UNIVERSIDAD CATÓLICA LOS ÁNGELES DE CHIMBOTE

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL GRUPO SIAS SAC. – CHIMBOTE; 2017.

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTORA:

BACH. CLOTILDE ESTHER FLORES VILLANUEVA

ASESORA:

MGTR. ING. MARÍA ALICIA SUXE RAMÍREZ

CHIMBOTE – PERÚ

2017

JURADO EVALUADOR DE TESIS Y ASESOR

DR. ING. CIP. VÍCTOR ÁNGEL ANCAJIMA MIÑÁN

PRESIDENTE

MGTR. ING. CIP. ANDRÉS DAVID EPIFANÍA HUERTA

MIEMBRO

MGTR. ING. CIP. CARMEN CECILIA TORRES CECLEN

MIEMBRO

MGTR. ING. CIP. MARÍA ALICIA SUXE RAMÍREZ

ASESORA

DEDICATORIA

A mis padres: Guadalupe Flores Arteaga y Modesta Villanueva de Flores; que me dieron la vida y han estado conmigo en todo momento. Gracias por todo papá y mamá por darme una carrera para mi futuro y creer en mí, aunque hemos pasado momentos difíciles siempre han estado apoyándome y brindándome todo su amor.

A mis hermanos Rebeca y Juan, gracias por estar conmigo y apoyarme siempre, los quiero mucho.

A mi familia en general, porque me han brindado su apoyo incondicional y por compartir conmigo buenos y malos momentos.

A mis compañeros y amigos con los que forje una bonita amistad dentro de la universidad y a todas las personas que aportaron su ayuda directa o indirectamente.

Clotilde Esther Flores Villanueva

AGRADECIMIENTO

A la Universidad Católica los Ángeles de Chimbote, por darme la oportunidad de estudiar y ser un profesional.

A mi Asesora de tesis, Mgtr. María Alicia Suxe Ramírez por su visión crítica de muchos aspectos cotidianos de la vida, por su rectitud en su profesión como docente, por sus consejos, que ayudan a formarte como persona e investigador.

A todo el personal docente de la Facultad de Ingeniería de Sistemas, por compartir sus conocimientos y enseñanzas, el cual me permite a lo largo de mi vida profesional ser competente y llegar a lograr mis metas.

También quiero dar las gracias a Jorge Serrano Soto (Gerente) y a Lesly Flores (Jefa de Gestión Humana) del GRUPO SIAS SAC por su colaboración en el suministro de los datos necesarios para la realización de esta investigación.

Clotilde Esther Flores Villanueva

RESUMEN

El presente trabajo de tesis corresponde a la línea de investigación: Implementación de las tecnologías de información y comunicación para la mejora continua de la calidad en las Organizaciones del Perú, de la escuela profesional de Ingeniería de Sistemas de la Universidad Católica los Ángeles de Chimbote. Cuyo objetivo principal fue diseñar del sistema de gestión de seguridad de la información para el GRUPO SIAS SAC. – Chimbote; 2017, con la finalidad de administrar adecuadamente la información de la empresa. El tipo de investigación fue cuantitativa, porque nos permitió examinar los datos de manera científica, y de manera más específica en forma numérica, con ayudas de herramientas de estadística descriptiva. Se contó con una población muestra constituida por 60 trabajadores del Área administrativa de la Oficina Principal, determinándose que: 100.00% de los trabajadores encuestados expresaron que NO existen políticas de seguridad de la información en el GRUPO SIAS SAC. Y que el 78.33% de los trabajadores encuestados NO tienen conocimiento acerca de las políticas de seguridad de la información en las labores administrativas que ellos realizan dentro la empresa. Estos resultados permiten afirmar que la hipótesis formulada queda aceptada; por tanto, la investigación concluye que, resulta beneficiosa el diseño del sistema de gestión de seguridad de la información para el GRUPO SIAS SAC. – Chimbote.

Palabras clave: Políticas, Seguridad, Sistema, TIC.

ABSTRACT

The present thesis work corresponds to the line of research: implementation of technologies of information and communication for the continuous improvement of the quality in the organizations of Peru, of the professional school of systems engineering of the Universidad Católica de Chimbote Ángeles. Whose main objective was to design the information security management system for the Group SIAS SAC. - Chimbote; 2017, in order to properly manage the information of the company. The type of inquiry was quantitative, because it allowed us to examine the data in a scientific way, and more specifically in numerical form, with the aid of descriptive statistics tools. We had a population shows consisting of 60 workers in the administrative Area of the main office, determining that: 100.00% of surveyed workers expressed that information security policies there are at the SIAS SAC group. And that the 78.33% of surveyed workers have NO knowledge about the policies of is security of information in administrative tasks that they perform within the company. These results allow to affirm that the hypothesis is accepted; Therefore, the investigation concluded that the design of the management of information security system is beneficial to group SIAS SAC. -Chimbote.

Keywords: policy, security, system, ICT.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE GRAFICOS

I. INTRODUCCIÓN

Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información como todo proceso de gestión. Un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno (1).

Desde hace unos cuantos años, la información ha llegado a ser considerada como el activos más valioso dentro de las empresas ya que juega un papel muy importante a la hora de la toma de decisiones y definición de nuevas estrategias de negocios, algunos de ustedes se preguntarán ¿por qué?, otros sabrán que esto es verdad, pues la información como fuente del conocimiento otorga un bien a quien la posee, incluso en la actualidad es común escuchar acerca del espionaje, tráfico y/o robo de información como delito grave, puesto que la información se ha convertido punto clave para el crecimiento, desarrollo o éxito personal, profesional y empresarial, ya que, entre mayor sea el conocimiento adquirido a través de la información mayor será el beneficio obtenido (2).

ESET - Buenos Aires, Argentina, compañía líder en detección proactiva de amenazas, lanza el Eset Security Report 2016, informe que analiza el estado de la seguridad informática en Latinoamérica y presenta los resultados de encuestas realizadas a más de 3000 profesionales de distintas organizaciones. El reporte cuenta con datos de empresas de Argentina, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú y Venezuela. En el informe se destaca que el 40% de las empresas encuestadas sufrieron un incidente relacionado con malware en el último año. Los países más afectados por códigos maliciosos son Nicaragua, que ocupa el primer lugar con el 58.3%, seguido de Guatemala con el 55.8% y Ecuador con 51.9%. Asimismo, Argentina (29.7%), Chile (29.2%) y Venezuela (24.1%) resultaron los países menos afectados por casos de malware

en las empresas. En segundo lugar, con el 16% aparece el phishing como uno de los incidentes de seguridad más frecuentes. A pesar de ser una técnica cada vez más conocida y relativamente fácil de detectar, logra su propósito a través de la aplicación efectiva de técnicas de Ingeniería Social. Según la última encuesta realizada el 2016 por Eset Latinoamérica (3).

De esta manera se hace necesario diseñar un sistema de gestión de seguridad información (SGSI) que permita salvaguardar los recursos informáticos de GRUPO SIAS SAC, ayudando a la organización a cumplir sus objetivos. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Debido a esta situación problemática se planteó el siguiente enunciado del problema: ¿De qué manera el diseño de un sistema de gestión de seguridad de la información, permitirá una adecuada administración de la información en la empresa GRUPO SIAS SAC?

Con la finalidad de dar solución a esta situación problemática se planteó el siguiente objetivo general: Realizar el diseño del sistema de gestión de seguridad de la información para el GRUPO SIAS SAC. – CHIMBOTE; 2017. Con la finalidad de administrar adecuadamente la información de la empresa. Con el propósito de lograr cumplir con el objetivo general, se definieron los siguientes objetivos específicos:

1. Determinar los riesgos que se presentan con la información que se maneja en la empresa.
2. Clasificar el nivel de impacto de los riesgos.
3. Construir planes de mitigación de riesgos (disminuir los riesgos).
4. Utilizar herramientas tecnológicas y de desarrollo que permitan la gestión de los procesos que avalen la seguridad de la información.

Considerando la justificación de la investigación esta se justifica por la necesidad de tener una descripción clara del nivel de gestión del proceso, esto

permitirá evaluar un Sistema de Gestión de Seguridad de la información aplicando la norma ISO/IEC 27001 en el GRUPO SIAS SAC, que requiere de un sistema de seguridad de la información para salvaguardar sus activos.

La información junto con los procesos que la administran además de cada una de las personas que hacen parte de los mismos siendo estos el pilar fundamental para la organización. Uno de los parámetros fundamentales a medir y analizar son los incidentes, es decir, los eventos no deseados que se detectan en la red o en los servicios y que pueden poner en riesgo la disponibilidad, la confidencialidad o la integridad de la información.

Cada evento debe ser registrado y calificado para así poder determinar cómo reaccionar ante cada incidente. Por ello, los mecanismos de seguridad necesitan de un sistema de gestión basada en el ISO/IEC 27001 que los integre a las políticas generales de la empresa. Es así como GRUPO SIAS SAC se beneficiaría con la evaluación de un sistema de gestión de seguridad de la Información basada en el ISO/IEC 27001 pues éste permitirá establecer políticas, procedimientos, objetivos y procesos claros que permitan determinar y establecer controles de seguridad que ayuden a tratar los riesgos en la seguridad de la información comprendiendo espacios físicos, procesos automáticos y manuales, gestión del personal, usuarios de los sistemas y equipos para optimizar la gestión de los incidentes que se detecten y generar resultados en concordancia con las políticas y objetivos generales de la Empresa.

Esta investigación tiene un alcance y limitaciones que busca proponer un sistema de gestión de seguridad de la Información para el GRUPO SIAS SAC. El alcance del presente proyecto, abarca un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001, para resguardar la confidencialidad, disponibilidad e integridad de los activos de información del GRUPO SIAS SAC. El alcance del proyecto solo estará precedido por un diagnóstico de la situación actual de la seguridad de la información, que

permita un análisis comparativo de los controles a ser implantados o requeridos en la empresa. Las limitaciones del proyecto de tesis consistirán solo en un Diseño del sistema de gestión de la seguridad de la información basada en la norma ISO/IEC 27001, pero no abarca la parte de la implementación del SGSI en la organización.

II. REVISIÓN DE LA LITERATURA

2.1. Antecedentes

2.2.1. Antecedentes A Nivel Internacional

Yagual, C. y Chilán, L. (4), en la tesis "Análisis para la integración de un Sistema de Gestión de Seguridad de Información (SGSI) ISO-27001 Utilizando OSSIM para empresa Industrial". Realizado en la Universidad Politécnica SALESIANA, ubicado en el país de Ecuador, en el año 2014. La presente investigación tiene como objetivo general minimizar los riesgos de seguridad de la información mediante el análisis previo a la implementación de la norma ISO 27001 combinando las herramientas de seguridad que ofrece OSSIM logrando así el fortalecimiento de un sistema de gestión de control eficiente para el área de Tecnología de información, como también proponer políticas y objetivos para la seguridad de la información, identificar los activos más críticos de los diferentes procesos de la empresa, donde aplicara controles adecuados previniendo riesgos encontrados, permitirá la visualización de análisis de eventos de vulnerabilidad que pudieran presentarse dentro de la infraestructura de la empresa mediante la consola de aplicación OSSIM.

Barragán, I.; Góngora I. y Martínez, E. (5), en la tesis "Implementación de políticas de seguridad informática para la municipalidad de Guayaquil aplicando la norma ISO/IEC 27002". Realizado en la Escuela Superior Politécnica del Litoral, ubicado en el país de Ecuador, en el año 2013. La investigación realizada en su objetivo, fue formular un modelo de política de seguridad de la información que sirva de punto de partida para la elaboración de políticas correspondientes tomando como base estándares internacionales, se decidió basar el modelo en la norma ISO/IEC 27002,como un marco de referencias para la gestión de

la seguridad de la información, concluyendo que la forma de conseguir el mayor beneficio en seguridad de la información es contar con una adecuada evaluación de riesgos, que oriente las inversiones, que minimicen el impacto en caso de incidentes , dando a conocer que la seguridad de la información no es una responsabilidad únicamente del área de tecnología , debe fluir desde la alta gerencia hacia todos los procesos de negocios.

Aguirre, J. y Aristizabal, C. (6), en la tesis "Diseño del sistema de gestión de seguridad de la información para el Grupo Empresarial La Ofrenda", Realizado en la Universidad Tecnológica de Pereira, ubicado en el país de Ecuador, en el año 2013. El propósito de la investigación fue diseñar el sistema de gestión de seguridad de la información para el grupo Empresarial La ofrenda ya que dicha organización no contaba con un SGSI, para así poder determinar los riegos que se presentan con la información que se maneja en la empresa, utilizando herramientas tecnológicas y de desarrollo que permitan la gestión de los procesos que avalen la SI, aplicar los controles de la Norma ISO 27001 que permitan administrar el funcionamiento de un sistema de detección de intrusos dentro de un SGSI, se aplicó el modelo COBIT que se basa en un conjunto de herramientas de soporte del gobierno TI que les permitió a los gerentes cubrir la brecha entre los requerimientos de control , los aspectos técnicos y riesgos del negocio, concluyo que actualmente se vive en una época en que la información y los datos poseen una importancia decisiva en la gran mayoría de las organizaciones, convirtiéndose así en su activo más importante, se debe tener en cuenta que hay que recalcar que de nada sirve contar con un SGSI, que consideren todos los posibles riesgos y controles para mitigarlos o contar con toda la tecnología posible para asegurar la información de la compañía si no se da una debida importancia a la seguridad de la

información por parte de la alta gerencia y no se cumplen las políticas y procedimientos establecidos por parte del personal de la empresa.

Guachi, T. y Guevara D. (7), en la tesis "Norma De Seguridad Informática ISO 27001 Para Mejorar La Confidencialidad, Integridad Y Disponibilidad De Los Sistemas De Información Y Comunicación En El Departamento De Sistemas De La Cooperativa De Ahorro Y Crédito San Francisco Ltda.". Realizado en la Universidad Técnica de Ambato, ubicado en el país de Ecuador, en el año 2012. El presente proyecto reúne la información necesaria para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001, se ha concebido esta norma para garantizar la selección de controles de seguridad adecuados y proporcionales. Ello ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

2.2.2. Antecedentes A Nivel Nacional

Talavera, V. (8), en la tesis titulada: "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". Realizado en la Pontifica Universidad Católica del Perú, ubicado en Lima, en el año 2016. En esta investigación trata de que las instituciones públicas han sido llamadas a realizar la implementación de diversos controles a través de un Sistema de Gestión de Seguridad de la Información y de diferentes normas, entre ellas la Norma Técnica NTP ISO/IEC 27001 con la finalidad de asegurar el buen uso y protección de la información crítica que manejen, ya sea de clientes o información estratégica interna. En la actualidad los

sistemas que se utilizan para almacenar, procesar y transmitir información se encuentran en toda clase de instituciones de diferentes rubros y funciones. Los sistemas de información se han vuelto más complejos debido a la globalización que tiene por consecuencia que las distancias geográficas ya no supongan un obstáculo. De esta forma se tiene que existe una cantidad cada vez mayor de personas que tienen acceso a información que podría ser crítica para las diferentes empresas e instituciones en las que trabajan. Adicionalmente a este riesgo interno, siempre se tiene presente el riesgo que supone la fuga de información sensible ya sea por medio de personas que cuentan con acceso a dicha información, como por terceros que han accedido a ella mediante algún mecanismo de ataque.

Aguirre, D. (9), en la tesis titulada "Diseño De Un Sistema De Gestión De Seguridad De Información Para Servicios Postales Del Perú S.A.". Realizado en la Pontifica Universidad Católica del Perú, ubicado en Lima, en el año 2014. En esta investigación, tiene como exigencia de la implementación de la norma técnica peruana NTP-ISO/IEC 27001:2008 en las entidades públicas nace de la necesidad de gestionar adecuadamente la seguridad de la información en cada una de estas empresas. Sin embargo, el desconocimiento de estos temas por parte de la alta dirección, ha ocasionado que no se tomen las medidas necesarias para asegurar el éxito de este proyecto en el tiempo estimado por la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), entidad responsable de apoyar a las entidades públicas durante el proceso de implementación de la norma. Debido a ello, para la realización de este proyecto de fin de carrera, se decidió trabajar con una entidad pública como caso de estudio, a fin de diseñar un Sistema de Gestión de Seguridad de Información o SGSI que se acople a la normativa a la cual está sujeta la organización y que

pueda, en un futuro, servir como referencia para la implementación del mismo. Por último, se presenta un documento llamado Declaración de Aplicabilidad en el cual se indica que controles de la NTP ISO/IEC 17799:2007 se pueden implementar dentro de la organización basado en el trabajo realizado dentro de la organización.

Espinoza, H. (10), en la tesis titulada: "Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo". Realizado en la Pontifica Universidad Católica del Perú, ubicado en Lima, en el año 2013. En esta investigación el problema presentado en la empresa es en cuanto al manejo de la seguridad de la información. En el cual se planteó el análisis y diseño de un sistema de gestión de seguridad de información, basado en la norma ISO/IEC 27001:2005 para una empresa dedicada a la producción y comercialización de alimentos de consumo masivo. De las cuales era Inventariar los procesos de negocio, los procesos de tecnologías de información (TI) que dan soporte al proceso de negocio y finalmente los activos relacionados con estos procesos. Además era Identificar y analizar los riesgos de seguridad de información de los principales procesos identificados y Elaborar el sistema de gestión de seguridad de información (SGSI) en base a la norma ISO/IEC 27001:2005 para el SGSI que se quiere diseñar, y elegir los controles basándose en la norma ISO/IEC 27002. Los resultados esperados es el inventariado de los procesos la cual se verificará en el documento en sí y con la matriz de riesgo determinar y entender qué procesos son esenciales para la continuidad de las operaciones, calcular su posible impacto y los tiempos máximos tolerables de interrupción así como sus tiempos estimados de recuperación. Para ello se realiza el análisis

de riesgos. Documento con la declaración de aplicabilidad de la norma ISO 27001 para el SGSI que se quiere diseñar. Documentación obligatoria exigida por la norma ISO 27001 para implantar un SGSI.

Montoya, N. (11), en la tesis "Diseño de un sistema de gestión de seguridad de información para un centro cultural binacional". Realizado en la Pontificia Universidad Católica del Peru, ubicado en Lima, en el año 2012. La finalidad de esta investigación es proteger los activos de la información ante las amenazas a las cuales están expuestas, y de esta manera dar un tratamiento a los riesgos de información en los procesos de la Municipalidad , este proyecto se realizó siguiendo lo propuesto en la Norma ISO/IEC 27001:2005 para elaborar el diseño de un SGSI donde se establezcan una política, objetivos , procesos y procedimientos ,concluyendo así que el Centro Cultural, y las organizaciones en general deben tomar en cuenta la seguridad de la información de la empresa y de esa forma proteger su activo más valioso que es la información.

2.2. Bases teóricas

2.2.1. El rubro de la empresa

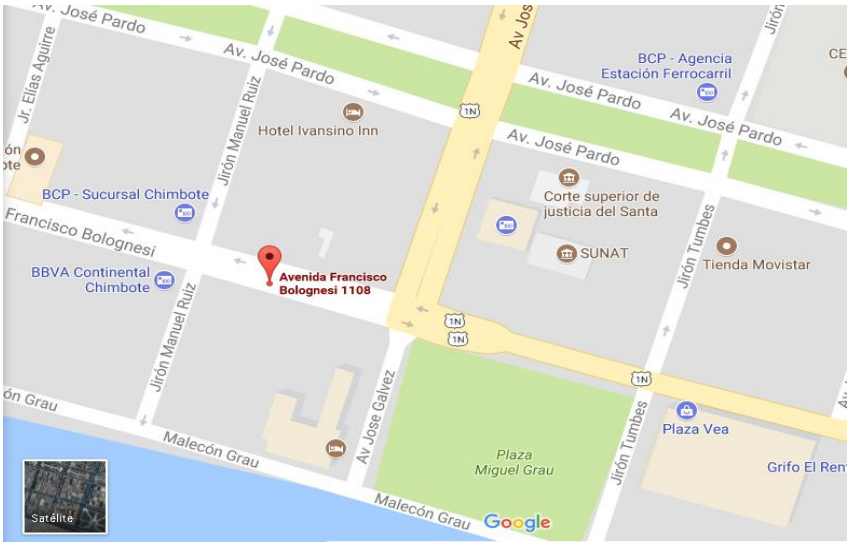
El GRUPO SIAS SAC, es una Empresa que se dedica a la venta al por menor de productos farmacéuticos y médicos, cosméticos y artículos de tocador en comercios especializados.

2.2.2. La Empresa investigada

a) Información General

En GRUPO SIAS SAC, es una empresa que se encuentra ubicada en Jirón Bolognesi N° 1108 – P.J. Miramar Bajo (a 2 Cdras de Plaza Vea). Distrito de Chimbote, en la Provincia del Santa, y Departamento de Ancash.

Gráfico Nro. 1: Ubicación de la Empresa



Fuente: Google Maps (12).

b) Historia

Grupo SIAS S.A.C se constituye formalmente en el año 2003, es una empresa de comercialización de medicamentos a través de sus formatos de BOTICAS con las marcas “FARMA DÍA Y NOCHE”, en el 2007 con “FARMAHORRO” y a partir del 2011 con “MAX FARMA”, en total tenemos 25 tiendas en la región Ancash.

En el año 2016 se fusionó con IMPORTACIONES FARMA SS EIRL y lanzan su nueva y única marca comercial FARMAHORRO; aperturando nuevas unidades de negocio en la ciudad de Nuevo Chimbote.

Operan en ciudades pequeñas (10000 -12000 habitantes) de la sierra conexas a la actividad minera, por lo general no hay delincuencia, la comida es más barata y el precio del metro cuadrado es tres veces menor que en la costa, por el tamaño de la población y el difícil acceso geográfico no son mercados atractivos para las grandes cadenas de boticas.

Las boticas son atendidas por una sola persona del sector salud: enfermeras, obstetras o farmacéuticos, personal altamente calificado para una buena atención. Son formatos modernos tipo cadena de la costa, con buena iluminación, ubicado en la plaza de armas o sitios de alto tránsito, ordenados, limpios y que cumplen con todos los requisitos legales. El apoyo logístico desde la sede central en la ciudad de Chimbote permite adecuado control de los inventarios, facilitando la actividad comercial.

Nuestras boticas se posicionan en la mente del consumidor con la percepción de alto valor de servicio y mejor precio local. Los servicios percibidos son: Atención profesional, stock apropiado de medicinas, campañas médicas, una buena atención al cliente, horarios. Es así que las boticas competidoras son generalmente Ilegales, no cuentan con permiso del Ministerio de Salud, no tienen variedad de productos, el formato es tipo botica tradicional antiguo, servicio bajo y el precio es alto en comparación a nuestros precios.

Según cifras de la respetada consultora IMS, el mercado farmacéutico creció más de 66% en los últimos cinco años, al pasar de US$ 492 millones en enero del 2007 a US$ 821 millones a enero del 2011. “El 2006, el Perú era el mercado más chico de Sudamérica, pero en poco tiempo casi ha duplicado su tamaño y todo indica que para el 2016 correrá la misma suerte. Con esas características quién no querría entrar a invertir”, precisa Luis Caballero, ex gerente general de Corporación “INFARMASA”.

El crecimiento sostenido del Perú en los próximos años en el sector minero y agro comercial hace que las ciudades pequeñas conexas a estas, brinden oportunidades de negocios para el modelo empresarial que desarrollamos en la región Ancash, el cual nos ha dado mucho éxito.

c) Objetivos Organizacionales

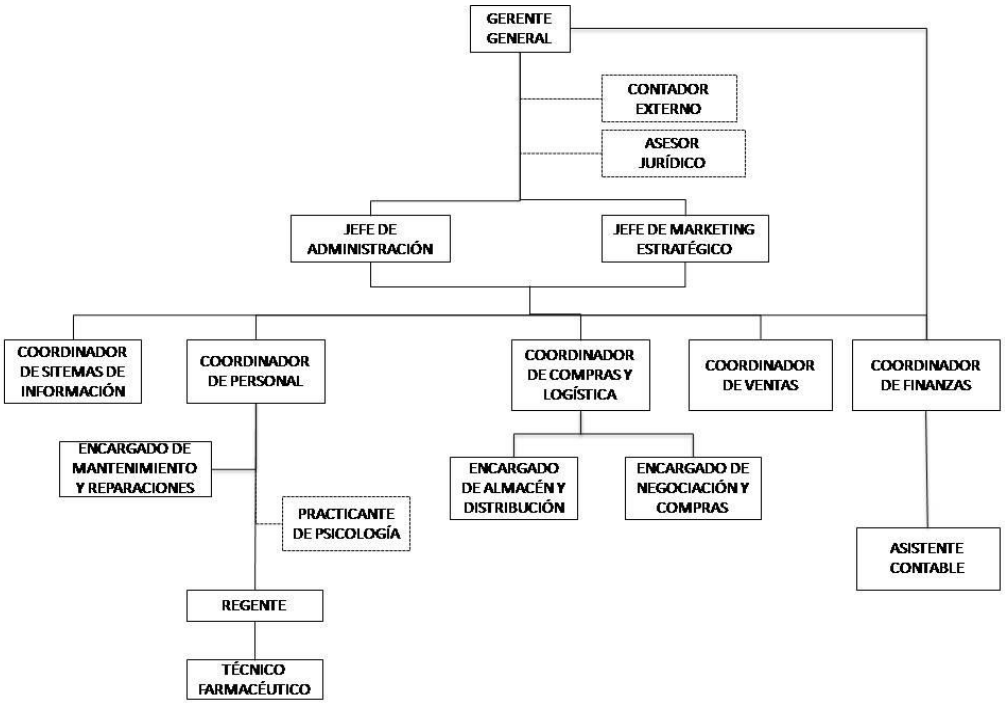
El objetivo del Grupo SIAS S.A.C , es que para el año 2025, ser la cadena líder de boticas habiendo alcanzado ya 50 sucursales operando en el Perú y manteniendo alianzas estratégicas con laboratorios Indios vendiendo sus productos de manera exclusiva.

d) Funciones

Grupo SIAS S.A.C., es una empresa peruana comercializadora de fármacos a nivel nacional enfocados en atender las necesidades de los clientes de manera personalizada y con la mejor calidad del mercado. Creciendo conjuntamente con nuestros empleados, comunidades de las zonas donde operamos y generando rentabilidad para nuestros accionistas.

e) Organigrama

Gráfico Nro. 2: Organigrama GRUPO SIAS SAC



Fuente: GRUPO SIAS S.A.C. (13).

f) Infraestructura tecnológica existente

HARDWARE

Tabla Nro. 1: Computadoras de Escritorio

COMPUTADORAS DE ESCRITORIO	CANTIDAD
Case – Procesador	
INTEL PENTIUM G620 2.6 GHz	1
INTEL CORE i3-2100 3.1 GHz	1
PENTIUM DUAL CORE E5300 2.6 GHz	1
PENTIUM DUAL CORE E5400 2.7 GB	1
AMD PHENOM II X2 560 3.3 GHz	1
PENTIUM DUAL CORE E5700 3.0 GHz	1
PENTIUM DUAL CORE E5300 2.6 GHz.	2
AMD FX 4100 QUAD CORE 3624 MHz.	1
INTEL CORE QUAD Q8400 2.66 GHz.	1
INTEL CORE i3-2100 3.1 GHz.	1
INTEL CORE 2 DUO E8400 3.0 GHz.	1
INTEL CORE i5 - 3230M 2.6GHz	1
INTEL CORE i3 4130 3.4 GHz.	1
PENTIUM DUAL CORE E5800 3.2 GHz.	1
AMD SEMPRON 140 2.7 GHz.	1
Monitores	
AOC 1619SW	1
SAMSUNG 632NW	1
SAMSUNG S19A300N	1
SAMSUNG S19B300N	1
SAMSUNG B1630N	1
SAMSUNG B2030	1
LG FLATRON W1943SS-PF	2
LG FLATRON W1643S-PF	1
LG E1951C-BN	3
LG FLATRON E1941S	1
LG E1951S	1
LG FLATRON W1943SB	1
LG FLATRON E1941S-BN	1
LG FLATRON W1943SS	2

Fuente: Elaboración Propia

Tabla Nro. 2: Impresoras

IMPRESORAS	CANTIDAD
KONICA MINOLTA BIZHUB C3110	1
EPSON LX350	1
HP LASEJET P1002W	1
CANON PIXMA MG3510	1

Fuente: Elaboración Propia

Tabla Nro. 3: Dispositivos de Redes

DISPOSITIVOS DE REDES	CANTIDAD
TP-LINK TLSF1024D	1
SATRA SA-SF1008D	2
ASKEY RTV9015VW	1

Fuente: Elaboración Propia

Tabla Nro. 4: Ticketera

TICKETERAS	Cantidad
BIXOLON SRP-270	8

Fuente: Elaboración Propia

SOFTWARE

Tabla Nro. 5: Aplicativos de la Empresa

NOMBRE	VERSION
MICROSOFT OFFICE	2010
MICROSOFT OFFICE	2013
MICROSOFT SQL SERVER	2008
SAP BUSINESS ONE	9.0
SAP CRYSTAL REPORT	14.0
TEAMVIEWER	12.0
CORELDRAW GRAPHICS	2017
ADOBE PHOTOSHOP	2017
GOOGLE CHROME	60.0.3
ESET NOD 32 ANTIVIRUS	10.0
AVIRA ANTIVIRUS	15.0
WINRAR	5.4

Fuente: Elaboración Propia

2.2.3. Las tecnologías de la información y comunicaciones (TIC)

a) Definición

Son un conjunto de tecnologías de desarrollos y dispositivos avanzados que integran funcionalidades de almacenamiento, transmisión de datos y procesamiento. Que constan de equipos de programas informáticos y medios de comunicación para obtener, producir, almacenar y también presentar información en cualquier formato ya sea voz, datos, textos e imágenes.

Instrumentos creados por el hombre, que hacen más fácil que uno pueda tener acceso a datos o que uno las TIC representa una innovación importante en la sociedad y a la larga un cambio en la educación, en las relaciones interpersonales y en la forma de difundir y generar conocimientos que pueda intercambiar experiencias, comentarios, opiniones, puntos de vista con otras personas (14).

Por ejemplo, las TIC van desde instrumentos relativamente muy sencillos como el telégrafo y el teléfono fijo, hasta instrumentos ya más avanzados como los instrumentos que utilizan las ondas electromagnéticas para enviar y recibir información en lugares apartados (como los celulares o los teléfonos satelitales), entre otros (15).

b) Historia

Las TICs surgen de manera aproximativa a raíz de la invención del telégrafo (1833) y el posterior despliegue de redes telegráficas por la geografía nacional, que en España se desarrolla entre los años 1850 y 1900. Actualmente, estamos acostumbrados a coexistir con todo tipo de servicios que nos facilitan la comunicación entre personas, pero la experiencia con estos sistemas es relativamente reciente (15).

