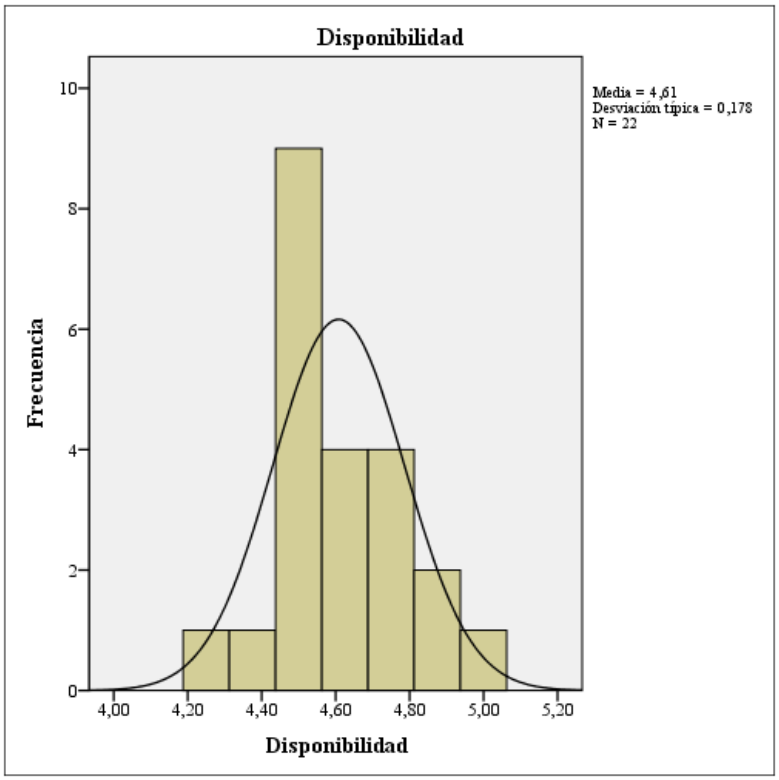


Figura 25 Disponibilidad de la información
Fuente: Elaboración propia

3.2. Prueba de normalidad

Ho: La muestra proviene de una distribución normal

Ha: La muestra no proviene de una distribución normal

Decisión: Si sig < 0.05 se rechaza la Ho y se acepta la Ha

Tabla 37 Pruebas de Normalidad

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Confidencialidad	,182	22	,055	,954	22	,382
Integridad	,420	22	,000	,390	22	,000
Disponibilidad	,228	22	,004	,927	22	,108

a. Corrección de la significación de Lilliefors
Fuente: Elaboración propia

Como la muestra es muy pobre, de tan solo 22 encuestas, aun cuando los estadísticos de normalidad de Kolmogorov-Smirnov nos indican que la variable Confidencialidad proviene de una distribución normal, optamos por realizar un análisis no paramétrico en

las tres variables en estudio. Tener presente que de las variables Integridad y Disponibilidad su Sig < 0.05 con lo cual se rechaza la Ho y se acepta las Ha, es decir la muestra de ambas variables no proviene de una distribución normal.

3.3. Contrastación de las hipótesis

Confidencialidad de la información

Ho: la firma de un documento de confidencialidad de la información no influye en la Confidencialidad de la información

Ha: la firma de un documento de confidencialidad de la información influye en la Confidencialidad de la información

Tabla 38 Confidencialidad

Estadísticos de contraste[b]

	Confidencialidad - Han firmado un documento de confidencialidad de la información
Z	-2,787[a]
Sig. asintót. (bilateral)	,005

a. Basado en los rangos negativos.

b. Prueba de los rangos con signo de Wilcoxon

Fuente: Elaboración propia

Como sig =0.005 < 0.05 entonces se rechaza la Ho, aceptándose la Ha, es decir con la firma de un documento de confidencialidad de la información mejora la Confidencialidad de la información

Integridad de la información

Ho: la identificación de los riesgos que corren la información y los medios de procesamiento de información de la organización y se implementan los controles apropiados antes de otorgar acceso no influye en la Integridad de la información

Ha: la identificación de los riesgos que corren la información y los medios de procesamiento de información de la organización y se implementan los controles apropiados antes de otorgar acceso influye en la Integridad de la información

Tabla 39 Integridad

Estadísticos de contraste[b]

	Integridad - Se identifican los riesgos que corren la información y los medios de procesamiento de información de la organización y se implementan los controles apropiados antes de otorgar acceso.
Z	-3,947[a]
Sig. asintót. (bilateral)	,000

a. Basado en los rangos negativos.

b. Prueba de los rangos con signo de Wilcoxon

Fuente: Elaboración propia

Como sig =0.000 < 0.05 entonces se rechaza la Ho, aceptándose la Ha, es decir la identificación de los riesgos que corren la información y los medios de procesamiento de información de la organización y se implementan los controles apropiados antes de otorgar acceso influye en la Integridad de la información

Disponibilidad de la información

Ho: la realización de las copias de back up o respaldo de la información comercial y software esencial y las pruebas regulares de acuerdo a la política no influye en la Disponibilidad de la información

Ha: la realización de las copias de back up o respaldo de la información comercial y software esencial y las pruebas regulares de acuerdo a la política influye en la Disponibilidad de la información

Tabla 40 Disponibilidad

Estadísticos de contraste[b]

	Disponibilidad - Se realizan copias de back up o respaldo de la información comercial y software esencial y se prueban regularmente de acuerdo a la política
Z	-4,058[a]
Sig. asintót. (bilateral)	,000

a. Basado en los rangos positivos.

b. Prueba de los rangos con signo de Wilcoxon

Fuente: Elaboración propia

Como sig =0.000 < 0.05 entonces se rechaza la Ho, aceptándose la Ha, es decir la realización de las copias de back up o respaldo de la información comercial y software esencial y las pruebas regulares de acuerdo a la política influye en la Disponibilidad de la información

Análisis de los indicadores de Confidencialidad, Integridad y Disponibilidad

Tabla 41 Escala

Totalmente de acuerdo	De acuerdo	Parcialmente	En desacuerdo	Totalmente en desacuerdo
1	2	3	4	5

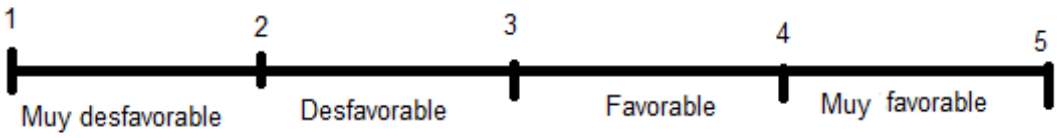
Fuente: Elaboración propia

Tabla 42 Confidencialidad, Integridad, Disponibilidad

Estadísticos

		Confidencialidad	Integridad	Disponibilidad
N	Válidos	22	22	22
	Perdidos	0	0	0
Media		2,8052	4,6500	4,6080
Desv. típ.		,22714	,57982	,17802
Varianza		,052	,336	,032

Fuente: Elaboración propia



Se puede observar que el indicador de Confidencialidad es de 2.8 estando ubicado entre 2 y 3, lo cual indica que la Confidencialidad de la Seguridad de la Información en la empresa es desfavorable

Se puede observar que el indicador de Integridad es de 4.65 estando ubicado entre 4 y 5, lo cual indica que la Integridad de la Seguridad de la Información en la empresa es muy favorable

Se puede observar que el indicador de Disponibilidad es de 4.61 estando ubicado entre 4 y 5, lo cual indica que la Disponibilidad de la Seguridad de la Información en la empresa es muy favorable

IV. DISCUSIÓN

Del análisis realizado se ha podido determinar que la disponibilidad, integridad y confidencialidad de la información de la empresa Automatisoft SA no es confiable es más bien variable, dado que aún no cuenta con el sistema de Seguridad de la información, que posibilitara a la empresas mejorar la seguridad de la información que es tan necesario para garantizar precisamente que la información no caiga en manos extrañas, perjudicando de esta manera a la cualquier organización, en partículas a la empresa Automatisoft S.A.

