UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL INGENIERÍA DE SISTEMAS E INFORMÁTICA

"APLICACIÓN DE LA NORMA ISO/IEC 27001 PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN EN LA OFICINA GENERAL DE ADMISIÓN DE LA UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO, 2018"

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

AUTOR:
Bach. FREDY NORBERTO ALVARADO JAMANCA

ASESOR:
Ing. LUIS RUPERTO ALVARADO CÁCERES

HUARAZ – PERÚ
2018

N° de Registro: T181

DEDICATORIAS

A mis padres

Por haberme apoyado en todo momento, por ser las personas que me han acompañado durante todo mi trayecto estudiantil y de mi vida, por sus consejos, sus valores, por la motivación constante que ha permitido ser hombre de bien, pero más que nada, por su amor y ternura.

A mis hermanos

Que con su amor me han enseñado a salir adelante. Gracias por su paciencia, gracias por compartir sus vidas, pero sobre todo por estar en los momentos tan importante de mi vida.

AGRADECIMIENTOS

A Dios, por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.

A la Universidad Nacional Santiago Antúnez de Mayolo, por haberme aceptado ser parte de ella y abierto las puertas de su seno científico para poder estudiar mi carrera.

A mis Docentes que sin esperar nada a cambio, han sido pilares en nuestro camino, formando parte de este logro que me abre puertas imaginables en mí desarrollo profesional.

PRESENTACIÓN

Señores Miembros del Jurado:

En cumplimiento con el Reglamento de Grados y Títulos de la Escuela Profesional de Ingeniería de Sistemas e Informática, Facultad de Ciencias de la Universidad Nacional Santiago Antúnez de Mayolo, me permito presentar la tesis titulada: "Aplicación de la Norma ISO/IEC 27001 para mejorar la Seguridad de la Información en la Oficina General de Admisión de la Universidad Nacional Santiago Antúnez de Mayolo, 2018." Con la finalidad de obtener el título profesional de Ingeniero de Sistemas e Informática.

El informe de investigación está conformado por IX capítulos: En el Capítulo I se determinan la realidad problemática, enunciado del problema, hipótesis, objetivos, Justificación, limitaciones, descripción y sustentación de la solución. En el Capítulo II se consideró los antecedentes, así como las teorías que sustentan el trabajado. En el Capítulo III se define los materiales, métodos, técnicas, procedimientos utilizados. En el Capítulo IV se realiza el análisis y diagnóstico de la situación actual. En el Capítulo V la arquitectura tecnológica de la solución, diseño de estructura de la solución. En el Capítulo VI se realiza la construcción. En el Capítulo VII monitoreo y evaluación de la solución. En el Capítulo VIII se exponen los resultados obtenidos. En el Capítulo IX se discute los resultados. Finalmente se presenta las conclusiones y recomendaciones.

Se espera, que está investigación concuerde con las exigencias establecidas por nuestra Universidad y merezca su aprobación.

HOJA DE VISTO BUENO

Dr. Carlos Antonio Reyes Pareja
Presidente

Ing. Esteban Julio Medina Rafaile
Secretario
Reg. C.I.P. N° 88145

Ing. Luis Ruperto Alvarado Cáceres
Vocal
Reg. C.I.P. N° 116530

RESUMEN

El presente trabajo de investigación consiste en la Aplicación de la Norma ISO/IEC 27001 para mejorar la Seguridad de la Información en la Oficina General de Admisión de la Universidad Nacional Santiago Antúnez de Mayolo, con el Diseño de un Sistema de Gestión de Seguridad de la Información, el cual se describe en el Documento de Aplicabilidad que al ser ejecutado tendrá como resultado un adecuado aseguramiento de la información, manteniéndolo al margen o fuera de riesgo los activos de información.

Para este diseño de un Sistema de Gestión de Seguridad de la Información, se usó la norma ISO/IEC 27001 y a su vez en la metodología MAGERIT, todo ello con el fin de poder identificar y mitigar los riesgos y amenazas a los que está expuestas la información, con las cuales se obtuvo como resultado la Declaración de Aplicabilidad.

Palabras Claves: ISO/IEC 27001, Gestión de Seguridad, Seguridad de la Información, MAGERIT, Declaración de Aplicabilidad.

ABSTRACT

The present research work consists in the Application of the ISO / IEC 27001 Standard to improve the Information Security in the General Office of Admission of the National University Santiago Antúnez de Mayolo, with the Design of a Security Management System of the Information, which is described in the Applicability Document that, when executed, will result in an adequate assurance of information, keeping information assets out of the way or out of risk.

For this design of an Information Security Management System, the ISO / IEC 27001 standard was used, as well as the MAGERIT methodology, all in order to identify and mitigate the risks and threats to which it is exposed. Information, with which the Declaration of applicability was obtained as a result.

Keywords: ISO/IEC 27001, Security Management, Security of the information, MAGERIT, Declaration of Applicability.

ÍNDICE GENERAL

CAPÍTULO I: GENERALIDADES

1.1. Realidad problemática

Hoy en día, la información se ha convertido en un activo que al igual que otros activos importantes del negocio, representa un valor significativo para toda organización. En consecuencia, requiere de un tratamiento que asegure su adecuada protección. Esto es muy importante en un creciente ambiente interconectado de negocios, ya que producto de esto la información está expuesta a un mayor rango de amenazas, y encara un mayor número de vulnerabilidades propias del entorno organizacional, que se generan debido a las diversas formas que puede adoptar la información (impresa, escrita en papel, almacenada electrónicamente, transmitida por correo electrónico o por medios electrónicos, mostrada en un video o hablada en una conversación). Independientemente de la forma que tome la información o el medio por el que se distribuya, debe protegerse. (ISO 27002)

La Universidad Nacional Santiago Antúnez de Mayolo (UNASAM) es una institución de educación superior que está comprometida con el proceso de enseñanza-aprendizaje y como cualquier organismo actual, maneja información sensible de gran importancia para el cumplimiento de sus metas y objetivos misionales, tal es el caso del proceso y almacenamiento de datos académicos y administrativos. Sin embargo no existe una política de seguridad de la información claramente definida lo cual genera riesgos y amenazas que pueden impactar negativamente en el desarrollo normal de sus procesos institucionales.

La Oficina General de Admisión (OGAD) de la UNASAM tiene como función fundamental coordinar, brindar asesoramiento técnico y apoyo logístico a la comisión de admisión para el desarrollo del proceso de admisión y por ello manejan gran cantidad de información respecto a cada proceso de admisión. Conforme a los objetivos de la UNASAM, la oficina ha ido implementando tecnologías de información para el soporte y ayuda de sus procesos y manejo de la información. Por lo que es un ente donde podría existir riesgo en la seguridad de la información por la preservación de la Disponibilidad, Integridad y Confidencialidad de la información. A partir de esta preocupación y además de la carencia de estrategias que salvaguarden la información en todo nivel dentro de la UNASAM, se procedió a la elaboración de un trabajo de investigación que permita avizorar los problema concernientes a la seguridad de la información dentro del OGAD, precisando como objeto de estudio la falta de políticas de seguridad y un sistema de gestión de seguridad de la información en dicha oficina.

Por tales motivos, el propósito de este proyecto de investigación es diseñar un Sistema de Gestión de Seguridad de la Información en la OGAD de la UNASAM mediante la aplicación de la norma ISO/IEC 27001:2013, con el fin de clasificar los riesgos y amenazas a los que están expuestos los activos de la información, elaborar un documento de aplicabilidad de controles de la norma, mantener la continuidad del negocio y dar soporte a los procesos de la oficina.

1.2. Enunciado del problema

¿En qué medida influye el diseño de un Sistema de Gestión de Seguridad de Información mediante la aplicación de la norma ISO/IEC 27001:2013 en la mejora de la Seguridad de la Información en la Oficina General de Admisión de la UNASAM?

1.3. Hipótesis

Con el diseño de un Sistema de Gestión de Seguridad de Información mediante la aplicación de la norma ISO/IEC 27001:2013 mejorará significativamente la seguridad de la información en la Oficina General de Admisión de la UNASAM.

1.4. Objetivos

1.4.1. Objetivo General

Diseñar un Sistema de Gestión de Seguridad de Información mediante la aplicación de la norma ISO/IEC 27001:2013 para mejorar la seguridad de la información en la Oficina General de Admisión de la UNASAM.

1.4.2. Objetivos Específicos

1) Analizar el estado actual en el que se encuentra la seguridad de la información en la Oficina General de Admisión de la UNASAM.

2) Identificar y evaluar los activos de la información de los procesos encontrados en la Oficina General de Admisión de la UNASAM.

3) Estudiar, evaluar y tratar los riesgos a los que están expuestos los activos de la información.

4) Elaborar la documentación de aplicabilidad requerida por la norma para el Sistema de Gestión de Seguridad de la Información.

1.5. Justificación

1.5.1. Justificación teórica

Se justifica la investigación a nivel teórica por el desarrollo del documento del Sistema de Gestión de Seguridad de la Información la cual permitirá poseer las políticas de seguridad para así poder cumplirlas en el ámbito de la Oficina.