El uso de nuevos tipos de señales y el desarrollo de nuevos medios de transmisión, adaptados a las crecientes necesidades de comunicación, han sido fenómenos paralelos al desarrollo de la historia. Otros hitos y hechos importantes que han marcado la evolución de las telecomunicaciones y, por tanto, el devenir de las tecnologías de la información y comunicaciones:

- 1876 (10 de marzo): Grahan Bell inventa el teléfono, en Boston, mientras Thomas Watson construye el primer aparato.
- 1927 (11 de Enero): Se realiza la primera transmisión de radiotelefonía de larga distancia, entre USA y el Reino Unido, a cargo de AT&T y la British Postal Office.
- 1948 (1 de Julio): Tres ingenieros de Bell Laboratories inventaron el transistor, lo cual, sin ninguna, supuso un avance fundamental para toda la industria de telefonía y comunicaciones.
- 1951 (17 de Agosto): Comienza a operar el primer sistema transcontinental de microondas, entre Nueva York y San Francisco.
- 1956 (a lo largo del año): Comienza a instalarse el primer cable telefónico trasatlántico.
- 1963 (10 de Noviembre): Se instala la primera central pública telefónica, en USA, con componentes electrónicos e incluso parcialmente digital.
- 1965 (11 de Abril): En Succasunna, USA, se llega a instalar la primera oficina informatizada, lo cual, sin duda, constituyó el nacimiento del desarrollo informático.
- 1984 (1 de Enero): Por resolución judicial, la compañía AT&T se divide en siete proveedores (the Baby Bells), lo que significó el comienzo de la liberación del segmento de operadores de telecomunicaciones, a nivel mundial, el cual

progresivamente se ha ido materializando hasta nuestros días.

- Desde 1995 hasta el momento actual los equipos han ido incorporando tecnología digital, lo cual ha posibilitado todo el cambio y nuevas tendencias a las que asistimos. Se abandona la transmisión analógica y nace la Modulación por Impulsos Codificados o, lo que es lo mismo, la frecuencia inestable se convierte en código binario, estableciendo los datos como único elemento de comunicación (15).

c) Las TIC más utilizadas en la empresa investigada

El GRUPO SIAS S.A.C., usa las redes sociales (Facebook) para que los clientes interesados en adquirir servicios puedan comunicarse y ver qué tipos de servicios brinda la empresa.

También usa correos electrónicos para poder comunicarse con sus Clientes, Proveedores y Trabajadores, enviándole boletines, noticias, ofertas sin ningún costo alguno. Así mismo la empresa como medida de seguridad la empresa usa e implementa antivirus para así proteger sus datos y la de sus clientes.

2.2.4. Tecnología de la investigación

2.2.4.1. Seguridad

Característica que indica que un sistema está libre de todo peligro, daño o riesgo (16).

2.2.4.2. Información

Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje (16).

2.2.4.3. Activos de Información

Los activos de información son los recursos que tienen valor o utilidad para la organización, sus operaciones comerciales y su continuidad, los cuales son necesarios para que la organización funcione y alcance los objetivos que propone su dirección (17).

Los activos de información se pueden clasificar en las siguientes categorías:

- Activos de información (Datos, manuales del usuario)
- Documentos de papel (contratos, resoluciones)
- Activos de software (aplicación, software de sistemas)
- Personal (trabajadores, población)
- Imagen de la empresa y reputación
- Servicios (comunicaciones)

2.2.4.4. Sistemas Informáticos

Es el conjunto de elementos hardware, software y periféricos que conectados entre sí, forman un ordenador que permiten la digitalización de todo un volumen de información reduciendo el espacio ocupado, pero, sobre todo, facilitando su análisis y procesado. Se gana en 'espacio', acceso, rapidez en el procesado de dicha información y mejoras en la presentación de dicha información (18).

2.2.4.5. Sistemas de Información

Un sistema de información es un conjunto de elementos orientados al tratamiento y administración de datos e

información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo (18).

2.2.4.6. Seguridad Informática

Es la que permite lograr que todos los sistemas informáticos utilizados en cualquier contexto, se encuentren seguro de cualquier daño o riesgos, ya sea por parte de personas ajenas que en forma voluntaria o involuntaria lo pueda hacer o de cualquier desastre natural. En este sentido, la protección de la información requiere de un conjunto de software o aplicativos diseñados, documentos estándares y metodologías existentes que permitan aplicar las normativas certificables internacionalmente y técnicas apropiadas para llevar un control en la seguridad. Se expresa control en la seguridad, porque se considera un tanto difícil garantizar la seguridad de la información en forma completa o llevada a un 100%, por cuanto intervienen diferentes amenazas a las que las organizaciones y/o personas se encuentran continuamente expuestas (19).

Considerar aspectos de seguridad significa:

- Conocer el peligro
- Clasificarlo
- Protegerse de los impactos o daños de la mejor manera posible.

En este sentido, la Seguridad Informática sirve para la protección de la información, en contra de amenazas o peligros, para evitar daños y para minimizar riesgos, relacionados con ella (19).

2.2.4.7. Normativas de Seguridad

Existen diferentes normativas de seguridad que las empresas de hoy implantan para la seguridad de la información. Todas estas normativas persiguen los mismos objetivos, ya que están diseñadas para incluir a todas las unidades o departamentos que estructura a la empresa para obtener una seguridad mínima de la información procesada y transferida por el personal que hace parte de ella (20).

Se trataran en forma general la normativa encargada de la gestión de la seguridad de la información, por lo que se enfatizará en la normativa ISO/IEC 27001, teniendo en cuenta que es las más actual certificable internacionalmente utilizada (21).

2.2.4.8. Estructura de las Normativas de Gestión de la Seguridad

Las normativas de seguridad, tienen la finalidad de presentar los lineamientos necesarios para que las empresas puedan implantar un sistema de gestión de la seguridad de la información (SGSI) (21).

Un Sistema de Gestión de la seguridad de la información se implanta mediante un proceso ordenado que consiste en establecer los mecanismos necesarios de seguridad de manera documentada y conocida por todos los miembros de la empresa. Sin embargo es importante que se tenga claro que la implantación de un SGSI no garantiza la protección en su totalidad ya que su propósito como lo anuncia claramente la ISO en su portal ISO27000.es, “garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y

minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías" (22).

2.2.4.9. Origen de las Normativas de Seguridad

El Instituto británico de estándares (British Standard Institute), fue la primera organización que vio la necesidad de la creación de normativas, con el objetivo de ayudar a las empresas a mejorar sus diferentes actividades de negocio. Fue la precursora de muchas normativas que se han aplicado en otros países e inclusive es un organismo colaborador de ISO (23).

2.2.4.10. Sistema de gestión de seguridad de información (SGSI)

Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. La siguiente figura ilustra este modelo basado en los procedimientos esenciales para un SGSI (24).

Gráfico Nro. 3: Procesos de un Sistema de Gestión de Seguridad de Información

Fuente: Lopez, A. y Ruiz, J. (24).

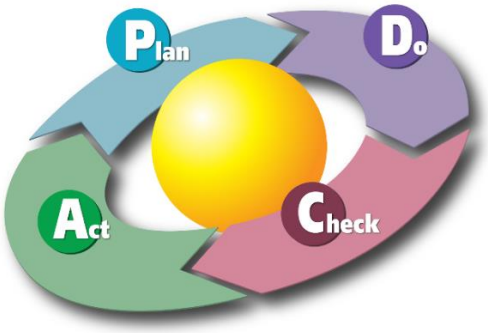
Ciclo PDCA (Edward Deming)

Para la implantación de un sistema de Gestión de la seguridad de la información, se requiere del desarrollo de actividades que marquen un orden lógico para llevar organizado todo el proceso. El modelo PDCA (Plan, do, check, act), en su equivalencia en español es Planificar, hacer, verificar y actuar (PHVA), es una estrategia de mejora continua de calidad en cuatro pasos. Este modelo es muy utilizado para implantación de sistemas de gestión, como los sistemas de gestión de la calidad que muchas empresas de hoy lo implantan para la calidad administrativa y de servicios con el objetivo de perfeccionarlos y continuar en un proceso de mejora continua.

Para el caso de la implantación de Sistemas de Gestión de la Seguridad informática, el ciclo PDCA es una estrategia efectiva para la organización y documentación que se requiere en este proceso. La siguiente figura ilustra este modelo basado en los procedimientos esenciales para un SGSI (24).

Es una estrategia de mejora continua de la calidad en cuatro pasos (PDCA).

Gráfico Nro. 4: Ciclo PDCA para la implementación de SGSI



Fuente: Karn G. Bulsuk (25)

PLAN: Establecer con planificación

a. Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.

b. Definir una política de seguridad que:
   - Incluya el marco general y los objetivos de seguridad de la información de la organización.
   - Considere requerimientos legales o contractuales relativos a la seguridad de la información.
   - Esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI.
   - Establezca los criterios con los que se va a evaluar el riesgo.
   - Esté aprobada por la dirección.

c. Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles (existen numerosas metodologías estandarizadas para la evaluación de riesgos, aunque es perfectamente aceptable definir una propia).

d. Identificar los riesgos:
   - Identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios.
   - Identificar las amenazas en relación 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.

e. Analizar y evaluar los riesgos:
   - Evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información.
   - Evaluar de forma realista 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.

f. 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 el riesgo, mediante el cese de las actividades que lo originan.
   - Transferir el riesgo a terceros, en compañías aseguradoras o proveedores de outsourcing.

g. Seleccionar los objetivos de control y los controles del Anexo A de ISO 27001 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.

h. Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI.

i. 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 y controles del Anexo A excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.

En relación a los controles de seguridad, el estándar ISO 27002 (antigua ISO 17799) proporciona una completa guía de implantación que contiene 133 controles, según 39 objetivos de control agrupados en 11 dominios. Esta norma es referenciada en ISO 27001, en su segunda cláusula, en términos de "documento indispensable para la aplicación de este documento" y deja abierta la posibilidad de incluir controles adicionales en el caso de que la guía no contemplase todas las necesidades particulares.

DO: Implementar y utilizar el SGSI

a. 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.

b. Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.

c. Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.

d. Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.

e. Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.

f. Gestionar las operaciones del SGSI.

g. Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.

h. Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

i. Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.

CHECK: Monitorizar y revisar el SGSI

La organización deberá:

a. Ejecutar procedimientos de monitorización y revisión para:
   - Detectar a tiempo los errores en los resultados generados por el procesamiento de la información.
   - Identificar 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.

b. 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.

c. Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.

d. Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior-requerimiento legal, obligaciones contractuales, etc.

e. Realizar periódicamente de auditorías internas del SGSI en intervalos planificados.

f. Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.

g. Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.

h. Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

ACT: Mantener y mejorar el SGSI

La organización deberá regularmente:

a. Implantar en el SGSI las mejoras identificadas.

b. Realizar las acciones preventivas y correctivas adecuadas en relación a la cláusula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.

c. Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.

d. Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

2.2.4.11. Estándar De Gestión De La Seguridad De La Información

A. La organización ISO

International Standarization Organization, es la Organización Internacional para la Estandarización que se encarga de la normalización a nivel mundial, las cuales desarrollan bajo diferentes grupos o comités especializados las normativas, modelos o patrones a seguir con el objetivo de definir ciertas características que debe poseer un objeto o producto (24).

La finalidad principal de las normas ISO es:

- Orientar
- Coordinar
- Simplificar
- Unificar los usos, Para conseguir menores costes y efectividad.

Familia de las normas ISO/IEC 27000

La serie ISO/IEC 27000, es un conjunto de normas de gestión de la seguridad de la información con la IEC (International Electrotechnical Commission), comisión internacional de electrotecnia. Cada una de las normas de la familia 27000, define y centra todos los aspectos importantes en el contexto de la gestión de la seguridad de la información en cualquier empresa pequeña, mediana o grande, así como públicas y privadas (24).

Tabla Nro. 6: Relación de serie de las normas ISO/IEC 27000

NORMAS	DEFINICIÓN
ISO 27000	Gestión de la seguridad de la información
ISO 27001	Especificaciones para un SGSI
ISO 27002	Código de buenas prácticas
ISO 27003	Guía de implantación de un SGSI
ISO 27004	Sistema de métricas e indicadores
ISO 27005	Guía de análisis y gestión de riesgos
ISO 27006	Especificaciones para Organismos Certificadores de SGSI.
ISO 27007	Guía para auditar un SGSI.

Fuente: Elaboración Propia

A continuación se presenta un breve resumen de cada una de las normas relacionadas anteriormente para una mayor ilustración.

ISO 27000: Gestión de la seguridad de la información (Fundamentos y vocabulario)

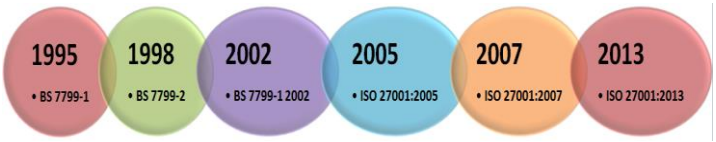
Esta norma fue publicada el 1 de mayo de 2009 y contemplan en forma introductoria todos los aspectos fundamentales que enfoca un sistema de gestión de seguridad de la información (SGSI), una descripción del ciclo PDCA, al igual que las definiciones de los términos que se emplean en toda la serie 27000.

ISO 27001 Especificaciones para un SGSI

Esta norma fue publicada el 15 de Octubre de 2005, la cual enmarca los requisitos y/o especificaciones del sistema de Gestión de la seguridad de la información. Fue originaria de la BS 7799-2:2002,

siendo identificada actualmente como norma ISO 27001:2013. Esta es la norma certificable en la actualidad por los auditores externos de los SGSI de las diferentes empresas. En esta norma se enumera en forma resumida, los objetivos de control y controles, para que sean seleccionadas por las empresas que desean implantar el SGSI. Si bien es cierto que no es de carácter obligatorio que se implementen todos los controles de esta norma, la empresa debe justificar ante los auditores la no aplicabilidad de los controles cuando estén en el proceso de evaluación para una certificación.

Gráfico Nro. 5: Evolución estructural del ISO 27001



Fuente: PMG-SSI (26).

ISO 27002: código de buenas prácticas

Publicado el 1 de julio de 2007. Esta norma no certificable, es una guía de buenas prácticas que detalla los objetivos de control y controles recomendables en los aspectos de seguridad de la información.

ISO 27003: Guía de implantación de un SGSI

Publicado el 1 de Febrero de 2010. Esta norma no es certificable y proporciona una guía que contempla todos los aspectos necesarios para el diseño e implementación de un SGSI de acuerdo a

la norma certificable ISO/IEC 27001:2013. El objetivo de esta norma es describir las especificaciones y diseño en el proceso de la implementación del SGSI.

ISO 27004: Sistema de métricas e indicadores

Publicada el 15 de Diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.

ISO/IEC 27005

Publicada en segunda edición el 1 de Junio de 2011 (primera edición del 15 de Junio de 2008). No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

ISO/IEC 27006: Especificaciones para Organismos Certificadores de SGSI.

Esta norma fue publicada en su primera edición el 1 de marzo de 2007 y su segunda edición el 1 de diciembre de 2011. Esta norma específica los requisitos para la acreditación de entidades de auditoría y certificación de SGSI.

ISO 27007: Guía para auditar un SGSI.

Esta norma fue publicada el 14 de Noviembre de 2011. Es una guía para la aplicación de auditorías a un SGSI como complemento especificado en ISO 19011, no es una norma certificable.

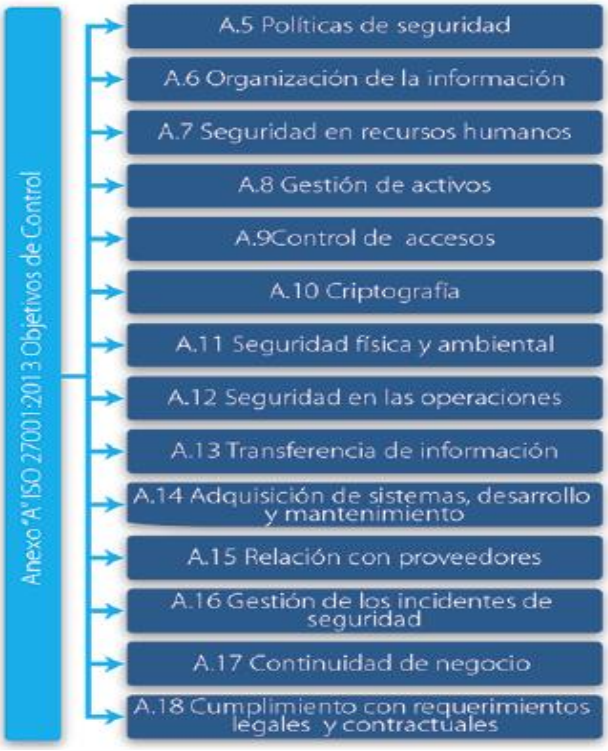
2.2.4.12. La Normativa ISO/IEC 27001:2013

Estructura ISO/IEC 27001:2013

El estándar El ISO/IEC 27001: 2013, para los Sistemas Gestión de la Seguridad de la Información es un modelo de gestión de seguridad de la información, que permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

Se define como un conjunto de lineamientos el cual especifica los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. Estos requisitos describen cual es el comportamiento esperado del sistema de Gestión una vez que esté en funcionamiento (24).

Gráfico Nro. 6: Dominios de seguridad normativa ISO/ 27001:2013



Fuente: Gonzales, D (20).

Cada dominio estipula unos objetivos en el Sistema de Gestión de Seguridad de Información, los controles de seguridad y la función.

A.5. Políticas de seguridad

En este dominio se especifica la forma de creación de un documento de política de seguridad, el cual debe ser elaborado por el equipo de trabajo que la dirección designa para la implementación del SGSI. Dicho documento debe ser revisado y aprobado por la dirección. En el documento de política de seguridad, se debe especificar toda la normativa interna de la institución con el objetivo de que los funcionarios conozcan y cumplan las medidas de seguridad

implantadas a través del (SGSI). Así mismo contempla todos los aspectos orientados al acceso a la información, utilización de los activos físicos y lógicos de la organización y el comportamiento que deben tener en caso de que ocurra un incidente de seguridad. La elaboración del documento debe ser con un lenguaje claro y sencillo con el objetivo de que cualquier funcionario de la empresa u organización lo pueda interpretar. La subdivisión de este control es la siguiente:

A.5.1.1 Documento de política de seguridad de la información

A.5.1.2 Revisión de la política de seguridad de la información.

A.6 Organización de la Información

Aquí se establece los parámetros internos y externos de la organización. Los internos, hacen referencia al compromiso que la dirección asume para la implantación del SGSI, la designación del equipo de personal que incluye el coordinador de seguridad y la asignación de responsabilidades entre otros. Los parámetros externos hacen referencia a los Riesgos relacionados con el acceso a terceros, seguridad con respecto a los clientes y contratación con terceros. Los subdominios o controles se relacionan a continuación.

A.6.1 Interna

- A.6.1.1 Compromiso de la Dirección con la seguridad de la información
- A.6.1.2 Coordinación de la seguridad de la información
- A.6.1.3 Asignación de responsabilidades relativas a la seguridad de la información

- A.6.1.4 Proceso de autorización de recursos para el procesado de la información
- A.6.1.5 Acuerdos de confidencialidad
- A.6.1.6 Contacto con las autoridades
- A.6.1.7 Contacto con grupos de especial interés
- A.6.1.8 Revisión independiente de la seguridad de la información

A.6.2 Externa (Terceros)

- A.6.2.1 Identificación de los riesgos derivados del acceso de terceros
- A.6.2.2 Tratamiento de la seguridad en la relación con los clientes
- A.6.2.3 Tratamiento de la seguridad en contratos con terceros

A.7 Seguridad ligada a los recursos humanos:

Este dominio hace énfasis en todo el talento humano de la organización y demás personal contratado de manera externa, los cuales deben conocer las responsabilidades que adquieren para proteger la información, garantizar la seguridad y buen uso, así como mantener confidencialidad a la información que tienen acceso con este carácter. Es tarea de la organización hacer todo tipo de verificación jurídica al personal antes de ser contratado y establecer las debidas cláusulas contractuales para el cumplimiento de sus funciones, responsabilidades que tiene sobre los activos que utilizará entre otros. También deberá definir los procedimientos que se deben realizar cuando un trabajador tenga cambio de funciones o cambio de cargo o haya salido de la empresa por diferentes motivos.

A.7.1 Antes de la contratación

Las responsabilidades de la seguridad se deberían definir antes de la contratación laboral mediante la descripción adecuada del trabajo y los términos y condiciones del empleo.

Todos los candidatos para el empleo, los contratistas y los usuarios de terceras partes se deberían seleccionar adecuadamente, especialmente para los trabajos sensibles. Los trabajadores, contratistas y usuarios de terceras partes de los servicios de procesamiento de la información deberían firmar un acuerdo sobre sus funciones y responsabilidades con relación a la seguridad.

Conjuntamente con RRHH, de debería asegurar que se emplea un proceso de verificación de antecedentes proporcional a la clasificación de seguridad de aquella información a la que va a acceder el trabajador a contratar. Dicho simplemente, el proceso de contratación de un administrador de sistemas TI debería ser muy diferente del de un administrativo. Haga comprobaciones de procedencia, formación, conocimientos, etc.

A.7.2 Durante la contratación

Se debería definir las responsabilidades de la Dirección para garantizar que la seguridad se aplica en todos los puestos de trabajo de las personas de la organización. A todos los usuarios trabajadores, contratistas y terceras personas se les debería proporcionar un adecuado nivel

de concienciación, educación y capacitación en procedimientos de seguridad y en el uso correcto de los medios disponibles para el procesamiento de la información con objeto de minimizar los posibles riesgos de seguridad. Se debería establecer un proceso disciplinario normal para gestionar las brechas en seguridad.

La responsabilidad con respecto a la protección de la información no finaliza cuando un trabajador se va a casa o abandona la organización. Asegure que esto se documenta claramente en materiales de concienciación, contratos de empleo, etc. Contemple la posibilidad de una revisión anual por RRHH de los contratos junto con los trabajadores para refrescar las expectativas expuestas en los términos y condiciones de empleo, incluyendo su compromiso con la seguridad de la información.

A.7.3 Cese o cambio de puesto de trabajo

Se deberían establecer las responsabilidades para asegurar que el abandono de la organización por parte de los trabajadores, contratistas o terceras personas se controla, que se devuelve todo el equipamiento y se eliminan completamente todos los derechos de acceso.

Los cambios en las responsabilidades y empleos en la organización se deberían manejar, en el caso de su finalización en línea con esta sección, La devolución de los activos de la organización cuando un trabajador se marcha sería mucho más sencilla de verificar si el inventario de activos ha sido actualizado y verificado regularmente. Examine qué accesos necesita revocar en

primer lugar cuando un trabajador presenta su carta de dimisión: ¿cuáles son los sistemas más críticos o vulnerables?

Haga un seguimiento del uso del e-mail por estas personas antes de salir definitivamente de la empresa, por si comienzan a sacar información confidencial (sujeto a las políticas aplicables y a consideraciones legales sobre privacidad).

A.8 Gestión de Activos

El objetivo del presente dominio es que la organización tenga conocimiento preciso sobre los activos que posee como parte importante de la administración de los riesgos.

Algunos ejemplos de activos son:

- Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad y contingencia, información archivada, etc.
- Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo y publicación de contenidos, utilitarios, etc.
- Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, máquinas de fax, contestadores automáticos, switches de datos, etc.), medios magnéticos (cintas, discos, dispositivos móviles de almacenamiento de datos – pen drives, discos externos, etc.), otros equipos técnicos (relacionados con el suministro

eléctrico, unidades de aire acondicionado, controles automatizados de acceso, etc.), mobiliario, lugares de emplazamiento, etc.

- Servicios: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

A.8.1 Responsabilidad sobre los activos

Todos los activos deberían ser justificados y tener asignado un propietario y se deberían identificar a los propietarios para todos los activos y asignarles la responsabilidad del mantenimiento de los controles adecuados. La implantación de controles específicos podría ser delegada por el propietario convenientemente. No obstante, el propietario permanece como responsable de la adecuada protección de los activos. El término "propietario" identifica a un individuo o entidad responsable, que cuenta con la aprobación del órgano de dirección, para el control de la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término "propietario" no significa que la persona disponga de los derechos de propiedad reales del activo.

Use códigos de barras para facilitar las tareas de realización de inventario y para vincular equipos de Tecnología de Información que entran y salen de las instalaciones.

A.8.2 Clasificación de la información

Se debería clasificar la información para indicar la necesidad, prioridades y nivel de protección previsto para su tratamiento.

La información tiene diversos grados de sensibilidad y criticidad. Algunos ítems podrían requerir niveles de protección adicionales o de un tratamiento especial. Debería utilizarse un esquema de clasificación de la información para definir el conjunto adecuado de niveles de protección y comunicar la necesidad de medidas especiales para el tratamiento.

A.8.3 Manejo de los soportes de almacenamiento

Los medios deberían ser controlados y físicamente protegidos.

Se deberían establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizadas.

A.9 Control de Accesos

El objetivo del presente dominio es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática.

Para impedir el acceso no autorizado a los sistemas de información se deberían implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

A.9.1 Requisitos de negocio para el control de accesos
Se deberían controlar los accesos a la información, los recursos de tratamiento de la información y los procesos de negocio en base a las necesidades de seguridad y de negocio de la Organización.

Las regulaciones para el control de los accesos deberían considerar las políticas de distribución de la información y de autorizaciones.

A.9.2 Gestión de acceso de usuario

Se deberían establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información.

Los procedimientos deberían cubrir todas la etapas del ciclo de vida del acceso de los usuarios, desde del registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas y servicios de información.

A.9.3 Responsabilidades del usuario

La cooperación de los usuarios autorizados es esencial para una seguridad efectiva.

Los usuarios deberían ser conscientes de sus responsabilidades en el mantenimiento de controles de acceso eficaces, en particular respecto al uso de contraseñas y seguridad en los equipos puestos a su disposición.

Se debería implantar una política para mantener mesas de escritorio y monitores libres de cualquier información con objeto de reducir el riesgo de accesos no autorizados o el deterioro de documentos, medios y recursos para el tratamiento de la información.

A.9.4 Control de acceso a sistemas y aplicaciones

Los medios deberían ser controlados y físicamente protegidos.

Se deberían establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizadas.

A.10 Criptografía

El objetivo del presente dominio es el uso de sistemas y técnicas criptográficas para la protección de la información en base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad. La aplicación de medidas de cifrado se debería desarrollar en base a una política sobre el uso de controles criptográficos y al establecimiento de una gestión de las claves que sustenta la aplicación de las técnicas criptográficas.

A.10.1 Controles criptográficos

Controles con el objetivo de proteger la confidencialidad, autenticidad o integridad de la información mediante la ayuda de técnicas criptográficas.

Las organizaciones deberían utilizarán controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios, para la transmisión de información clasificada y/o para el resguardo de aquella información relevante en atención a los resultados de la evaluación de riesgos realizada por la organización.

A.11 Seguridad Física y Ambiental

El objetivo es minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles de protección de las instalaciones de procesamiento de información crítica o sensible de la organización, contra accesos físicos no autorizados.

El control de los factores ambientales de origen interno y/o externo permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

A.11.1 Áreas seguras

Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización.

Los medios de procesamiento de información crítica o confidencial deberían ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados.

Los medios de procesamiento deberían estar físicamente protegidos del acceso no autorizado, daño e interferencia.

A.11.2 Seguridad de los equipos

Deberían protegerse los equipos contra las amenazas físicas y ambientales. La protección del equipo es

necesaria para reducir el riesgo de acceso no autorizado a la información y su protección contra pérdida o robo.

Así mismo, se debería considerar la ubicación y eliminación de los equipos. Se podrían requerir controles especiales para la protección contra amenazas físicas y Para salvaguardar servicios de apoyo como energía eléctrica e infraestructura del cableado.

A.12 Seguridad en las Operaciones

El objetivo es controlar la existencia de los procedimientos de operaciones y el desarrollo y mantenimiento de documentación actualizada relacionada.

Adicionalmente, se debería evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando las responsabilidades correspondientes y administrando los medios técnicos necesarios para permitir la segregación de los ambientes y responsabilidades en el procesamiento.

Con el fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario, sería necesario monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad.

A.12.1 Responsabilidades y procedimientos de operación

Asegurar la operación correcta y segura de los medios de procesamiento de la información mediante el desarrollo de los procedimientos de operación apropiados.

Se deberían establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información.

Se debería implantar la segregación de tareas, cuando sea adecuado, para reducir el riesgo de un mal uso del sistema deliberado o por negligencia.

A.12.2 Protección contra código malicioso

El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos y se requiere tomar precauciones para evitar y detectar la introducción de códigos de programación maliciosos y códigos con capacidad de reproducción y distribución automática no autorizados para la protección de la integridad del software y de la información que sustentan.

El código malicioso es código informático que provoca infracciones de seguridad para dañar un sistema informático. El malware se refiere específicamente a software malicioso, pero el código malicioso incluye además scripts de sitios web (applets de Java, controles de ActiveX, contenido insertado, plug-ins, lenguajes de scripts u otros lenguajes de programación en páginas

web y correo electrónico) que pueden aprovechar vulnerabilidades con el fin de descargar un malware.

A.12.3 Copias de seguridad

Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación. Se deberían establecer procedimientos rutinarios para conseguir la estrategia aceptada de respaldo para realizar copias de seguridad y probar su puntual recuperación.
Implante procedimientos de backup y recuperación que satisfagan no sólo requisitos contractuales sino también requisitos de negocio "internos" de la organización.

A.12.4 Registro de actividad y supervisión

Los sistemas deberían ser monitoreados y los eventos de la seguridad de información registrados.

El registro de los operadores y el registro de fallas deberían ser usados para garantizar la identificación de los problemas del sistema de información.

La organización debería cumplir con todos los requerimientos legales aplicables para el monitoreo y el registro de actividades. El monitoreo del sistema debería ser utilizado para verificar la efectividad de los controles adoptados y para verificar la conformidad del modelo de política de acceso.

A.12.5 Control del software en explotación

Se trata de minimizar los riesgos de alteración de los sistemas de información mediante controles de implementación de cambios imponiendo el

cumplimiento de procedimientos formales que garanticen que se cumplan los procedimientos de seguridad y control, respetando la división de funciones. Verificar que los cambios sean gestionados por personal autorizado y en atención a los términos y condiciones que surjan de la licencia de uso.