De esta manera podemos indicar que la implantación de un sistema de seguridad de la información, al igual que (Álvarez, 2015) podemos decir que dicho sistema "se encuentra estrechamente relacionado con la gestión de riesgos de una institución y tal como se puede evidenciar en el presente documento, el análisis que realiza no está sesgado a los activos o controles tecnológicos que la institución pueda tener o requiera.

Por otro lado, al igual que (Zacarias, 2017), el cual indica que la implementación de un modelo de seguridad de la información basada en la norma ISO/IEC 27001:2013 influye positivamente en la mitigación de las amenazas de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, podemos indicar que llegamos a resultados parecidos, pues con la implementación de un sistema de seguridad e la información, se minimizan los riesgos de perdida de información.

Finalmente, al igual que (Ibáñez, 2015) que indica "que la Integridad de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada

para posteriores controles o auditorías", podemos indicar que arribamos a la misma conclusión, pues es muy relevante que la información este siempre completa e integra, de tal manera que se puedan tomar decisiones seguras y confiables a partir de la misma

V. CONCLUSIONES

La Planificación de un Sistema de Gestión de la Seguridad de la Información ISO/IEC 27001:2013, para garantizar la integridad, confidencialidad y disponibilidad de su información, es el medio para lograr que la empresa opere en un ambiente seguro, donde no haya filtros de información, perdida de la misma ni tampoco indisponibilidad, ya que estas situaciones perjudican el accionar de cualquier empresa.

El Adecuar los procesos a las normativas de protección de datos, para mejorar la integridad de la información en la empresa, es trascendental para lograr dicho objetivo tal como lo hemos podido observar que el indicador de Integridad es de 4.65 estando ubicado entre 4 y 5, lo cual indica que la Integridad de la Seguridad de la Información en la empresa es muy favorable

El Implementar las políticas de seguridad de la información para mejorar la confidencialidad de la información en la empresa, es muy relevante para lograr dicho objetivo, que entre otras cosas garantiza la continuidad del servicio, esto lo hemos podido determinar porque se ha observado que el indicador de Disponibilidad es de 4.61 estando ubicado entre 4 y 5, lo cual indica que la Disponibilidad de la Seguridad de la Información en la empresa es muy favorable. Esta disponibilidad no podría haberse dado tampoco si no se implementan las herramientas tecnológicas para mejorar la disponibilidad de la información en la empresa. La implementación de herramientas tecnológicas ayuda a minimizar las amenazas y vulnerabilidades de la información de la empresa, es importante una implementación, de acuerdo a los resultados obtenidos por autores que implementaron afirman que las herramientas tecnológicas minimizan las amenazas y vulnerabilidades de la información.

VI. RECOMENDACIONES

Se sugiere Planificar y llevar a cabo un Sistema de Gestión de la Seguridad de la Información ISO/IEC 27001:2013, para garantizar la integridad, confidencialidad y disponibilidad de su información, este proceso de implementación tiene que ser progresivo, iniciándose primero en las áreas de cómputo, para posteriormente ir abarcando a toda la empresa, porque la información, no solo esta en los medios de cómputo sino también en todo medio, impreso, video, entre otros.

Se sugiere iniciar con la adecuación de los procesos a las normativas de protección de datos, para mejorar la integridad de la información en la empresa, siendo este un paso importante, porque garantizar la integridad de los datos es trascendental para la toma de decisiones confiables.

Se sugiere implementar las políticas de seguridad de la información para mejorar la confidencialidad de la información en la empresa, esto debido, a que si la información confidencial pasa a manos extrañas puede generar múltiples reclamos.

Se sugiere implementar herramientas tecnológicas para mejorar la disponibilidad de la información en la empresa, porque de esta manera se estaría garantizándose la continuidad del negocio, facilitando la interacción con los usuarios finales.

REFERENCIAS BIBLIOGRÁFICAS

Airitio. (2008). Seguridad de la Informacion redes, informaticas y sistemas de informacion.

Alvarez. (2008). Seguridad de la Informacion.

Alvarez, S. c. (2013). Implementacion Iso 27001 Empresa Ficticia.

Álvarez, V. R. (2015). Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la iso/iec 27001:2013.

Ayala, O. A. (2011). Seguridad Informatica.

Barrantes Porras, C. e. (2012). Diseño e implementacion de un sistema de gestion de seguridad de la información en procesos tecnológicos. Lima, Perú.

Baud, J.-L. (2016). *Itil V3 Entender el enfoque y adoptar las buenas practicas.*

Belaunde, G. (2012). Herramientas Para Reforzar el Control Interno. Lima, Perú.

Bermejo. (2012). Gobierno de seguridad de la información.

BETANCUR, J. G. (2016). 47.

Bolaños, D. E. (2013). RIESGOS, AMENAZAS Y VULNERABILIDADES DE LOS SISTEMAS DE.

CajaPiura. (10 de Noviembre de 2017). *Política de privacidad general.* Obtenido de Caja Piura: https://www.cajapiura.pe/_files/PDFs/Protecci%C3%B3n-Datos-Personales/Pol%C3%ADtica-General-Privacidad.pdf

Cama, E. (11 de Junio de 2020). El 51% de las compañías en el Perú sostienen que la relación entre ciberseguridad y sus líneas de negocio es inexistente o neutral. Lima.

Campo, S. d. (2012). *ESTEREOTIPOS DE GÉNERO EN LA PUBLICIDAD DE LA SEGUNDA REPÚBLICA ESPAÑOLA: CRÓNICA Y BLANCO.*

Carlessi, H. S. (2006). *Diseño metodológico.*

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

Corcho, A. F. (2014). Riesgo y control Informatico.

Corrales, J. D. (2005). *Ayudante técnico de informática de la Junta de andalucía.*

Definicion.de. (2008). Acceso.

Desongles, J. (2005). *Ayudantes tecnicos en Informatica vol 2.*

Díaz, A. F. (2012). En a. t. Implementación de un sistema de gestión de seguridad de la información (SGSI) en la comunidad nuestra señora de gracia. Colombia.

Frett, N. (26 de 08 de 2013). 11 Principios Básicos Proceso Gestión Riesgos Norma ISO 31000.

Garzón, D. S. (2008). Metodología de análisis de vulnerabilidades para empresas de media y pequeña escala. Bogotá, Colombia.

Gestion.pe. (12 de 11 de 2020). Ciberseguridad en el Perú: ¿Qué tan preparados estamos para enfrentar la ciberdelincuencia? Lima.

Gonzalez, J. C. (2016). DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION-SGSI BAJO LA NORMA ISO/IEC 27001:2013 PARA LA EMPRESA “EN LINEA FINANCIERA” DE LA CIUDAD DE CALI-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, F. y. (2010). *Metodologia de la Investigacion, Quinta edicion.*

Him, C. (2012). Vulneravilidades Informaticas.

Ibáñez, P. A. (2015). Diseño de un Sistema de Gestion de Seguridad de la Informacion en el área de Sistemas de la empresa RYMCOS S.A bajo la norma Iso/Iec 27001:2013.

IBM. (2014). La Politica de la Seguridad Informatica.

Isaca. (2009). Risk IT Framework.

Isaca. (2009). Risk IT Framework.

Isaca. (2013). Modelo de Negocios para la Seguridad de la Información.

Isaca. (2013). Modelo de Negocios para la Seguridad de la Información.

Isaca. (2013). Modelo de Negocios para la Seguridad de la Información.

iso27000. (2012). ¿Qué es un SGSI?

Iso27001:2013. (2015). Iso 27001: Ciclo de Deming.

ISOTools. (2015). ¿Cómo utilizar la criptografía en un Sistema de Gestión de Seguridad de la Información?