1.5.2. Justificación operativa

Ayudará a mejorar la gestión de los procesos en la Oficina General Admisión puesto que al contar con procedimientos ordenados y documentados, se podrá determinar las medidas necesarias para un adecuado tratamiento de la información asimismo identificar los mecanismo para salvaguardarla evitando pérdidas, invasión de la privacidad de la misma. Permitiendo asegurar la confidencialidad, la disponibilidad e integridad de los procesos (activos e instalaciones) de la oficina en un marco de cumplimiento de la Norma ISO/IEC 27001:2013. Esta oficina cuenta con el personal calificado, el cual fácilmente puede ser capacitado para garantizar el cumplimiento de los lineamientos que se establezcan en cuanto a la seguridad informática, no presentando mayores inconvenientes si se hace de manera oportuna.

1.5.3. Justificación tecnológica

El presente proyecto se justifica tecnológicamente factible puesto que con el pasar de los años la oficina ha ido mejorando su tecnología de la información y porque el SGSI adoptara y establecerá un conjunto de controles establecidos por la norma ISO/IEC 27001 para reducir las amenazas que pueda afectar los procesos de la oficina y garantizar la continuidad del negocio.

1.5.4. Justificación social

Permitirá mejorar la gestión de los procesos y de los riesgos en la OGAD, lo cual es verá reflejado en la mejora de la calidad del servicio al contar con información debidamente salvaguardada y con controles adecuados, por lo que puedan brindar un servicio eficiente y segura a la población.

1.5.5. Justificación económica

El presente proyecto es económicamente viable porque llega hasta la fase de diseño, obteniendo al final una propuesta (Declaración de Aplicabilidad) que dependerá de las autoridades la aplicación y puesta en marcha de la misma.

1.5.6. Justificación normativa

El presente proyecto tiene su justificación legal en la ISO/IEC 27001:2013, un estándar para la seguridad de la información, para que sean seleccionadas por las organizaciones en el diseño de sus SGSI. Este fue aprobado y publicado como estándar internacional en octubre de 2005 por la ISO y por la comisión IEC. Que,

mediante Resolución Ministerial Nº 129-2012-PCM se estableció un nuevo cronograma y la incorporación del rol del oficial de seguridad para el proceso de implementación de la Norma Técnica Peruana "NTP-ISO /IEC 27001:2008", además teniendo en cuenta la Resolución Ministerial N° 004-2016-PCM, donde aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014, en todas las entidades integrantes del Sistema Nacional de Informática.

1.5.7. Justificación practica

Por medio del presente estudio se podrá utilizar el SGSI como marco normativo para poder realizar todas las actividades relacionadas al uso de las tecnologías de la información y comunicación dentro de la Oficina.

1.6. Limitaciones

La propuesta y diseño del proyecto se llevará a cabo en la Universidad Nacional Santiago Antúnez de Mayolo, específicamente en la Oficina General de Admisión.

- El presente proyecto de tesis consiste en el diagnóstico, análisis y diseño de un Sistema de Gestión de Seguridad de la Información para la Oficina General de Admisión, basado en la norma ISO/IEC 27001:2013, pero no abarca las fases de implementación, revisión y mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información.

- En el presente proyecto de tesis no se aplicó la propuesta de declaración de aplicabilidad ya que es decisión de las autoridades de la Universidad poner en marcha y la disposición de este.

- La presente tesis plantea algunos controles, que serán indispensables para proteger los activos de información más importantes en la Oficina General de Admisión, pero si cambia alguna regulación a nivel nacional e incluso internacional, la cual le exija a la oficina muchos controles extras, la propuesta que se plantea no podrá abarcar esa necesidad contractual.

1.7. Descripción y sustentación de la solución

El presente proyecto de tesis propone el Diseño de un SGSI mediante la aplicación de la norma ISO/IEC 27001:2013 para mejorar la seguridad de la información en la Oficina General de Admisión, que mediante la aplicación de la metodología de mejora continua PHVA se lograra el objetivo y que a continuación detallaremos:

Planear: Establecer política, objetivos, procesos y procedimientos para un SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.

Acciones a realizar: Definir el problema a resolver, la forma en que se buscara resolverlo, definir el objetivo general y objetivos específicos, definir el alcance y las limitaciones que tendrá el proyecto de tesis, realizar la planificación temporal del proyecto y elegir los métodos y procedimientos que se emplearan.

Hacer: Implementar y operar la política, controles, procesos y procedimientos de un SGSI.

Acciones a realizar: Desarrollo del proyecto, documentar y controlar las acciones realizadas, levantar información, implementación del SGSI para el tipo de empresa seleccionada, etc.

Verificar: Valorar donde sea aplicable y medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas de SGSI y reportar los resultados para su revisión.

Acciones a realizar: Después del desarrollado e implementado el SGSI, volver a revisar los datos obtenidos y analizarlos, comparándolos con los objetivos específicos iniciales, para evaluar si se han obtenido los resultados esperados.

Actuar: Realizar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.

Acciones a realizar: Modificar y corregir algunos aspectos errados encontrados en la etapa anterior, con el fin de garantizar que se obtengan los resultados esperados del proyecto, aplicar mejoras y terminar de documentar todo el proyecto.

El presente proyecto solo abarca el análisis y diseño del SGSI, por lo que solo se tomó en cuenta las etapas de “Planear” y “Hacer” de la metodología PHVA, para las otras dos fases se estableció solo pautas a seguir, como base el proyecto.

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes

2.1.1. Antecedentes internacionales

- Moyano y Suarez (2017), en su tesis “Plan de Implementación del SGSI basado en la Norma ISO 27001:2013 para la Empresa Interfaces y Soluciones”, cuyo objetivo fue Establecer un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la Norma ISO 27001:2013 para los procesos del área de Tecnología de la Información en la Empresa Interfaces y Soluciones. Concluyo: La gestión de riesgo realizada en la compañía estableció las bases para la mejora continua del SGSI. Por lo tanto se identificaron y clasificaron los activos, se identificaron las amenazas, las vulnerabilidades y se estimaron los riegos de acuerdo a los criterios de confidencialidad, disponibilidad e integridad de la seguridad de la información y prioridades de la organización.

- Ardila Navarrete (2016), en su tesis “Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma ISO/IEC 27001 para Positiva Compañía de Seguros S.A en la Ciudad de Bogotá”, cuyo objetivo fue Diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) para la Casa Matriz de Positiva Compañía de Seguros S.A. en la ciudad de Bogotá; basado en la Norma NTC-ISO-IEC 27001:2013, con tipo de investigación Descriptiva. Concluyo: El diseño de un Sistema de Gestión de Seguridad de la Información basado en el estándar ISO/IEC 27001:2013,

permite identificar los aspectos relevantes a tener en cuenta a la hora de establecer un modelo de seguridad de la información sólido y sostenible.

- Bermúdez y Bailón (2015), en su tesis “Análisis en Seguridad Informática y Seguridad de la Información basado en la Norma ISO/IEC 27001 - Sistemas de Gestión de Seguridad de la Información dirigido a una Empresa de Servicios Financieros”, cuyo objetivo fue analizar los procesos críticos de Credigestión respecto a las gestiones de seguridad adecuadas para garantizar confidencialidad, integridad y disponibilidad de la información, mediante la formulación recomendaciones de seguridad y controles basado en la norma ISO/IEC 27001, con tipo de investigación descriptiva. Concluyo: el análisis realizado demuestra que los activos de información de las áreas consideradas críticas y la situación actual de la empresa con respecto a la seguridad de la información, refleja potencial de índices de riesgo, los cuales exponen a la información de daños, robo y modificaciones que puedan causar un impacto negativo dentro de las actividades del negocio.

2.1.2. Antecedentes nacionales

- Vilca Mosquera (2017), en su tesis “Diseño e Implementación de un SGSI ISO 27001 para la Mejora de la Seguridad del Área de Recursos Humanos de la Empresa Geosurvey de la Ciudad de Lima”, cuyo objetivo fue determinar la relación entre Sistema de Gestión de la Seguridad de la Información y el Seguridad en la empresa GEOSURVEY S.A., con tipo de investigación enfoque cuantitativo, diseño pre experimental. Concluyo: Se logró una

optimización en los procesos de capacitación y formación de seguridad en cuanto al uso de la información y equipos en la empresa GEOSURVEY tras la intervención.

- Atalaya Vásquez (2016), en su tesis "Propuesta de un Sistema de Seguridad de la información para la oficina de Admisión y Registro Académico de la Universidad privada Antonio Guillermo Urrelo, 2016", cuyo objetivo fue Diagnosticar y formular una propuesta para el Departamento de Admisión y registro Académico de la Universidad privada Antonio Guillermo Urrelo – 2016", tomo a la ISO/IEC 27000 como la estrategia a seguir para proponer un SGSI. Concluyo que los activos del DARA tienen riesgos que podría afectar la continuidad de los procesos.