Efectuar un análisis de riesgos previo a los cambios en atención al posible impacto por situaciones adversas.

Aplicar los cambios en sistemas de prueba y/o de manera escalonada empezando por los sistemas menos críticos además de aplicar medidas de backups y puntos de restauración junto a actividades adicionales que permitan retornar los sistemas al estado de estabilidad inicial con ciertas garantías.

Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.

Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar sus operaciones y envolver a usuarios finales en pruebas de aceptación del nuevo estado.

A.12.6 Gestión de la vulnerabilidad técnica

Se trata de minimizar los riesgos de alteración de los sistemas de información mediante controles de implementación de cambios imponiendo el cumplimiento de procedimientos formales que

garanticen que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

A.12.7 Consideraciones de las auditorías de los sistemas de información

Maximizar la efectividad del proceso de auditoría de los sistemas de información y minimizar las intromisiones a/desde éste proceso.

Durante las auditorías de los sistemas de información debieran existir controles para salvaguardar los sistemas operacionales y herramientas de auditoría.

A.13 Transferencia de información (Telecomunicaciones)

El objetivo es asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte.

La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección.

La información confidencial que pasa a través de redes públicas suele requerir de controles adicionales de protección.

A.13.1 Gestión de la seguridad en las redes

Se deberían controlar los accesos a servicios internos y externos conectados en red.

El acceso de los usuarios a redes y servicios en red no debería comprometer la seguridad de los servicios en red si se garantizan:

- Que existen interfaces adecuadas entre la red de la Organización y las redes públicas o privadas de otras organizaciones
- Que los mecanismos de autenticación adecuados se aplican a los usuarios y equipos
- El cumplimiento del control de los accesos de los usuarios a los servicios de información

A.13.2 Intercambio de información con partes externas

Se deberían realizar los intercambios sobre la base de una política formal de intercambio, según los acuerdos de intercambio y cumplir con la legislación correspondiente. Se deberían establecer procedimientos y normas para proteger la información y los medios físicos que contienen información en tránsito.

A.14 Adquisición de sistemas, desarrollo y mantenimiento de los sistemas de información

El objetivo es asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información.

Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

Definir los métodos de protección de la información crítica o sensible.

A.14.1 Requisitos de seguridad de los sistemas de información

El diseño e implantación de los sistemas de información que sustentan los procesos de negocio pueden ser cruciales para la seguridad. Los requisitos de seguridad deberían ser identificados y consensuados previamente al desarrollo y/o implantación de los sistemas de información. Todos los requisitos de seguridad deberían identificarse en la fase de recogida de requisitos de un proyecto y ser justificados, aceptados y documentados como parte del proceso completo para un sistema de información.

A.14.2 Seguridad en los procesos de desarrollo y soporte

Se deberían controlar estrictamente los entornos de desarrollo de proyectos y de soporte.

Los directivos responsables de los sistemas de aplicaciones deberían ser también responsables de la seguridad del proyecto o del entorno de soporte. Ellos deberían garantizar que todas las propuestas de cambio en los sistemas son revisadas para verificar que no comprometen la seguridad del sistema o del entorno operativo.

A.14.3 Datos de prueba

Se debería evitar la exposición de datos sensibles en entornos de prueba. Para proteger los datos de prueba se deberían establecer normas y procedimientos que contemplen prohibir el uso de bases de datos operativas.

A.15 Relaciones con Suministradores (Proveedores)

El objetivo es implementar y mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados en línea con los acuerdos de entrega de servicios de terceros.

A.15.1 Seguridad de la información en las relaciones con suministradores

La seguridad de la información de la organización y las instalaciones de procesamiento de la información no debería ser reducida por la introducción de un servicio o producto externo.

Debería controlarse el acceso de terceros a los dispositivos de tratamiento de información de la organización.

A.15.2 Gestión de la prestación del servicio por suministradores

La organización debería verificar la implementación de acuerdos, el monitoreo de su cumplimiento y gestión de los cambios con el fin de asegurar que los servicios que se ser prestan cumplen con todos los requerimientos acordados con los terceros.

A.16 Gestión de los incidentes de Seguridad

El objetivo es garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno. Las organizaciones cuentan con innumerables activos de información, cada uno expuesto a sufrir incidentes de

seguridad. Resulta necesario contar con una capacidad de gestión de dichos incidentes que permita comenzar por su detección, llevar a cabo su tratamiento y colaborar en la prevención de futuros incidentes similares.

A.16.1 Gestión de incidentes de seguridad de la información y mejoras

Deberían establecerse las responsabilidades y procedimientos para manejar los eventos y debilidades en la seguridad de información de una manera efectiva y una vez que hayan sido comunicados.

A.17 Continuidad de Negocio

El objetivo es preservar la seguridad de la información durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad.

Se deberían analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio y desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales, manteniendo las consideraciones en seguridad de la información utilizada en los planes de continuidad y función de los resultados del análisis de riesgos.

A.17.1 Continuidad de la seguridad de la información

Se deberían determinar los requisitos de seguridad de la información al planificar la continuidad de los procesos de negocio y la recuperación ante desastres.

La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y cambios de implementación para mantener los controles de seguridad de la información existentes durante una situación adversa.

Si los controles de seguridad no pueden continuar resguardando la información ante situaciones adversas, se deberían establecer, implementar y mantener otros controles para mantener un nivel aceptable de seguridad de la información.

A.17.2 Redundancias

Se deberían considerar los componentes o arquitecturas redundantes cuando no se pueda garantizar el nivel de disponibilidad requerido por las actividades de la organización a través de arquitecturas sencillas típicas o los sistemas existentes se demuestren insuficientes.

A.18 Cumplimiento con Requerimientos Legales y Contractuales

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales. Los requisitos normativos y contractuales pertinentes a cada sistema de información deberían estar debidamente definidos y documentados.

El objetivo es cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la organización y/o a los trabajadores que incurran en

responsabilidad civil o penal como resultado de incumplimientos.

A.18.1 Cumplimiento de los requisitos legales y contractuales

El diseño, operación, uso y gestión de los sistemas de información pueden ser objeto de requisitos estatutarios, reguladores y de seguridad contractuales. Los requisitos legales específicos deberían ser advertidos por los asesores legales de la organización o por profesionales adecuadamente cualificados.

Los requisitos que marca la legislación cambian de un país a otro y pueden variar para la información que se genera en un país y se transmite a otro país distinto (por ej., flujos de datos entre fronteras). Obtenga asesoramiento legal competente, especialmente si la organización opera o tiene clientes en múltiples jurisdicciones.

A.18.2 Revisiones de la seguridad de la información

Se deberían realizar revisiones regulares de la seguridad de los sistemas de información.

Las revisiones se deberían realizar según las políticas de seguridad apropiadas y las plataformas técnicas y sistemas de información deberían ser auditados para el cumplimiento de los estándares adecuados de implantación de la seguridad y controles de seguridad documentados.

2.2.4.13. El modelo de madurez de la seguridad de la información La Gestión de la Seguridad de la Información debe pasar por varios niveles o escalones, cada uno con su coste asociado y contexto de aplicabilidad. Se comienza a perfilar una escala de progresión en lo que ahora conocemos como Sistemas de Gestión de Seguridad de la Información basados en la norma ISO 27001.

Gráfico Nro. 7: Modelo de madurez de la seguridad de la información

Fuente: Interpretación y Auditoria ISO 27001 (27).

Considerando los avances y las preocupaciones actuales, esta escala se compondría de los siguientes niveles:

- **Nivel 0 (Sistema Inexistente):** el "sentido común". Procesos Inexistentes
- **Nivel 1 (Sistema Intermitente):** el cumplimiento de la legislación obligatoria. Procesos desorganizados.
- **Nivel 2 (Sistema Intuitivo):** evaluación del proceso de Gestión de Seguridad. Procesos Inconsistentes.

- **Nivel 3 (Sistema Definido):** analizar el riesgo y la gestión de su resolución. Procesos Documentados y comunicados
- **Nivel 4 (Sistema Administrado):** adquisición de productos para integrarlos en los Sistemas de Gestión. Procesos medidos y monitoreados.
- **Nivel 5 (Sistema Optimizado):** integración de los componentes certificados en sistemas compuestos y su certificación. Mejores Prácticas.

2.2.4.14. Gestión de Riesgos

Es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo (28).

Análisis De Riesgos

El análisis de riesgos es uno de los procesos más relevantes y prioritarios para la implantación de SGSI, por ser el procedimiento que permite analizar en forma metódica cada uno de los procesos, actividades y demás labores de la empresa que pueden estar en riesgo, así como determinar las necesidades de seguridad, las posibles vulnerabilidades y las amenazas a las que se encuentra expuesta. En tal sentido, el resultado que se obtiene de todo un proceso de análisis de riesgo es la información sobre el estado actual de la empresa en cuanto a sus niveles, controles de seguridad y los riesgos (28).

Existen dos aspectos principales que determinarán el análisis de riesgo:

- Probabilidad: posibilidad de ocurrencia del riesgo, la cual se puede medir con criterios de frecuencia.
- Impacto: consecuencias que pueden ocasionar la materialización del riesgo en la organización.

Evaluación del riesgo

La evaluación involucra comparar niveles de riesgo con criterios definidos en el contexto. El objetivo de esta evaluación es la de identificar y evaluar los riesgos, los cuales son calculados por una combinación de valores de activos y niveles de requerimiento de seguridad. Con base en esta comparación, se puede considerar la necesidad de tratamiento; además las decisiones se deben tomar de acuerdo con los requisitos legales, reglamentarios y otros (28).

- Dejar de conducir ciertas actividades.
- Desplazar activos de información de un área riesgosa a otra.
- Decidir no procesar cierto tipo de información y no se consigue la protección adecuada.
- La decisión por la opción de "evitar el riesgo" debe ser balanceada contra las necesidades financieras y comerciales de la empresa.
- Aceptar el riesgo cuando no es posible mitigarlo y se debe continuar la actividad que lo originó.

Reducir el riesgo

Para los riegos donde la opción de reducirlos ha sido escogida, se deben implementar los apropiados controles para disminuirlos a los niveles de aceptación previamente indefinidos por la empresa (28).

- Reduciendo la posibilidad que la vulnerabilidad sea explotada por las amenazas.
- Reduciendo la posibilidad de impacto si el riesgo ocurre detectando eventos no deseados, reaccionado y recuperándose de ellos.
- Transferir el riesgo fuera del apetito de riesgo, el riesgo se comparte con una o varias partes, pueden ser agentes externos.

Controles

Son las políticas, procedimientos, prácticas y estructuras organizacionales para reducir riesgos y que además proveen cierto grado de certeza de que se alcanzarán los objetivos del negocio (28).

Existen varias formas de establecer controles sobre riesgos organizacionales:

- Disuasivos: su presencia disuade de la comisión de acciones en contra de alguna política o procedimiento establecido y considerado correcto.
- Preventivos: detectan problemas antes que ocurran por medio de monitoreo constante.
- Detectivos: detectan y reportan los problemas suscitados por errores u omisiones, en el momento en que éstos ocurren.
- Represivos: Reduce el daño que el incidente está provocando a la Organización o empresa.
- Correctivos: minimizan el impacto de una amenaza ya consumada.

- Evaluativos: Se aplican para identificar evidencias para que sean analizadas y determinar las causas que lo provocaron, además de las acciones que se realizaron para la recuperación de la situación ocurrida.

Los activos pueden tener vulnerabilidades que son aprovechadas por las amenazas, las cuales conlleva al riesgo inminente en la empresa. En este orden se describe de manera sucinta cada elemento (28).

Activos

Los activos son todos los elementos que requiere una empresa u organización para el desarrollo de sus actividades misionales y las que serán tratadas durante el proceso de análisis de riegos. Los activos pueden ser físicos como servidores, equipos, cableados, entre otros y lógicos como aplicaciones, bases de datos, sitios web, entre otros.

Amenazas

Son todos aquellos hechos que pueden ocurrir en una empresa, perjudicando directamente los activos ya sea en el funcionamiento incorrecto o eliminación del mismo.

Vulnerabilidades

Son todas las debilidades de seguridad en la cual se encuentran los activos que se han identificado en el análisis y son susceptibles de amenazas para su daño o destrucción.
Las vulnerabilidades pueden clasificarse en las siguientes categorías:

Falta de entrenamiento en seguridad, carencia de toma de conciencia en seguridad, falta de mecanismos de monitoreo, falta de políticas para el uso correcto de las telecomunicaciones, no eliminar los accesos al término del contrato de trabajo, carencia de procedimiento que asegure la entrega de activos al término del contrato de trabajo, trabajadores desmotivados.

III. HIPÓTESIS

3.1. Hipótesis principal

El diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017, permitirá una adecuada administración de la información de GRUPO SIAS SAC.

3.2. Hipótesis especificas

1. La evaluación de los riesgos permitirá identificar y ponderar los riesgos a los cuales los sistemas de información, sus activos o servicios están expuestos, con la finalidad de identificar y seleccionar los controles apropiados.
2. La clasificación del nivel de impacto de los riesgos permitirá determinar cuáles son los riesgos más posibles de ocurrir.
3. La definición de planes de mitigación de riesgos permitirá reducir la probabilidad de ocurrencia del riesgo o reducir el impacto que pueda causar.
4. La utilización de herramientas tecnológicas y de desarrollo permitirán la mejora continua de la gestión de los procesos que avalen la seguridad de la información.

IV. METODOLOGÍA

4.1. Diseño de la investigación

Por las características de la investigación será de un enfoque cuantitativo. Rojas, E. (29); considera que: "La investigación cuantitativa es aquella que permite examinar los datos de manera científica, o más específicamente en forma numérica, generalmente con ayuda de herramientas del campo de la Estadística".

De acuerdo a la naturaleza del estudio de la investigación, reúne por su nivel, las características de un estudio descriptivo. Según Vásquez, I. (30); afirma que: "Los estudios descriptivos sirven para analizar cómo es y cómo se manifiesta un fenómeno y sus componentes. Permiten detallar el fenómeno estudiado básicamente a través de la medición de uno o más de sus atributos".

El diseño de la investigación fue no experimental, Según Arias, F. (31), afirma que: "Los Diseños no experimentales, son aquellos en los que se identifica un conjunto de entidades que representan el objeto del estudio y se procede a la observación de los datos."

$$M \rightarrow O$$

Donde:

M = Muestra

O = Observación

4.2. Población y Muestra

4.2.1. Población

La población a investigar consta de todos los trabajadores del GRUPO SIAS SAC, el cual asciende a 70 trabajadores en total.

4.2.2. Muestra

La muestra para la presente investigación está delimitada por 60 trabajadores, que son aquellos involucrados directamente en los procesos, para cada una de las variables en estudio sobre sistemas de gestión de seguridad de la información.

$$n = \frac{Z^2 * (p * q) * N}{E^2 * (N - 1) + Z^2 (p * q)}$$

Dónde:

n = tamaño de la muestra

Z = es una constante que depende del nivel de confianza que asignemos, para este caso será de 95,5%.

Z	1,15	1,28	1,44	1,65	1,96	2	2,58
Nivel de confianza	75%	80%	85%	90%	95%	95,5%	99%

p = es la proporción de individuos que poseen en la población la característica de estudio. Este dato es generalmente desconocido y se suele suponer que p=q=0.5 que es la opción más segura.

q = es la proporción de individuos que no poseen esa característica, es decir, es 1-p.

N = Población General

E = 5 % de error de tolerancia.

Remplazando los valores de la muestra, quedó establecida de la siguiente manera:

$$n = \frac{2\ ^2\ (0.5*0.5)\ 70}{0.05^2\ (70\ -1)\ +\ 2^2\ (0.5\ *\ 0.5)}$$

n = 60 Trabajadores

4.3. Definición operacional de las variables en estudio.

Tabla Nro. 7: Matriz de operacionalizacion de la variable

Variable	Definición conceptual	Dimensiones	Indicadores	Escala de medición	Definición Operacional
Activos de información	Identificar y proteger sus activos de información, evitando la destrucción, la divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, empleados, precios y otros	Nivel de conocimiento y uso del software y hardware	- Control de accesos y Criptografía - Seguridad en recursos humanos - Gestión de activos - Seguridad en la operaciones	Ordinal	- Disponibilidad y facilidad de uso de las herramientas tecnológicas para el desarrollo de las labores. - Conformidad con los sistemas actuales para el desarrollo de las labores. - Seguridad en los accesos a dispositivos y correos de la empresa.
Diseño del sistema de gestión de la seguridad de la información	La seguridad de la información se consigue implantando un conjunto adecuado de controles, tales como políticas, prácticas, procedimientos, estructuras organizativas y funciones de software. Estos controles han sido establecidos para asegurar que se cumplen los objetivos específicos de seguridad de la empresa	Nivel de conocimiento de políticas de seguridad de la información en la gestión administrativa	- Políticas de seguridad - Gestión de los incidentes de seguridad - Organización de la información - Transferencia de información y Documentos - Riesgos		- Información confiable, segura y disponible que permita la ayuda a la toma de decisiones - Claridad y definición de los procesos en que el área se desarrolla - Conformidad del personal involucrado en el correcto desarrollo de sus labores. - Conocimientos sobre las políticas de seguridad de la información existentes den la empresa.

Fuente: Elaboración propia.

4.4. Técnicas e instrumentos de recolección de datos

4.4.1. Técnica

Se utilizara la Técnica de la observación directa, con la finalidad de captar los hechos que acontecen en la empresa para obtener los datos más próximos que ocurren en la realidad.

La Entrevista, por medio de esta técnica, se recaudara información proveniente de la Gerencia con el fin de realizar análisis, gestión y evaluación de los riesgos asociados a los activos de información el cual nos permitirá obtener toda la información empírica necesaria para determinar los valores o respuestas de las variables motivo de estudio.

4.4.2. Instrumentos

Se realizara una Cuestionario de preguntas (Encuesta), a fin de obtener toda la información empírica necesaria para determinar los valores o respuestas de las variables motivo de estudio

Este cuestionario se redactó de acuerdo a los objetivos específicos, de tal modo que las preguntas que se realizan se respondan a la información que se desea obtener.

4.5. Plan de Análisis

A partir de los datos que se obtuvieron, se creará una base de datos temporal en el software Microsoft Excel 2013, y se procederá a la tabulación de los mismos. Se realizará el análisis de datos con cada una de las preguntas establecidas dentro del cuestionario dado permitiendo así resumir los datos en un gráfico que muestra el impacto porcentual de las mismas.

4.6. Matriz de consistencia.

<table>
<tr><th>Título</th><th>Caracterización del problema</th><th>Objetivo general</th><th>Hipótesis General</th></tr>
<tr><td rowspan="3">DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL GRUPO SIAS SAC. – CHIMBOTE; 2017.</td><td>• Control de acceso inadecuado.
• Puntos de accesos remotos no seguros y no vigilados.
• Contraseñas reutilizadas, sencillas o fáciles de adivinar a nivel de estación de trabajo.
• Cuentas de usuarios con privilegios exclusivos.
• Servidores con malas configuraciones.
• Inadecuada implementación de políticas de seguridad.</td><td>Realizar el diseño del sistema de gestión de seguridad de la información para el GRUPO SIAS SAC. – Chimbote; 2017., con la finalidad de administrar adecuadamente la información de la empresa.</td><td>El diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017, permitirá una adecuada administración de la información de GRUPO SIAS SAC.</td></tr>
<tr><td>Enunciado del problema</td><td>Objetivos Específicos</td><td>Hipótesis Específicos</td></tr>
<tr><td>¿De qué manera el diseño de un sistema de gestión de seguridad de la información, permitirá una adecuada administración de la información en el GRUPO SIAS SAC?</td><td>• Determinar los riesgos que se presentan con la información que se maneja en la Empresa.
• Clasificar el nivel de impacto de los riesgos.
• Construir planes de mitigación de riesgos (disminuir los riesgos).
• Utilizar herramientas tecnológicas y de desarrollo que permitan la gestión de los procesos que avalen la seguridad de la información.</td><td>• La evaluación de los riesgos permitirá identificar y ponderar los riesgos a los cuales los sistemas de información, sus activos o servicios están expuestos, con la finalidad de identificar y seleccionar los controles apropiados.
• La clasificación del nivel de impacto de los riesgos permitirá determinar cuáles son los riesgos más posibles de ocurrir.
• La definición de planes de mitigación de riesgos permitirá reducir la probabilidad de ocurrencia del riesgo o reducir el impacto que pueda causar.
• La utilización de herramientas tecnológicas y de desarrollo permitirán la mejora continua de la gestión de los procesos que avalen la seguridad de la información.</td></tr>
</table>

4.7. Principios éticos.

La investigación casi nunca ocurre de forma independiente. Muchas investigaciones requieren interactuar con personas, grupos o instituciones. Estas interacciones enfrentan al investigador con situaciones éticas. Por lo tanto, un código de ética es importante para asegurar el bienestar del investigador y de las personas que se estudien.

En esta investigación se ha tomado en cuenta los siguientes principios éticos:

- Transparencia en la recolección de datos de la población en estudio
- Énfasis en la autenticidad de los resultados obtenidos
- Confidencialidad en las respuestas a las encuestas aplicadas
- Honestidad al momento de realizar el análisis
- Veracidad de los resultados

V. RESULTADOS

5.1. Resultados

5.1.1. Dimensión I: Nivel de conocimiento y uso del software y hardware

Tabla Nro. 8: Acceso al ambiente donde se encuentran los servidores

Distribución de frecuencias y respuestas relacionadas con el Acceso al ambiente donde se encuentran los servidores; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

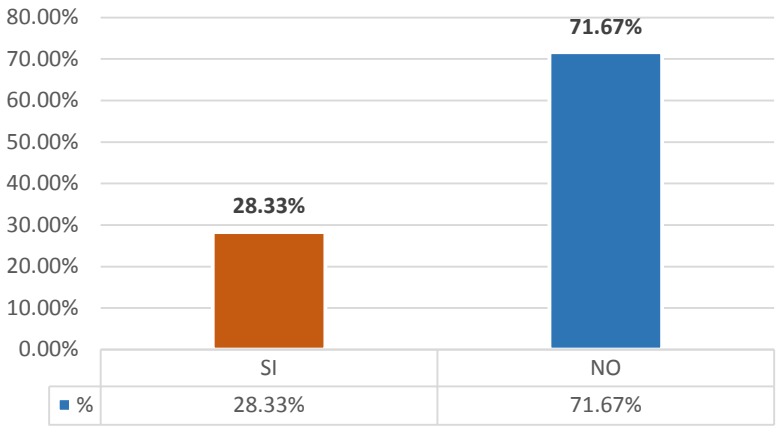
Alternativas	n	%
SI	17	28.33
NO	43	71.67
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Se registran los accesos de personas a las áreas donde se encuentran los equipos (servidores)?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 8; se observa que el 71.67% de los trabajadores encuestados expresaron que NO se registran los accesos de personas a las áreas donde se encuentran los equipos (Servidores), mientras que el 28.33% indican que SI se registran los accesos.

Gráfico Nro. 8: ¿Se registran los accesos de personas a las áreas donde se encuentran los equipos (servidores)?



Fuente: Tabla Nro. 8

Tabla Nro. 9: Uso de Equipo UPS

Distribución de frecuencias y respuestas relacionadas con el Uso de Equipo UPS; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

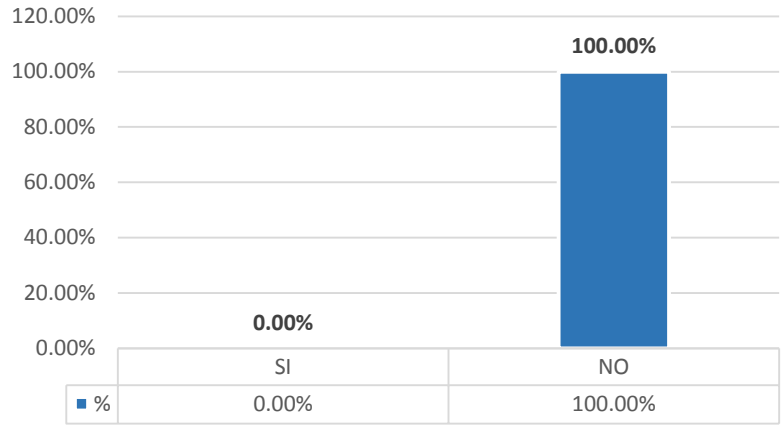
Alternativas	n	%
SI	0	0.00
NO	60	100.00
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Los equipos de cómputo en el área tienen fuente de poder interrumpible (UPS), Generadores de energía, baterías ante cortes de energía eléctrica?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 9; se observa que el 100.00% de los trabajadores encuestados expresaron que NO cuentan con UPS, Generadores de energía, baterías ante cortes de energía eléctrica.

Gráfico Nro. 9: ¿Los equipos de cómputo en el área tienen fuente de poder interrumpible (UPS), Generadores de energía, baterías ante cortes de energía eléctrica?



Fuente: Tabla Nro. 9

Tabla Nro. 10: Activos importantes, en relación con la información

Distribución de frecuencias y respuestas relacionadas con los Activos importantes en relación con la información; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

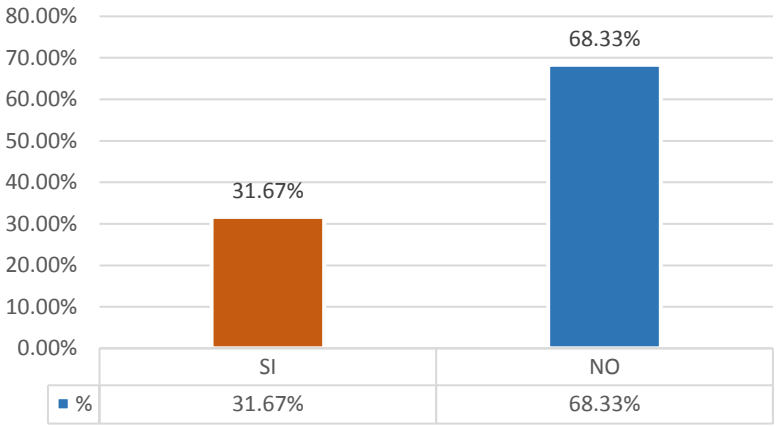
Alternativas	n	%
SI	19	31.67
NO	41	68.33
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: Frente a cualquier desastre natural, provocado o humano ¿Ud. conoce cuales son los activos más importantes que debe proteger en relación a la información?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 10; se observa que el 68.33% de los trabajadores encuestados expresaron que NO conocen los activos más importantes con respecto a la información de la empresa, mientras que el 31.67% indican que SI conocen.

Gráfico Nro. 10: Frente a cualquier desastre natural, provocado o humano ¿Ud. conoce cuales son los activos más importantes que debe proteger en relación a la información?



Fuente: Tabla Nro. 10

Tabla Nro. 11: Uso correcto de equipos informáticos

Distribución de frecuencias y respuestas relacionadas con el Uso correcto de los equipos informáticos; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

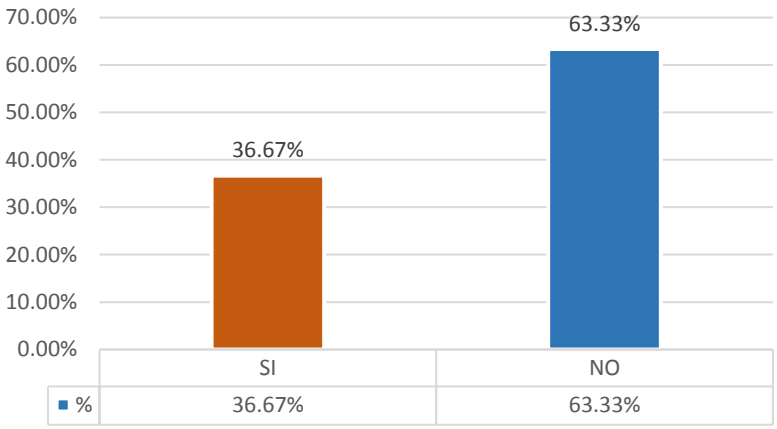
Alternativas	n	%
SI	22	36.67
NO	38	63.33
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Usted apaga los equipos informáticos (PC) correctamente después de utilizarlos?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 11; se observa que el 63.33% de los trabajadores encuestados expresaron que NO apagan los equipos informáticos (PC) después de utilizarlos, mientras que el 36.67% indican que SI.

Gráfico Nro. 11: ¿Usted apaga los equipos informáticos correctamente después de utilizarlos?



Fuente: Tabla Nro. 11

Tabla Nro. 12: Bloqueo de Sesión en PC

Distribución de frecuencias y respuestas relacionadas con el Bloqueo de Sesión en PC; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

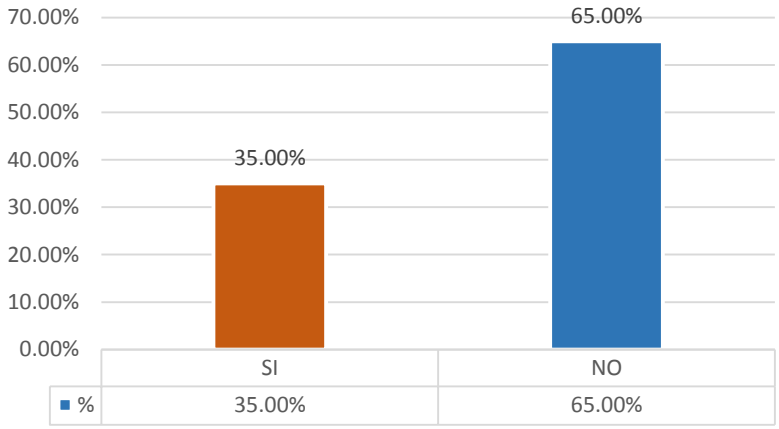
Alternativas	n	%
SI	21	35.00
NO	39	65.00
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Cuándo se ausenta de su oficina deja bloqueada la PC?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 12; se observa que el 65.00% de los trabajadores encuestados expresaron que NO bloquean la PC cuando se ausentan de la Oficina, mientras que el 35.00% indican que SI.

Gráfico Nro. 12: ¿Cuándo se ausenta de su oficina deja bloqueada la PC?