Kosutic, D. (2013). Lista de apoyo para implementación de ISO 27001.

Medina, D. t. (2017). *Introduccion a la ingenieris de software.* Mexico.

Mendoza, M. Á. (2015). COBIT para la seguridad en las organizaciones.

Mendoza, M. Á. (2017). *Consideraciones previas a la implementación del SGSI.*

Miranda, C. V. (2017). *Informática Industrial.*

Miranda, C. V. (2017). *Informática Industrial.*

MitEdu. (2013). MitEdu.

MuniMolina. (2003). Plan de contingencia Informatico.

Notimex. (03 de 01 de 2018). Protección de datos, prioridad para las empresas. Obtenido de elEconomista: eleconomistaamerica.pe/empresas-eAm-mexico/noticias/8845524/01/18/Proteccion-de-datos-prioridad-para-las-empresas.html

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

OpenPlaza. (03 de Junio de 2015). *Open Plaza.* Obtenido de POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES: http://www.openplaza.com.pe/opplapepr/Angamos/Ley/fuente

OpticalNews. (2013). Webfilter, la ventaja para una Navegación Segura.

Orellana, A. O. (2014). Seguridad de la Informacion. 100.

Orellana, A. O. (s.f.). Seguridad de la Informacion. 100.

Orueta, G. D. (2014). *Proceso de herramientas para la Seguridad de Redes.*

Palacios, A. M. (2015). Tecnologia de Informacion y Comunicacion. 7.

Peruano, E. (Septiembre de 2012). Proyecto de reglamento de la ley N° 29733. *Ley de proteccion de datos personales*, pág. 2.

Peshazur, E. y. (1991). *Measurement, desig, and analysis. An integrated approach.*

Pozo, R. P. (2016). Tecnologia de Informacion y Comunicacion. 14.

Pozo, R. P. (2016). Tecnologia de Informacion y Comunicacion. 14.

Prandini, P. (2013). Vulnerabilidades, amenazas y riesgo en "texto claro". *Magazcitum*.

Publicay. (2019). La información, el activo más valioso de las empresas. *Publicay*.

Pulido, J. A. (Mayo de 2014). Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá. Colombia.

PWC. (2017). Encuesta Global de Seguridad. 5. Argentina.

Rizzuti, D. (2013). Que se entiende por Integridad de Datos.

Rojas, R. (2010). Herramientas de monitoreo y análisis de redes. *CioPeru*.

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

Salinas, Z. I. (2015). DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA UNA EMPRESA INMOBILIARIA ALINEADO A LA NORMA ISO/IEC 27001:2013.

Santos, L. M. (Junio de 2012). Guía para la evaluación de seguridad en un sistema.

SecureIT. (2016). Procesos de Gobierno IT.

Soriano, M. (Diciembre de 2013). Seguridad en redes y seguridad de la informacion.

Suárez, E. C. (2015). diseño e implementación de un SGSI para el área de informática de la curaduría urbana segunda de pasto bajo la norma ISO/IEC 27001. Pasto, Colombia.

Tecnologia, D. d. (2017). Seguridad logica y fisica.

Trends, L. a. (Septiembre de 2016). Aplicación práctica (y progresiva) del nuevo Reglamento europeo de protección de datos. España.

Vidal, J. A. (2004). *La gestion del conocimiento como motor de la innovacion.*

Zacarias, J. C. (2017). Modelo de la seguridad de la informacion basado en la Iso/IEC 27001:2013 para mitigar los riesgos de los activos de imformacion en la central de operaciones policiales de la region policial Junin.

ANEXOS

Anexo 1: Matriz de Consistencia

Tabla A01.1:
Matriz de Consistencia

Problemas General	Objetivos General	Hipótesis General	Variables Independiente	Indicador V.I.	Variables Dependiente	Indicador V.D.
¿En qué medida el SGSI ayudará a garantizar la integridad, confidencialidad y disponibilidad de la información en la empresa?	Planificar un Sistema de Gestión de la Seguridad de la Información ISO/IEC 27001:2013, para garantizar la integridad, confidencialidad y disponibilidad de su información.	Si se planifica un Sistema de Gestión de la Seguridad de la Información ISO/IEC 27001:2013, entonces garantizará la integridad, confidencialidad y disponibilidad de su información.	*Sistema de gestión de la seguridad de la información*	*Si / No*	*Integridad, confidencialidad y disponibilidad de la información*	--
Problemas Especifico	**Objetivos Específicos**	**Hipótesis Especificas**				
¿Cómo adecuar los procesos a las normativas de protección de datos, para mejorar la integridad de la información en la empresa?	Adecuar los procesos a las normativas de protección de datos, para mejorar la integridad de la información en la empresa.	Si se adecuan los procesos a las normativas de protección de datos entonces se mejora la integridad de la información en la empresa.	normativas de protección de datos	Si / No	Integridad	Nivel de integridad de datos
¿Cómo implementar las políticas de seguridad de la información para mejorar la confidencialidad de la información en la empresa?	Implementar las políticas de seguridad de la información para mejorar la confidencialidad de la información en la empresa.	Si se implementan las políticas de seguridad de la información entonces se mejora la confidencialidad de la información en la empresa.	políticas de seguridad de información	Si / No	Confidencialidad	Nivel de confidencialidad de la información
¿Cómo implementar las herramientas tecnológicas para mejorar la disponibilidad de la información en la empresa?	Implementar las herramientas tecnológicas para mejorar la disponibilidad de la información en la empresa.	Si se implementan las herramientas tecnológicas entonces se mejora la disponibilidad de la información en la empresa.	Herramientas tecnológicas	Si / No	Disponibilidad	Nivel de disponibilidad de la información

Elaboración propia

Anexo 2: Instrumento de recolección de datos

CUESTIONARIO DE SEGURIDAD DE LA INFORMACIÓN

Estimado colaborador con el objeto de mantener y garantizar la seguridad de la información de la empresa, se le solicita responda con la mayor veracidad las siguientes preguntas.

	ESCALA	Totalmente de acuerdo	De acuerdo	Parcialmente	En desacuerdo	Totalmente en desacuerdo
N°	**CONFIDENCIALIDAD**	**1**	**2**	**3**	**4**	**5**
1	La gerencia apoya activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explicita y reconocimiento de las responsabilidades de la seguridad de información.					
2	Las actividades de seguridad de la información son coordinadas por representantes de diferentes partes de la organización con funciones y roles laborales relevantes.					
3	Se definen claramente las responsabilidades de la seguridad de la información					
4	Se define e implementa un proceso de autorización gerencial para los nuevos medios de procesamiento de información					
5	Se identifica y revisa regularmente los requerimientos de confidencialidad de la información					
6	Se revisa independientemente a intervalos planeados, o cuando ocurran cambios significativos la seguridad de la información					
7	Han firmado un documento de confidencialidad de la información					
	INTEGRIDAD	1	2	4	4	5
8	Se identifican los riesgos que corren la información y los medios de procesamiento de información de la organización y se implementan los controles apropiados antes de otorgar acceso.					
9	Se tratan todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o activos de la organización					
10	Los acuerdos que involucran acceso, procesamiento, comunicación o manejo por parte de terceras personas a la información a los medios de procesamiento de información de la organización, agregar productos o servicios a los medios de procesamiento de la información abarcan los requerimientos de seguridad necesarios relevantes					
11	Se requiere que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves					
12	Se adopta una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de información.					
13	Los usuarios sólo tienen acceso a los servicios para los cuales han sido específicamente autorizados.					