- Santos Llanos (2016), en su tesis "Establecimiento, Implementación, Mantenimiento y Mejora de un Sistema de Gestión de Seguridad de la Información, Basado en la ISO/IEC 27001:2013, para una Empresa de Consultoría de Software", cuyo objetivo fue desarrollar un Sistema de Gestión de Seguridad de Información (SGSI) para una empresa de consultoría en desarrollo y calidad de software, tomando como marco normativo el estándar ISO/IEC 27001:2013, concluyo que para elaborar adecuadamente los componentes que permitan cumplir los requisitos del estándar 27001 deben considerarse aquellos estándares que, aunque no son referenciados, forman parte del dominio de algunos de los requisitos del SGSI.

- Zavaleta Rodríguez (2016), en su tesis “Implementación de un Sistema de Gestión de Seguridad de la Información aplicando NTP ISO/IEC 27001:2014 en el sector Hospitalario, 2016”, cuyo objetivo fue proponer la implementación un sistema de gestión de seguridad de la información para hospitales, de acuerdo a la NTP ISO/IEC 27001:2014, con un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de la organización para conseguir los objetivos de negocio, con tipo de investigación enfoque holístico, diseño tipo transversal. Concluyo: La propuesta de implementar un sistema de gestión de seguridad de la información aplicando la norma NTP ISO/IEC 27001:2014, va a permitir una reducción en los riesgos ya que implica una reducción en los costos, asegura la rentabilidad de la inversión realizada en materia de seguridad, mayor prestigio y credibilidad en el mercado y a la vez alinearse con las normas legales que están determinadas.

2.1.3. Antecedente local

- Benites Arango (2017), en su tesis “Implementación de una Guía Metodología Basada en la NTP ISO/IEC 27001:2008, NTP ISO/IEC 17799:2007 y COBIT 5 para Mejorar la Seguridad de la Información en la Municipalidad Distrital de Tarica - 2014”, cuyo objetivo fue determinar la relación entre Guía Metodología Basada en la NTP ISO/IEC 27001:2008, NTP ISO/IEC 17799:2007 y COBIT 5 y la Mejora de Seguridad de la Información, con tipo de investigación de análisis de datos aplicada y

descriptiva. Concluyo: con la implementación de la Guía Metodológica mejoro considerablemente el nivel de seguridad de los activos de la información con el 43% alto y muy alto de aceptación del personal de la municipalidad.

- Mory Garay (2015), en su tesis "Aplicación de la Norma ISO 27001 para mejorar la Seguridad de la Información en la Empresa HM Contratistas S.A." cuyo objetivo fue Diseñar un Sistema de Gestión de Seguridad de Información basado en la aplicación de la norma ISO/IEC 27001 para mejorar la seguridad de la información en la empresa HM Contratistas S.A. de la ciudad de Huaraz, con tipo de investigación experimental, concluyo: que la empresa no cuenta con un comité responsable de seguridad de información que estructure un plan estratégico encaminado a proteger los activos de información así mismo de las políticas controles y amenazas.

2.2. Teorías que sustentan el trabajo

2.2.1. Sistema de Gestión de Seguridad de la Información

Un SGSI consiste en políticas, procedimientos, directrices, recursos asociados y actividades, gestionadas colectivamente por una organización, en la búsqueda de la protección de sus activos de información. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos de negocio. Se basa en la evaluación del riesgo y los niveles de aceptación del riesgo de la organización, diseñada para tratar y gestionar los riesgos de manera

efectiva. Analizar requisitos para la protección de los activos de información aplicar los controles adecuados para garantizar su protección, según sea necesario, contribuye a la implementación exitosa de un SGSI. (ISO/IEC 27001).

a) Seguridad informática

Seguridad Informática, es la disciplina que se encarga de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que articulados con prácticas de gobierno de tecnología de información establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo.

b) Seguridad de la información

Es el conjunto de medidas preventivas y reactivas de las organizaciones que permiten resguardar y proteger la información buscando mantener las dimensiones (confidencialidad, disponibilidad e integridad) de la misma. (ISO/IEC 27001).

Dimensiones de la Seguridad de la Información:

- **Confidencialidad:** Es la propiedad que impide la divulgación de información a personas o sistemas no autorizados, asegura el acceso a la

información únicamente a aquellas personas que cuenten con la debida autorización.

- **Disponibilidad:** Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

- **Integridad:** Es mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados y busca mantener los datos libres de modificaciones no autorizadas.

c) Activos de la información

Se denomina activo a aquello que tiene algún valor para la organización y por tanto debe protegerse. De manera que un activo de información es aquel elemento que contiene o manipula información.

Activos de información son ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, software del sistema, equipos informáticos, equipo de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales como por ejemplo calefacción, iluminación, energía y aire acondicionado y las personas, que son al fin y al cabo las que en última instancia generan, transmiten y destruyen información, es decir dentro de

un organización se han de considerar todos los tipos de activos de información

d) Gestión de riesgos

La gestión de riesgos implica seleccionar e implantar las medidas técnicas y organizativas necesarias para impedir, reducir o controlar los riesgos identificados, de forma que los perjuicios que puedan causar se eliminen o, si esto no es posible, se reduzcan lo máximo posible.

Un resultado del análisis de riesgos habrá sido el criterio para determinar cuáles van a ser los niveles de riesgo aceptables y, en consecuencia, cuáles van a ser los niveles inaceptables y que por lo tanto son susceptibles de ser gestionados.

Amenazas: En las organizaciones, los activos de información están sujetos a distintas formas de amenazas. Una amenaza es todo aquello, ya sea físico o lógico que puede causar un incidente no deseado, generando daños materiales o inmateriales a la organización y a sus activos, como la perdida de información, o de su privacidad, o bien un fallo en los equipos físicos.

Vulnerabilidades: Las vulnerabilidades son debilidades de seguridad asociadas con los activos de información de una organización.

Impacto: El impacto en un activo es la consecuencia sobre éste de la materialización de una amenaza.

Impacto: El impacto en un activo es la consecuencia sobre éste de la materialización de una amenaza. De forma dinámica, es la diferencia en las estimaciones del estado de seguridad del activo antes y después de la materialización de la amenaza sobre éste.

Riesgos: El riesgo es la posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.

El proceso de identificación y evaluación de riesgos y el de clasificación de activos, permite determinar qué tan expuestos se encuentran los activos de información a ataques por la presencia de vulnerabilidades propias o inherentes a la actividad de la organización. (CNB - INDECOPI, 2008)

Controles: Son las políticas, procedimientos, prácticas y estructuras organizacionales para reducir riesgos y que además proveen cierto grado de certeza de que se alcanzaran los objetivos del negocio [ISACA, 2011].

e) Análisis y valoración de los riesgos

En primer lugar, conviene clarificar qué se entiende por riesgo. Dentro del contexto de un análisis de riesgos, es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente.

Antes de saber qué es un análisis de riesgos y lo que conlleva es importante conocer qué son otro tipo de conceptos muy relacionados con los Análisis de Riesgos y la seguridad de la información. Estos son los más importantes:

Amenaza: es la causa potencial de un daño a un activo.

Vulnerabilidad: debilidad de un activo que puede ser aprovechada por una amenaza.

Impacto: consecuencias de que la amenaza ocurra.

Riesgo intrínseco: cálculo del daño probable a un activo si se encontrara desprotegido.

Salvaguarda: medida técnica u organizativa que ayuda a paliar el riesgo.

Riesgo residual: riesgo remanente tras la aplicación de salvaguardas.

El análisis de riesgos se define como la utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

A la hora de diseñar un SGSI, es primordial ajustarse a las necesidades y los recursos de la organización para que se puedan cubrir las expectativas, llegando al nivel de seguridad requerido con los medios disponibles. Es relativamente sencillo calcular con cuántos recursos se cuenta (económicos, humanos, técnicos, etc.) pero no es tan fácil saber a ciencia cierta cuales son las necesidades de seguridad.

Hacer un análisis de riesgos permite averiguar cuáles son los peligros a los que se enfrenta la organización y la importancia de cada uno de ellos. Con esta información ya será posible tomar decisiones bien fundamentadas acerca de qué medidas de seguridad deben implantarse.

2.2.2. Normatividad y modelos

Familia de Normas ISO/IEC 27000

La Organización Internacional para la Estandarización ISO por sus siglas en inglés se encarga de publicar estándares sobre diferentes temas que tienen una gran importancia en diferentes aspectos relacionados con el comercio, fabricación, etc. Siguiendo el constante crecimiento que ha tenido el desarrollo del campo de las Tecnologías de Información, dicho ente ha emitido varios estándares que regulan el ciclo de DEMING del software, estándares de calidad, sistemas de información y seguridad de la información.

Correspondiente a este último grupo, se realizó la publicación de la familia de normas de la serie 27000, enfocadas directamente a la estandarización de los aspectos relacionados con la gestión de la seguridad de la información en las empresas y organizaciones que requieran contar con sistemas de gestión para este fin. A continuación, se detallan las principales normas pertenecientes a esta serie, algunas de las cuales servirán de soporte para realizar los procesos requeridos para completar el presente proyecto.

- **ISO 27001:2013**, Information security management systems Requirements

Especifica los requisitos a cumplir para poder establecer el Sistema de Gestión de Seguridad de la Información.

- **ISO 27002:2013**, Code of practice for information security controls

Presenta una guía de recomendaciones y buenas prácticas a seguir en la gestión de seguridad de la información.