Fuente: Tabla Nro. 12

Tabla Nro. 13: Uso de dispositivos externos

Distribución de frecuencias y respuestas relacionadas con el Uso de dispositivos externos, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

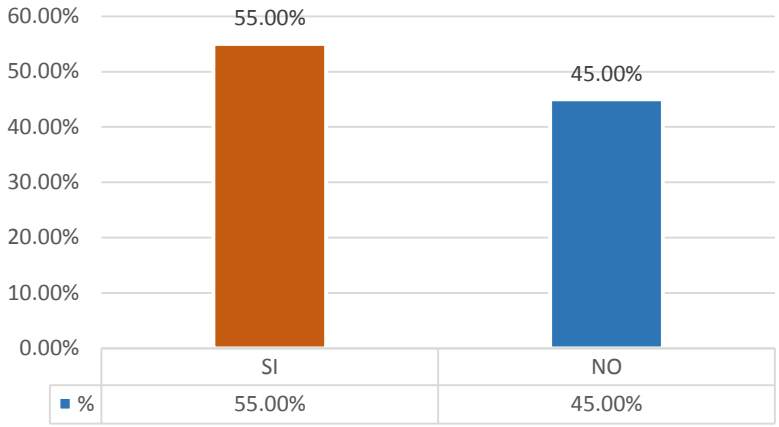
Alternativas	n	%
SI	33	55.00
NO	27	45.00
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Has utilizado algún dispositivo externo (USB, Celular, Discos Externos) para extraer algún tipo de información de trabajo o de su interés?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 13; se observa que el 55.00% de los trabajadores encuestados expresaron que SI utilizan dispositivos externos para extraer algún tipo de información de trabajo o de su interés, mientras que el 45.00% indican que NO.

Gráfico Nro. 13: ¿Has utilizado algún dispositivo externo (USB, Celular, Discos Externos) para extraer algún tipo de información de trabajo o de su interés?



Fuente: Tabla Nro. 13

Tabla Nro. 14: Uso de Antivirus

Distribución de frecuencias y respuestas relacionadas con el Uso de Antivirus, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

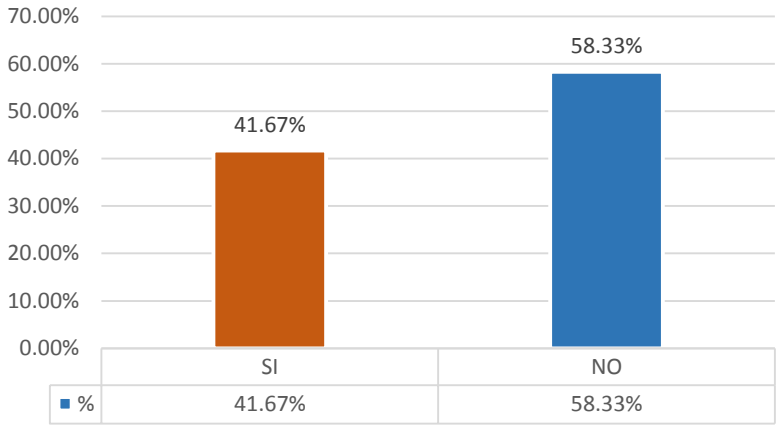
Alternativas	n	%
SI	25	41.67
NO	35	58.33
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Usted ha detectado que el antivirus del Grupo SIAS SAC funciona adecuadamente y que se encuentra actualizado?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 14; se observa que el 58.33% de los trabajadores encuestados expresaron NO, el antivirus no funciona correctamente y no está actualizado, mientras que el 41.67% indican que SI.

Gráfico Nro. 14: ¿Usted ha detectado que el antivirus del Grupo SIAS SAC funciona adecuadamente y que se encuentra actualizado?



Fuente: Tabla Nro. 14

Tabla Nro. 15: Uso de Alarmas (Incendios, Robos, etc.)

Distribución de frecuencias y respuestas relacionadas con el Uso de Alarmas (Incendios, Robos, etc.), para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

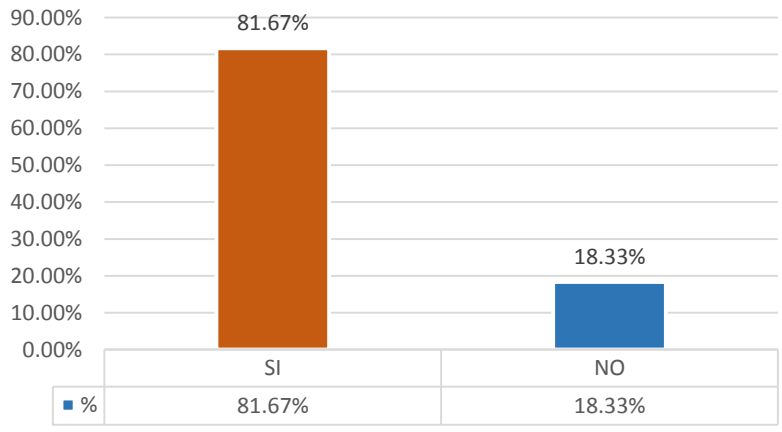
Alternativas	n	%
SI	49	81.67
NO	11	18.33
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Existe alguna alarma contra incendios, robos, otros?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 15; se observa que el 81.67% de los trabajadores encuestados expresaron que SI existe alarmas contra incendios, robos y otros en la empresa, mientras que el 18.33% indican que NO.

Gráfico Nro. 15: ¿Existe alguna alarma contra incendios, robos, otros?



Fuente: Tabla Nro. 15

Tabla Nro. 16: Inventario de Activos

Distribución de frecuencias y respuestas relacionadas con el Inventario de Activos, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

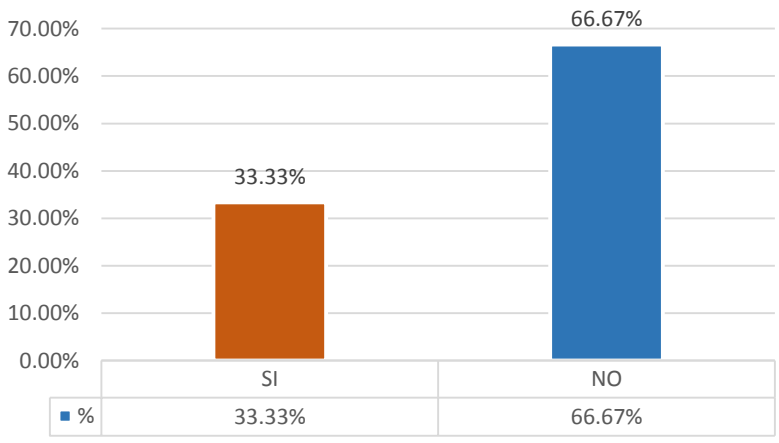
Alternativas	n	%
SI	20	33.33
NO	40	66.67
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Existen un inventario de activos actualizado?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 16; se observa que el 66.67% de los trabajadores encuestados expresaron que NO existe un inventario de activos actualizado, mientras que el 33.33% indican que SI.

Gráfico Nro. 16: ¿Existen un inventario de activos actualizado?



Fuente: Tabla Nro. 16

Tabla Nro. 17: Contenido del Inventario de Activos

Distribución de frecuencias y respuestas relacionadas con el Contenido del Inventario de Activos, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

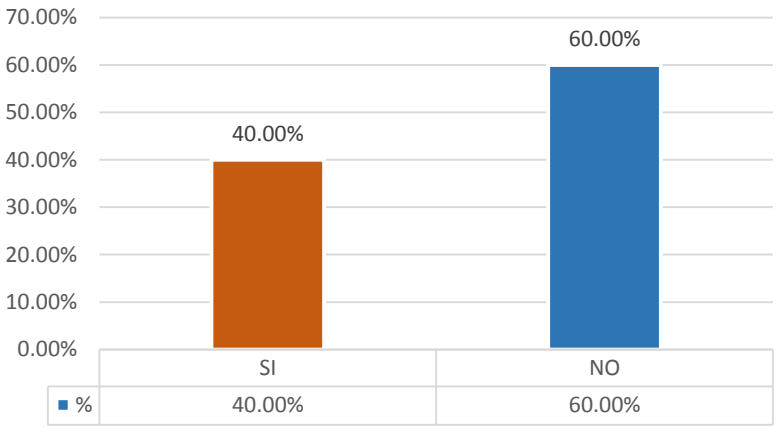
Alternativas	n	%
SI	24	40.00
NO	36	60.00
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿El Inventario contiene activos de datos, software, equipos y servicios?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 17; se observa que el 60.00% de los trabajadores encuestados expresaron que NO existe un inventario con los activos (Equipos, Software y Servicios), mientras que el 40.00% indican que SI.

Gráfico Nro. 17: ¿El Inventario contiene activos de datos, software, equipos y servicios?



Fuente: Tabla Nro. 17

Tabla Nro. 18: Clasificación de la Información

Distribución de frecuencias y respuestas relacionadas con la Clasificación de la Información, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

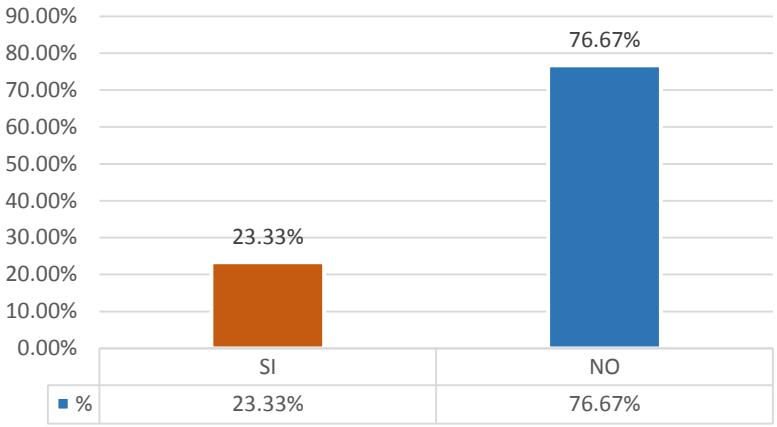
Alternativas	n	%
SI	14	23.33
NO	46	76.67
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Se dispone de una clasificación de la información según la criticidad de la misma (Documentos, Expedientes, Órdenes de compra, Contratos, etc.?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 18; se observa que el 76.67% de los trabajadores encuestados expresaron que NO existe una clasificación de la información según la criticidad, mientras que el 23.33% indican que SI.

Gráfico Nro. 18: ¿Se dispone de una clasificación de la información según la criticidad de la misma (Documentos, Expedientes, Órdenes de compra, Contratos, etc.?



Fuente: Tabla Nro. 18

Tabla Nro. 19: Responsable de Activos

Distribución de frecuencias y respuestas relacionadas con el Responsable de Activos, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

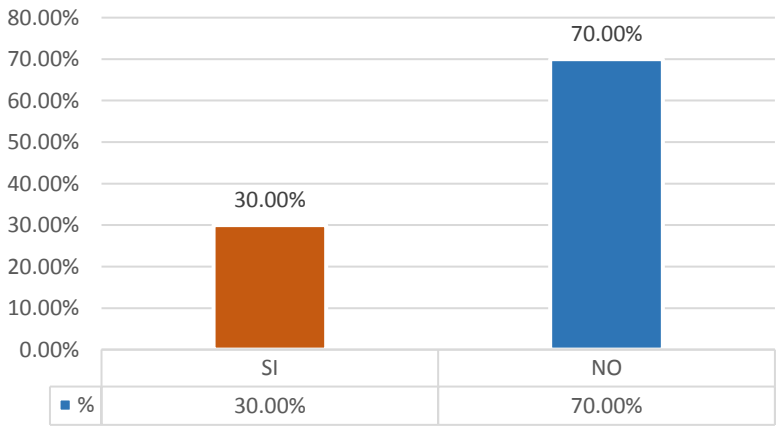
Alternativas	n	%
SI	18	30.00
NO	42	70.00
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Existe un responsable de los activos?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 19; se observa que el 70.00% de los trabajadores encuestados expresaron que NO existe un responsable de Activos, mientras que el 30.00% indican que SI.

Gráfico Nro. 19: ¿Existe un responsable de los activos?



Fuente: Tabla Nro. 19

Tabla Nro. 20: Claves de Acceso a PC

Distribución de frecuencias y respuestas relacionadas con las Claves de Acceso a PC, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

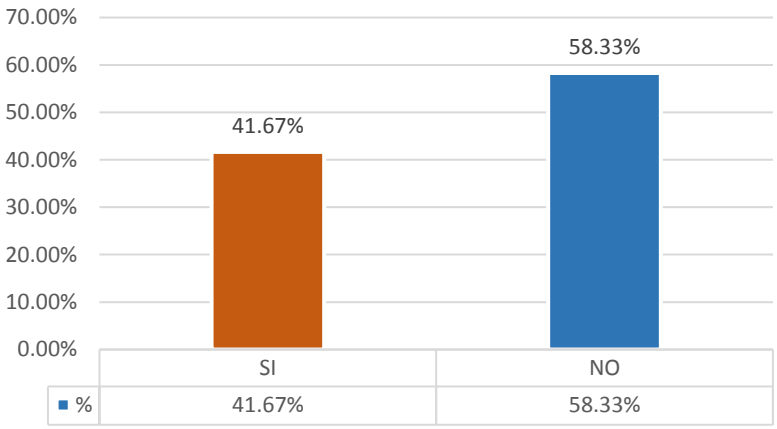
Alternativas	n	%
SI	25	41.67
NO	35	58.33
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿La clave de acceso es la misma para todos los sistemas y/o PC con los que cuenta el Grupo SIAS SAC?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 20; se observa que el 58.33% de los trabajadores encuestados expresaron que NO, son las mismas claves de acceso para las PC y/o sistemas en todos los equipos de la empresa, mientras que el 41.67% indican que SI.

Gráfico Nro. 20: ¿La clave de acceso es la misma para todos los sistemas y/o PC con los que cuenta el Grupo SIAS SAC?



Fuente: Tabla Nro. 20

Tabla Nro. 21: Comparte sus claves de acceso

Distribución de frecuencias y respuestas relacionadas con Comparte sus claves de acceso, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

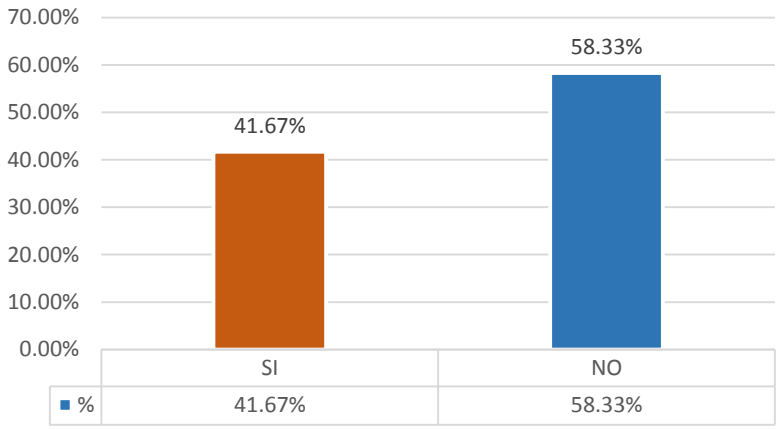
Alternativas	n	%
SI	35	58.33
NO	25	41.67
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Comparte sus claves de acceso de su PC con sus compañeros de trabajo?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 21; se observa que el 58.33% de los trabajadores encuestados expresaron que SI comparten sus claves de acceso con sus compañeros, mientras que el 41.67% indican que NO.

Gráfico Nro. 21: ¿Comparte sus claves de acceso de su PC con sus compañeros de trabajo?



Fuente: Tabla Nro. 21

Tabla Nro. 22: Cambio de Claves de acceso

Distribución de frecuencias y respuestas relacionadas con el Cambio de Claves de acceso, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

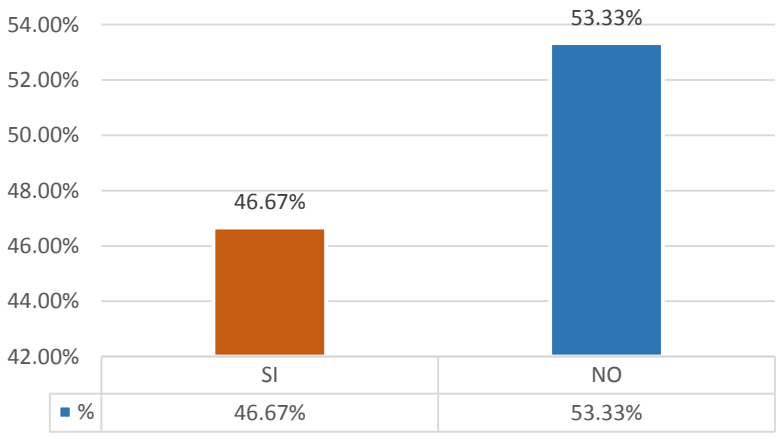
Alternativas	n	%
SI	28	46.67
NO	32	53.33
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Ud. cambia con frecuencia sus Claves de acceso?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 22; se observa que el 53.33% de los trabajadores encuestados expresaron que NO cambian con frecuencia la clave de acceso de sus equipos, mientras que el 46.67% indican que SI.

Gráfico Nro. 22: ¿Ud. cambia con frecuencia sus Claves de acceso?



Fuente: Tabla Nro. 22

5.1.2. Dimensión II: Nivel de conocimiento de políticas de seguridad de la información en la gestión administrativa

Tabla Nro. 23: Políticas de Seguridad de la Información

Distribución de frecuencias y respuestas relacionadas con las Políticas de Seguridad de la Información; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

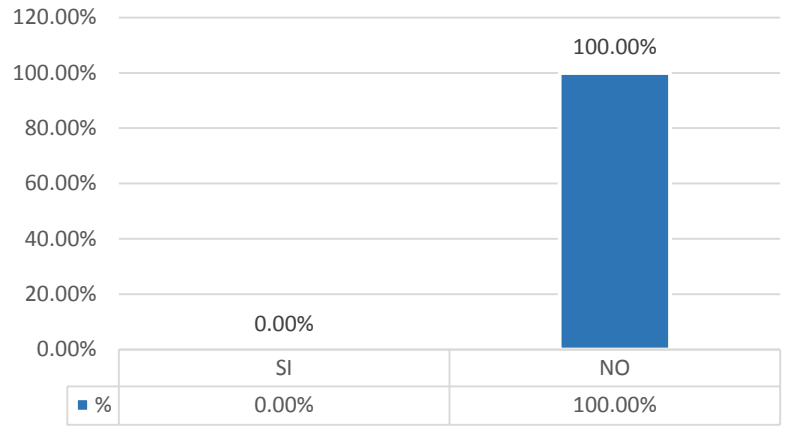
Alternativas	n	%
SI	0	0.00
NO	60	100.00
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿En el Grupo SIAS SAC, cuentan con políticas de seguridad de la información?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 23; se observa que el 100.00% de los trabajadores encuestados expresaron que NO existen políticas de seguridad de la información en el Grupo SIAS SAC.

Gráfico Nro. 23: ¿En el Grupo SIAS SAC, cuentan con políticas de seguridad de la información?



Fuente: Tabla Nro. 23

Tabla Nro. 24: Nivel de conocimiento de Políticas de seguridad de información

Distribución de frecuencias y respuestas relacionadas con el Nivel de conocimiento de Políticas de seguridad de información; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

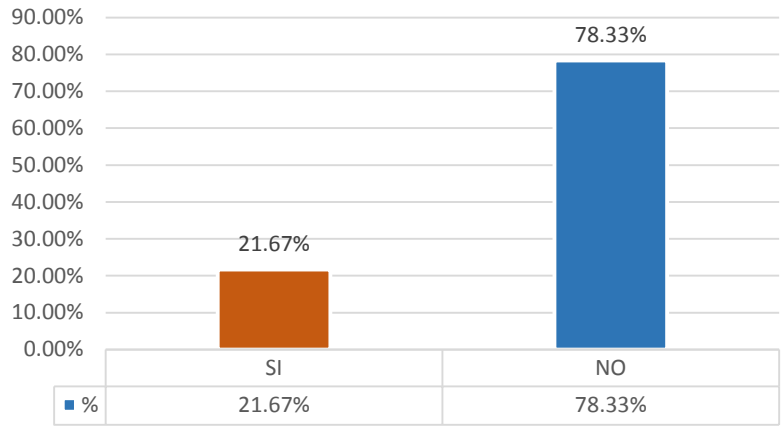
Alternativas	n	%
SI	13	21.67
NO	47	78.33
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Conoce UD. que son las Políticas de seguridad de la Información?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 24; se observa que el 78.33% de los trabajadores encuestados expresaron que NO conocen sobre que son las políticas de seguridad de la información, mientras que el 21.67% indicaron que SI conocen.

Gráfico Nro. 24: ¿Conoce UD. que son las Políticas de seguridad de la Información?



Fuente: Tabla Nro. 24

Tabla Nro. 25: Existe algún documento de Políticas de seguridad de la información en la empresa

Distribución de frecuencias y respuestas relacionadas con que si Existe algún documento de Políticas de seguridad de la información en la empresa; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

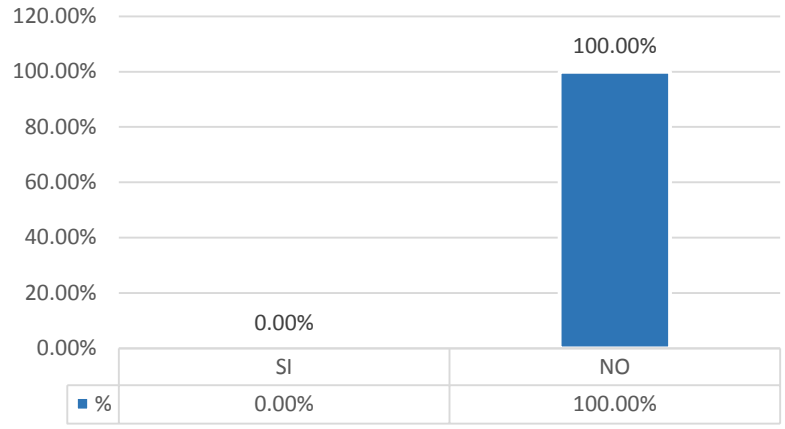
Alternativas	n	%
SI	0	0.00
NO	60	100.00
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Existe algún tipo de manual y/o documento donde se especifique los controles para la seguridad de la información del GRUPO SIAS SAC?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 25; se observa que el 100.00% de los trabajadores encuestados expresaron que NO existen ningún documento en la empresa sobre políticas de seguridad de la información.

Gráfico Nro. 25: Existe algún tipo de manual y/o documento donde se especifique los controles para la seguridad de la información del GRUPO SIAS SAC?



Fuente: Tabla Nro. 25

Tabla Nro. 26: Uso correcto de la Importancia de la información

Distribución de frecuencias y respuestas relacionadas con el Uso correcto de la Importancia de la información; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

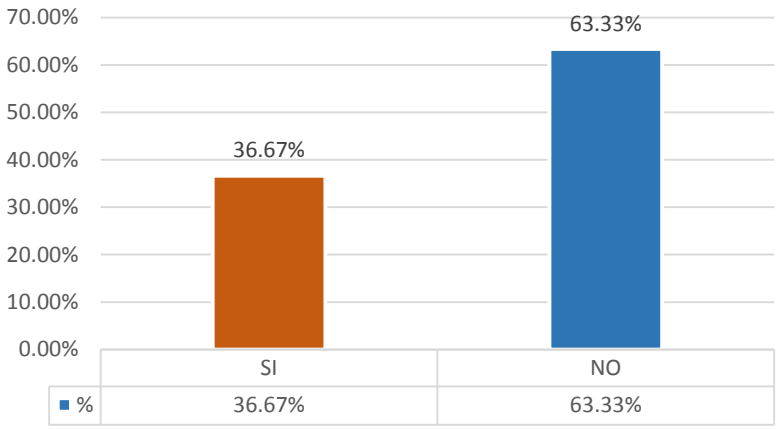
Alternativas	n	%
SI	22	36.67
NO	38	63.33
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Ud. sabe distinguir la información que es estrictamente confidencial, de uso interno o público?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro.26; se observa que el 63.33% de los trabajadores encuestados expresaron que NO saben distinguir el uso correcto de la información de la empresa, mientras el 36.67% indican que SI saben.

Gráfico Nro. 26: ¿Ud. sabe distinguir la información que es estrictamente confidencial, de uso interno o público?



Fuente: Tabla Nro. 26

Tabla Nro. 27: Información (Documentación)

Distribución de frecuencias y respuestas relacionadas con la Información (Documentación); para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

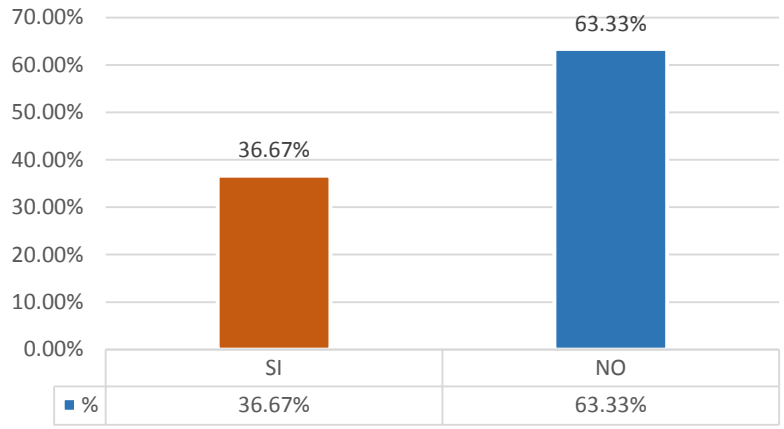
Alternativas	n	%
SI	22	36.67
NO	38	63.33
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Cuándo se ausenta de su oficina deja documentación visible en su escritorio?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 27; se observa que el 63.33% de los trabajadores encuestados expresaron que NO dejan documentación visible cuando se ausentan de la oficina, mientras que el 36.67% indicaron que SI

Gráfico Nro. 27: ¿Cuándo se ausenta de su oficina deja documentación visible en su escritorio?



Fuente: Tabla Nro. 27

Tabla Nro. 28: Uso de Correo Electrónico de la empresa

Distribución de frecuencias y respuestas relacionadas con el Uso de Correo Electrónico de la empresa; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

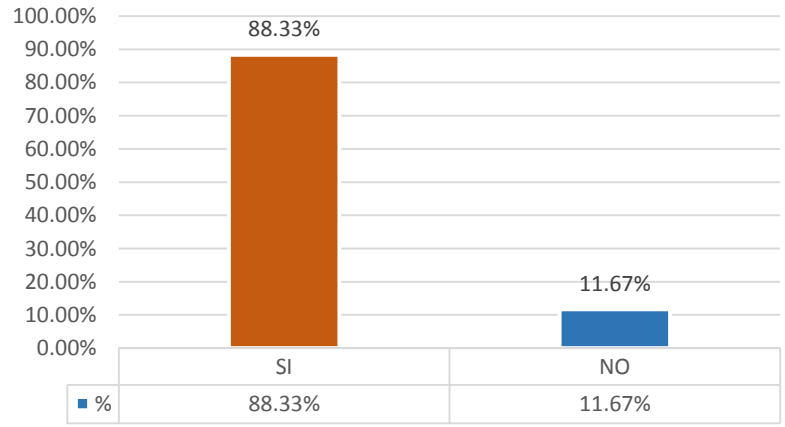
Alternativas	n	%
SI	53	88.33
NO	7	11.67
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Cuenta con correo electrónico de la empresa?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 28; se observa que el 88.33% de los trabajadores encuestados expresaron que SI cuentan con correo eléctrico de la empresa, mientras que el 11.67% indican que NO.

Gráfico Nro. 28: ¿Cuenta con correo electrónico de la empresa?



Fuente: Tabla Nro. 28

Tabla Nro. 29: Comparte el acceso de su correo electrónico

Distribución de frecuencias y respuestas relacionadas con Comparte el acceso de su correo electrónico; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

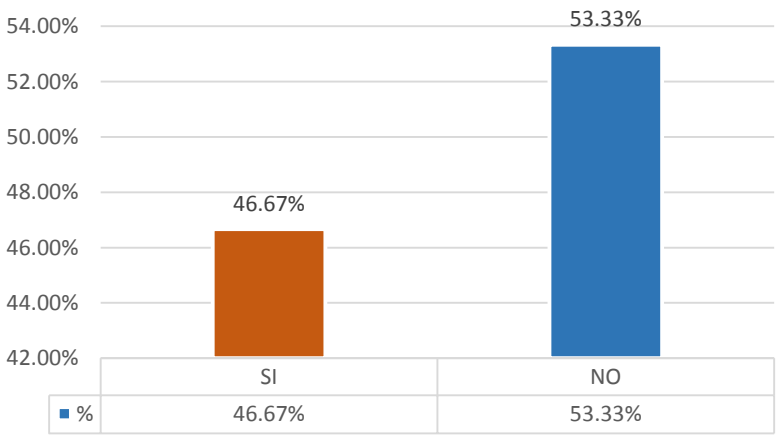
Alternativas	n	%
SI	28	46.67
NO	32	53.33
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Comparte su clave de Correo, con sus compañeros de trabajo? para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 29; se observa que el 53.33% de los trabajadores encuestados expresaron que NO comparten su clave de acceso de su correo con sus compañeros, mientras que el 46.67% indican que SI.

Gráfico Nro. 29: ¿Comparte su clave de Correo, con sus compañeros de trabajo?



Fuente: Tabla Nro. 29

Tabla Nro. 30: Destrucción de información

Distribución de frecuencias y respuestas relacionadas con la Destrucción de información; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

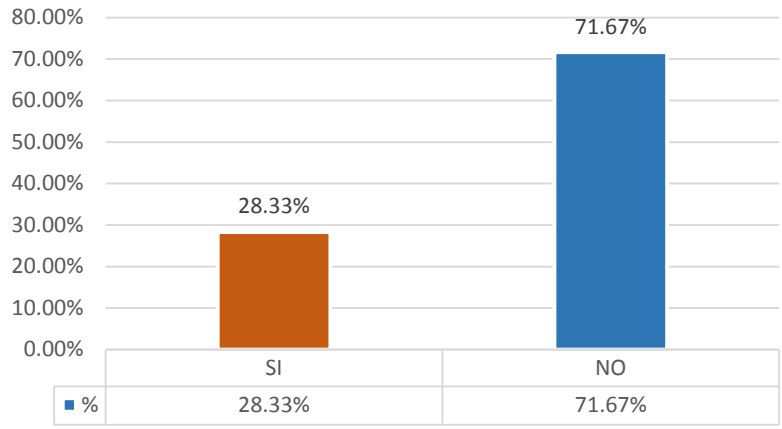
Alternativas	n	%
SI	17	28.33
NO	43	71.67
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Usted Desecha la información (Documentación) que ya no necesita?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 30; se observa que el 71.67% de los trabajadores encuestados expresaron que NO Desechan la información que ya no necesitan, mientras que el 28.33% indican que SI.