14	Se utilizan métodos de autenticación para controlar el acceso de usuarios remotos.					
15	Se considera la identificación automática del equipo como un medio para autenticar las conexiones desde equipos y ubicaciones específicas					
16	Se controla el acceso físico y lógico a los puertos de diagnóstico y configuración					
17	Los servicios de información, usuarios y sistemas de información están desagregados en las redes					
18	Se restringe la capacidad de conexión de los usuarios en las redes compartidas					
19	Se controla el acceso a los servicios operativos mediante un procedimiento de registro seguro					
20	Todos los usuarios tienen un identificador singular (ID de usuario) para su uso personal y exclusivo					
21	Los sistemas de manejo de claves deben ser interactivos y deben asegurar la calidad de las claves.					
22	Se restringe y controla estrictamente el uso de los programas de utilidad que podrían superar al sistema y los controles de aplicación					
23	Las sesiones inactivas se cierran después de un periodo de inactividad definido.					
24	Se utilizan restricciones sobre los tiempos de conexión para proporcionar seguridad adicional a las aplicaciones de alto riesgo					
25	Se restringe el acceso de los usuarios y personal de soporte al sistema de información y aplicación en concordancia con la política de control de acceso definida.					
26	Los sistemas sensibles tienen un ambiente de cómputo dedicado					
27	Todos los ítems de equipo que contengan medios de almacenaje son chequeados para asegurar que se haya removido o sobre escrito de manera segura cualquier data confidencial y software con licencia antes de su eliminación.					
	DISPONIBILIDAD	1	2	3	4	5
28	Los equipos están protegidos para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.					
29	Los equipos están protegidos de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.					
30	El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información están protegidos de la intercepción o daño.					
31	Los equipos son mantenidos correctamente para permitir su continua disponibilidad e integridad					
32	Los equipos, información o software no son sacados fuera de la propiedad sin previa autorización.					
33	Se realizan copias de back up o respaldo de la información comercial y software esencial y se prueban regularmente de acuerdo a la política					
34	Las redes son manejadas y controladas adecuadamente para poderlas proteger de amenazas y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo información en tránsito.					
35	Se identifican los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red, ya sea que estos servicios sean provistos en casa o sean abastecidos externamente					

Muchas gracias…

Validación del Instrumento por parte 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:

PLANIFICAR LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA LA INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD DE SU INFORMACIÓN EN LA EMPRESA AUTOMATISOFT S.A.C

PRESENTADO POR (Tesista): **Bach. Lucas Asencio, Jesús Lorenzo**

DATOS GENERALES DEL EXPERTO NRO: 1

1.1. Apellidos y Nombres : Hidalgo Palomino, Fernando Guillermo.
1.2. Grado Académico : Magister .....
1.3. Cargo e Institución donde Labora: Docente en la 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				X	
4. ORGANIZACION	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. METODOLOGIA	Responde al propósito del trabajo bajo los objetivos a lograr.					X

II. OPCION DE APLICABILIDAD : MUY BUENO.....

III. PROMEDIO DE VALORACIÓN : 80%.....

IV. RECOMENDACIÓNES : Aplicar el instrumento .....

Firma del experto: .....

Fecha: 22/ 03 / 2022 DNI 06844769

UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA
FACULTAD DE CIENCIAS E INGENIERÍA

INGENIERÍA DE SISTEMAS E INFORMATICA

VALIDACIÓN DE INSTRUMENTO

TÍTULO DE LA TESIS:

PLANIFICAR LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA LA INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD DE SU INFORMACIÓN EN LA EMPRESA AUTOMATISOFT S.A.C

PRESENTADO POR (Tesista): **Bach. Lucas Asencio, Jesús Lorenzo**

DATOS GENERALES DEL EXPERTO NRO: 2.

1.1. Apellidos y Nombres : Santos Matos, Carmen Silvia

1.2. Grado Académico : Magister .....

1.3. Cargo e Institución donde Labora: Docente en la Universidad de Educación Enrique Guzmán y Valle,

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. ORGANIZACION	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. METODOLOGIA	Responde al propósito del trabajo bajo los objetivos a lograr.					X

II. OPCION DE APLICABILIDAD : EXCELENTE.....

III. PROMEDIO DE VALORACIÓN : 90%.....

IV. RECOMENDACIÓNES : Aplicar la encuesta .....

Firma del experto: .....

Fecha: 22/ 03 / 2022 DNI 07580701

UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA
FACULTAD DE CIENCIAS E INGENIERÍA

INGENIERÍA DE SISTEMAS E INFORMATICA

VALIDACIÓN DE INSTRUMENTO

TÍTULO DE LA TESIS:

PLANIFICAR LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA LA INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD DE SU INFORMACIÓN EN LA EMPRESA AUTOMATISOFT S.A.C

PRESENTADO POR (Tesista): **Bach. Lucas Asencio, Jesús Lorenzo**

DATOS GENERALES DEL EXPERTO NRO: 3.

1.1. Apellidos y Nombres : Julia Norma Parco Huaringa

1.2. Grado Académico : Magister .....

1.3. Cargo e Institución donde Labora: Consultora de proyectos

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. ORGANIZACION	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. METODOLOGIA	Responde al propósito del trabajo bajo los objetivos a lograr.				x	

II. OPCION DE APLICABILIDAD : MUY BUENO.....

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

IV. RECOMENDACIÓNES : Aplicar la encuesta .....

Fecha: 22/ 03 / 2022

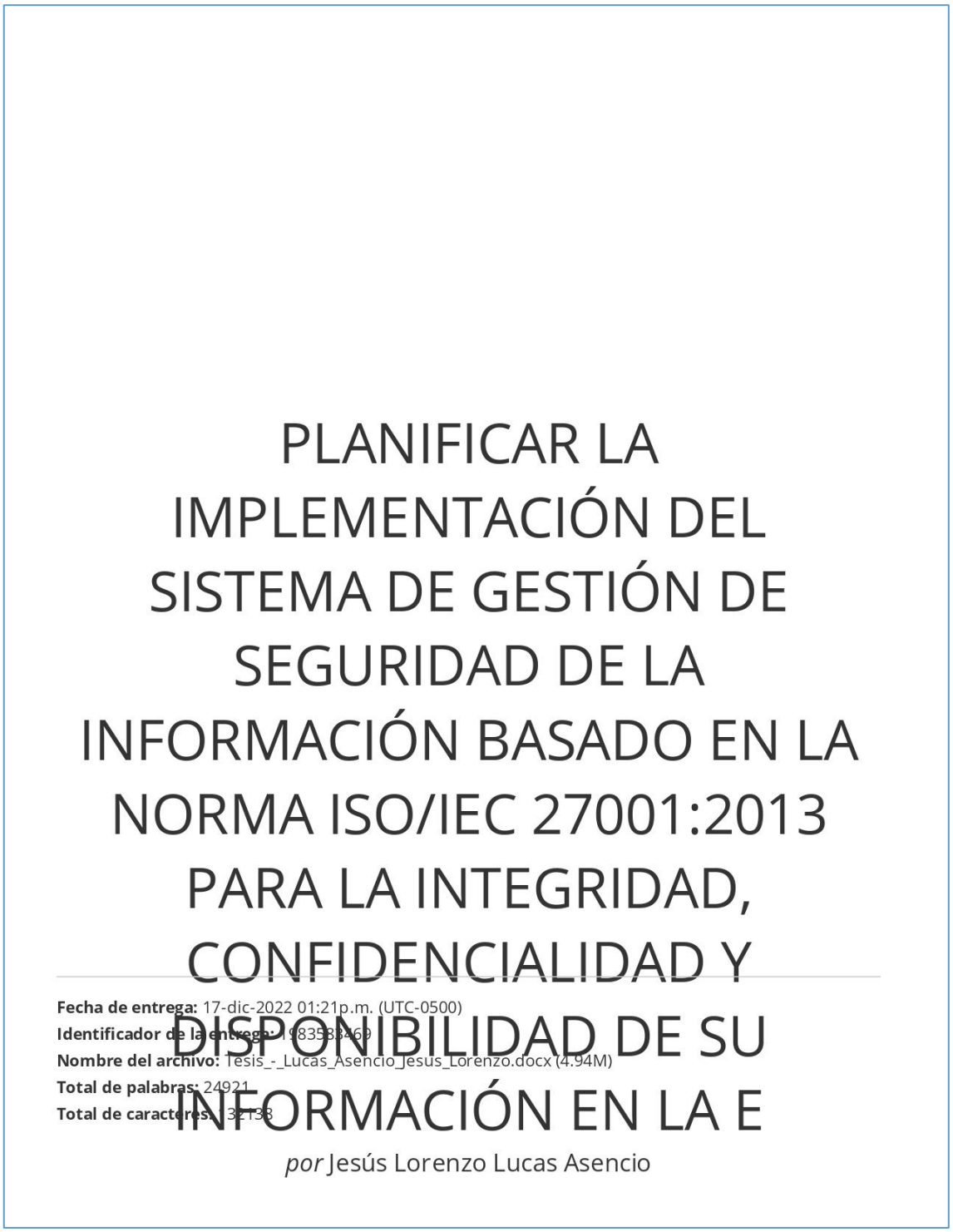
Firma del experto:

DNI 40161394

Anexo 3: Base de datos

ID	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	p31	p32	p33	p34	p35
1	3	3	3	4	3	2	1	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	3	5	5	5	5	2	4	5	5	5
2	3	3	3	4	3	2	1	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	3	5	5	5	5	2	4	5	5	5
3	3	3	3	4	3	2	1	4	4	5	55	5	5	5	5	5	5	5	5	5	5	5	5	5	5	3	5	5	5	5	2	4	5	5	5
4	3	3	3	4	3	2	1	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	3	5	5	5	5	2	4	5	5	5
5	4	3	3	4	3	2	1	4	4	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	3	5	5	5	5	2	5	5	5	4
6	4	3	3	4	3	2	1	4	4	4	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	2	4	5	5	4
7	4	3	3	3	3	2	1	4	4	4	5	5	5	4	5	5	5	4	5	5	4	5	5	5	5	3	5	5	5	5	5	5	5	5	4
8	4	3	3	4	3	2	2	4	4	4	5	5	5	3	5	5	5	4	5	5	4	5	5	5	5	3	4	5	3	5	5	5	5	5	5
9	4	3	3	3	3	2	2	4	4	4	5	5	5	3	5	5	5	5	5	5	5	5	5	5	5	3	4	5	5	5	5	5	5	5	4
10	4	3	4	3	3	2	2	4	4	4	5	5	5	3	5	5	5	5	5	5	5	5	5	5	5	3	5	5	3	5	5	5	5	5	4
11	4	3	4	3	3	2	3	5	3	4	5	5	5	3	5	5	5	5	5	5	5	5	5	5	5	3	5	5	3	5	3	5	5	5	5
12	5	2	4	3	2	1	3	5	3	5	5	5	5	3	5	5	5	4	5	5	5	5	5	5	5	3	5	5	3	5	5	4	5	5	4
13	5	2	4	3	2	1	3	3	3	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	3	5	5	3	5	3	4	5	5	4
14	5	2	4	3	2	1	3	3	3	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	5	5	5	3	4	5	5	5
15	3	2	4	3	2	1	1	3	3	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	4	4	5	5	5	3	4	5	5	5
16	3	2	4	3	2	2	2	3	3	3	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	5	5	5	3	4	5	5	5
17	3	2	2	3	3	2	3	2	5	3	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	4	4	5	5	5	3	5	5	5	5
18	3	1	2	3	3	3	3	2	5	3	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	4	5	5	5	5	5	5	5	5
19	3	1	2	3	3	3	3	1	5	4	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	3	5	5	5	5	3	5	5	5	5
20	3	1	3	3	4	3	3	1	3	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	3	5	5	5	5	3	5	5	5	5
21	3	2	3	4	4	3	3	2	3	5	5	5	5	5	5	5	5	3	5	5	3	5	5	5	5	3	5	5	5	5	1	5	5	5	5
22	4	2	3	4	4	3	3	3	2	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	3	5	5	5	5	1	5	5	5	5

Anexo 4: Evidencia de similitud digital



PLANIFICAR LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA LA INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD DE SU INFORMACIÓN EN LA E

INFORME DE ORIGINALIDAD

17%	16%	5%	%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	www.youblisher.com Fuente de Internet	3%
2	hdl.handle.net Fuente de Internet	2%
3	repositorio.upci.edu.pe Fuente de Internet	2%
4	Vicente Juvenal Mendoza-Noriega, Darwin Gabriel García-Herrera, Claudio Fernando Guevara-Vizcaíno, Juan Carlos Erazo-Álvarez. "Microsoft Teams como entorno virtual de la enseñanza y aprendizaje de la asignatura de Física", CIENCIAMATRIA, 2020 Publicación	1%
5	repositorio.ucv.edu.pe Fuente de Internet	1%
	bibcyt.ucla.edu.ve	

6	Fuente de Internet	1 %
7	repositorio.unp.edu.pe Fuente de Internet	1 %
8	idoc.pub Fuente de Internet	1 %
9	www.dspace.espol.edu.ec Fuente de Internet	1 %
10	repositorio.uss.edu.pe Fuente de Internet	<1 %
11	repositorio.udh.edu.pe Fuente de Internet	<1 %
12	repositorioacademico.upc.edu.pe Fuente de Internet	<1 %
13	repository.unad.edu.co Fuente de Internet	<1 %
14	Mónica Leonor Pintado-Crespo, Darwin Gabriel García-Herrera, Nancy Marcela Cárdenas-Cordero, Juan Carlos Erazo-Álvarez. "Aula Invertida como estrategia didáctica para la enseñanza de la Química en Bachillerato", CIENCIAMATRIA, 2020 Publicación	<1 %
15	(Carlinda Leite and Miguel Zabalza). "Ensino superior: inovação e qualidade na docência",	<1 %

	Repositório Aberto da Universidade do Porto, 2012. Publicación	
16	virtual.urbe.edu Fuente de Internet	<1 %
17	repositorio.undac.edu.pe Fuente de Internet	<1 %
18	ri.ues.edu.sv Fuente de Internet	<1 %
19	creativecommons.org Fuente de Internet	<1 %
20	repositorio.uladech.edu.pe Fuente de Internet	<1 %
21	dspace.unitru.edu.pe Fuente de Internet	<1 %
22	dspace.espoch.edu.ec Fuente de Internet	<1 %
23	ri.uaemex.mx Fuente de Internet	<1 %
24	Ana Doris Mondragon-Lainez, Carlos Alberto Zúniga-Gonzalez. "Reflexiones para medir el impacto socio económico del bono productivo alimenticio", Revista Iberoamericana de Bioeconomía y Cambio Climático, 2017 Publicación	<1 %

25	documentop.com Fuente de Internet	<1 %
26	qdoc.tips Fuente de Internet	<1 %
27	"Tendencias en la Investigación Universitaria. Una visión desde Latinoamérica", Alianza de Investigadores Internacionales SAS, 2020 Publicación	<1 %
28	José-Antonio García-Martínez, Noemi Cubeiro-Rodríguez, Francisco-José Santos-Caamaño, Manuel-Arturo Fallas-Vargas. " Learning at the university through technology-mediated activities ( ) ", Culture and Education, 2022 Publicación	<1 %
29	dspace.ucuenca.edu.ec Fuente de Internet	<1 %

Excluir citas	Activo	Excluir coincidencias	< 15 words
Excluir bibliografía	Activo		

Anexo 5: Autorización de publicación en repositorio

UPCI
CAMINO AL ÉXITO
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: LUCAS ASENCIO JESUS LORENZO

DNI: 45553994 Correo electrónico: lucas.asencio@gmail.com

Domicilio: BQ. YARUSYACAN S/N PBLO. YARUSYACAN - PASCO

Teléfono fijo: _____ Teléfono celular: 931552230

2.- IDENTIFICACIÓN DEL TRABAJO Ó TESIS

Facultad/Escuela: INGENIERIA DE SISTEMAS E INFORMATICA

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

Título del Trabajo de Investigación / Tesis:

"PLANIFICAR LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA LA INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD DE SU INFORMACIÓN EN LA EMPRESA AUTOMATISOFT SAC."