Dado el alcance del presente proyecto, se utilizarán las normas ISO 27001 como soporte de la implementación de lo indicado por la Norma Técnica Peruana 27001.

Norma Técnica Peruana NTP ISO/IEC 27001

Es una norma elaborada por el Comité Técnico Permanente de Codificación e Intercambio Electrónico de Datos, publicada en el año 2009 y establecida como de uso obligatorio mediante la Resolución Ministerial N° 129-2012-PCM el año 2012, se encuentra alineada al estándar ISO/IEC 27001 - estándar internacional publicado en el año 2005 que provee un modelo a seguir para el establecimiento y mantenimiento de un SGSI. El objetivo principal de esta norma es establecer los requisitos que se deben cumplir para la implementación del SGSI utilizando un enfoque a procesos, lo cual requiere que se tenga disponible la mayor cantidad de documentación respecto a los mismos.

La norma utiliza la metodología Plan-Do-Check-Act, también llamado ciclo de Deming para definir las fases de vida y mejora continua del SGSI a través de un seguimiento de este que asegura el mantenimiento de los controles y los cambios

necesarios para poder mitigar los posibles nuevos riesgos que aparezcan luego de la implementación del sistema. A continuación, se presenta un diagrama que detalla las etapas de esta metodología.

El diseño del SGSI siguiendo las fases del ciclo de Deming comprende las siguientes etapas:

- Establecimiento

Se dan las recomendaciones a seguir para establecer el alcance que tendrá el sistema sobre la organización sobre la que se está trabajando. A continuación, se realiza un análisis de identificación de activos de información en conjunto con los riesgos y amenazas a los que se encuentran expuestos, además de realizar la valoración tanto de los activos como de los riesgos asociados y los posibles controles que podrían implementarse para mitigar los mismos.

- Implementación

En esta fase se implementan las políticas y planes de mitigación que se requieren para poder tratar el riesgo identificado en el alcance del sistema. Como parte de esta etapa se detallan las acciones específicas que se deben realizar como parte del plan de mitigación.

- Monitoreo y revisión

El establecimiento de políticas que rijan los procesos desde el punto de vista de la seguridad de los activos de información que los mismos utilizan, requiere que

se establezcan también métricas y procedimientos con los cuales se pueda evaluar su eficiencia y determinar si es necesario realizar algún cambio para mejorar su desempeño, el cual es el objetivo principal de esta etapa.

- Mantenimiento y mejora continúa

Luego de realizar las evaluaciones de desempeño del SGSI en la etapa anterior, se puede identificar cambios que son necesarios para reajustar el alcance o mejorar su eficacia en el control de riesgos.

Esto, sumado a que el SGSI es una entidad que continua vigente a lo largo del tiempo de vida de la organización, hace que el mantenimiento de este sea una tarea crítica como parte de su ciclo de DEMING.

Recientemente, mediante la Resolución Ministerial N°129-2012/PCM (PRESIDENCIA DEL CONSEJO DE MINISTROS, 2012), fue aprobado el uso obligatorio de esta norma para todas las entidades que pertenezcan al Sistema Nacional de Informática entre ellas el Ministerio de Salud y todas sus dependencias – siguiendo el cronograma de implementación incremental determinado por la Oficina Nacional de Gobierno Electrónico e Informática, el cual determina las fases y duración del desarrollo de estas.

Para el presente proyecto de fin de carrera, además de seguir los requisitos establecidos por la presente norma. Debido a su carácter de obligatoriedad, está estrechamente relacionada con la problemática que ataca este proyecto y representa uno de los documentos más importantes a seguir durante el desarrollo

del Sistema de Gestión de Seguridad de la Información. 2008 (CNB - INDECOPI, 2008) (ISO 27001, 2013)

La norma ISO 27002

La ISO 27002 es una guía de buenas prácticas de seguridad de la información que presenta una extensa serie de controles de seguridad. Es la única norma que no sólo cubre la problemática de la seguridad de las tecnologías de información, sino que hace una aproximación holística a la seguridad de la información corporativa, abarcando todas las funcionalidades de una organización en cuanto a la seguridad de la información que maneja. La norma considera también los riesgos organizacionales, operacionales y físicos de una empresa, con todo lo que esto implica. (AltoSec Blog).

Desde el 1 de julio de 2007, la ISO 27002 es el nuevo nombre de ISO 17799:2005. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable, sólo hace recomendaciones sobre el uso de 133 controles de seguridad diferentes aplicados en 11 áreas de control o dominios.

MAGERIT

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información nace como una iniciativa por parte del Consejo Superior de Informática, entidad perteneciente al Gobierno Español como respuesta a la

regulación establecida en el Real Decreto 3/2010 el cual regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Esta metodología de gestión de riesgos tiene los siguientes objetivos:

1) Concientizar a los responsables de las organizaciones sobre la presencia de riesgos y la necesidad e importancia de gestionarlos.

2) Ofrecer un método para analizar los riesgos a los que estén expuestos los activos de información.

3) Descubrir y planificar los controles a implementar para mitigar y controlar los riesgos.

4) Preparar a la organización para los futuros procesos de evaluación, auditoría o certificación que pueda requerir.

El esquema de trabajo que sigue la presente metodología permite cubrir todos los resultados referentes al análisis, documentación y control de los riesgos a los que se encuentra expuesta la información de la organización. Esto se puede ver en los pasos que la metodología establece para realizar el análisis de riesgos:

a) Determinar los activos relevantes para la organización, su interrelación y su valor (entendido como el costo de que éstos se vean afectados como consecuencia de algún riesgo).

b) Determinar las amenazas a las que se encuentran expuestos los activos identificados.

c) Determinar las medidas de protección actuales y la eficacia de estas frente al riesgo.

d) Estimar el impacto, es decir el daño que ocasionaría al activo de información la materialización de una amenaza.

e) Estimar el nivel de riesgo, el cual se calcula utilizando el impacto ponderado con la tasa de ocurrencia que se espera de la amenaza.

Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista (MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS, 2012 - España).

2.3. Definición de términos

Investigación: Está determinada por la averiguación de datos o la búsqueda de soluciones para ciertos inconvenientes.

Norma: Regla o conjunto de reglas que hay que seguir para llevar a cabo una acción, porque está establecido o ha sido ordenado de ese modo.

ISO: Organización de Estandarización Internacional Internacional (ISO/IEC 27000, 2014).

Activo: Algo que tenga valor para lo organización. Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información,

datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [ISO 13335].

Amenaza: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización. [ISO 13335]

Análisis de riesgos: Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

Confidencialidad: Propiedad o característica consistente en que la información ni se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. [ISO 13335]

Control: Herramienta de la gestión del riesgo, incluido: políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal. [ISO 27002]

Disponibilidad: Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados [ISO 13335]

Enunciado de aplicabilidad: Enunciado documentado que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de la organización. [ISO 27001]

Integridad: Propiedad o característica consistente en que el activo no ha sido alterado de manera no autorizada. [ISO 27000]

OGAD: Oficina General de Admisión

Admisión: Proceso de selección de un grupo por medio de concurso bajo una prueba. (Definición OGAD)

Postulante: Persona que se inscribe al proceso de admisión. (Definición OGAD)

Vulnerabilidad: Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza. Propiedades intrínsecas de que algo se produzca como resultado de una sensibilidad a una fuente de riesgo que puede conducir a un suceso con una consecuencia.

Control: Herramienta de la gestión del riesgo, incluido: políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal (ISO/IEC 27000, 2014).

Proceso: Conjunto de actividades interrelacionadas y ordenadas que transforman unas entradas en salidas (ISO/IEC 27000, 2014).

CID: Acrónimo en español de confidencialidad integridad y disponibilidad, las dimensiones básicas de la seguridad de la información (ISO/IEC 27000, 2014).

Alcance: Ámbito de la organización que queda sometida al SGSI (ISO/IEC 27000, 2014).

CAPÍTULO III: MÉTODOS Y MATERIALES

3.1. Materiales

3.1.1. Instrumentos usados

3.1.1.1. Laboratorios

Las instalaciones de la Facultad de Ciencias, así como también la Oficina General de Admisión en su conjunto.

3.1.1.2. Software

- Sistema Operativo Windows 10
- Microsoft Word 2016
- Microsoft Excel 2016
- Microsoft PowerPoint 2016
- Microsoft Visio 2016

3.1.1.3. Hardware

- Computadora personal
- Computadora portátil
- Impresora Multifuncional
- Disco duro externo
- Memoria USB

3.1.2. Población y muestra

3.1.2.1. Población

La población es el personal directivo, técnico y de apoyo que participa en el proceso de admisión en el año 2018, como se muestra en la siguiente tabla:

Tabla 3.1
Población

N°	Descripción	Población total
1	Personal	14

Fuente: OGAD

3.1.2.2. Muestra

Tabla 3.2
Muestra

N°	Descripción	Población	Muestra
1	Personal	14	14
		Total	14

Fuente: Elaboración Propia.

Tamaño de muestra para una proporción; siendo el tamaño de muestra igual a 14 para la población, teniendo en cuenta un nivel de confianza del 95%, error de muestreo de 5% y uso de la fórmula general.