Gráfico Nro. 30: *¿Usted Desecha la información (Documentación) que ya no necesita?*



Fuente: Tabla Nro. 30

Tabla Nro. 31: Clasificación de la Información

Distribución de frecuencias y respuestas relacionadas con la Clasificación de la Información; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

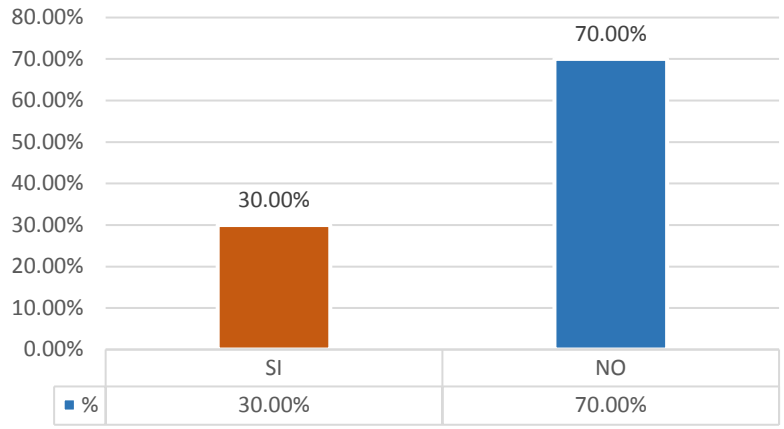
Alternativas	n	%
SI	18	30.00
NO	42	70.00
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Existen procedimientos para clasificar la información (Documentación)?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 31; se observa que el 70.00% de los trabajadores encuestados expresaron que NO existen procedimientos para clasificar la información (Documentación), mientras que el 30.00% indican que SI.

Gráfico Nro. 31: ¿Existen procedimientos para el resguardo de la información?



Fuente: Tabla Nro. 31

Tabla Nro. 32: Resguardo de la Información

Distribución de frecuencias y respuestas relacionadas con el Resguardo de la Información; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

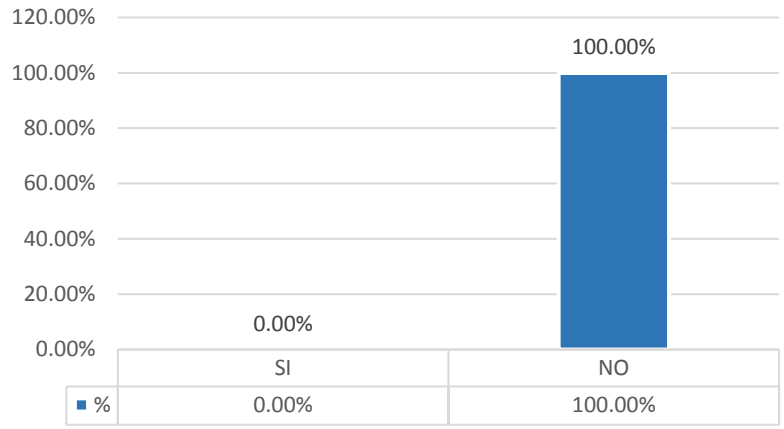
Alternativas	n	%
SI	0	0.00
NO	60	100.00
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Existen procedimientos para el resguardo de la información (Documentación)?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 32; se observa que el 100.00% de los trabajadores encuestados expresaron que NO existen ningún procedimiento para el resguardo de la información (Documentación).

Gráfico Nro. 32: ¿Existen procedimientos para el resguardo de la información (Documentación)?



Fuente: Tabla Nro. 32

Tabla Nro. 33: Existe roles y responsabilidades definidos

Distribución de frecuencias y respuestas relacionadas con la Existencia de roles y responsabilidades definidos; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

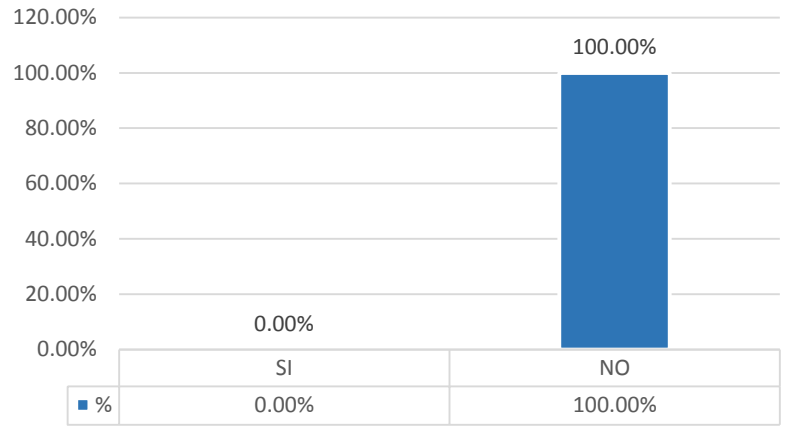
Alternativas	n	%
SI	0	0.00
NO	60	100.00
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Existen roles y responsabilidades definidos para las personas implicadas en la seguridad de la Información?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 33; se observa que el 100.00% de los trabajadores encuestados expresaron que NO existen roles y responsabilidades para la seguridad de la Información.

Gráfico Nro. 33: ¿Existen roles y responsabilidades definidos para las personas implicadas en la seguridad de la Información?



Fuente: Tabla Nro. 33

Tabla Nro. 34: Participación en temas de seguridad de la información

Distribución de frecuencias y respuestas relacionadas con la Participación en temas de seguridad de la información; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

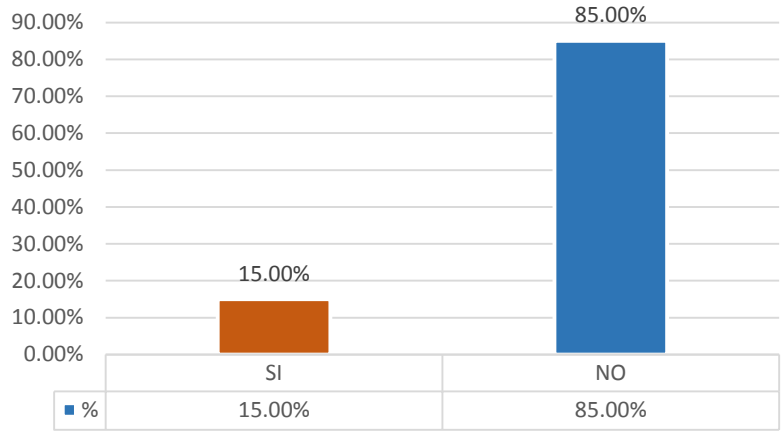
Alternativas	n	%
SI	9	15.00
NO	51	85.00
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿La Dirección y las áreas de la Organización participa en temas de seguridad de la información?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 34; se observa que el 85.00% de los trabajadores encuestados expresaron que NO existe participación de la Direccion y de las áreas en temas seguridad de la información, mientras que el 15.00% indican que SI.

Gráfico Nro. 34: ¿La Dirección y las áreas de la Organización participan en temas de seguridad de la información?



Fuente: Tabla Nro. 34

Tabla Nro. 35: Confidencialidad de Información

Distribución de frecuencias y respuestas relacionadas con la Confidencialidad de Información; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

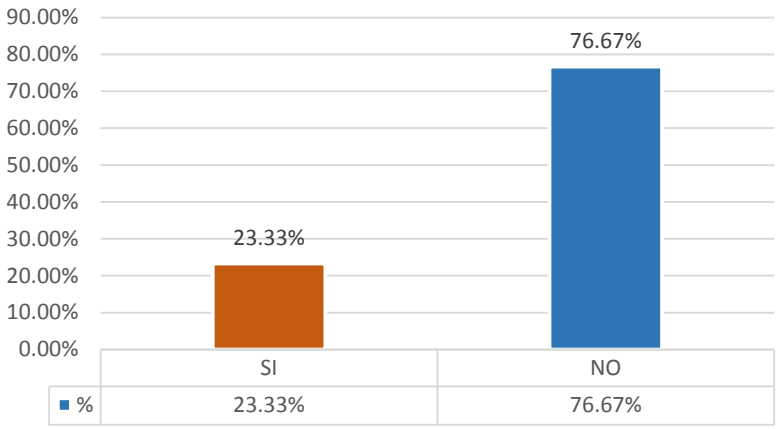
Alternativas	n	%
SI	14	23.33
NO	46	76.67
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Existe un acuerdo de confidencialidad, con respecto a la información que se maneja en la empresa?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 35; se observa que el 76.67% de los trabajadores encuestados expresaron que NO existe un acuerdo de confidencialidad con respecto a la información, mientras que el 23.33% indican que SI.

Gráfico Nro. 35: ¿Existe un acuerdo de confidencialidad, con respecto a la información que se maneja en la empresa?



Fuente: Tabla Nro. 35

Tabla Nro. 36: Selección del Personal

Distribución de frecuencias y respuestas relacionadas con la Selección del Personal; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

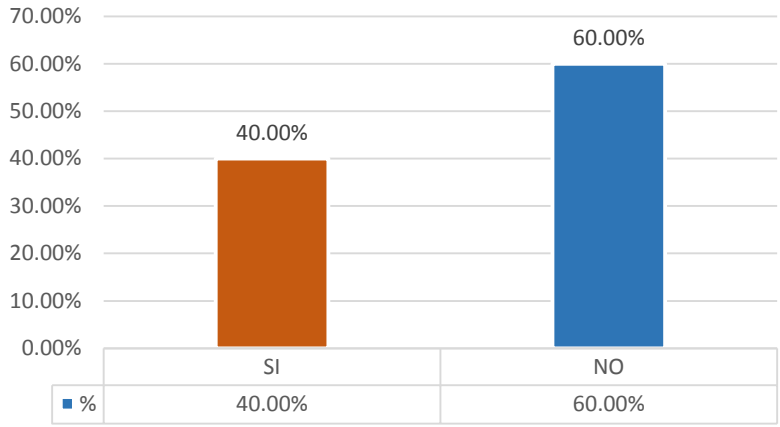
Alternativas	n	%
SI	24	40.00
NO	36	60.00
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta ¿Se tiene en cuenta la seguridad de la información que se maneja en la empresa al momento de selección y baja del personal?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 36; se observa que el 60.00% de los trabajadores encuestados expresaron que NO se tiene en cuenta la seguridad de la información al momento de realizar la selección del personal, mientras que el 40.00% indican que SI.

Gráfico Nro. 36: ¿Se tiene en cuenta la seguridad de la información que se maneja en la empresa al momento de selección y baja del personal?



Fuente: Tabla Nro. 36

Tabla Nro. 37: Condiciones de confidencialidad

Distribución de frecuencias y respuestas relacionadas con las Condiciones de confidencialidad; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

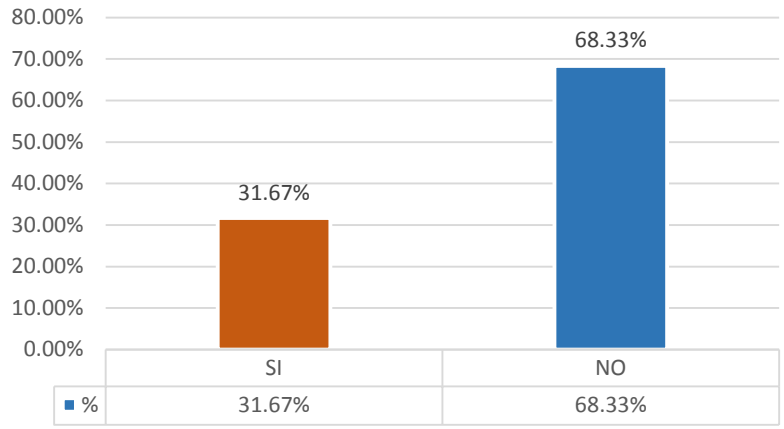
Alternativas	n	%
SI	19	31.67
NO	41	68.33
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Se plasman las condiciones de confidencialidad y responsabilidades en los contratos?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 37; se observa que el 68.33% de los trabajadores encuestados expresaron que NO existe condiciones de confidencialidad en los contratos, mientras que el 31.67% indican que SI.

Gráfico Nro. 37: ¿Se plasman las condiciones de confidencialidad y responsabilidades en los contratos?



Fuente: Tabla Nro. 37

Tabla Nro. 38: Proceso disciplinario a trabajadores

Distribución de frecuencias y respuestas relacionadas con el Proceso disciplinario a trabajadores; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

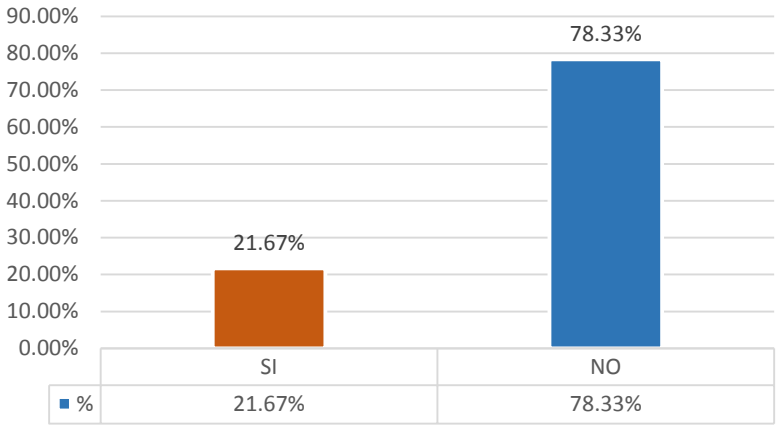
Alternativas	n	%
SI	13	21.67
NO	47	78.33
Total	60	100.00

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta ¿Existe un proceso disciplinario, relacionado con la falta de confidencialidad de los trabajadores hacia la empresa?, para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 38; se observa que el 78.33% de los trabajadores encuestados expresaron que NO existe un proceso disciplinario con respecto a la confidencialidad de la información, mientras que el 21.67% indican que SI.

Gráfico Nro. 38: ¿Existe un proceso disciplinario, relacionado con la falta de confidencialidad de los trabajadores hacia la empresa?



Fuente: Tabla Nro. 38

5.1.3. Resultados - Dimensión I

Tabla Nro. 39: Dimensión I - Nivel de conocimiento y Uso del Software y Hardware

Distribución de frecuencias y respuestas relacionadas con la Dimensión I - Nivel de conocimiento y Uso del Software y Hardware; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Alternativas	n	%
SI	12	20.00
NO	48	80.00
Total	60	100.00

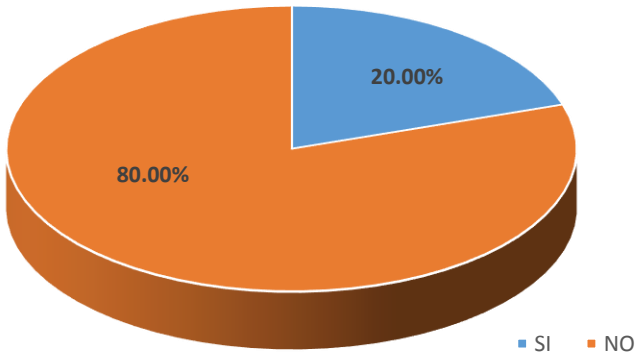
Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto al Nivel de conocimiento y Uso del Hardware - Software del GRUPO SIAS SAC , para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 39; se observa que el 80.00% de los trabajadores encuestados NO tienen conocimiento y no realizan un buen uso del Hardware y Software de la empresa, mientras que el 20.00% de los trabajadores SI realizan un buen uso de los equipos.

Gráfico Nro. 39: Resultados de la Dimensión I - Nivel de conocimiento y Uso del Software y Hardware

Distribución porcentual de las frecuencias y respuestas relacionadas con la Dimensión I - Nivel de conocimiento y Uso del Software y Hardware; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.



Fuente: Tabla Nro. 39

5.1.4. Resultado - Dimensión II

Tabla Nro. 40: Dimensión II - Nivel de conocimiento de Políticas de Seguridad de la Información en la Gestion Administrativa

Distribución de frecuencias y respuestas relacionadas con la Dimensión II - Nivel de conocimiento de Políticas de Seguridad de la Información en la Gestion Administrativa; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Alternativas	n	%
SI	1	1.67
NO	54	98.33
Total	60	100.00

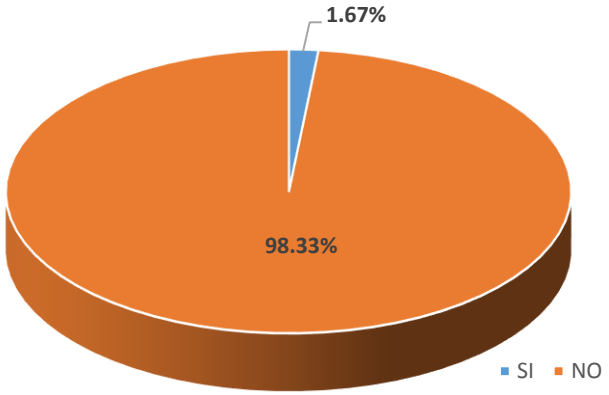
Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto al conocimiento de Políticas de Seguridad de información, en las labores administrativas que se realizan en el GRUPO SIAS SAC , para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 40; se observa que el 98.33% de los trabajadores encuestados NO tienen conocimiento acerca de las políticas de se seguridad de la información en las labores administrativas que ellos realizan, mientras que el 1.67% de los trabajadores SI lo conocen.

Gráfico Nro. 40: Resultados de la Dimensión II - Nivel de conocimiento de Políticas de Seguridad de la Información en la Gestion Administrativa

Distribución porcentual de las frecuencias y respuestas relacionadas con la Resultados de la Dimensión II - Nivel de conocimiento de Políticas de Seguridad de la Información en la Gestion Administrativa; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.



Fuente: Tabla Nro. 40

5.1.5. Resumen General - Dimensiones

Tabla Nro. 41: Resumen General de Dimensiones

Distribución de frecuencias y respuestas relacionadas con las 02 dimensiones definidas para determinar el nivel de conocimiento de los trabajadores; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.

DIMENSIONES	SI		NO		TOTAL	
	n	%	n	%	n	%
Nivel de conocimiento y Uso del Software y Hardware	12	20.00	48	80.00	60	100.00
Nivel de conocimiento de Políticas de Seguridad de la Información en la Gestion Administrativa	1	1.67	59	98.33	60	100.00

Fuente: Aplicación del instrumento para el conocimiento de los trabajadores encuestados acerca del conocimiento de las 02 dimensiones definidas para la investigación, en el GRUPO SIAS SAC – Chimbote; 2017.

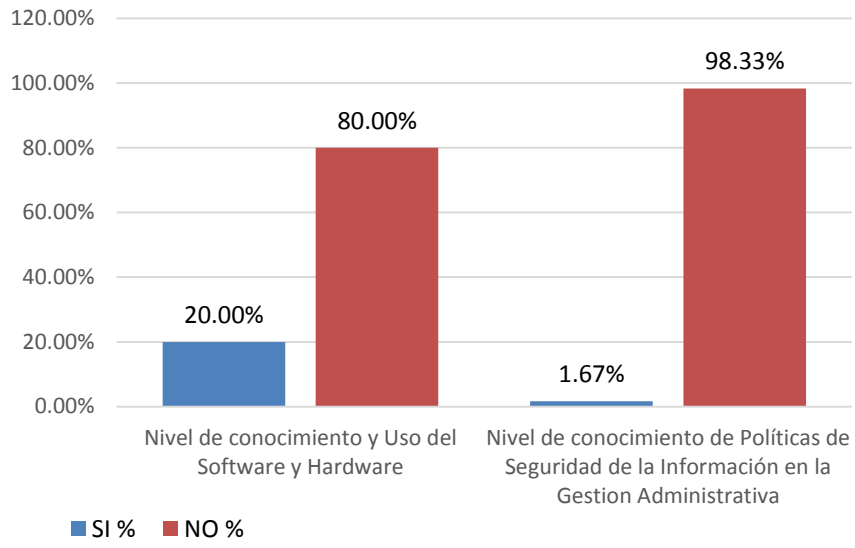
Aplicado por: Flores, C.; 2017.

En la Tabla Nro. 41; se puede observar que: La Dimensión I el mayor porcentaje de los trabajadores encuestados expresan que NO conocen el uso correcto del Hardware y Software, mientras que un menor porcentaje indican que SI.

La Dimensión II el mayor porcentaje de los trabajadores encuestados expresan que NO conocen sobre políticas de seguridad de la información, mientras que un menor porcentaje indican que SI.

Gráfico Nro. 41: Resumen General de Dimensiones

Distribución porcentual de las frecuencias y respuestas relacionadas con las 02 dimensiones definidas para determinar el niveles de conocimiento de los trabajadores; para el diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017.



Fuente: Tabla Nro. 41

5.2. Análisis de resultados

Según los resultados de las encuestas aplicadas a los trabajadores del GRUPO SIAS SAC, y desde un ámbito general se tiene una perspectiva negativa en varios puntos clave como: En la Tabla Nro. 8 que corresponde a la dimensión de nivel de conocimiento y uso de Hardware y Software, se evidencia que 71.67% de los trabajadores encuestados expresaron que NO se registran los accesos de personas a las áreas donde se encuentran los equipos (Servidores); En la Tabla Nro. 23, que corresponde a la dimensión de nivel de conocimiento de políticas de seguridad de la información en la gestión administrativa, el 100% de los trabajadores encuestados expresaron que NO existen políticas de seguridad de la información en el GRUPO SIAS SAC.

Esto lleva a los resultados finales en que para:

Dimensión 1, referente al nivel de conocimiento y uso de Hardware y Software, el 80.00% de los trabajadores encuestados NO realizan un correcto uso del Hardware y Software de la empresa.

Barrantes, C. y Hugo, J. (En el año 2012) en su tesis "Diseño e Implementación de un Sistema de Seguridad de Información en Procesos Tecnológicos" concluye que: Aún después de implementar un buen sistema de gestión de seguridad de información, en el futuro se presentan más activos de información, más amenazas, vulnerabilidades y por lo tanto, mayores riesgos. Este escenario no se puede evitar; es por ello que se concluye, que se debe estar preparado para actuar de manera inmediata ante cualquier nueva vulnerabilidad que se identifique. Este estudio concluye con un resultado similar a la investigación realizada (32).

Dimensión 2, referente al nivel de conocimiento de políticas de seguridad de la información en la gestión administrativa, el 98.33% de los trabajadores encuestados NO tienen conocimiento acerca de las

políticas de se seguridad de la información en las labores administrativas que ellos realizan.

Justino, Z. (En el año 2015), en su tesis titulada "Diseño de un Sistema de Gestión de Seguridad de Información para una Empresa Inmobiliaria Alineado a la Norma ISO/IEC 27001:2013" concluye que: Es necesario establecer una Política de Seguridad de Información que contenga los lineamientos para una eficiente administración de la información con el fin de garantizar la seguridad de los sistemas que satisfaga el requerimiento del negocio y de mantener la integridad de la información, de la infraestructura de procesamiento y minimizar el impacto de vulnerabilidades e incidentes de seguridad. Este resultado concuerda con los resultados obtenidos en el estudio respecto al diseño de un Sistema de Gestión de Seguridad de la Información (33).

Luego de todo lo mencionado se concluye el Diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017. Mejorará el control de la información que se maneja en la empresa, ayudar a establecer políticas y procedimientos en relación a los objetivos de negocio de la organización, y así mantener un nivel de exposición siempre menor.

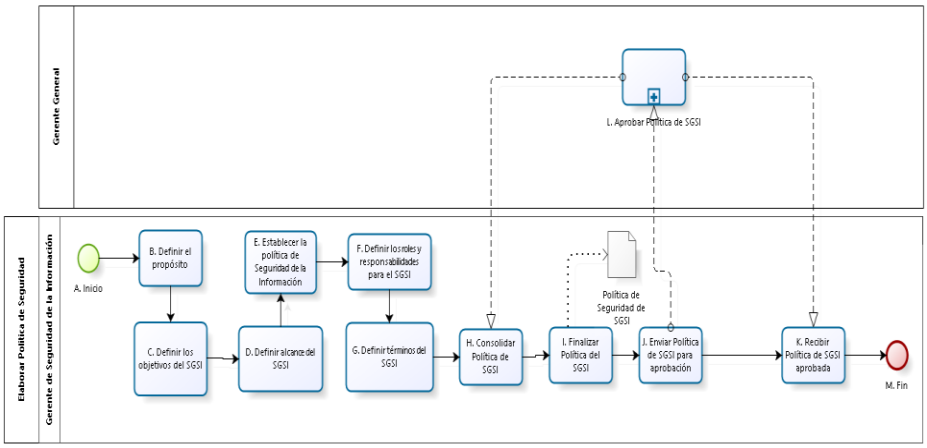
5.3. Propuesta de Mejora

Debido a los resultados obtenidos en la investigación y con el objetivo de mejorar el control y gestión de información mediante la implementación de un modelo de sistema de gestión de la información, a consecuencias de la gestión artesanal de la información que se lleva actualmente en la empresa, se propone los nuevos procesos, teniendo en cuenta lo analizado.

5.3.1. Proceso – Elaborar Política de seguridad de la información

A continuación se presenta el proceso de implementación de la política de seguridad de la información:

Gráfico Nro. 42: Elaborar Política de seguridad de la información



Fuente: Elaboración Propia

A continuación, se presenta la caracterización del proceso de política de seguridad de la Información:

Tabla Nro. 42: Caracterización – Elaborar Política de seguridad de la información

ENTRADA	ACTIVIDAD	SALIDA	DESCRIPCIÓN	RESPONSABLE
	A. Inicio	Necesidad de creación de una política del SGSI	Inicio de la elaboración de la Política de SGSI	Gerente de Seguridad de la Información
Identificar necesidad de creación de una política del SGSI	B. Definir el propósito	Propósito definido	La empresa debe definir el propósito de documentar la política de SGSI	Gerente de Seguridad de la Información
Propósito definido	C. Definir los objetivos del SGSI	Objetivo del SGSI definido	Toda política de SGSI debe contar con objetivos establecidos para poder medirla.	Gerente de Seguridad de la Información
Objetivo del SGSI definido	D. Definir alcance del SGSI	Alcance del SGSI establecido	Esta política de SGSI debe de tener un alcance determinado y acorde a los objetivos de la empresa.	Gerente de Seguridad de la Información
Alcance del SGSI establecido	E. Establecer la política de Seguridad de la Información	Política de la seguridad de la información establecida	Detallar los puntos dentro de la política de Seguridad de Información	Gerente de Seguridad de la Información
Política de la seguridad de la información establecida	F. Definir los roles y responsabilidades para el SGSI	Roles definidos	Definir una relación de roles a manejar dentro del SGSI	Gerente de Seguridad de la Información
Roles definidos	G. Definir términos del SGSI	Términos definidos	Definir todos los términos que se explican dentro de la Política de SGSI	Gerente de Seguridad de la Información
Términos definidos	H. Consolidar Política del SGSI	Política del SGSI consolidada	Agrupar todo el avance realizado para la Política del SGSI	Gerente de Seguridad de la Información
Política del SGSI consolidada	I. Finalizar Política del SGSI	Política del SGSI Finalizada por aprobar	Generar el documento final para entregar a Directorio	Gerente de Seguridad de la Información
Política del SGSI Finalizada por aprobar	J. Enviar Política de SGSI para aprobación	Política del SGSI Finalizada enviada por aprobar	Se envía el documento al Directorio para su aprobación	Gerente de Seguridad de la Información
Política del SGSI Finalizada enviada por aprobar	K. Recibir Política de SGSI para aprobación	Política del SGSI Finalizada enviada por aprobar	Se recibe el documento generado	Gerente de Seguridad de la Información
Política del SGSI Finalizada enviada por aprobar	L. Aprobar Política de SGSI	Política del SGSI aprobada/no aprobada	Se verifica la conformidad con el documento generado.	Gerente General
Política del SGSI aprobada y firmada	O. Fin		Política de SGSI Finalizada y documentada	Gerente de Seguridad de la Información

Fuente: Elaboración Propia

5.3.2. Proceso – Definir Roles y responsabilidades

Estableciendo Los Roles Y Responsabilidades

Gerencia General o Directorio

La responsabilidad de la gerencia general o del directorio es la siguiente:

- Aprobar el proyecto y la política de seguridad de la información.
- Compromiso con la política y el programa de seguridad de la información.

Gerente/Oficial de la seguridad de la información

La persona encargada de la gerencia de la seguridad de la información es responsable de realizar las siguientes actividades:

- Comprometer a la alta gerencia con el programa de seguridad de la información.
- Participar en la elaboración de la política de seguridad de la información, objetivos, alcance y estrategia.
- Revisar los reportes del estado del SGSI y aprobar las decisiones correspondientes para su continua mejora.
- Revisar y aprobar la documentación realizada por el Departamento de Seguridad de la Información.

Este rol tiene la función de involucrar y comprometer a las demás gerencias y al directorio con la seguridad de la información dentro de la organización.

Analista de seguridad de la información

La persona encargada de administrar la seguridad de la información debe realizar las siguientes actividades:

- Desarrollar la política de seguridad de la información, objetivos, alcance y estrategia.

- Definir el alcance del SGSI en la organización.
- Elaborar el procedimiento para la evaluación de riesgos.
- Participar en la primera evaluación de riesgo de la organización.
- Elaborar el plan de tratamiento de los riesgos identificados.
- Seleccionar los objetivos de control y controles correspondientes para satisfacer los objetivos del negocio.
- Monitorear el registro de los incidentes de seguridad de la organización, incluyendo la identificación de la causa raíz y su respectiva acción correctiva a realizar.
- Reportar a la gerencia y al directorio el estado y el progreso de la implementación del SGSI, así como los incidentes, problemas, acciones preventivas y correctivas, entre otros.
- Comunicar la política de seguridad de la información a las diferentes áreas de la organización.
- Realizar auditorías para corroborar que el estado del SGSI.
- Hacer cumplir la política de seguridad con respecto a los proveedores externos.

Para las organizaciones pequeñas, las decisiones y preguntas deben ser dirigidas hacia este rol.

Administrador de las Tecnologías de la información

Las actividades correspondientes al rol de "administrador de TI" dentro del SGSI son las siguientes:

- Asegurar la concientización del personal de TI sobre la seguridad de la información que se almacena en los sistemas y dispositivos de la organización.
- Proveer los recursos técnicos necesarios al departamento de Seguridad de la Información.
- Reportar las vulnerabilidades técnicas e incidentes relacionados a las Tecnologías de la Información.

- Participar en la identificación y evaluación de riesgos de TI.
- Participar en la planificación de la continuidad de negocio.
- Asegurar que los antivirus se aplican adecuadamente a los computadores de la organización.
- Asegurar que las políticas de usuarios y contraseñas se cumplen adecuadamente.