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 24 días del mes de FEBRERO de 2023.

Firma

Anexo 6: Planificar el SGSI

PLANIFICAR LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA LA INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD DE SU INFORMACIÓN EN LA EMPRESA AUTOMATISOFT S.A.C

6.1 Situación actual

Integridad de los datos

Una de las problemáticas que actualmente se observa es de la protección de datos, la empresa cuenta con bases de datos las cuales no son otra cosa que datos personales como (apellidos, dirección del hogar, e-mail, etc.), o quizás datos sensibles que afecten a las personas.

Esta información se almacena en la base de datos de la empresa, existen encargados que, si saben protegerlas y salvaguardarlas ya que es necesario un usuario y una contraseña frente a cualquier tipo de incidente, el problema es que las claves y/o contraseñas no son alcanzadas a un responsable o a una persona que está a cargo de la seguridad de la información.

Es así que nuestros registros de información que se encuentran en nuestra base de datos se llegaron a extraviar o eliminar por empleados que ya no laboran en la empresa.

En la figura 26, se muestra las diferentes bases de datos creadas en MySQL donde contienen diferentes tipos de datos.

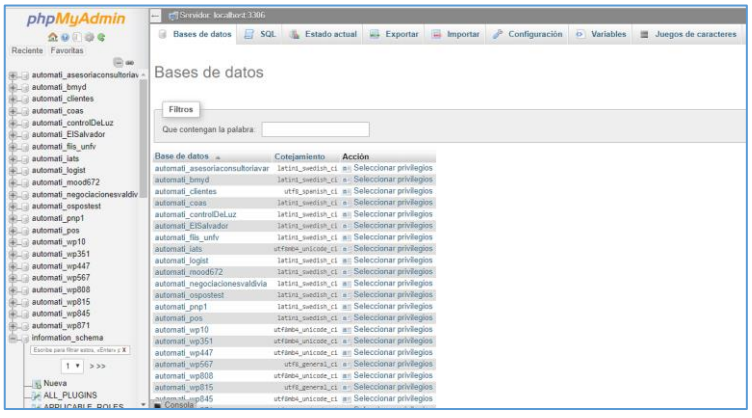


Figura 26 Base de datos de la empresa
Fuente: Elaboración propia

Se considera que en nuestra empresa se conoce poco del tema de protección de datos personales e incluso existe una ley que estaría afectando a la gran mayoría de las empresas, no existe un plan donde podemos garantizar el derecho fundamental de los datos personales realizando un adecuado tratamiento a los mismos.

Como se mencionó en el marco conceptual de esta investigación la ley para la protección de datos personales se dice que los empleados deben de conocer la restricción y el tratamiento de la información la cual no se cumple en la empresa.

Por otro lado, tenemos redundancia de datos nuestra información se registra y almacena en diferentes archivos y a la vez hay archivos innecesarios del personal que labora en la empresa esto causa problemas en nuestra base de datos porque ocupa espacio y no consideramos la cantidad de datos que se va a almacenar.

Los activos de información

La empresa no cuenta con un inventario de activos de tipo software, hardware y servicios, cada trabajador dispone de una computadora, todo software utilizado dispone de licencias pertinentes (más conocido como piratería de software), además dispone de 6 impresoras que se utiliza por área o a la vez por todo el personal de la empresa.

La falta de formación y desconocimiento por parte de los trabajadores de la empresa es perjudicial, la mayoría no hace un uso adecuado y seguro de los equipos o aparatos que administran.

En cuanto al acceso al área donde se encuentra el servidor, esta se encuentra en un mismo lugar, sin estar separada físicamente fuera de la empresa, el acceso a la habitación solo ingresa el jefe de área de TI ya que él tiene la llave de este ambiente.

Sin embargo, si sucediera algo en la empresa ya se cualquier tipo de problema no tenemos ninguna credencial de login de dichos servidores ya que estos deben ser conocidos o estar disponible por lo menos para otra persona y no solo por el jefe de TI.

A continuación, se observa las instalaciones de donde se encuentra el rack de servidor. (Ver Figura 27)

Figura 27 Servidor de la empresa
Fuente: Elaboración Propia

Seguridad física y controles de acceso

Aun no se dispone de ningún mecanismo de seguridad en la empresa con la finalidad de identificar a personas que accedan a las instalaciones, es debido a que es una empresa pequeña ni mucho menos contamos con identificaciones para invitados de manea para que se identifiquen.

La empresa está casi expuesta sufrir ciertas pérdidas de información ya sea por personas que están fuera de la empresa o quizás por los mismos empleados, es así que la empresa no toma medidas para restringir el acceso a las instalaciones.

Solo el control de acceso que se tiene hoy es de los usuarios y que cada uno tiene un identificador que es usuario y contraseña que permitirá acceder a su computadora.

6.2 Propuesta del SGSI

Adecuar los procesos a las normativas de protección de datos en la empresa, como se ha podido ver en este trabajo de investigación este es uno de los problemas que acontece.

La empresa cuenta con una base de datos donde se encuentra numerosa información tanto de los empleados, clientes y personas que normalmente hacen consultas, lo cual interactúan con nosotros.

Para empezar, se designará a un responsable de la administración de la base de datos de la empresa donde identificara qué usuarios tienen acceso a insertar, actualizar o eliminar

datos y a la vez estará muy bien informado de la ley Nro. 29733 Ley de Protección de Datos.

Estamos muy interesados en ofrecer a nuestros clientes la seguridad más efectiva y sobre todo proteger la confidencialidad de los datos personales, nuestra página web de la empresa fue creada y diseñada con la finalidad de hacer llegar a las personas interesadas donde sea un medio donde se realizan consultas relacionadas a nuestros servicios y también para el proceso de reclutamiento que convoca la empresa a través que remiten los currículums.

Legislación: De acuerdo a la ley N° 29733 Ley de protección de datos aprobado por el Decreto Supremo N° 003-2013- JUS. Nos da a entender que los datos personales ya sea alfabética, acústica, fotográfica, grafica o cualquier tipo concerniente a una persona natural que la identifique o es identificable a través de los medios que puedan utilizar.

También nos da a entender que por tratamiento de datos personales a cualquier operación ya sea un procedimiento técnico, donde permiten recopilación, un registro, almacenamiento, organización, comunicación por transferencia que facilite un acceso, etc., podemos llegar a una conclusión de los tratamientos de la información personal:

- **Sección (contacto)** de nuestra página web, atiende y gestiona las consultas, sugerencias y reclamos de las personas que están interesados en nuestros servicios que brinda la empresa.

Viendo este caso si la persona es un cliente potencial, sus datos serán exclusivamente almacenados en un banco de datos llamado “clientes potenciales” de la titularidad de la empresa. En la dirección donde se encuentra dicha empresa.