Tamaño de muestra de la población:

$$n = \frac{NZ^2PQ}{e^2(N-1) + Z^2PQ}$$

Donde:

N=35 (Población),
Z=1.96 (Nivel de confianza del 95%),
P=0.5 (Proporción de éxito),

Q=0.5 (Proporción de fracaso) y
e=0.05 (Margen de error).

3.1.2.3. Muestreo

Para el presente trabajo de investigación el tipo de muestreo elegido fue no probabilístico.

3.2. Métodos

3.2.1. Tipo de investigación

3.2.1.1. De acuerdo a la orientación

Es aplicada, porque se buscó la aplicación o utilización del conocimiento adquirido relacionado con instrumento teórico y metodológico, la cual está basada en el diseño de un sistema de gestión de seguridad de la información.

3.2.1.2. De acuerdo a la técnica de contrastación

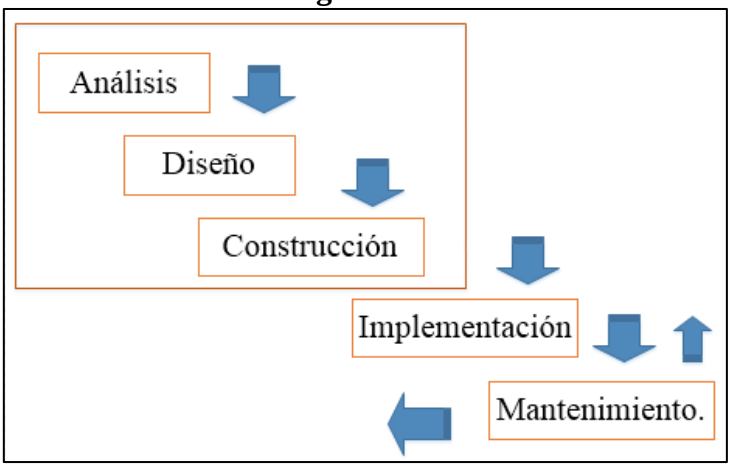
Es descriptiva, puesto que se basó en la observación directa de la situación actual y se obtuvo datos en relación a las necesidades, problemas u oportunidades de mejora, sin la manipulación o alteración.

3.2.2. Metodología de desarrollo

El presente proyecto de investigación se fundamenta utilizando la metodología del “Ciclo de vida del Software” de Roger Pressman, la cual tiene una mejor afinidad con el tema de la tesis.

De acuerdo a Roger Pressman, las etapas metodológicas o fases del ciclo de vida del sistema de información se establecen de la siguiente manera: Análisis, Diseño, Construcción, Implementación y Mantenimiento.

Gráfico 3.1.
Metodología de desarrollo



Fuente: Roger Pressman

En la siguiente investigación por ser un tipo de investigación descriptiva, se desarrollara las dos primeras etapas del ciclo de vida de Roger Pressman, basándonos en la estructura del informe de tesis del reglamento de grados y títulos de la escuela profesional de ingeniería de sistemas e informática, y en el reglamento del PTCT-FC-UNASAM-2018.

3.2.3. Definición de variables

3.2.3.1. Variables independiente (VI)

Aplicación de la Norma ISO/IEC 27001

3.2.3.2. Variable dependiente (VD)

Seguridad de la información

3.2.4. Operacionalización de variables

Tabla 3.3
Matriz de operacionalización de variables

Investigación	Objetivo	Hipótesis	Variables	Dimensiones	Indicadores	Escala
	General	**General**	**Independiente**			
Aplicación de la Norma ISO/IEC 27001 para Mejorar la Seguridad de la Información en la Oficina General de Admisión de la Universidad Nacional Santiago Antúnez de Mayolo.	Diseñar un Sistema de Gestión de Seguridad de Información mediante la aplicación de la norma ISO/IEC 27001:2013 para mejorar la seguridad de la información en la en la Oficina General de Admisión de la UNASAM.	Con el diseño de un Sistema de Gestión de Seguridad de Información mediante la aplicación de la norma ISO/IEC 27001:2013 mejorará significativamente la seguridad de la información en la Oficina General de Admisión de la UNASAM.	Aplicación de la Norma ISO/IEC 27001	Sistema de Gestión de Seguridad de la Información	Políticas de seguridad Identificación y valoración de activos Identificación de Amenazas	Muy Alto Alto Medio Bajo Muy Bajo
	Especifico		**Dependiente**			
	- Realizar un análisis de la situación actual acorde a los dominios y objetivos de control de la norma ISO/IEC 27001:2013. - Identificar y evaluar los activos de la información a los procesos encontrados en la OGAD de la UNASAM. - Identificar, analizar los riesgos y valorar dichos riesgos a los que están expuestos los activos encontrados. - Elaboración la documentación requerida por la norma para el Sistema de Gestión de Seguridad de la Información.		Mejorar la Seguridad de la Información	Seguridad de la información	Nivel de riesgos de la información Tratamiento de riesgos de la información Declaración de Aplicabilidad	Muy Alto Alto Medio Bajo Muy Bajo

Fuente: Elaboración propia

3.2.5. Diseño de investigación

El diseño de la investigación está dado bajo un enfoque no experimental ya que "se realiza sin manipular deliberadamente las variables" y se observan los fenómenos tal como se dan en su contexto natural para su posterior análisis. Dicho esto, el diseño de investigación apropiado, bajo el enfoque anterior, es el transversal o transaccional, ya que recopila datos en un momento único y "su propósito es describir variables y analizar su incidencia e interrelación en un momento dado".

3.3. Técnicas

3.3.1. Instrumento de recolección de datos

- **Observación:** Es el método con el que iniciamos para definir algunos análisis y la problemática en una primera instancia en el área en estudio, ya que nos permite observar los hechos tal cual son y ocurren, y sobre todo aquellos que son de interés y significativos para la investigación.

- **Análisis documental:** La investigación de estudio requirió realizar una selección de información por parte del tesista, asimismo los usuarios hicieron llegar algunas quejas y sugerencias para el control de su información.

- **Entrevista:** Esta dinámica de preguntas y respuestas abiertas, para socializar sobre la temática de estudio, relacionada con la problemática.

- **Encuesta:** Es el estudio observacional que se realizó, que no debe ser modificado ni alterado, se ha elaborado de acuerdo a los indicadores de la tabla de operacionalización de variables, en base a preguntas.

3.3.2. Técnicas de procesamiento de información

La presente investigación utilizó las siguientes técnicas de recopilación y procesamiento de información:

- Encuestas dirigidas al personal que labora en un proceso admisión, procesadas en Microsoft Excel, lo cual nos permitirá obtener un consolidado de los resultados, así como gráficos para su interpretación.

- Análisis de las entrevistas realizadas (guía de entrevistas), así como también de los documentos, libros y guías (digital e impreso) que se estén empleando para la realización de este proyecto.

- Análisis de las observaciones realizadas durante la recopilación de información.

En base a estas técnicas de procesamiento de información, se establece la situación actual de la oficina y las necesidades a ser resueltas en base al problema planteado.

3.4. Procedimiento

Para el diseño de un Sistema de Gestión de Seguridad de la Información basado en la aplicación de la norma ISO/IEC 27001:2013, se realizó lo siguiente:

1) Definir el Alcance. Determinar el departamento, servicios y procesos sobre los cuáles aplicará el Sistema de Gestión de la Seguridad de la Información.

2) Realizar el Análisis Diferencial. Realizar el Análisis Diferencial de los Dominios, Objetivos de Control y Controles de Seguridad (ISO/IEC 27002:2013) de acuerdo al Anexo A del estándar ISO 27001:2013.

3) Definir la Política de Seguridad. Determinar los objetivos primordiales relativos a la seguridad de la información y en base a las necesidades de la institución, estableciendo los lineamientos generales conformes a garantizar la confidencialidad, integridad y disponibilidad de la información.

4) Identificar los Activos de Información. Realizar el levantamiento de los activos de información que serán abarcados por el Sistema de Gestión de la Seguridad de la Información.

5) Definir la Metodología de Análisis y Evaluación de Riesgos. Definir la Metodología de Evaluación de Riesgos y realizar el Análisis de Riesgos de los activos de información inventariados e identificar las vulnerabilidades y amenazas.

6) Tratamiento de Riesgos. Definir la forma en cómo se tratarán los riesgos.

7) Declaración de aplicabilidad. Definir el documento de aplicabilidad.

CAPÍTULO IV: ANÁLISIS

4.1. Análisis de la situación actual

La Universidad Nacional Santiago Antúnez de Mayolo, fue fundada el 14 de junio de 1987, su sede principal se encuentra ubicada en la Av. Centenario N° 200, distrito de Independencia, provincia de Huaraz, región Ancash. La universidad desde sus inicios tuvo una álgida preocupación por permanecer en constante desarrollo tecnológico y científico, con miras a convertirse en una de las mejores universidades nacionales, brindando una educación de calidad y formando profesionales competitivos y acordes a nuestra realidad. Para ello, de manera institucional, ha sido conformada por distintos órganos de apoyo que en conjunto con los altos mandos, se espera que lleven a esta universidad al cumplimiento de sus objetivos.