Administrador de Operaciones

El Administrador de Operaciones es el encargado de realizar las siguientes actividades:

- Identificar las amenazas de los sistemas de bases de datos y redes de la organización.
- Evaluar los riesgos que implican las bases de datos y las redes de comunicación de la organización.
- Implementar las medidas de seguridad relacionadas con las contraseñas, firewalls y controles de acceso físicos a los ambientes más críticos del departamento de sistemas.
- Configurar los sistemas y la red de la organización de acuerdo a la política de seguridad establecida.
- Establecer e implementar indicadores y registros con respecto a la seguridad de la información en las bases de datos y las redes de comunicación.
- Implementar un procedimiento de control de cambios.
- Elaborar, mantener y probar los planes de contingencia para asegurar la disponibilidad de la información y la continuidad del negocio.

Usuarios del negocio

Las responsabilidades de los usuarios del negocio son las siguientes:

- Cumplir la política y procedimientos de la seguridad de la información.
- Cumplir con los controles de seguridad, tales como la política de escritorio limpio, contraseñas, entre otros.
- Realizar respaldos de información importante para el usuario.
- Reportar incidentes de seguridad.

Implementando Los Roles Y Responsabilidades

Estructura Organizativa

Para definir los roles y responsabilidades, es muy importante revisar los recursos humanos de la organización. De esta manera, es posible obtener una visión clara de los recursos disponibles en la empresa y aquellos que hacen falta para poder asignar los roles y responsabilidades descritos en el acápite "Roles y Responsabilidades".

Departamento de Seguridad de la Información

Según las recomendaciones de clase mundial o buenas prácticas es necesario crear un departamento de seguridad de la información separado del departamento de tecnología o sistemas de la organización. Esta recomendación permite tener una mayor objetividad en las labores de seguridad de la información, tales como la elaboración de reportes, presentación de resultados, entre otros.

Sin embargo, en organizaciones pequeñas donde no se pueda contar con los recursos humanos necesarios para asignar un rol por persona, es posible asignarle más de una responsabilidad a un solo individuo. Asimismo, si no es posible crear un departamento independiente de seguridad de la información, se pueden asignar los roles descritos en "Roles

y responsabilidades" al personal del departamento de sistemas.

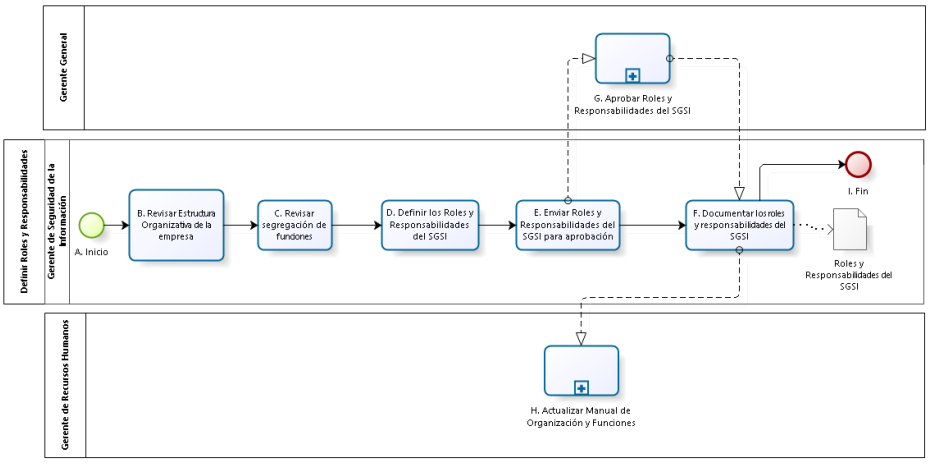
Segregación de funciones

La segregación de funciones es un método para reducir el riesgo del uso indebido de los privilegios y funciones dentro de las organizaciones. Este método evita la posibilidad de que una sola persona pueda ser responsable de diversas funciones críticas que puedan afectar el funcionamiento del negocio, en este caso, la seguridad de la información.

La segregación de funciones es un significado importante cuando se refiere a la prevención y descubrimiento de actos fraudulentos o maliciosos.

Este concepto debe de ser evaluado al momento de asignar los roles y responsabilidades, descritos en este documento, en la organización. Por lo general, mientras menos personal disponible haya en una organización, es más complicado realizar una tarea de segregación de funciones.

Gráfico Nro. 43: Definir Roles y Responsabilidades



Fuente: Elaboración Propia

A continuación, se presenta la caracterización del proceso de política de seguridad de la información:

Tabla Nro. 43: Caracterización – Definir Roles y Responsabilidades

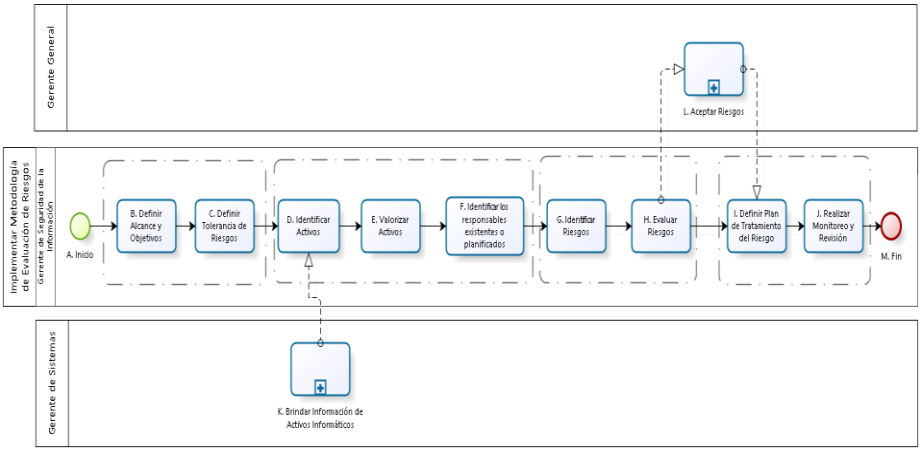
ENTRADA	ACTIVIDAD	SALIDA	DESCRIPCIÓN	RESPONSABLE
	A. Inicio	Política del SGSI Finalizada	Inicio del proceso	Gerente de Seguridad de Información
Política del SGSI Finalizada	B. Revisar Estructura Organizativa de la empresa	Estructura Organizativa revisada (Organigrama)	Se procede a revisar cómo está organizada la empresa y la estructura que tiene	Gerente de Seguridad de Información
Estructura Organizativa revisada (Organigrama)	C. Revisar segregación de funciones	Funciones del SGSI segregadas y documentadas	Se procede a revisar la segregación de funciones; es decir, verificar que una persona pueda tener uno o más roles sin que esto afecte el negocio.	Gerente de Seguridad de Información
Funciones del SGSI segregadas y documentadas	D. Definir los Roles y Responsabilidades del SGSI	Roles y Responsabilidades definidos	Se definen los roles y responsabilidades para el SGSI.	Gerente de Seguridad de Información
Roles y Responsabilidades definidos	E. Enviar Roles y Responsabilidades del SGSI para aprobación	Roles y Responsabilidades definidos por aprobar	Se envían los Roles y Responsabilidad definidos para la aprobación del Gerente General.	Gerente de Seguridad de Información
Roles y Responsabilidades definidos y aprobados	F. Documentar los roles y responsabilidades del SGSI	Roles y responsabilidades del SGSI documentados	Se documentan los Roles y Responsabilidades del SGSI.	Gerente de Seguridad de la Información
Roles y Responsabilidades definidos por aprobar	G. Aprobar Roles y Responsabilidades del SGSI	Roles y Responsabilidades definidos y aprobados	Se aprueban o desaprueban los Roles y Responsabilidades del SGSI por el Gerente General.	Gerente General
Roles y responsabilidades del SGSI documentados	H. Actualizar Manual de Organización y Funciones	Manual de Organización y Funciones	El departamento de RRHH debe actualizar el manual de organización y funciones.	Gerente de Recursos Humanos
Roles y responsabilidades del SGSI documentados	I. Fin			Gerente de Seguridad de Información

Fuente: Elaboración Propia

5.3.3. Proceso – Implementar Metodología de evaluación de riesgos

A continuación se presenta el proceso de implementación de la política de seguridad de la información:

Gráfico Nro. 44: Proceso Implementar Metodología de Evaluación de Riesgos



Fuente: Elaboración Propia

A continuación se presenta la caracterización del proceso de Implementar la Metodología de Evaluación de Riesgos:

Tabla Nro. 44: Caracterización – Implementar Metodología de Evaluación de Riesgos

ENTRADA	ACTIVIDAD	SALIDA	DESCRIPCIÓN	RESPONSABLE
	A. Inicio	Necesidad de definir Alcance	Inicio del proceso	Gerente de Seguridad de la Información
Necesidad de definir alcance	B. Definir Alcance y Objetivos	Alcance y objetivos definidos	Es importante definir el alcance y los objetivos de la evaluación de riesgos para saber los límites que plantea la empresa	Gerente de Seguridad de la Información
Alcance y objetivos definidos	C. Definir Tolerancia de Riesgos	Tolerancia de riesgos definida	En esta actividad, la organización debe definir los parámetros para aceptar o rechazar al riesgo	Gerente de Seguridad de la Información
Tolerancia de riesgos definida	D. Identificar Activos	Inventario de activos completo	Se identifican los activos registrándolos en el Inventario de Activos	Gerente de Seguridad de la Información

Inventario de activos completo	E. Valorizar Activos	Valorización de activos completa	Se asigna un valor a cada uno de los activos de la empresa, permitiendo que exista una priorización.	Gerente de Seguridad de la Información
Valorización de activos completa	F. Identificar los responsables existentes o planificados	Identificación de los propietarios de los activos finalizada	Se identifica al propietario del activo para que pueda responder ante cualquier consulta que se tenga sobre el mismo y pueda velar por la mitigación de riesgos correspondientes al activo.	Gerente de Seguridad de la Información
Identificación de los propietarios de los activos finalizada	G. Identificar Riesgos	Riesgos Identificados	Se identifica cada uno de los posibles riesgos existentes en la empresa y a partir de ello se elabora un listado.	Gerente de Seguridad de la Información
Riesgos Identificados	H. Evaluar los Riesgos	Riesgos evaluados por aceptar	Se analizan los riesgos y se define, uno por uno, los criterios de aceptación del riesgo.	Gerente de Seguridad de la Información
Riesgo evaluado y no aceptado	I. Definir Plan de Tratamiento del Riesgo	Plan de Tratamiento del Riesgo definido	En caso no se acepte el riesgo, se debe identificar una manera de mitigarlo y ésta es elaborando un plan de tratamiento del riesgo	Gerente de Seguridad de la Información
Plan de Tratamiento del Riesgo definido	J. Realizar Monitoreo y Revisión	Monitoreo y revisión del riesgo realizado	Monitorear las actividades definidas en el Plan de Tratamiento del Riesgo para verificar la mitigación de los mismos.	Gerente de Seguridad de la Información
Necesidad de información de activos informáticos	K. Brindar Información de Activos Informáticos	Información de Activos Informáticos brindada	El área de sistemas entrega la información de los activos informáticos utilizados en la compañía.	Gerente de Sistemas
Riesgos evaluados por aceptar	L. Aceptar Riesgos	Riesgo evaluado y no aceptado	Se decide la aceptación del riesgo por parte de la Gerencia General.	Gerente General
Monitoreo y revisión del riesgo realizado Consolidados	M. Fin		Fin del Proceso	Gerente de Seguridad de la Información

Fuente: Elaboración Propia

5.3.4. Metodología de evaluación de riesgos

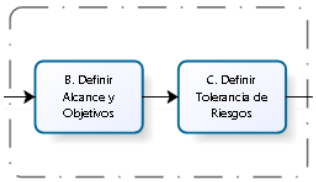
Para lograr obtener resultados exactos sobre una evaluación de riesgos, se debe seguir una metodología, la cual consiste, de manera resumida, en establecer el contexto, identificar los activos y los riesgos, para luego evaluar la factibilidad del riesgo en la organización.

Esta metodología busca ser sencilla sin dejar de lado la objetividad de lo establecido en la ISO 27001, esto permitirá que la empresa tenga la posibilidad de certificarse sin la necesidad de elaborar mucha documentación.

Esta metodología cuenta con cuatro fases que permitirán que la organización logre una correcta evaluación de cada uno de los riesgos a los que se encuentra expuesta.

1. Fase 1: Establecer el contexto

Gráfico Nro. 45: Fase 1 - Establecer el contexto



Fuente: Elaboración Propia

En esta primera fase de la metodología, la organización debe tomar consciencia de la necesidad de identificar las debilidades que existen tanto de manera física o lógica. Esto va a permitir que se desarrolle con correcta normalidad el proceso de evaluación de las amenazas y vulnerabilidades de cada uno de los activos.

En primer lugar, la organización debe definir un alcance y objetivos que permitan establecer de manera sencilla y

directa lo que se busca lograr con esta evaluación de riesgos. Estos puntos debe ser documentados, tienen que ir alineados a los objetivos de negocio y debe ser comunicados con todo el personal.

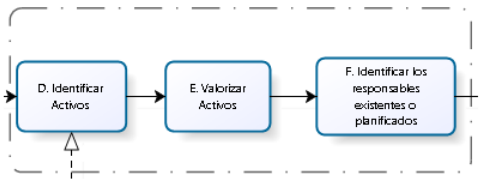
La definición del alcance necesita tomar en cuenta las dependencias que tienen la evaluación de riesgos con otras partes de la organización, otras organizaciones, proveedores externos, o cualquier entidad fuera del programa de seguridad de la información.

Los objetivos deben ser claros, medibles y con un periodo determinado para cumplirse. Esto permite que la organización evite reestructurar los mismos y se ocupe, únicamente, del desarrollo de la evaluación.

Por otro lado, también se debe definir la tolerancia del riesgo, la cual es identificada y aprobada por la administración. Una tolerancia del riesgo permite definir el criterio para la aceptación del riesgo. En este caso, la organización tolera los riesgos que no afectan al funcionamiento del negocio; sin embargo, los mitiga para evitar que sean mayores y puedan afectar los ingresos económicos de la misma.

2. Fase 2: Identificación y valorización de los activos

Gráfico Nro. 46: Fase 2 - Identificación de activos



Fuente: Elaboración Propia

Como parte de realizar una evaluación de riesgos, es importante identificar todos los activos que son importantes para el negocio y asignarles un valor relativo para cada uno.

Este proceso permite facilitar la decisión sobre que activos deben ser protegidos. Si existen muchos activos para gestionar, es recomendable agruparlos por similitud en categorías que permitan que el proceso de evaluación se realice de manera eficiente. Para ello, se propone una plantilla para realizar el inventario de activos, la cual contiene una manera sencilla de registrar cada activo.

Tabla Nro. 45: Inventario de activos

	Activo						Información		Seguridad de información			
Nr.	ID Activo	Nombre del activo	Descripción del activo	Categoría de activo	Ubicación	Dueño del activo	Información almacenada	Tipo de Acceso	Confidencialidad	Disponibilidad	Integridad	Nivel de sensibilidad
1												
2												
3												
4												
5												

Fuente: Elaboración Propia

Cada registro de activos debe contener el detalle de todas estas características por cada activo registrado. Así también de la documentación específica correspondiente al activo según su categoría.

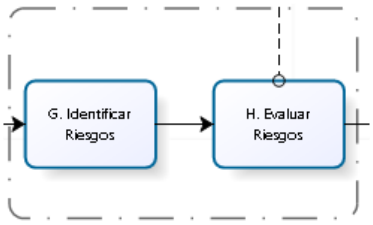
La contabilidad para los activos permite asegurar que la información adecuada se mantenga. Cada activo identificado deberá contar con un encargado de monitorear y de garantizar la seguridad apropiada a través de controles establecidos por el mismo.

Luego de haber identificado correctamente a cada uno de los activos se procede a valorizar los según la importancia en el negocio, siendo el factor más importante el ratio de beneficio que le da al negocio para lograr mayores ingresos.

En este caso el mismo formato de Inventario de Activos cuenta con una sección que indica la valorización de activos.

3. Fase 3: Evaluación de Riesgos

Gráfico Nro. 47: Fase 3 - Amenazas y Vulnerabilidades de activos



Fuente: Elaboración Propia

Luego de haber realizado la identificación de los activos, la organización debe de identificar los riesgos asociados a cada uno de ellos.

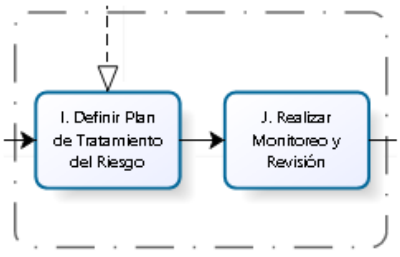
Para ello existen categorías de Amenazas que permitirán identificar correctamente cada una de las mismas y asociarlas con la vulnerabilidad que puede generar en la empresa.

Es importante recalcar que estas vulnerabilidades tienen un grado de impacto potencial que generan al negocio si es que llegan a suceder:

- Alto: Es cuando la vulnerabilidad es propensa a suceder en cualquier momento y no existen garantías para evitar ello. Existen controles que se han aplicado para intentar evitarlo, pero éstos no son los correctos.
- Medio: Es cuando la vulnerabilidad cuenta con controles que la soportan pero no son los suficientes para poder lograrlo.
- Bajo: Es poco probable que la vulnerabilidad suceda debido.

4. Fase 4: Tratamiento del Riesgo

Gráfico Nro. 48: Fase 4 - Tratamiento del riesgo



Fuente: Elaboración Propia

Luego de completar la evaluación de riesgos, se debe determinar la decisión tomar sobre cómo tratar el riesgo. Existen varias posibilidades sobre cómo llevar el tratamiento del riesgo:

- Evitar el riesgo evitando la actividad para que no se cree el riesgo.
- Aplicar controles apropiados para el activo logrando reducir el riesgo.
- Transferir el riesgo o su impacto hacia terceros.
- Aceptar el riesgo.

Siempre existen riesgos residuales, los cuales deben ser evaluados y categorizados como aceptables o no-aceptables. Debe haber un comité que decida su aceptación y qué controles deben ser implementados en el futuro.

5.3.5. Guía de Inventario de Activos

Realizar un inventario/registro de los activos de la organización es uno de los primeros trabajos que se debe de realizar al implementar un SGSI. Posteriormente, en base al inventario de activos se realiza la evaluación y clasificación de riesgos.

Es importante asegurar que el inventario de activos debe de estar "razonablemente" completo. Este documento brinda una estructura para comenzar a trabajar, un punto de partida para pensar acerca de todos los activos que se posee en una organización, de esta manera, es posible asegurar los activos más críticos y poner una menor importancia a aquellos que no representan un gran riesgo a la organización.

Categorías de activos

Como parte del proceso de evaluación de riesgos en una organización, ésta debe identificar todos los activos importantes que posee. Estos activos deben de clasificarse y

ordenarse en categoría para permitir una mejor organización e identificación de los mismos.

A continuación, se propone una clasificación y ejemplos de cada una.

Tabla Nro. 46: Categoría de activos

CATEGORÍA	EJEMPLOS DE ACTIVO		
Activos de información	Libros financieros	Inventarios	Información de ventas
	Información archivada	Servicios de información	Información de marketing
	Procedimientos de respaldo	Procedimientos y documentos de operación	Acuerdos de nivel de servicio
	Planes de continuidad de negocio	Registros organizacionales	Presentaciones
	Contratos	Contratos de terceros	Documentos de software
	Información corporativa	Registros de clientes	Documentación de sistemas
	Detalles de cliente	Detalles de pago a empleados	Material de entrenamiento
	Bases de datos	Fotografías	Manuales de usuario
	Planes de recuperación de desastres (DRP)	Información de productos	Información del personal
	Información financiera	Información de investigación	Otros
	Procedimientos de tratamiento de incidentes		
Activos de software	Aplicaciones desarrolladas	Software de comunicación	Aplicaciones especializadas
	Aplicaciones estándares (Word, Excel, etc.)	Herramientas de encriptación	Antivirus
	Herramientas de desarrollo	Licencias de software	Sistema operativo
Activos físicos (no digitales)	Fax	Cables	Edificios
	Celulares	CD's	Aire acondicionado
	Módems	USB's	UPS
	Redes	Computadoras	Fotocopiadoras
	Routers	Laptops	Impresoras
	Cintas	Periféricos	Generadores
	Teléfonos	Tarjetas magnéticas	Switches
	Libros	Tabletas	
Activos de personal	Administradores	Practicantes	Personal de seguridad
	Personal de limpieza	Gerentes	Personal temporal
	Personal de comunicaciones	Personal de redes	Personal informático
		Desarrolladores	Terceros
Activos intangibles	Nombres de la marca	Copyright	Patentes Reputación

Fuente: Elaboración Propia

Registrar activos

Es necesario registrar todos los activos de la organización en una matriz centralizada para poder identificarlos y tener un control sobre éstos.

Tabla Nro. 47: Inventario de activos

	Activo						Información		Seguridad de información			
Nr.	ID Activo	Nombre del activo	Descripción del activo	Categoría de activo	Ubicación	Dueño del activo	Información almacenada	Tipo de Acceso	Confidencialidad	Disponibilidad	Integridad	Nivel de sensibilidad
1												
2												
3												
4												
5												

Fuente: Elaboración Propia

En la matriz presentada, es necesario completar los siguientes campos para cada registro (activo de información):

- **ID Activo:** Identificador único del activo.
- **Nombre del activo:** Denominación de un activo.
- **Descripción del activo:** Explicar, de manera detallada y ordenada, las características del activo.
- **Categoría del activo:** Clasificar al activo según la categoría a la que pertenece (ver “Categorías de activos”).
- **Ubicación:** Indicar la localización geográfica en la que se encuentra el activo de información.
- **Dueño del activo:** Indicar quién es el responsable (Nombre del personal) de responder frente a cualquier evento con relación a determinado activo.
- **Información almacenada:** Indicar la información que se encuentra en el activo de información registrado.
- **Tipo de acceso:** Indicar el nivel de acceso requerido por el activo, estos pueden ser:

- Público: Puede ser accesible por cualquier persona, ya sea interna o externa a la organización.
- Interno: Solamente puede ser accesible a personal interno de la organización.
- Restringido: Información accesible solamente a personal establecido por las políticas de la organización.
- Confidencial: Información disponible solamente bajo autorización o a personal con cargos altos en la organización.

- **Seguridad de la información:** Indicar el nivel de sensibilidad de acuerdo a los siguientes criterios de los principios de la información:

Tabla Nro. 48: Criterios de sensibilidad de la información

Componente	Bajo - 1	Medio - 2	Alto - 3
Confidencialidad	Información disponible al público en general.	Información del procesos que no requiere de medidas complejas de seguridad.	Información que sólo puede ser accedida con autorización del dueño.
Integridad	Información que de ser modificada no impacta al proceso del negocio.	Información que de ser modificada afectar al resultado del procesos de negocio.	Información que sólo puede ser modificada con autorización del dueño.
Disponibilidad	La información no es vital para la toma de decisiones.	Información requerida para la toma de decisiones dentro de las primeras 24 horas.	Información requerida para la toma de decisiones dentro de las primeras 4 horas.

Guía de la evaluación de riesgos

El siguiente paso luego de haber identificado los activos de información de la organización, es realizar un análisis de los riesgos a los que la organización se encuentra expuesta, con el objetivo de tener claras las amenazas y vulnerabilidades de seguridad de la información.

Para realizar el análisis de riesgos, basada en los controles de seguridad de la información citados por el anexo A de la norma ISO/IEC 27001.

Tabla Nro. 49: Plantilla de evaluación de riesgos

Evaluación de riesgos SGSI						
Riesgo		Descripción del control	Referencia ISO 27001	Información Requerida	Hallazgo	Conclusión
A5. Políticas de seguridad de la información						
La inexistencia de una política de seguridad de la información no permite que la alta dirección se involucre y comprometa con las tareas de seguridad de la información en la organización	1	La política de seguridad de la información debe de ser definida y aprobada por la gerencia, publicada y comunicada a todos los colaboradores y terceros relevantes para la organización	5.1.1	- Políticas de SGSI - Evidencia de publicación de la política - Evidencia de monitoreo y revisión de la política		
	2	La política de seguridad de la información debe ser revisada en intervalos planificados o si se producen cambios significativos para asegurar su conveniencia, adecuación y eficacia.	5.1.2			
	3	Se deben de definir y/o actualizar los contactos apropiados con las autoridades relevantes en la gestión de la seguridad de la información.	6.1.2			
A6. Organización de la seguridad de la información						
La falta de roles y responsabilidades no permite una correcta gestión de un marco interno de seguridad de la información	1	Todas las responsabilidades de la seguridad de la información deben de ser definidas y asignadas.	6.1.1	- Organigrama de la organización - Manual de organización y funciones - Roles y Responsabilidades del SGSI		
	2	Las funciones en conflicto y las áreas responsables deben de ser separadas para reducir las oportunidades de modificación o mal uso, no autorizadas o sin intención, de los activos de la organización.	6.1.5			
La inexistencia de políticas para el uso de dispositivos móviles o teletrabajo no permite asegurar la seguridad de la información utilizada por estos medios	1	gestionar los riesgos introducidos por el uso de dispositivos móviles	6.2.1	- Políticas para el uso de dispositivos móviles - Política de teletrabajo		
	2	Se definirá y adoptará una política y medidas de seguridad para proteger la información a la cual se accede, procesa o almacena en los lugares de teletrabajo.	6.2.2			

- **Riesgo:** Descripción del riesgo de seguridad de la información que puede existir en una organización.
- **Descripción del control:** Detalle de los controles a implementar, según la ISO 27001, para poder mitigar el riesgo de seguridad de la información.
- **Referencia ISO 27001:** Sección de la norma en la que se describe o menciona el control.
- **Información requerida:** Información que se solicita o verifica en una organización para poder definir la existencia de los riesgos y los controles de seguridad de la información.
- **Hallazgo:** Descripción de la situación de la organización con respecto al riesgo evaluado y a los documentos solicitados.
- **Conclusión:** De acuerdo al hallazgo, se define la existencia del riesgo de seguridad de la información en la organización, las posibilidades son las siguientes:

- Efectivo: Si el hallazgo satisface todos los controles definidos o se evidencia que el riesgo se encuentra debidamente controlado.
- Con oportunidad de mejora: Si el hallazgo satisface de manera parcial los controles definidos o no se evidencia que el riesgo se encuentre controlado.
- Inefectivo: Si los controles no forman parte de la cultura organizacional de la empresa y no se reconoce el riesgo de seguridad de la información.
- No aplica: No existe el riesgo debido a que el proceso en el que surge la amenaza no se encuentra implementado en la organización.

5.3.6. Estableciendo el plan de tratamiento de riesgos

El plan debe mostrar cómo cada riesgo identificado en el proceso de evaluación de riesgos será tratado o mitigado, las garantías o salvaguardias que ya se han implementado, las garantías adicionales a considerar y los tiempos designados para la implementación de las mismas.

Una vez que el plan de tratamiento de riesgos se ha culminado, los recursos pueden ser asignados a sus correspondientes actividades para comenzar su implementación. El plan de tratamiento de riesgos debe de contener las siguientes consideraciones:

Tabla Nro. 50: Plan de tratamiento de riesgos

Plan de tratamiento de riesgos				
Riesgo	Nivel de madurez AS-IS	Nivel de madurez TO-BE	Plan de acción	Responsable

- **Riesgo:** Descripción del riesgo de seguridad de la información identificado según la evaluación de riesgos.
- **Nivel de madurez AS-IS:** Se debe de indicar el nivel de madurez en el que se encontró el riesgo de seguridad de la información. El nivel de madurez se define según la siguiente tabla:

Tabla Nro. 51: Niveles de madurez

Nivel de Madurez	Descripción
0 - Inexistente	No se reconoce la necesidad del control interno. El control no es parte de la cultura o misión organizacional. Existe un alto riesgo de deficiencias e incidentes de control.
1 - Inicial / ad hoc	Se reconoce algo de la necesidad del control interno. El enfoque hacia los requerimientos de riesgo y control es ad hoc y desorganizado, sin comunicación o supervisión. No se identifican las eficiencias. Los empleados no están concientes de sus responsabilidades.
2 - Repetible pero intuitivo	Existen controles pero no están documentados. Su operación depende del conocimiento y motivación de los individuos. La efectividad no se evalúa de forma adecuada. Existen muchas debilidades de control y no se resuelven de forma apropiada; el impacto puede ser severo. Las medidas de la gerencia para resolver problemas de control no son consistentes ni tienen prioridades. Los empleados ueden no estar concientes de sus responsabilidades.
3 - Proceso definido	Existen controles y están documentados de forma adecuada. Se evalúa la efectividad operativa de forma periódica y existe un número promedio de problemas. Sin embargo, el proceso de evaluación no está documentado. Aunque la gerencia puede manejar la mayoría de los problemas de control de forma predecible, algunas debilidades de control persisten y los impactos pueden ser severos. Los empleados están concientes de sus responsabilidades de control.
4 - Administrado y medible	Existe un ambiente efectivo de control interno y de administración de riesgos. La evaluación formal y documentada de los controles ocurre de forma periódica. Muchos controles están automatizados y se realizan de forma periódica. Es probable que la gerencia detecte la mayoría de los problemas de control, aunque no todos los problemas se identifican de forma rutinaria. Hay un seguimiento consistente para manejar las debilidades de control identificadas. Se aplica un uso de la tecnología táctico y limitado a los controles automatizados.
5 - Optimizado	Existe un ambiente efectivo de control interno y de administración de riesgos. La evaluación formal y documentada de los controles ocurre de forma periódica. Muchos controles están automatizados y se realizan de forma periódica. Es probable que la gerencia detecte la mayoría de los problemas de control, aunque no todos los problemas se identifican de forma rutinaria. Hay un seguimiento consistente para manejar las debilidades de control identificadas. Se aplica un uso de la tecnología táctico y limitado a los controles automatizados.

- **Nivel de madurez TO-BE:** Se debe de indicar el nivel de madurez al que se desea llegar luego de aplicar el tratamiento de riesgos o plan de acción.

- **Plan de acción:** Se debe de indicar las decisiones y acciones que se van a realizar para mitigar el riesgo identificado.

Responsable: Persona responsable del tratamiento del riesgo e implementación de las actividades elegidas.