La recolección de datos personales permitirá a nuestra empresa a mantener informado a nuestros clientes sobre nuestros servicios o nuevos servicios que se ofrecerá a futuro de su interés por un plazo determinado, salvo que el cliente o persona no se encuentre interesando en lo informado los datos serán cancelados. (Ver Figura 28)

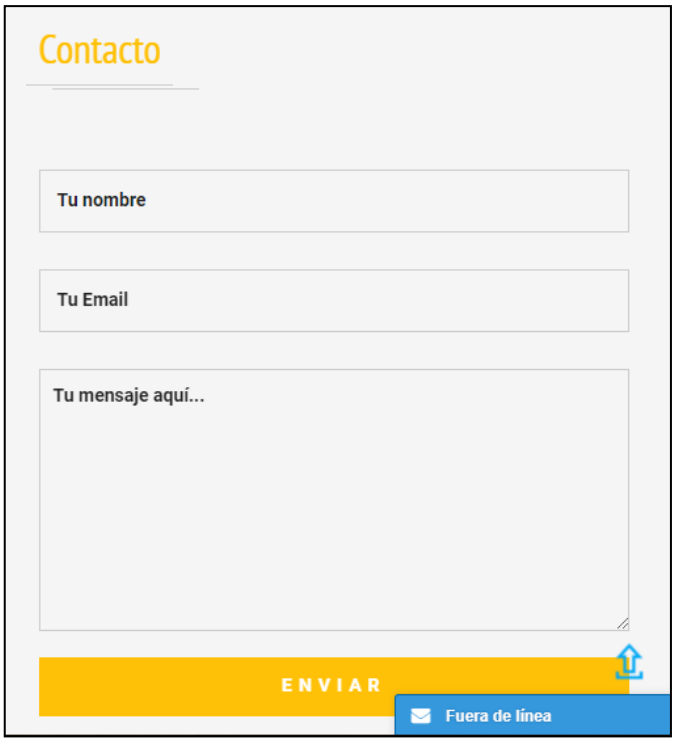


Figura 28 Sección contactos de la empresa
Fuente: web de la empresa

- **Sección (trabaja con nosotros)** al recibir los currículums vitae de estas personas interesadas en este reclutamiento de nuevo personal que convoque la empresa.

Estos datos personales serán tratados exclusivamente para su participación en el proceso de selección de personal.

Tendremos un banco de datos de titularidad de la empresa ha sido debidamente inscritos en el Registro de Protección de Datos de la Autoridad de Protección de Datos Personales, cumpliendo lo señalado en el artículo 79º del Reglamento.

Los datos personales que faciliten las personas solo podrán ser conocidos por nuestro personal a cargo de la empresa que necesiten conocer la información para realizar o ejecutar sus labores, como contestar las consultas formuladas por las personas seleccionadas o para llevar a cargo el proceso de reclutamiento, estos datos serán tratados de forma muy legal, licita y no será utilizados para otras finalidades inadecuadas y/o diferente en lo señalado. (Ver Figura 29)

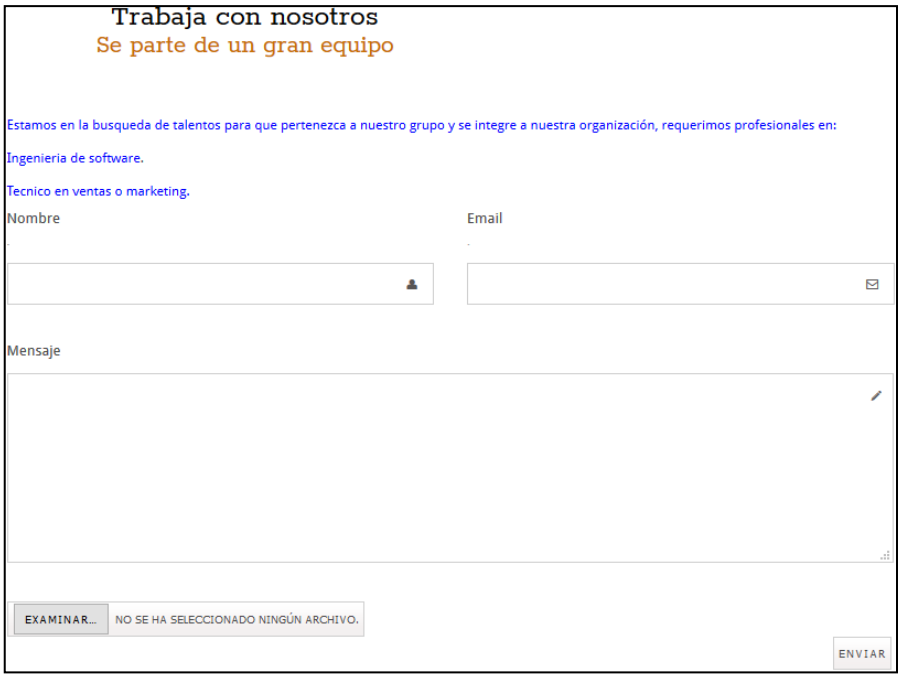


Figura 29 Sección Trabaja con Nosotros
Fuente: web de la empresa

Proceso donde nos adecuamos a la ley para cumplirlas:

a. Detallar quién obtiene los datos en nuestra empresa, quién los guarda, si son transferidos a terceros, dónde se encuentran y que tiempo estará almacenado.

b. Hacer un análisis interno de cómo se muestran los datos personales en la empresa, localizar los bancos de datos que recogen la información. Por lo habitual no hay una sola base de datos y están en diferentes áreas de la empresa.

c. Comprobar cómo utilizamos los datos en la empresa y de acuerdo a la norma debemos asegurarlos en cuanto lo utilizamos o lo guardamos. Para hacerlo es necesario tener un sistema de gestión de la seguridad de la información, para el mecanismo de control.

d. Implementación de un plan para corregir los problemas encontrados identificados en la base de datos para poder subsanarlos y que sea conforme a lo que sea establecido de acuerdo a ley.

6.3 Planificar la propuesta de implementación del SGSI

Planificar el Proyecto de Implementación, para minimizar los riesgos de información en la empresa, como se ha podido notar en el trabajo de investigación este es uno de los problemas que acontece.

Así que la propuesta es Planear, diseñar y recomendar la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) enfocado a los procesos de las áreas de: Tecnología de la información, control interno, administración servicios al personal, seguridad física en la empresa.

Para la implementación del Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad. (Ver Figura 30)

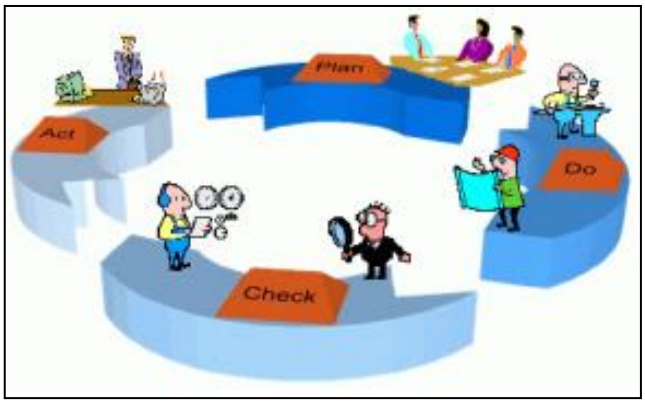


Figura 30 Ciclo continuo PDCA
Fuente: Iso27000.es

Plan (planificar): establecer el SGSI.

Do (hacer): implementar y utilizar el SGSI.

Check (verificar): monitorizar y revisar el SGSI.

Act (actuar): mantener y mejorar el SGSI.

Para la estructura para el plan de proyecto detallaremos de cómo se establecerá el plan de implementación:

6.3.1 Implementación: Plan

Establecer el alcance del SGSI con finalidades de negocio, la organización, su localización, activos y tecnológicos, teniendo en cuenta detalles y justificación de cualquier descarte.

Tener en cuenta políticas de seguridad que:

- incluya la actividad de la empresa y los objetivos de seguridad de la información;
- considere requerimientos legales relativos a la seguridad de la información;
- esté alineada con el contexto estratégico de gestión de riesgos (GPTI) de la organización en el que se establecerá y mantendrá el SGSI;
- establezca los criterios con los que se va a evaluar el riesgo (relativos a la seguridad); métricas cuantitativas o cualitativas;
- establezca los procesos a seguir si un riesgo ocurre.
- esté aprobada por la dirección.
- Establezca los sistemas de comunicación para las políticas se difundan en la organización y así sean conocidas por todos.