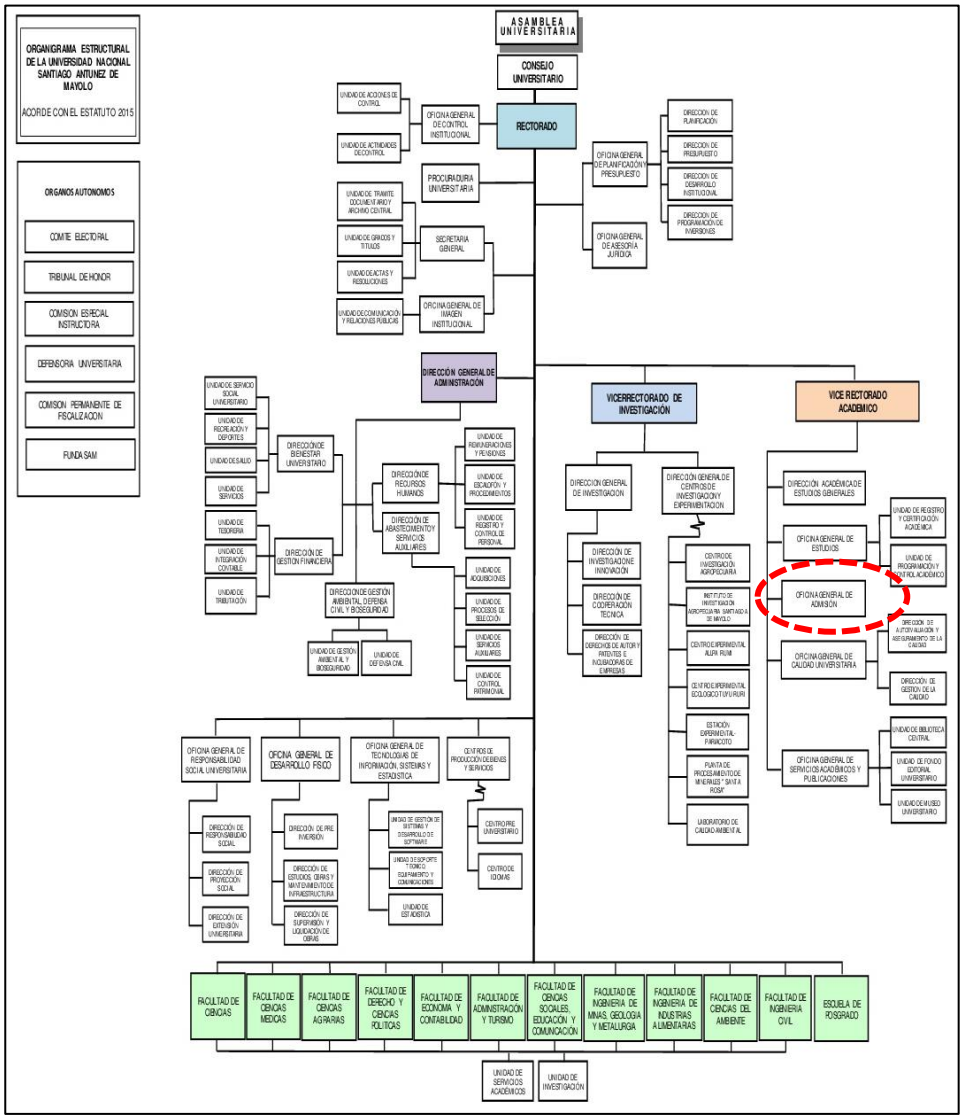
La Oficina General de Admisión de la UNASAM, es el órgano de línea dependiente del Vicerrectorado Académico, es la encargada de planificar, organizar y conducir los Procesos de Admisión a nivel de Pregrado, Posgrado y Segunda Especialización, de acuerdo a las modalidades y reglas establecidas en la Ley Universitaria, el Estatuto, el Reglamento General y su correspondiente reglamento. [ROF de la UNASAM]

La Oficina General de Admisión de la UNASAM busca establecer procesos y procedimientos que permita a los colaboradores de la oficina manejar y tratar la información dentro de los procedimientos de seguridad adecuados y establecidos.

4.1.1. Análisis del organigrama funcional estratégico

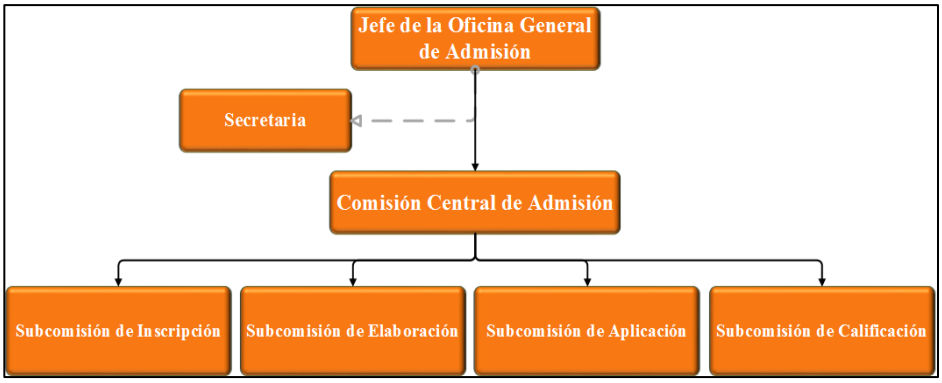
Para hacer un análisis del organigrama funcional, es necesario ubicar a la Oficina General de Admisión dentro del organigrama estructural de la UNASAM, como veremos a continuación:

Gráfico 4.1.
Organigrama estructural de la UNASAM



Fuente: Manual de Organización y Funciones de la UNASAM

Gráfico 4.2.
Organigrama estructural de la OGAD de la UNASAM



Fuente: Oficina General de Admisión de la UNASAM.

Como se muestra la estructura del organigrama tiene niveles, en el nivel superior se encuentra el jefe de admisión quien organiza, coordina, ejecuta y evalúa los estándares de evaluación académica al proceso de admisión. Así mismo brinda asesoramiento técnico y apoyo logístico a la comisión central de admisión. Estos son los responsables del buen funcionamiento e interrelación con las otras oficinas de la universidad.

4.1.2. Evaluación de la capacidad instalada

4.1.2.1. Personal

El personal que actualmente labora en la Oficina General de Admisión es el jefe, una secretaria, asistente administrativa y responsable del área informática. Así mismo se conforma la Comisión Central de Admisión por cada proceso de admisión, y se contrata un administrador de sistemas, administrador de base de datos, uno de soporte técnico, un asistente técnico de administración y uno de difusión, las competencias que presentan se puede observar en el Cuadro:

Cuadro 4.1
Competencias del personal implicado en la Oficina de General Admisión.

Personal	Funciones	Perfil
Jefe de la Oficina General de Admisión	• Organizar, coordinar, ejecutar y evaluar los estándares de evaluación académica al proceso de admisión. • Coordinar el proceso de admisión de postulantes con la comisión de admisión. • Brindar asesoramiento técnico y apoyo logístico a la comisión de admisión. • Formular el Plan Operativo Institucional. • Presentar la memoria anual para su aprobación ante el rectorado. • Conducir las reuniones de trabajo de la oficina.	• Título profesional universitario que incluya estudios relacionados con la especialidad. • Amplia experiencia en el proceso de admisión. • Capacitación especializada en el campo de su competencia.
Secretaria de la Oficina General de Admisión	• Recepcionar, revisar, registrar, distribuir y archivar los documentos de la Oficina y otras dependencias. • Redactar y dirigir los documentos administrativos de acuerdo a las normas de administración pública. • Organizar, ejecutar el control y mantener al día el registro de los expedientes de la Oficina de Admisión. • Efectuar acciones previsoras de conservación y seguridad de los bienes de la OGA. • Cumplir otras funciones que le asigne el Jefe de la OGA, según su competencia.	• Bachillerato en administración secretarial otorgado por una entidad autorizada. • Capacitación certificada en idiomas extranjeros otorgados por una entidad autorizada. • Amplia experiencia en labores de secretaria, contar con una experiencia mínima de cuatro años.
Responsable de informática y sistemas	• Participar en los diferentes procesos de admisión, con la supervisión del sistema informático	• Título profesional de ingeniero de sistemas • Tener experiencia en manejo de

	• Supervisar la implementación de los sistemas informáticos en la OGAD. • Evaluar y/o desarrollar los sistemas informáticos para el mejor funcionamiento de la OGAD.	sistemas informáticos

Fuente: Oficina General de Admisión de la UNASAM.

4.1.2.2. Equipos

La Oficina General de Admisión de la UNASAM actualmente cuenta con los siguientes equipos:

- Computadoras de escritorio
- Computadoras portátiles
- Lectoras de barras
- Impresoras
- Lectora de Tarjeta OMR
- Scaner

4.1.2.3. Análisis de fortalezas, oportunidades, debilidades y amenazas

Con el fin de identificar y analizar la situación actual de la Oficina General de Admisión de la UNASAM, se realizó un análisis FODA (Fortalezas, debilidades, Oportunidades y Amenazas) la cual permitió conocer la situación actual de la Oficina. Teniendo como base que el análisis FODA es un instrumento de planificación estratégica que permite la identificación y evaluación de las fortalezas y debilidades de la organización, así como las oportunidades y amenazas que esta presenta.