5.3.7. Formulario Para Autodiagnóstico

1	**POLÍTICAS DE SEGURIDAD**	**SI**	**NO**
	Existen documento(s) de políticas de seguridad de SI		
	Existe normativa relativa a la seguridad de los SI		
	Existen procedimientos relativos a la seguridad de SI		
	Existe un responsable de las políticas, normas y procedimientos		
	Existen mecanismos para la comunicación a los usuarios de las normas		
	Existen controles regulares para verificar la efectividad de las políticas		
2	**ORGANIZACIÓN DE LA SEGURIDAD**	**SI**	**NO**
	Existen roles y responsabilidades definidos para las personas implicadas en la seguridad		
	Existe un responsable encargado de evaluar la adquisición y cambios de SI		
	La Dirección y las áreas de la Organización participa en temas de seguridad		
	Existen condiciones contractuales de seguridad con terceros y outsourcing		
	Existen criterios de seguridad en el manejo de terceras partes		
	Existen programas de formación en seguridad para los empleados, clientes y terceros		
	Existe un acuerdo de confidencialidad de la información que se accesa.		
	Se revisa la organización de la seguridad periódicamente por una empresa externa		
3	**ADMINISTRACIÓN DE ACTIVOS**	**SI**	**NO**
	Existen un inventario de activos actualizado		
	El Inventario contiene activos de datos, software, equipos y servicios		
	Se dispone de una clasificación de la información según la criticidad de la misma		
	Existe un responsable de los activos		
	Existen procedimientos para clasificar la información		
	Existen procedimientos de etiquetado de la información		
4	**SEGURIDAD DE LOS RRHH**	**SI**	**NO**
	Se tienen definidas responsabilidades y roles de seguridad		
	Se tiene en cuenta la seguridad en la selección y baja del personal		
	Se plasman las condiciones de confidencialidad y responsabilidades en los contratos		
	Se imparte la formación adecuada de seguridad y tratamiento de activos		

	Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad		
	Se recogen los datos de los incidentes de forma detallada		
	Informan los usuarios de las vulnerabilidades observadas o sospechadas		
	Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades		
	Existe un proceso disciplinario de la seguridad de la información		
5	**SEGURIDAD FÍSICA Y DEL AMBIENTE**	**SI**	**NO**
	Existe perímetro de seguridad física (una pared, puerta con llave).		
	Existen controles de entrada para protegerse frente al acceso de personal no autorizado		
	Un área segura ha de estar cerrada, aislada y protegida de eventos naturales		
	En las áreas seguras existen controles adicionales al personal propio y ajeno		
	Las áreas de carga y expedición están aisladas de las áreas de SI		
	La ubicación de los equipos está de tal manera para minimizar accesos innecesarios.		
	Existen protecciones frente a fallos en la alimentación eléctrica		
	Existe seguridad en el cableado frente a daños e intercepciones		
	Se asegura la disponibilidad e integridad de todos los equipos		
	Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente		
	Se incluye la seguridad en equipos móviles		
6	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**	**SI**	**NO**
	Todos los procedimientos operativos identificados en la política de seguridad han de estar documentados		
	Están establecidas responsabilidades para controlar los cambios en equipos		
	Están establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad		
	Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas		
	Existe una separación de los entornos de desarrollo y producción		
	Existen contratistas externos para la gestión de los Sistemas de Información		
	Existe un Plan de Capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento		
	Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones		
	Controles contra software maligno		
	Realizar copias de backup de la información esencial para el negocio		
	Existen logs para las actividades realizadas por los operadores y administradores		
	Existen logs de los fallos detectados		
	Existen rastro de auditoría		
	Existe algún control en las redes		

	Hay establecidos controles para realizar la gestión de los medios informáticos.(cintas, discos, removibles, informes impresos)		
	Eliminación de los medios informáticos. Pueden disponer de información sensible		
	Existe seguridad de la documentación de los Sistemas		
	Existen acuerdos para intercambio de información y software		
	Existen medidas de seguridad de los medios en el tránsito		
	Existen medidas de seguridad en el comercio electrónico.		
	Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada		
	Existen medidas de seguridad en las transacciones en línea		
	Se monitorean las actividades relacionadas a la seguridad		
	CONTROL DE ACCESOS	**SI**	**NO**
7	Existe una política de control de accesos		
	Existe un procedimiento formal de registro y baja de accesos		
	Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario		
	Existe una gestión de los password de usuarios		
	Existe una revisión de los derechos de acceso de los usuarios		
	Existe el uso del password		
	Se protege el acceso de los equipos desatendidos		
	Existen políticas de limpieza en el puesto de trabajo		
	Existe una política de uso de los servicios de red		
	Se asegura la ruta (path) desde el terminal al servicio		
	Existe una autenticación de usuarios en conexiones externas		
	Existe una autenticación de los nodos		
	Existe un control de la conexión de redes		
	Existe un control del routing de las redes		
	Existe una identificación única de usuario y una automática de terminales		
	Existen procedimientos de log-on al terminal		
	Se ha incorporado medidas de seguridad a la computación móvil		
	Está controlado el teletrabajo por la organización		
	DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	**SI**	**NO**
8	Se asegura que la seguridad está implantada en los Sistemas de Información		
	Existe seguridad en las aplicaciones		
	Existen controles criptográficos.		
	Existe seguridad en los ficheros de los sistemas		
	Existe seguridad en los procesos de desarrollo, testing y soporte		
	Existen controles de seguridad para los resultados de los sistemas		
	Existe la gestión de los cambios en los SO.		
	Se controlan las vulnerabilidades de los equipos		
	ADMINISTRACIÓN DE INCIDENTES	**SI**	**NO**
9	Se comunican los eventos de seguridad		
	Se comunican los debilidades de seguridad		

	Existe definidas las responsabilidades antes un incidente.		
	Existe un procedimiento formal de respuesta		
	Existe la gestión de incidentes		
10	**GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**	**SI**	**NO**
	Existen procesos para la gestión de la continuidad.		
	Existe un plan de continuidad del negocio y análisis de impacto		
	Existe un diseño, redacción e implantación de planes de continuidad		
	Existe un marco de planificación para la continuidad del negocio		
	Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio.		
11	**CUMPLIMIENTO CON REQUERIMIENTOS LEGALES Y CONTRACTUALES**	**SI**	**NO**
	Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas		
	Existe el resguardo de la propiedad intelectual		
	Existe el resguardo de los registros de la organización		
	Existe una revisión de la política de seguridad y de la conformidad técnica		
	Existen consideraciones sobre las auditorías de los sistemas		

5.3.8. Plantilla – Política y Objetivos de Seguridad de la Información

POLÍTICA Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

<Nombre de la empresa>

Versión

<x.y>

CONTROL DE LA DOCUMENTACIÓN

Este documento cuenta con una versión electrónica, la cual está reconocida como la única versión válida para su uso.

Ubicación del Documento	<Directorio donde se encuentre el documento>
Contacto	<Información sobre la persona a contactar que conoce de la estructura del documento – Esta persona no es el dueño de la política>
Frecuencia de revisión	Este documento deberá ser revisado cada XX <meses/años>
Coordinador del documento	<Información para contactar a la persona responsable del documento>
Sensibilidad del documento	<Nivel de sensibilidad del documento: Alta/Media/Baja>

HISTORIAL DE APROBACIONES

Aprobador	Puesto	Fecha de aprobación
<Nombre de la persona o departamento que aprueba el documento>	<Nombre del rol de la persona que aprueba el documento>	<DD/MM/AAAA>

HISTORIAL DE REVISIONES

Versión N°	Fecha de la Versión	Resumen de Modificaciones	Modificado por
<X.YY>	<DD/MM/AAAA>	**Punto1** Detalle1 Detalle2 **Punto2** Detalle1 Detalle2	<Nombre de la persona que realizó la modificación>

1. PROPÓSITO

[Nombre de la organización] se basa en la confidencialidad, integridad y disponibilidad de su información y sistemas tecnológicos para llevar mejor su negocio y proveer un mayor cuidado a sus clientes. Es esencial que esa información y sistemas tecnológicos sean continuamente protegidos y utilizados de una manera segura y controlada.

La legislación, directivas regulatorias y prácticas de la industria requieren de [Nombre de la organización] para actuar con diligencia en la seguridad de la información. Los clientes esperan y confían que la [Nombre de la organización] proteja la confidencialidad, privacidad e integridad de su información y que los servicios que brinda la misma estén disponibles. La preservación de esas expectativas es esencial para mantener la seguridad y fidelidad del cliente, conservando la confianza del mismo.

Esta política de seguridad de información asigna la propiedad, responsabilidad, procesos y otros temas que son aplicables a la seguridad, como reportes y la supervisión. Este documento también indica los objetivos

que [Nombre de la organización] busca cumplir con un Sistema de Gestión de Seguridad de la Información.

2. OBJETIVO

Es imposible eliminar todos los riesgos. La seguridad de la información es un medio a través del cual los riesgos relacionados con la seguridad pueden ser gestionados en niveles apropiados y los grupos interesados pueden gestionar y conservar.

Los mecanismos de seguridad y las prácticas pueden ser implementadas para proteger apropiadamente la información recolectada, usada, almacenada, transmitida, divulgada o intercambiada por [Nombre de la organización], y para asegurar la continua prestación de servicios a través del uso de los sistemas de información.

3. ALCANCE Y APLICABILIDAD

La política de seguridad de información busca proveer una guía de alto nivel para la alta dirección de la organización en el enfoque de la seguridad de información que plantea [Nombre de la organización]. Esta política de seguridad de la información puede ser respaldada por políticas de temas en específico, estándares y procedimientos operativos.

La política de seguridad de la información aplica a todas las actividades y empleados dentro de [Nombre de la organización] y a todos los proveedores de materias primas y proveedores de servicios de [Nombre de la organización] que involucra el acceso o manipulación de

la información de alguno de los clientes de [Nombre de la organización].

4. DECLARACIÓN DE POLÍTICA

[Nombre de la organización] se compromete a:

- Proteger la confidencialidad, integridad y disponibilidad de la información de acuerdo con las obligaciones legales y los requisitos razonables de las partes interesadas que controlan la información, los administradores de la información, los custodios y los usuarios autorizados;
- Proteger la integridad y la disponibilidad de los servicios de información basados en tecnología; y
- Mantener a los usuarios individuales responsables de su acceso no autorizado o inapropiado, uso, revelación, eliminación, modificación o interferencia con la información o servicios sensibles.

La información y los servicios asociados deben ser asegurados en línea con requisitos legales y de negocio a través de sus ciclos de vida con la finalidad de optimizar la combinación de valor neto derivado y el riesgo incurrido.

PROGRAMA DE SEGURIDAD DE LA INFORMACIÓN

En relación con los principios de seguridad de información indicados anteriormente, [Nombre de la organización] empleará un programa de gestión de seguridad que abarca lo siguiente:

- Establecimiento de un gobierno, estrategia y un marco de política para la seguridad de información.

- Definición de un enfoque para el programa de la seguridad de la información; así como en los procesos que proporcionan la operación continúa del programa.
- Definir entrenamiento y marco de conciencia para la seguridad de la información.
- Monitorear y reportar el estado del programa de la seguridad de la información; y Guía para las operaciones de la seguridad de la información.

GOBIERNO

Un marco de referencia de política y de gobierno debe ser establecido para que permita fuertes vínculos entre los elementos del gobierno. Este marco de referencia debe establecer una apropiada estructura organizacional, roles y responsabilidades para establecer e implementar políticas y guías mientras se monitorea continuamente y se reporta sobre la efectividad de los procesos de gobierno.

- Esta política de seguridad de información debe ser revisado cada dos años y actualizado según se necesite. La política debe ser aprobada por cualquier responsable asignado para el programa de seguridad de la información; y
- Las directivas operacionales de la seguridad de la información deben respaldar la política mediante la definición del programa de la seguridad de la información y del Sistema de Gestión de Seguridad de la Información en gran detalle, clarificando las responsabilidades y competencias de dirección, y la especificación de los resultados requeridos de gestión de seguridad de la información.

EDUCACIÓN Y CONCIENTIZACIÓN

Las políticas de la seguridad de la información, estándares y guías deben ser comunicadas a todos los empleados y proveedores de servicios para asegurar que se entienda como sus roles y responsabilidades son afectados por la seguridad de la información. Estos programas de concientización deben incluir normas, requerimientos, guías, responsabilidades, medidas de fuerza mayor y consecuencias del no-cumplimiento.

CLASIFICACIÓN DE LA INFORMACIÓN

La gestión debe identificar, valorar y documentar los activos de información y asignar los niveles de sensibilidad, criticidad y propiedad. Todos los custodios de información deben controlar apropiadamente y gestionar adecuadamente sus activos de información con respecto a la integridad y disponibilidad. Todos los clientes y su información personal deben ser clasificados como confidencial y tratada con el más alto nivel de sensibilidad.

TRANSMISIÓN DE LA INFORMACIÓN

Las normas y los controles deben ser establecidos para asegurar que la comunicación y la transmisión de la información es la apropiada. Esto incluye los controles y la vigilancia sobre el intercambio de información con entidades relacionadas o proveedores de servicios pertinentes.

CONTROL DE ACCESO

Los controles lógicos y físicos apropiados deben ser establecidos para balancear el acceso a la información y a los sistemas tecnológicos en contra de los riesgos potenciales que la información puede generar desde la adquisición hasta la destrucción. Esto incluye el establecimiento de controles apropiados para autenticar y autorizar a los usuarios mientras proveen acceso a la información y a los sistemas tecnológicos, logrando completar sus roles y responsabilidades.

SEGURIDAD FÍSICA

Las medidas apropiadas deben ser tomadas para asegurar el acceso físico a la información y a los sistemas tecnológicos que controla.

POLÍTICAS GENERALES DE EVALUACIÓN Y TRATAMIENTO DE RIESGO

- Es responsabilidad de la Gerencia de [Riesgo y Seguridad Informática] asegurar que todo personal de la compañía y terceros conozcan los riesgos a las cuales se encuentran expuestos los documentos digitales y aplicativos informáticos dentro y fuera de la custodia de la organización.
- Es responsabilidad de la Gerencia de [Riesgo y Seguridad Informática] asegurar que todo personal de la compañía y trabajadores externos conozcan los riesgos a las cuales se encuentran expuestos los documentos físicos.

PLANES DE CONTINUIDAD DEL NEGOCIO

Los planes y medidas apropiadas de continuidad del negocio deben ser desarrollados y mantenidos en anticipación de significativas disrupciones del servicio. Se debe tomar consideración de los riesgos y consecuencias asociadas con alguna interrupción en la entrega del servicio.

Las consecuencias potenciales de los desastres, fallas de seguridad, y disrupciones del servicio deben ser analizadas para determinar la criticidad de los servicios y el respaldo de los componentes de infraestructura de TI. Los planes integrados deben ser desarrollados, implementados y probados para asegurar que todos los servicios críticos del negocio son mantenidos o pueden ser restaurados en un orden de prioridades, hacia un nivel aceptable y dentro de las escalas de tiempo requeridas, en caso de algún fallo. Los compromisos de continuidad del negocio para los servicios críticos deben ser incorporados en los Acuerdos de Nivel de Servicio con proveedores y clientes.

MONITOREO Y REPORTES

Hay dos aspectos importantes y distintos del monitoreo y reporte:

- Incidentes de la seguridad de la información – incluso si solo se sospeche o se resuelva sin impacto alguno – que tienen el potencial de impacto o consecuencia, o que involucre a los proveedores de servicios significativos, se deberá notificar al personal apropiado.
- La utilidad y/o efectividad del programa de seguridad

de la información de la organización debe ser medida y reportada para proveer una vista estratégica del programa.

5. ROLES Y RESPONSABILIDADES

Para que se establezca correctamente un Sistema de Gestión de la Seguridad de la Información, se debe asignar responsabilidades a todos los involucrados en el proyecto. Estas responsabilidades pueden agruparse creando un rol, el cual se podrá asignar a más de una persona y puede cambiar según la necesidad del negocio.

La sección de Roles y Responsabilidades incluyen los títulos de trabajo de las personas, y los departamentos relevantes que tienen roles específicos dentro del Programa de Gestión de Seguridad de la Información.

Cada rol explícitamente definido tiene sus responsabilidades asociadas. Los roles definidos para este programa de seguridad de la información por [Nombre de la organización] son los siguientes:

- Rol 1
- Rol 2
- Rol 3
- Rol 4

5.3.9. Plantilla – Roles y Responsabilidades

ROLES Y RESPONSABILIDADES

<Nombre de la empresa>

Versión

<x.y>

CONTROL DE LA DOCUMENTACIÓN

Este documento cuenta con una versión electrónica, la cual está reconocida como la única versión válida para su uso.

Ubicación del Documento	<Directorio donde se encuentre el documento>
Contacto	<Información sobre la persona a contactar que conoce de la estructura del documento – Esta persona no es el dueño de la política>
Frecuencia de revisión	Este documento deberá ser revisado cada XX <meses/años>
Coordinador del documento	<Información para contactar a la persona responsable del documento>
Sensibilidad del documento	<Nivel de sensibilidad del documento: Alta/Media/Baja>

HISTORIAL DE APROBACIONES

Aprobador	Puesto	Fecha de aprobación
<Nombre de la persona o departamento que aprueba el documento>	<Nombre del rol de la persona que aprueba el documento>	<DD/MM/AAAA>

HISTORIAL DE REVISIONES

Versión N°	Fecha de la Versión	Resumen de Modificaciones	Modificado por
<X.YY>	<DD/MM/AAAA>	**Punto1** Detalle1 Detalle2 **Punto2** Detalle1 Detalle2	<Nombre de la persona que realizó la modificación>

1. PROPÓSITO

El propósito de este documento es definir todos los roles y responsabilidades para cada uno de los involucrados dentro de un Sistema de Gestión de Seguridad de la Información. Para ello se detallarán los principales roles que, como mínimo, deberá contar un SGSI para su correcto funcionamiento. Esto deberá cumplirse con la finalidad de asegurar la distribución de responsabilidades a un número correcto de personas.

Para ello, [Nombre de la organización] se compromete a entregar los roles detallados en este documento a las personas que cumplen con el perfil necesario y los conocimientos necesarios para que esto se desempeñe de la mejor manera.

2. ROLES Y RESPONSABILIDADES

Para implementar un Sistema de Gestión de Seguridad de la Información se debe de contar con una relación de personas involucradas, las cuales tendrán ciertas responsabilidades agrupadas en roles, los cuales permitirán identificar los responsables de cada una de las actividades correspondientes a la ISO 27001.

A continuación, se detallan los roles y responsabilidades que se implementarán en [Nombre de la organización]:

GERENCIA GENERAL O DIRECTORIO

La responsabilidad de la gerencia general o del directorio es la siguiente:

- Aprobar el proyecto y la política de seguridad de la información.
- Compromiso con la política y el programa de seguridad de la información.

Gerente de la seguridad de la información

La persona encargada de la gerencia de la seguridad de la información es responsable de realizar las siguientes actividades:

- Comprometer a la alta gerencia con el programa de seguridad de la información.
- Participar en la elaboración de la política de seguridad de la información, objetivos, alcance y estrategia.
- Revisar los reportes del estado del SGSI y aprobar las decisiones correspondientes para su continua mejora.
- Revisar y aprobar la documentación realizada por el Departamento de Seguridad de la Información.

Administrador de seguridad de la información

La persona encargada de administrar la seguridad de la información deberá de realizar las siguientes actividades:

- Desarrollar la política de seguridad de la información, objetivos, alcance y estrategia.
- Definir el alcance del SGSI en la organización.
- Elaborar el procedimiento para la evaluación de riesgos.

- Participar en la primera evaluación de riesgo de la organización.
- Elaborar el plan de tratamiento de los riesgos identificados.
- Seleccionar los objetivos de control y controles correspondientes para satisfacer los objetivos del negocio.
- Monitorear el registro de los incidentes de seguridad de la organización, incluyendo la identificación de la causa raíz y su respectiva acción correctiva a realizar.
- Reportar a la gerencia y al directorio el estado y el progreso de la implementación del SGSI, así como los incidentes problemas, acciones preventivas y correctivas, entre otros.
- Comunicar la política de seguridad de la información a las diferentes áreas de la organización.
- Realizar auditorías para corroborar que el estado del SGSI.
- Hacer cumplir la política de seguridad con respecto a los proveedores externos.

Administrador de las Tecnologías de la información

Las actividades correspondientes al rol de "administrador de TI" dentro del SGSI son las siguientes:

- Asegurar la concientización del personal de TI sobre la seguridad de la información que se almacena en los sistemas y dispositivos de la organización.
- Proveer los recursos técnicos necesarios al departamento de Seguridad de la Información.
- Reportar las vulnerabilidades técnicas e incidentes relacionados a las Tecnologías de la Información.

- Participar en la identificación y evaluación de riesgos de TI.
- Participar en la planificación de la continuidad de negocio.
- Asegurar que los antivirus se aplican adecuadamente a los computadores de la organización.
- Asegurar que las políticas de usuarios y contraseñas se cumplen adecuadamente.

Administrador de Operaciones

El Administrador de Operaciones debe ser el encargado de realizar las siguientes actividades:

- Identificar las amenazas de los sistemas de bases de datos y redes de la organización.
- Evaluar los riesgos que implican las bases de datos y las redes de comunicación de la organización.
- Implementar las medidas de seguridad relacionadas con las contraseñas, firewalls y controles de acceso físicos a los ambientes más críticos del departamento de sistemas.
- Configurar los sistemas y la red de la organización de acuerdo a la política de seguridad establecida.
- Establecer e implementar indicadores y registros con respecto a la seguridad de la información en las bases de datos y las redes de comunicación.
- Implementar un procedimiento de control de cambios.
- Elaborar, mantener y probar los planes de contingencia para asegurar la disponibilidad de la información y la continuidad del negocio.

Usuarios del negocio

Las responsabilidades de los usuarios del negocio son las siguientes:

- Cumplir la política y procedimientos de la seguridad de la información.
- Cumplir con los controles de seguridad, tales como la política de escritorio limpio, contraseñas, entre otros.
- Realizar respaldos de información importante para el usuario.
- Reportar incidentes de seguridad.

3. REFERENCIAS Y DOCUMENTOS ASOCIADOS

Los siguientes documentos son referencias dentro de la política.

Referencia	Ubicación
ISO/IEC 27003:2010 Information technology - Security techniques – Information security management System implementation guidance	https://infosecprimer.files.wordpress.com/2013/06/iso_iec_27003.pdf

5.3.10. Plantilla – Plan de Tratamiento de Riesgos

PLAN DE TRATAMIENTO DE RIESGOS				
Riesgo	Nivel de madurez AS-IS	Nivel de madurez TO-BE	Plan de acción	Responsable

5.3.11. Plantilla – Inventario de Activos

Datos Generales

INVENTARIO DE ACTIVOS	
[Empresa]	
[Versión]	
Propietario	
Frecuencia de Revisión	
Última revisión	
Preparado por:	
Alcance	

Inventario de activos

	Activo						Información		Seguridad de información			
Nro.	ID Activo	Nombre del activo	Descripción del activo	Categoría de activo	Ubicación	Dueño del activo	Información almacenada	Tipo de Acceso	Confidencialidad	Disponibilidad	Integridad	Nivel de sensibilidad
1												
2												
3												
4												
5												

5.3.12. Plantilla – Evaluación de Riesgos

EVALUACIÓN DE RIESGOS SGSI						
Riesgo		Descripción del control	Referencia ISO 27001	Información Requerida	Hallazgo	Conclusión
A5. Políticas de seguridad de la información						
La inexistencia de una política de seguridad de la información no permite que la alta dirección se involucre y comprometa con las tareas de seguridad de la información en la organización	1	La política de seguridad de la información debe de ser definida y aprobada por la gerencia, publicada y comunicada a todos los colaboradores y terceros relevantes para la organización	5.1.1	- Políticas de SGSI. - Evidencia de publicación de la política. - Evidencia de monitoreo y revisión de la política.		
	2	La política de seguridad de la información debe ser revisada en intervalos planificados o si se producen cambios significativos para asegurar su conveniencia, adecuación y eficacia.	5.1.2			
	3	Se deben de definir y/o actualizar los contactos apropiados con las autoridades	6.1.2			

		relevantes en la gestión de la seguridad de la información.				
A6. Organización de la seguridad de la información						
La falta de roles y responsabilidades no permite una correcta gestión de un marco interno de seguridad de la información.	1	Todas las responsabilidades de la seguridad de la información deben de ser definidas y asignadas.	6.1.1	- Organigrama de la organización. - Manual de organización y funciones. - Roles y Responsabilidades del SGSI.		
	2	Las funciones en conflicto y las áreas responsables deben de ser separadas para reducir las oportunidades de modificación o mal uso, no autorizadas o sin intención, de los activos de la organización.	6.1.5			
La inexistencia de políticas para el uso de dispositivos móviles o teletrabajo no permite asegurar la seguridad de la	1	Se definirá y adoptará una política y medidas de seguridad para gestionar los riesgos introducidos por el uso de dispositivos móviles.	6.2.1	- Políticas para el uso de dispositivos móviles. - Política de teletrabajo.		
	2	Se definirá y adoptará una política y medidas de seguridad para proteger la	6.2.2			

información utilizada por estos medios		información a la cual se accede, procesa o almacena en los lugares de teletrabajo.				
A7. Seguridad en los recursos humanos						
Mal entendimiento o desconocimiento de las responsabilidades de los nuevos colaboradores y proveedores con respecto a la seguridad de la información de la organización	1	Se debe de revisar los antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes peruanas, regulaciones y ética relevante.	7.1.1	- Política de reclutamiento y selección. - Evidencia de que la política de seguridad de información está presente en el kit de bienvenida.		
	2	Como parte de la obligación contractual, los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información	7.1.2			
Los colaboradores y proveedores no son	1	La gerencia debe requerir que los empleados, contratistas y terceros apliquen	7.2.1	- Plan de concientización de seguridad de la información.		

conscientes de sus responsabilidades con respecto a la seguridad de la información		la seguridad en concordancia con las políticas y procedimientos establecidos de la organización.				
	2	Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales sobre seguridad de la información.	7.2.2	- Plan de capacitaciones del personal del área de seguridad de la información.		
	3	Debe existir un proceso disciplinario formal para los empleados que han cometido una violación con respecto a la política de seguridad de la información.	7.2.3			
Falta de protección de activos e intereses de la	1	Las responsabilidades de seguridad de la información y tareas que siguen válidas luego de la terminación o cambio de	7.3.1	- Políticas o procedimientos de cese o cambio de puesto de trabajo		

organización durante el proceso de cambio o término del empleado		empleo deben de ser definidas y comunicadas.				
	2	Todos los empleados y terceros deben de regresar todos los activos de la organización que poseen luego del término del empleo o contrato.	8.2.4			
A8. Gestión de activos de información						
La inadecuada identificación de los activos de información de la organización no permite la correcta definición de actividades de protección	1	Todos los activos deben estar claramente identificados, y se debe elaborar y mantener un inventario de todos los activos importantes de la organización.	8.1.1	- Inventario de activos de información, indicando responsable y clasificación.		
	2	Los activos identificados en el inventario deben de tener un propietario o responsable.	8.1.2			
La inadecuada clasificación de los	1	La información debe ser clasificada en términos de su valor, requerimientos	8.2.1			

activos de información puede conllevar a la carencia de un adecuado nivel de aseguramiento de los mismos		legales, confidencialidad y grado crítico para la organización.		- Inventario de activos de información, indicando responsable y clasificación.		
	2	Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.	8.2.2			
Falta de prevención de una divulgación, modificación, remoción o destrucción no autorizada de la información almacenada en los medios	1	Debe existir procedimientos para la gestión de medios removibles.	8.3.1	- Políticas y/o procedimientos para el etiquetado de activos de información. - Políticas y/o procedimientos de medios de transferencia de información físicos. - Políticas y/o procedimientos sobre el uso de dispositivos de almacenamiento removibles.		
	2	Se deben establecer los procedimientos para el manejo y almacenaje de la información para proteger dicha información de una divulgación no autorizada o un mal uso.	8.3.2			
	3	Los medios que contienen información deben de ser protegidos de accesos no autorizados, mal uso o corrupción durante el transporte de los mismos.	8.3.3			

A9. Control de accesos						
Accesos no autorizados a la información, sistemas, aplicaciones y servicios de la organización	1	Una política de control de accesos debe ser definida, documentada y revisada según los requerimientos del negocio y la seguridad.	9.1.1	- Política y/o procedimientos de gestión de accesos. - Listado de custodios de los sistemas de información. - Listado de aplicaciones que cuentan con una gestión de accesos. - Cronograma de revisión de usuarios, roles y/o perfiles en los sistemas de información. - Listado de cuentas genéricas utilizadas en los sistemas de información.		
	2	Debe existir un procedimiento formal para el registro y de-registro de acceso a todos los sistemas y servicios de información.	9.2.1			
	3	Se debe restringir y controlar la asignación y uso de los privilegios.	9.2.2			
	4	La asignación de claves se debe controlar a través de un proceso de gestión formal.	9.2.3			
	5	Los responsables de los activos deben de revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.	9.2.4			

	6	Los usuarios deben de utilizar contraseñas alineadas con la política de control de accesos de la organización.	9.3.1			
	7	El acceso a la información y a las funciones de las aplicaciones deben de ser restringidos de acuerdo a la política de control de accesos	9.4.1			
	8	El acceso a los sistemas y aplicaciones deben de ser controlados por un procedimiento de registro de accesos.	9.4.2			
	9	El acceso al código fuente de las aplicaciones debe de ser restringido solo al personal autorizado.	9.4.5			
A10. Criptografía						
Inapropiado e inefectivo uso de la criptografía para proteger la	1	Una política de controles criptográficos para la protección de la información debe de ser desarrollada e implementada.	10.1.1	- Políticas y/o procedimientos de gestión de llaves criptográficas.		

confidencialidad, autenticidad e integridad de la información						
A11. Seguridad física y ambiental						
Accesos físico, daño o interferencia no autorizada a la información de la organización	1	Se debe utilizar perímetros de seguridad (paredes, puertas, etc) para proteger áreas que contienen información y medios de procesamiento de información.	11.1.1	- Revisión del centro de procesamiento de datos. - Política de escritorio limpio. - Política y/o procedimiento de retiro e ingreso de equipos.		
	2	Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.	11.1.2			
	3	Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.	11.1.3			
	4	Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y	11.1.4			

		otras formas de desastre natural o creado por el hombre.				
	5	Se debe diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras.	11.1.5			
Pérdida, daño, robo e interrupción de las operaciones de la organización	1	El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.	11.2.1			
	2	El equipo debe de estar protegido de fallos de energía y otras interrupciones causadas por fallas en los servicios públicos.	11.2.2			
	3	El cableado de la energía y las telecomunicaciones que lleven "data" o sostienen los servicios de información deben ser protegidos de la intercepción o daño.	11.2.3			

	4	El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.	11.2.4			
	5	Equipos, información o software no deben ser sacados fuera de la propiedad de la organización sin previa autorización.	11.2.5			
	6	Se debe aplicar seguridad al equipo fuera del local tomando en cuenta los diferentes riesgos que implica trabajar fuera del local de la organización.	11.2.6			
	7	Se debe de adoptar una política de "escritorio limpio" para los documentos y medios de almacenamiento removibles y una política de "pantalla limpia" para los medios de procesamiento de la información.	11.2.9			
A12. Seguridad en las operaciones						

Falta de aseguramiento para el correcto y seguro procesamiento de la información	1	Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten	12.1.1	- Política y/o procedimiento de gestión de cambios (Producción de Sistemas). - Evidencia de la existencia de ambientes de desarrollo, integración, pruebas y producción sobre los principales sistemas de información.		
	2	Se deben controlar los cambios en los medios y sistemas de procesamiento de la información.	12.1.2			
	3	Se deben separar los medios de desarrollo, prueba y operacionales para reducir los riesgos de accesos no autorizados o cambios en el sistema de operación.	11.1.4			
Falta de protección contra malware	1	Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos maliciosos y se deben implementar procedimientos de conciencia apropiados.	12.2.1	- Evidencia de instalación de antivirus.		