Definir una metodología de evaluación del riesgo alineada a los requerimientos del negocio, que establezca los criterios de aceptación del riesgo y especifique los niveles de riesgo aceptable para el SGSI. Lo resultados de la metodología adoptada, que puede ser estándar o propia, deben comparables y repetibles. (Ver Figura 9)

Figura 31 Gestión de riesgos
Fuente: Iso27000.es

Identificar los riesgos:

- identificar los activos junto con sus responsables directos que están dentro del alcance del SGSI;
- identificar las amenazas a los activos;
- identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas;

- identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.

Analizar y evaluar los riesgos:

- evaluar el impacto en el negocio en relación a la pérdida de confidencialidad, integridad o disponibilidad de un activo de información;
- Estimar y evaluar la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados;
- estimar los niveles de riesgo;
- determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.

Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:

- aplicar controles adecuados;
- aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos;
- Evitar y/o mitigar el riesgo, por ejemplo, no realizar la actividad que genera el riesgo
- transferir el riesgo a terceros, por ejemplo, transferir el riesgo a compañías aseguradoras o proveedores de outsourcing.
- Seleccionar los objetivos de control y los controles del para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.
- Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI.
- Definir una declaración de aplicabilidad que incluya:
    - los objetivos de control y controles seleccionados y los motivos para su elección;
    - los objetivos de control y controles que actualmente ya están implantados;

- los objetivos de control, controles y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.

6.3.2 Implementación: Hacer

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar el plan de tratamiento de riesgos, para alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.
- Implementar los controles seleccionados que lleven a cumplir los objetivos de control.
- Definir métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.
- Establecer plan de comunicación y programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
- Gestionar las operaciones del SGSI.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento y mejora continua de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

6.3.3 Implementación: Verificar

- Ejecutar procedimientos de monitorización y revisión para:
    - Hallar en el tiempo adecuado los errores en los resultados generados por el procesamiento de la información
    - Distinguir las brechas e incidentes de seguridad;
    - ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto;

  - detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores;
  - determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

- Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.
- Calcular la efectividad de los controles para verificar su cumplimiento con los requisitos de seguridad.
- Periódicamente en intervalos planificados realizar evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que se hayan producido en la organización, tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.
- En intervalos planificados llevar a cabo auditorías internas del SGSI.
- La dirección examinará periódicamente el SGSI para garantizar que el alcance determinado es el adecuado y que las mejoras en el proceso del SGSI son ostensibles.
- Actualizar los planes de seguridad en relación a las conclusiones y los hallazgos encontrados durante las actividades de monitorización y revisión.
- Llevar registro de acciones y eventos que hallan impactado sobre la efectividad del SGSI.

6.3.4 Implementación: Actuar

- Implantar en el SGSI las mejoras identificadas.
- Ejecutar acciones preventivas y correctivas en relación a las experiencias propias y de otras organizaciones.
- Impartir acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado acordando si es pertinente la forma de proceder.
- Garantizar que las mejoras introducidas alcanzan los objetivos previstos.

6.3.5 Monitoreo

El monitoreo es muy primordial en los sistemas informáticos porque aseguran un buen funcionamiento, realiza diferente tipo de análisis, busca componentes defectuosos para evitar fallos en un futuro y realiza una serie de análisis para evitar fallas en la infraestructura, la forma en que se representa un monitoreo es en gráficas estadísticas, su función de una de las herramientas es que revisa el estado del equipo y cuando encuentra una falla alerta al usuario con algún mensaje o advertencia, también ayuda vigilar el flujo de redes de gran tamaño como el ancho de banda utilizado por los trabajadores, el uso de la memoria, el uso del CPU, la comunicación entre aplicaciones, etc.

A continuación, una herramienta de software que ayudarían a la mejora de la empresa en cuanto al monitoreo. (Ver Figura 32)

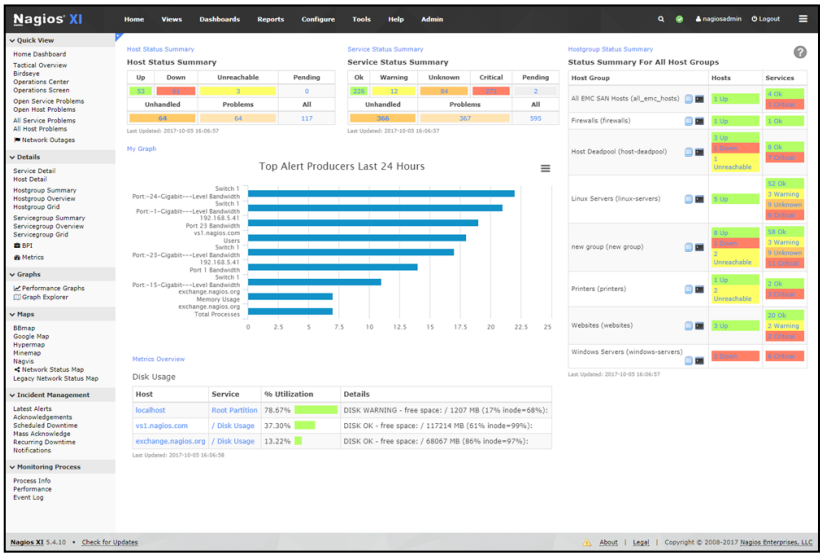


Figura 32 Herramienta Nagios XI
Fuente: Nagios.com

6.3.6 Auditoría

Es una herramienta muy importante ya que permite conocer y verificar la situación exacta del activo de información, además nos ayuda a evaluar todos los recursos para que de esta forma nos garantiza que el lugar auditado está operando con criterios de

integración y desempeño, también evalúa la seguridad y apoya mucho a la productividad.

En caso de no se estaría operando como se debiera pues se hace una serie de anotaciones, como puede ser llamada de atención, algunos resultados y sobre todo se hacen recomendaciones para que se aplique en las empresas de esta forma la próxima auditoria no se vuelve a presentar errores y aprender de estos.

Al utilizar esta herramienta se debe contar un personal totalmente capacitado con una experiencia en el campo porque debe tener el suficiente conocimiento para saber que va auditar y se debe realizar cada cierto tiempo según las políticas q se deben tener establecidas en la empresa.

Una de esta herramienta de software que ayudarían en cuanto a la auditoria seria la siguiente. (Ver Figura 33)

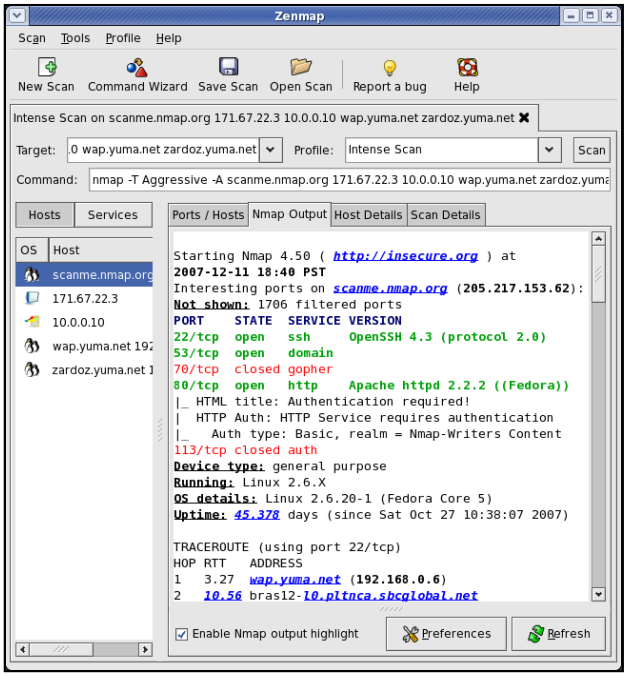


Figura 33 Herramienta Nmap
Fuente: nmap.org