Cuadro 4.2
Análisis FODA de la Oficina de General Admisión.

Fortalezas	Oportunidades
• Posee un presupuesto por cada proceso de admisión. • Tener un sitio de información en la página web. • Tener un sistema de inscripción – admisión web. • Instalaciones adecuadas. • Cuenta con equipos de última generación. • Bajos costos por derechos de inscripción.	• La gratuidad de la enseñanza para los alumnos ingresantes al pregrado. • Ampliar el alcance a nivel nacional. • Incrementar el ingreso por cada proceso de admisión. • Realizar convenios con instituciones. • Ser los mejores desarrollando los procesos de admisión en la región.
Debilidades	**Amenazas**
• No se cuenta con personal permanente. • No se cuenta con estrategias dentro de la oficina. • Servicio de internet lento. • Deficiente coordinación con las diferentes áreas que involucran los procesos de admisión. • Pérdida de datos importantes.	• La inestabilidad de la organización. • Críticas por parte de los usuarios y la prensa. • El auge y crecimiento de universidades particulares en la Región • Desinterés por parte de los postulantes.

Fuente: Oficina General de Admisión.

4.2. Identificación y descripción de requerimientos

Concluido en análisis de la situación contextual actual, los requerimientos identificados son los siguientes:

- Definir una política de seguridad.
- Establecer el marco general y los objetivos de seguridad de la información de la empresa.
- Requerimientos legales o contractuales relativos a la seguridad de la información.

- Definir el contexto estratégico de gestión de riesgos de la empresa.
- Establezca los criterios con los que se va a evaluar el riesgo.
- Definir una metodología de evaluación del riesgo.
- Establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable.
- Identificar los riesgos.
- Identificar los activos que están dentro del alcance del SGSI.
- Identificar las amenazas en relación a los activos.
- Identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.
- 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.
- Determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.
- Identificar y evaluar las distintas opciones de tratamiento de los riesgos.

4.3. Diagnóstico de la situación actual

Cuadro 4.3
Diagnóstico de la Situación Actual

N°	¿Qué actividades se desarrolla en el proceso de Admisión?	¿Cómo lo hace?	¿Con qué lo hace?	¿Quién interviene?
01	**Información al postulante.**	El personal de informes brinda información a los postulantes sobre las fechas, precios y vacantes.	Se realiza con materiales físicos como: afiches, volantes, mosquitos.	• Postulante. • Personal de Inscripciones.
02	**Inscripción del postulante.**	El postulante se dirige a los módulos: Módulo 1: Entrega carpeta del postulante y recepciona comprobante de pago original y copia. Módulo 2: Guía y verifica el llenado de formatos de carpeta de postulante. Módulo 3: Verifica la carpeta de los postulantes esté completa y registra la tarjeta OMR al sistema de cómputo. Módulo 4: Toma fotografía y captura la huella dactilar del postulante, finalizando con la impresión y entrega del carnet.	Se realiza con materiales físicos como: carpetas, tarjetas OMR, hojas bond, carnet.	• Soporte de inscripciones. • Administrador del sistema.
03	**Elaboración de pruebas.**	El encargado de la subcomisión pide al administrador del sistema que le proporcione la relación de cantidad por aulas de todos los postulantes para el proceso de admisión, ya que de acuerdo a ello se elaboran la cantidad de exámenes.	Se realiza con una computadora.	• Administrador del sistema. • Encargado de la subcomisión de elaboración
04	**Publicación de listado de postulantes.**	El encargado de la subcomisión de aplicación pide al administrador del sistema la lista y el padrón de postulantes por aula, el cual se pega en las respectivas	Se realiza con una computadora y materiales físicos para los listados	• Administrador del sistema. • Encargado de la subcomisión de aplicación.

		aulas correspondientes para que posteriormente los postulantes realicen el reconocimiento de sus aulas.	de postulantes.	
05	**Aplicación del examen de admisión.**	El día del examen de admisión los alumnos ingresan previa identificación del carnet y revisión de objetos prohibidos al examen de admisión ingresan a sus salones, donde se registrarán en el padrón de postulantes y llenan tarjeta OMR de identificación.	Se realiza con materiales físicos.	• Postulantes. • Todos los miembros de la comisión central de admisión.
06	**Calificación del examen de admisión.**	El encargado de la subcomisión de calificación se encarga de pedir la relación de los postulantes con su respectivo código para entregados al calificador el cual registrada al sistema de la calificadora. Posteriormente del examen, se recaban las tarjetas de identificación de los postulantes para ser ingresadas al sistema de calificación. Luego debe esperar a recabar tarjeta de respuestas para ser registradas al sistema y dar paso a dar los resultados de la calificación donde da el visto bueno un notario.	Se lleva acabo con materiales físicos como tarjetas OMR y un sistema de calificación.	• Encargado de la subcomisión de aplicación. • Calificador. • Notario.
07	**Publicación de resultados.**	Luego de ser validado la calificación por el notario, el calificador procede a imprimir la relación de ingresantes que serán visadas por el notario. El presidente de la comisión central de admisión ordena a un personal pegar los resultados en los paneles para ser vistos a los postulantes.	Se lleva acabo con materiales físicos como papel bond.	• Calificador • Notario. • Presidente de la comisión central de admisión. • Postulantes.
08	**Aprobación de la relación de ingresantes.**	La comisión central de admisión envía la relación de ingresantes a Consejo Universitario para formar parte de su agenda y se	Se lleva acabo con materiales físicos como papel bond.	• Presidente de la comisión central de admisión.

		apruebe mediante resolución de todos los ingresantes. Secretaría general remite la resolución con la que fueron aprobados los ingresantes.		• Consejo universitario.
09	**Regulariza_ción de documentos.**	Los ingresantes deben regularizar los documentos originales como: copia de DNI legalizado, certificados de estudio originales, partida de nacimiento original y declaración jurada en caso de ser menor de edad o antecedentes policiales en caso de ser mayores de edad.	Se lleva acabo con materiales físicos como carpeta del ingresante y documentos.	• Personal encargado de la regularización de documentos. • Ingresantes.
10	**Entrega de constancia de ingreso.**	De acuerdo a la resolución el administrador del sistema genera el código universitario para ser emitida la constancia de ingreso con los siguientes datos: número de resolución, apellidos y nombres, código universitario, carrera, facultad, modalidad y puntaje. Posteriormente será entregada al ingresante en las fechas del cronograma.	Se lleva acabo con una computadora y de manera física como papel bond.	• Administrador del sistema. • Ingresantes.
11	**Organiza_ción y clasificación de carpetas de los ingresantes.**	El personal de regularización organiza y clasifica las carpetas de los postulantes por carrera, facultad y si están completos. Realizando un informe detallado de cuántos ingresantes regularizaron y no regularizaron, el cual se entra a la comisión de admisión.	Se lleva cargo de manera física como las carpetas del ingresante.	• Personal de regularización de documentos.
12	**Envío de carpeta de ingresantes.**	La comisión central de admisión hace entrega las carpetas de los ingresantes al jefe de la oficina general de admisión quien enviará dichas carpetas a las facultades respectivas, para que los postulantes posteriormente se matriculen al semestre académico.	Se lleva cargo de manera física como las carpetas del ingresante.	• Comisión central de admisión. • Jefe de la oficina general de admisión.

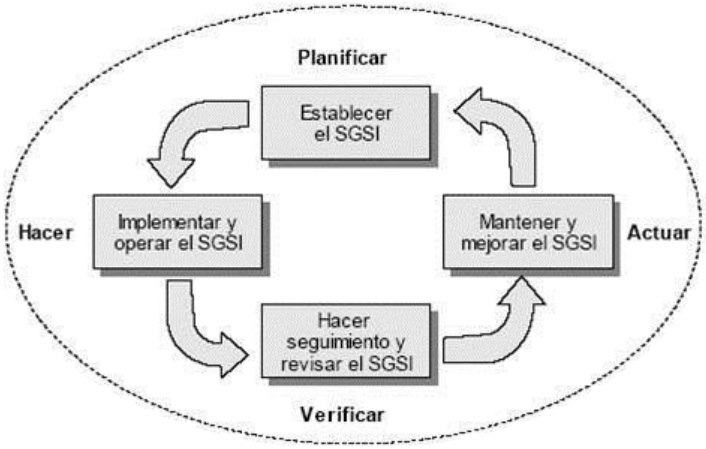
Fuente: Oficina General de Admisión de la UNASAM.

CAPÍTULO V: DISEÑO DE LA SOLUCIÓN

5.1. Arquitectura tecnológica de la solución

La norma ISO 27001:2013 incluye el ciclo de Deming, que consiste en Planificar-Hacer-Verificar-Actuar (PHVA) para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información.

Figura 5.1
Ciclo de PHVA



Fuente: Google imágenes

La metodología PHVA se puede describir de la siguiente forma:

Planificar: Se establece el Sistema de Gestión de Seguridad de la Información.