Falta de protección contra la pérdida de información	1	Se deben realizar copias de backup o respaldo de la información y software esencial y se deben probar regularmente de acuerdo a la política de backups	12.3.1	- Políticas y/o procedimientos de respaldo de información. - Política y/o procedimiento de restauración de cintas de respaldo de información.		
Inexistencia de registros de los eventos y generación de evidencias de las operaciones	1	Se deben producir registros de las actividades que realizan los usuarios (auditoría), excepciones y eventos de seguridad de la información y se deben mantener durante un periodo acordado para ayudar en investigaciones futuras y monitorear el control de acceso	12.4.1	- Política y/o procedimiento de creación, acceso y monitoreo de logs de auditoría en los sistemas de información. - Logs de auditoría de los principales sistemas de información.		
	2	Se deben de proteger los medios de registro y la información de registro contra alteraciones y acceso no autorizado.	12.4.2			
	3	Los relojes de los sistemas de procesamiento de información relevantes de una organización o dominio de	12.4.4			

		seguridad deben estar sincronizados con una fuente de tiempo exacta acordada.				
A13. Seguridad de las comunicaciones						
Inadecuada protección de la información en las redes de la organización	1	Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.	13.1.1	- Política y/o procedimiento para la transferencia de información. - SLAs establecidos con los usuarios internos para la transferencia de información. - SLA establecidos con los proveedores.		
	2	Se deben identificar 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 "in home" o sean abastecidos externamente.	13.1.2			
	3	Los servicios de información, usuarios y sistemas de información se deben segregar en las redes.	13.1.3			

Inadecuada gestión de la seguridad de la información y software intercambiados dentro de la organización y con cualquier entidad externa	1	Se debe de establecer una política, procedimientos y controles de intercambio formales para proteger la información tratada a través de todos los tipos de medios de comunicación.	13.2.1	- Política y/o procedimiento para la transferencia de información.		
	2	Se debe proteger adecuadamente los mensajes electrónicos.	13.2.3			
	3	Los requerimientos de confidencialidad y no-revelación de la información de la organización deben identificarse, regularse, revisarse y documentarse.	13.2.4			
A14. Adquisición, desarrollo y Mantenimiento de los sistemas de información						
La inadecuada gestión de nuevos sistemas puede atentar contra la integridad de la	1	Los enunciados de los requerimientos comerciales para sistemas nuevos, o mejorar los sistemas existentes deben especificar los requerimientos de los controles de seguridad.	14.1.1	- Procedimiento para el desarrollo de los sistemas de información (Estándares de programación).		

información de los sistemas de la organización	2	La información involucrada en servicios de aplicaciones que utilizan redes públicas debe ser protegida de las actividades fraudulentas y revelación no autorizada de la misma.	14.1.2			
	3	La información involucrada en servicios de transacciones debe ser protegida para prevenir transmisiones incompletas, alteraciones de la información no autorizadas, revelaciones no autorizadas, duplicación de información, etc.	14.1.3			
Las políticas de seguridad de la información no son consideradas en los nuevos desarrollos o adquisiciones de	1	Las reglas para el desarrollo de software y sistemas deben ser establecidas y aplicadas a los desarrollos dentro de la organización	14.2.1	- Evidencia de control de cambios de los nuevos sistemas.		
	2	La implementación de cambios se debe controlar mediante el uso de procedimientos formales de control de cambios.	14.2.2			

los sistemas de información	3	Cuando se cambian los sistemas operativos, se deben revisar y probar las aplicaciones críticas del negocio para asegurar que no exista un impacto adverso en las operaciones o seguridad organizacional.	14.2.3			
	4	No se deben fomentar las modificaciones a los paquetes de software, se deben limitar a los cambios necesarios y todos los cambios deben ser controlados estrictamente.	14.2.4			
	5	El desarrollo de software que ha sido tercerizado debe ser supervisado y monitoreado por la organización.	14.2.7			
A15. Relaciones con los proveedores						
Los proveedores cuentan con acceso no autorizado a la	1	Los requerimientos de seguridad de la información para mitigar los riesgos asociados con los accesos de los	15.1.1			

información de la organización		proveedores a la información de la organización deben ser documentados.		- Política y/o procedimiento para la gestión de contratación de proveedores.		
	2	Todos los requerimientos de seguridad de la información relevantes deben establecerse y acordarse con cada proveedor que tiene acceso a los procesos, almacenamiento, comunicación de la información de la organización.	15.1.2			
A16. gestión de incidentes de seguridad de la información						
Un inadecuad procedimiento de gestión de incidentes de información puede atentar contra la disponibilidad, integridad y	1	Se deben establecer las responsabilidades y procedimiento gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.	16.1.1	- Política y/o procedimiento para la atención de incidentes de seguridad. - Matriz de incidentes categorizados. - Procedimiento de monitoreo de sistemas de información para la detección de eventos de seguridad. - Listado de herramientas utilizadas para el monitoreo de sistemas de información.		
	2	Los eventos de seguridad de la información deben reportarse a través de los canales gerenciales apropiados lo más rápido posible.	16.1.2			

confidencialidad de la misma	3	Se debe requerir que todos los empleados, contratistas y terceros usuarios de los sistemas y servicios de información tomen nota y reporten cualquier debilidad observada o sospechada en la seguridad de los sistemas o servicios.	16.1.3			
	4	Deben existir mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.	16.1.6			
	5	Cuando la acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal, se debe recolectar, mantener y presentar evidencia para cumplir las reglas de evidencia establecidas en las jurisdicciones relevantes.	16.1.7			

A17. Gestión de continuidad de negocios						
Falta de protección de la información en cualquier momento y para anticipar los siniestros	1	La organización debe determinar los requerimientos para la seguridad de la información y la continuidad de la misma en situaciones adversas (p.e. durante un siniestro o desastre).	17.1.1	- Plan de continuidad del negocio.		
	2	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar los niveles requeridos de continuidad para la seguridad de la información durante las situaciones adversas.	17.1.2			
	3	La organización debe verificar los controles de continuidad de la seguridad de la información establecidos e implementados en intervalos regulares	17.1.3			

		para asegurar que siguen vigentes y efectivos.				
	4	El procesamiento de la información debe de considerar implementar la redundancia suficiente para satisfacer los requerimientos de disponibilidad.	17.2.1			
A18. Cumplimiento de la seguridad de la información						
La seguridad de la información no opera según los estándares y políticas establecidas por la organización	1	Los gerentes deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad sean realizados correctamente en cumplimiento con las políticas y estándares de seguridad establecidos por la organización.	18.2.1	- Política y/o procedimiento de sanciones - Manual de administración y custodia de documentos		
	2	Los sistemas de información deben verificarse regularmente para el cumplimiento con los estándares de implementación de la seguridad.	18.2.2			

Incumplimiento de obligaciones y normas legales, regulatorias y contractuales de seguridad de la información	1	Se deben definir explícitamente, documentar y actualizar todos los requerimientos reguladores y contractuales y el enfoque de la organización relevante para cada sistema de información y la organización.	18.1.1	- Listado de leyes, normas y/o políticas que se debe cumplir relacionado temas de seguridad de información		
	2	Se deben implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso de material con respecto a los derechos de propiedad intelectual y sobre el uso de los productos de software patentados	18.1.2			
	3	Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación en concordancia con los requerimientos legales, reguladores, contractuales y comerciales.	18.1.3			

	4	Se deben asegurar la protección y privacidad tal y como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable las cláusulas contractuales	18.1.4			

VI. CONCLUSIONES

De acuerdo con los resultados mostrados de la presente investigación, se concluye que la empresa tiene inconvenientes con la manera de cómo está generando, organizando y guardando la información, ya que se evidencia que no cuentan con procedimientos implementados actualmente, estos dificultan el desarrollo de sus actividades, lo cual, junto con la falta de un sistema de información, el proceso de gestión administrativa se torna ineficiente, teniendo perdida de datos, duplicidad de información, falta de centralización de información y malestar por parte de los trabajadores; es por ello que es El Diseño de un sistema de gestión de seguridad de la información, para el GRUPO SIAS SAC – Chimbote; 2017, permitirá una adecuada administración de la información.

En relación a las hipótesis específicas, mencionaremos:

1- Queda demostrado, que la empresa tiene serios riesgos con la gestión de información que maneja, a consecuencia de la falta de un sistema de información y la manera artesanal en que se está gestionando la información, conllevan a tomar malas decisiones y por ende genera pérdidas a la empresa.

2- De acuerdo al proceso actual cómo se maneja la información en el GRUPO SIAS SAC, se pudo determinar el alto nivel de riesgos que existe en el manejo de los activos de información dentro de la empresa, ello debido al poco control existente.

3- Es importante establecer los objetivos y políticas del sistema de gestión de seguridad de la información, ya que estos van delineando el camino hacia donde la organización desea dirigirse para preservar la confidencialidad, integridad y disponibilidad de la información y por lo tanto es relevante la participación de la alta gerencia. Y así disminuir los riesgos existentes.

4- Dentro un Sistema de Gestión de Seguridad de la Información, se encuentra la mejora continua lo cual hace que sea muy importante que la organización se asegure de crear procedimientos para el monitoreo y revisión del sistema, los mismos que deben cubrir incidentes de seguridad, auditorías internas y revisiones gerenciales. Estos elementos aportan retroalimentación al Sistema posibilitando conocer el estado del mismo y aplicar acciones correctivas, si fuera el caso, que permitan el cumplimiento de los planes y objetivos.

VII. RECOMENDACIONES

1. Se sugiere al GRUPO SIAS SAC implementar un sistema de gestión de Seguridad de la información, ya que esto les permitirá minimizar los riesgos.
2. Realizar campañas de concientización periódicas para el personal de la empresa con respecto a la seguridad de información, de tal manera que todos los empleados de las diversas áreas existentes, conozcan la importancia y las consecuencias de no seguir los lineamientos de seguridad en el día a día.
3. Se sugiere considerar al Sistema de Gestión de Seguridad de la Información como un proceso de mejoramiento continuo, en donde los nuevos requerimientos de seguridad se ajusten a los cambios de la empresa.
4. Realizar análisis periódicos de los riesgos y monitorear continuamente la situación, pues la seguridad que se va a proporcionar con un SGSI es permanente para lo cual es necesario de un proceso continuo.

REFERENCIAS BIBIOGRAFICAS

1. NewNet S.A. NewNet S.A. [Online].; 2012 [cited 2017. Available from: HYPERLINK "https://newnetsa.wordpress.com/2013/04/11/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/" https://newnetsa.wordpress.com/2013/04/11/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/ .

2. GOUJON A. welivesecurity. [Online].; 2013 [cited 2017. Available from: HYPERLINK "https://www.welivesecurity.com/la-es/2013/01/09/phishing-webmail-redes-sociales-bancos-servicios-mas-suplantados/" https://www.welivesecurity.com/la-es/2013/01/09/phishing-webmail-redes-sociales-bancos-servicios-mas-suplantados/ .

3. ESET. welivesecurity. [Online].; 2016 [cited 2017. Available from: HYPERLINK "https://www.welivesecurity.com/wp-content/uploads/2016/04/eset-security-report-latam-2016.pdf" https://www.welivesecurity.com/wp-content/uploads/2016/04/eset-security-report-latam-2016.pdf .

4. Yagual Del Valle C, Chilán Rodríguez L. Análisis para la integración de un sistema de información (SGSI) ISO-27001 utilizando OSSIM para empresa industrial. Tesis de Grado. Guayaquil: Universidad Politecnica Salesiana, Facultad de Ingenieria de Sistemas; 2014.

5. Barragán I, Góngora I, Martínez E. Implementación de políticas de seguridad informática para la m.i. municipalidad de Guayaquil aplicando la norma iso/iec 27002. Tesis de Grado. Guayaquil: Escuela Superior Politecnica del Litoral, Escuela de Diseño y Comunicacion Visual; 2013.

6. Aguirre Cordova JD, Aristizabal Betancourt C. Diseño del sistema de gestion de seguridad de la informacion para el Grupo Empresarial La Ofrenda. Tesis de Grado. Pereira: Universidad Tecnologica de Pereira, Facultad de Ingenieria; 2013.

7. Guachi Aucapiña TV, Guevara Aulestia DO. Norma de seguridad informatica ISO 27001 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de informacion y comunicacion en el Departamento de Sistemas de la Cooperativa de Ahorro y Credito San Francisco. Ltda. Tesis de Grado. Ambato: Universidad Tecnica de Ambato, Facultad de Ingenieria de Sistemas; 2012.

8. Talavera Álvarez VR. 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. Tesis de Grado. Lima: Pontificia Universidad Catolica del Peru, Facultad de Ciencias e Ingenieria; 2016.

9. Aguirre Mollehuanca DA. Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A. Tesis de Grado. Lima: Pontificia Universidad Catolica del Peru, Facultad de Ciencias e Ingeniria; 2014.

10. Espinoza Aguinaga HR. Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo. Tesis de Grado. Lima: Pontificia Universidad Catolica del Peru, Facultad de Ciencias e Ingenieria; 2013.

11. Montoya Pachas NK. Diseño de un sistema de gestión de seguridad de información para un centro cultural binacional. Tesis de Grado. Lima: Pontificia Universidad Catolica del Peru, Facultad de Ciencias e ingeniria; 2013.

12. Google Maps. Google Maps. [Online].; 2017 [cited 2017. Available from: HYPERLINK "https://www.google.com.pe/maps/place/Av.+Francisco+Bolognesi+1108,+Chimbote/@-9.0769603,-78.5888527,17z/data=!4m5!3m4!1s0x91ab816adbaeedc3:0x2cb9da91fd65dca0!8m2!3d-9.0774!4d-78.591256?hl=es-419" https://www.google.com.pe/maps/place/Av.+Francisco+Bolognesi+1108,+Chimbote/@-9.0769603,-78.5888527,17z/data=!4m5!3m4!1s0x91ab816adbaeedc3:0x2cb9da91fd65dca0!8m2!3d-9.0774!4d-78.591256?hl=es-419 .

13. Grupo SIAS SAC. PLAN DE TRABAJO GRUPO SIAS 2017. Informe Plan de Trabajo. Chimbote:, Jefatura de Gestion Humana; 2017.

14. Soria A. Las Tecnologías de la Información y la Comunicación aplicadas a la Formacion Continua Madrid: Gens, SL; 2005.

15. Belloch C. LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (T.I.C.). Valencia: Universidad de Valencia, Unidad de Tecnología Educativa.

16. Pastor Collado JA. Concepto de sistemas de información en las organizaciones Barcelona: Universitat Oberta de Catalunya; 2002.

17. Real ISMS. Activos de información. RealISO. [Online].; 2012 [cited 2017. Available from: HYPERLINK "https://sites.google.com/a/realiso.com/realisms-spa/gestao-de-risco/-3-3-ativos-de-informacao" https://sites.google.com/a/realiso.com/realisms-spa/gestao-de-risco/-3-3-ativos-de-informacao .

18. Laudon , Laudon JP. Sistemas de información gerencial: administración de la empresa digital. Octava Edicion ed. Mexico: PEARSON EDUCACION; 2004.

19. Ormella Meyer C. iso27000. [Online].; 2012 [cited 2017. Available from: HYPERLINK "http://www.iso27000.es/download/seguridad%20informaticavsinformacion.pdf" http://www.iso27000.es/download/seguridad%20informaticavsinformacion.pdf .

20. González Trejo D. magazcitum. [Online].; 2013 [cited 2017. Available from: HYPERLINK "http://www.magazcitum.com.mx/?p=2397" \l ".WduvY1vWzIV" http://www.magazcitum.com.mx/?p=2397#.WduvY1vWzIV .

21. Erb M. Protejete. [Online].; 2012 [cited 2017. Available from: HYPERLINK "https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/" https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/ .

22. Mifsud E. recursostic.educacion. [Online].; 2012 [cited 2017. Available from: HYPERLINK "http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1." http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1.

23. British Standards Institution (BSI). Bsigroup. [Online].; 1998 [cited 2017. Available from: HYPERLINK "https://www.bsigroup.com/es-ES/Sobre-BSI/Nuestra-historia/" https://www.bsigroup.com/es-ES/Sobre-BSI/Nuestra-historia/ .

24. Lopez Neira A, Ruiz Spohr J. iso27000. [Online].; 2005 [cited 2017. Available from: HYPERLINK "http://www.iso27000.es/" http://www.iso27000.es/ .

25. Karn G. Bulsuk. Bulsuk. [Online].; 2009 [cited 2017. Available from: HYPERLINK "http://www.bulsuk.com/2009/02/taking-first-step-with-pdca.html" http://www.bulsuk.com/2009/02/taking-first-step-with-pdca.html .

26. PMG-SSI. Pmg-ssi. [Online].; 2015 [cited 2017. Available from: HYPERLINK "http://www.pmg-ssi.com/2013/08/la-nch-iso-27001-origen-y-evolucion/" http://www.pmg-ssi.com/2013/08/la-nch-iso-27001-origen-y-evolucion/ .

27. Marojaspe. Es.Slideshare. [Online].; 2013 [cited 2017. Available from: HYPERLINK "https://es.slideshare.net/marojaspe/curso-ai-iso-27001" https://es.slideshare.net/marojaspe/curso-ai-iso-27001 .

28. Markus E. protejete. [Online].; 2012 [cited 2017. Available from: HYPERLINK "https://protejete.wordpress.com/gdr_principal/" https://protejete.wordpress.com/gdr_principal/ .

29. Rojas E. metodologiaeconomia2011.blogspot.pe. [Online].; 2011 [cited 2017. Available from: HYPERLINK "http://metodologiaeconomia2011.blogspot.pe/2011/05/investigacion-cuantitativa.html" http://metodologiaeconomia2011.blogspot.pe/2011/05/investigacion-cuantitativa.html .

30. Vásquez Hidalgo I. gestiopolis.com. [Online].; 2005 [cited 2017. Available from: HYPERLINK "https://www.gestiopolis.com/tipos-estudio-metodos-investigacion/" https://www.gestiopolis.com/tipos-estudio-metodos-investigacion/ .

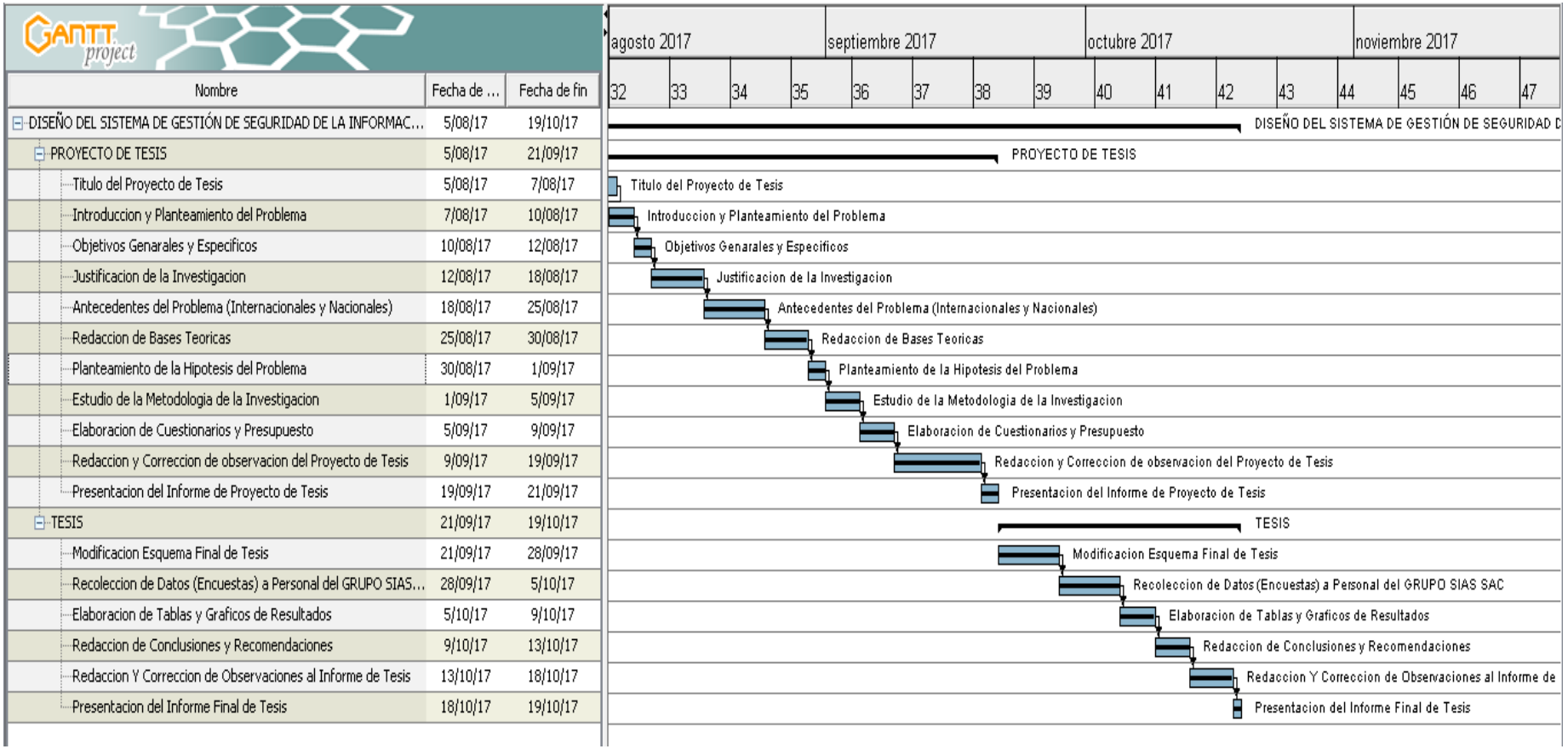
31. Arias FG. El Proyecto de Investigacion : Introduccion a la metodologia cientifica. Quinta ed. Caracas: Episteme; 2006.

32. Barrantes Porras CE, Hugo Herrera JR. Diseño e Implementacion de un sistema de gestion de seguridad de informacion en procesos tecnologicos. Tesis de Grado. Lima: Universidad de San Martin de Porres, Escuela Profesional de Ingenieria de Computacion y Sistemas; 2012.

33. Justino Salinas ZI. Diseño de un sistema de gestion de seguridad de informacion para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013. Tesis de Grado. Lima: Pontificia Universidad Catolica del Peru, Facultad de Ciencias e Ingenieria; 2015.

ANEXOS

ANEXO NRO. 01: CRONOGRAMA DE ACTIVIDADES



Nombre	Fecha de ...	Fecha de fin
DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMAC...	5/08/17	19/10/17
PROYECTO DE TESIS	5/08/17	21/09/17
Titulo del Proyecto de Tesis	5/08/17	7/08/17
Introduccion y Planteamiento del Problema	7/08/17	10/08/17
Objetivos Genarales y Especificos	10/08/17	12/08/17
Justificacion de la Investigacion	12/08/17	18/08/17
Antecedentes del Problema (Internacionales y Nacionales)	18/08/17	25/08/17
Redaccion de Bases Teoricas	25/08/17	30/08/17
Planteamiento de la Hipotesis del Problema	30/08/17	1/09/17
Estudio de la Metodologia de la Investigacion	1/09/17	5/09/17
Elaboracion de Cuestionarios y Presupuesto	5/09/17	9/09/17
Redaccion y Correccion de observacion del Proyecto de Tesis	9/09/17	19/09/17
Presentacion del Informe de Proyecto de Tesis	19/09/17	21/09/17
TESIS	21/09/17	19/10/17
Modificacion Esquema Final de Tesis	21/09/17	28/09/17
Recoleccion de Datos (Encuestas) a Personal del GRUPO SIAS...	28/09/17	5/10/17
Elaboracion de Tablas y Graficos de Resultados	5/10/17	9/10/17
Redaccion de Conclusiones y Recomendaciones	9/10/17	13/10/17
Redaccion Y Correccion de Observaciones al Informe de Tesis	13/10/17	18/10/17
Presentacion del Informe Final de Tesis	18/10/17	19/10/17

Fuente: Elaboración propia

ANEXO NRO. 02: PRESUPUESTO Y FINANCIAMIENTO

TITULO	:	Diseño del sistema de gestión de seguridad de la Información para el GRUPO SIAS SAC. – Chimbote; 2017.
TESISTA	:	Clotilde Esther Flores Villanueva
INVERSIÓN	:	S/. 5,456.00
FINANCIAMIENTO	:	Recursos propios

DESCRIPCIÓN	UNIDAD	CANTIDAD	COSTO UNITARIO	COSTO TOTAL
ASIGNACIONES				
Movilidad	Días	8	S/. 100.00	S/. 800.00
SERVICIO DE INTERNET				
Internet	Mes	4	S/. 80.00	S/. 320.00
MATERIALES VARIOS				
Laptop	Unidad	1	S/. 1,800.00	S/. 1,800.00
Lapiceros	Unidad	12	S/. 0.50	S/. 6.00
Fotocopias	Unidad	500	S/. 0.05	S/. 25.00
Hojas	Millar	2	S/. 22.00	S/. 44.00
Impresora	Unidad	1	S/. 400.00	S/. 400.00
Tinta para Impresora - Negro	Unidad	1	S/. 90.00	S/. 90.00
Tinta para Impresora - Colores	Unidad	1	S/. 130.00	S/. 130.00
Folder Manila	Unidad	20	S/. 0.50	S/. 10.00
			TOTAL PRESUPUESTO	**S/. 5,456.00**

ANEXO NRO. 03: CUESTIONARIO

TITULO : Diseño del sistema de gestión de seguridad de la información Para el GRUPO SIAS SAC. – Chimbote; 2017.

TESISTA : Clotilde Esther Flores Villanueva.

PRESENTACIÓN:

El presente instrumento forma parte del actual trabajo de investigación; por lo que se solicita su participación, respondiendo a cada pregunta de manera objetiva y veraz. La información a proporcionar es de carácter confidencial y reservado; y los resultados de la misma serán utilizados solo para efectos académicos y de investigación científica.

INSTRUCCIONES:

A continuación, se le presenta una lista de preguntas, agrupadas por dimensión, que se solicita se responda, marcando una sola alternativa con un aspa (“X”) en el recuadro correspondiente (Si o No) según considere su alternativa, de acuerdo al siguiente ejemplo:

NRO.	PREGUNTA	Si	No
1	¿Se registran los accesos de personas a las áreas donde se encuentran los equipos servidores?		**X**

Dimensión 1: Nivel de conocimiento y uso del software y hardware			
NRO.	**PREGUNTA**	**Si**	**No**
1	¿Se registran los accesos de personas a las áreas donde se encuentran los equipos (servidores)?		
2	¿Los equipos de cómputo en el área tienen fuente de poder interrumpible (UPS), ¿Generadores de energía, baterías ante cortes de energía eléctrica?		
3	Frente a cualquier desastre natural, provocado o humano ¿Ud. conoce cuales son los activos más importantes que debe proteger en relación a la información?		
4	¿Usted apaga los equipos informáticos (PC) correctamente después de utilizarlos?		
5	¿Cuándo se ausenta de su oficina deja bloqueada la PC?		
6	¿Has utilizado algún dispositivo externo (USB, ¿Celular, Discos Externos) para extraer algún tipo de información de trabajo o de su interés?		
7	¿Usted ha detectado que el antivirus del GRUPO SIAS SAC funciona adecuadamente y que se encuentra actualizado?		
8	¿Existe alguna alarma contra incendios, robos, otros?		
9	¿Existen un inventario de activos actualizado?		
10	¿El Inventario contiene activos de datos, software, equipos y servicios?		
11	Se dispone de una clasificación de la información según la criticidad de la misma (¿Documentos, Expedientes, Órdenes de compra, ¿Contratos, etc.?		
12	¿Existe un responsable de los activos?		
13	¿La clave de acceso es la misma para todos los sistemas y/o PC con los que cuenta el GRUPO SIAS SAC?		
14	¿Comparte sus claves de acceso de su PC con sus compañeros de trabajo?		
15	¿Ud. cambia con frecuencia sus Claves de acceso?		

Dimensión 2: Nivel de conocimiento de políticas de seguridad de la información en la gestión administrativa			
NRO.	**PREGUNTA**	**Si**	**No**
1	¿En el GRUPO SIAS SAC, cuentan con políticas de seguridad de la información?		
2	¿Conoce UD. que son las Políticas de seguridad de la Información?		
3	¿Existe algún tipo de manual y/o documento donde se especifique los controles para la seguridad de la información del GRUPO SIAS SAC?		
4	¿Ud. sabe distinguir la información que es estrictamente confidencial, de uso interno o público?		
5	¿Cuándo se ausenta de su oficina deja documentación visible en su escritorio?		
6	¿Cuenta con correo electrónico de la empresa?		
7	¿Comparte su clave de Correo, con sus compañeros de trabajo?		
8	¿Usted Desecha la información (Documentación) que ya no necesita?		
9	¿Existen procedimientos para clasificar la información (Documentación)?		
10	¿Existen procedimientos para el resguardo de la información (Documentación)?		
11	¿Existen roles y responsabilidades definidos para las personas implicadas en la seguridad de la Información?		
12	¿La Dirección y las áreas de la Organización participan en temas de seguridad de la información?		
13	¿Existe un acuerdo de confidencialidad, con respecto a la información que se maneja en la empresa?		
14	¿Se tiene en cuenta la seguridad de la información que se maneja en la empresa al momento de selección y baja del personal?		
15	¿Se plasman las condiciones de confidencialidad y responsabilidades en los contratos?		
16	¿Existe un proceso disciplinario, relacionado con la falta de confidencialidad de los trabajadores hacia la empresa?		