Hacer: Se implementa el Sistema de Gestión de Seguridad de la Información

Verificar: Revisión del Sistema de Gestión de Seguridad de la Información.

Actuar: En este paso del ciclo lo que se hace es mantener y mejorar el Sistema de Gestión de Seguridad de la Información.

5.2. Diseño de estructura de la solución

5.2.1. Planificar el Sistema de Gestión de Seguridad de la Información

5.2.1.1. Alcance del SGSI

El alcance del SGSI abarcará la Oficina General de Admisión, sus procesos, recursos informáticos y tecnología con el fin de establecer políticas para gestionar adecuadamente la seguridad de la información que debe ser aplicada y cumplida por el personal que labora.

5.2.1.2. Política de la seguridad de información

La Oficina General de Admisión pretende que la información que maneja se encuentre debidamente protegida con el fin de preservar y salvaguardar la confidencialidad, disponibilidad e integridad de la información y que garanticen el cumplimento de sus funciones.

5.2.1.3. Metodología de evaluación de riesgos

Para el proyecto de investigación se eligió la metodología de MAGERIT, que es una metodología para el análisis y la gestión de riesgo.

MAGERIT persigue los siguientes objetivos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.

- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).

- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

5.2.1.4. Análisis de riesgos basado en MAGERIT

5.2.1.4.1. Inventario de activos de información

Para proteger la información de riesgos y amenazas se realizó el inventario de activos teniendo en cuenta la metodología MAGERIT:

Tabla 5.1
Inventario de activos de información de la OGAD de la UNASAM

Recurso	Descripción
Copias de seguridad	Copias de seguridad de los diferentes sistemas de información de la oficina, base de datos y los equipos de cómputo.
Credenciales	Son credenciales de acceso. Por ejemplo contraseñas
Códigos fuentes	Archivos de códigos fuentes de los diferentes sistemas de información propios desarrollados.
File postulantes	Archivos de los postulantes, donde están datos personales y boucher de pago.
Examen de admisión	Es el examen que se elaboró y que posterior se le entrega al postulante para que desarrolle.
Resultados examen	Es el procesamiento digital de la ficha de respuestas
Correo electrónico	Es el medio por la cual se transmite información
Página web	Página web para el acceso al público.
Alojamiento de servidor web	Servicio de internet que provee un sistema para poder almacenar información, imágenes, vídeo, o cualquier contenido accesible vía web
Alojamiento de aplicaciones	Servicio de administración de alojamiento de aplicaciones Apache en la nube.

Software de desarrollo propio	Software desarrollado internamente por la oficina para cumplir sus necesidades a la medida.
Navegador web	Navegador web
Gestores de Bases de Datos	Administran y gestionan las bases de datos.
Ofimática	Software necesario para la realización de las actividades de la oficina.
Sistemas operativos	Software que administra los recursos de las computadoras.
Software de antivirus	Software para prevenir y eliminar virus informáticos
Computadoras portátiles	Permiten la realización de tareas del personal conectadas a través de la red interna.
Computadoras de escritorio	Permiten la realización de tareas del personal conectadas a través de la red interna.
Impresoras	Dispositivos para la impresión en papel.
Escáner	Dispositivos para transformar la información en formato digital.
Switch	Expandir la conexión de las computadoras
Teléfono IP	Es la encargada de transformar la voz en paquetes de datos para que se puedan enviar a través de Internet.
Dispositivos de respaldo	Dispositivos que almacenan la información y son útiles para la recuperación.
Conectividad inalámbrica	Permite la conectividad inalámbrica de las computadoras, así como amplía la cobertura.
Red de área local	Permite la interconexión de las computadoras que posee la oficina así como acceso a los diferentes servicios.
Internet	Permite el acceso a recursos de la web.
Cableado eléctrico	Provee energía eléctrica a las instalaciones y dispositivos.
Fibra óptica	Provee transmisión de datos a alta velocidad.
Oficina General de Admisión	Oficina donde se desarrollas las actividades
Administradores de sistemas	Administrador de sistema, personal técnico de procesos de admisión.

Fuente: Elaboración propia

5.2.1.4.2. Clasificación de activos de información

Tabla 5.2

Clasificación de los tipos de activos de información - MAGERIT

Tipo de activo	Nomen clatura	Definición
Activos Esenciales	[essential]	Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema.
Arquitectura del Sistema	[arch]	Se trata de elementos que permiten estructurar el sistema, definiendo su arquitectura interna y sus relaciones con el exterior.
Datos/ Información	[D]	Es aquella información que le permite a una organización prestar sus servicios.
Claves Criptográficas	[Keys]	La criptografía se emplea para proteger el secreto o autenticar a las partes.
Servicios	[S]	Función que satisface una necesidad de los usuarios
Software/ Aplicaciones Informáticas	[SW]	Son aquellos que procesan los datos y permiten brindar información para la prestación de servicios.
Hardware/ Equipamiento Informático	[HW]	Son los medios físicos donde se depositan los datos y prestan directa o indirectamente un servicio.
Redes de Comunicaciones	[COM]	Son los medios de transporte por donde viajan los datos.
Soportes de Información	[Media]	Son los dispositivos físicos que permiten el almacenamiento temporal o permanente de la información.
Equipamiento auxiliar	[AUX]	Equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
Instalaciones	[L]	Lugares donde se hospedan los sistemas de información y comunicaciones.
Personal	[P]	Personas relacionadas con los sistemas de información.

Fuente: MAGERIT – Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro II - Catálogo de Elementos.

Los activos se clasifican según el tipo de activo en la metodología MAGERIT de la siguiente manera:

Tabla 5.3

Clasificación por tipos de activos de información de la OGAD

Clasificación	Código	Subtipo	Descripción	Contenido
[D] Datos/ Información	D_BCK	[backup]	Copias de seguridad	Copias de seguridad de los diferentes sistemas de información de la oficina, base de datos y los equipos de cómputo.
	D_SRC	[source]	Códigos fuentes	Archivos de códigos fuentes de los diferentes sistemas de información propios desarrollados.
	D_PSW	[password]	Credenciales	Son credenciales de acceso.
	D_FPO	[files]	File postulantes	Archivos de los postulantes, donde están datos personales y boucher de pago.
	D_EXA	[files]	Examen de admisión	Es el examen que se elaboró y que posterior se le entrega al postulante para que desarrolle.
	D_RES	[files]	Resultados examen	Es el procesamiento digital de la ficha de respuestas.
[S] Servicios	S_WWW	[www]	Página Web	Página web para el acceso al público.
	S_MAI	[email]	Correo electrónico	Es el medio por la cual se transmite información.
	S_ASW	[www]	Alojamiento de servidor web	Servicio de internet que provee un sistema para poder almacenar información, imágenes, vídeo, o cualquier contenido.
	S_AAP	[hosting]	Alojamiento de aplicaciones	Servicio de administración de alojamiento de aplicaciones Apache en la nube.
[SW] Software	SW_SWP	[prp]	Software de desarrollo propio	Software desarrollado internamente por la oficina para cumplir sus necesidades a la medida.
	SW_DBS	[dbms]	Gestores de Bases de Datos	Administran y gestionan las bases de datos.
	SW_OFM	[office]	Ofimática	Software necesario para la realización de las actividades de la oficina.
	SW_AVS	[antivirus]	Software de antivirus	Software para prevenir y eliminar virus informáticos

Clasificación	Código	Subtipo	Descripción	Contenido
	SW_OPS	[os]	Sistemas operativos	Software que administra los recursos de las computadoras.
	SW_NW	[browser]	Navegador web	Navegador web.
[HW] Hardware	HW_BCK	[backup]	Dispositivos de respaldo	Dispositivos que almacenan la información y son útiles para la recuperación.
	HW_PCM	[pc]	Computadoras portátiles	Permiten la realización de tareas del personal conectadas a través de la red interna.
	HW_PCP	[pc]	Computadoras de escritorio	Permiten la realización de tareas del personal conectadas a través de la red interna.
	HW_PRT	[print]	Impresoras	Dispositivos para la impresión en papel.
	HW_SCN	[scaner]	Escáner	Dispositivos para transformar la información en formato digital.
	HW_SWH	[switch]	Switch	Expandir la conexión de las computadoras
	HW_TIP	[ipphone]	Teléfono IP	Es la encargada de transformar la voz en paquetes de datos.
[COM] Comunicación	COM_INT	[internet]	Internet	Permite el acceso a recursos de la web.
	COM_LAN	[lan]	Red de área local	Permite la interconexión de las computadoras así como acceso a los diferentes servicios.
	COM_WIF	[wifi]	Conectividad inalámbrica	Permite la conectividad inalámbrica de las computadoras, así como amplía la cobertura.
[AUX] Equipos Auxiliares	AUX_FBO	[fiber]	Fibra Óptica	Provee transmisión de datos a alta velocidad.
	AUX_WIR	[wire]	Cableado eléctrico	Provee energía eléctrica a las instalaciones y dispositivos.
[L] Instalaciones	L_SIT	[site]	Oficina General de Admisión	Oficina donde se desarrollas las actividades.
[P] Personal	P_ADSI	[admsi]	Administradores de sistemas	Administrador de sistema, personal técnico de procesos de admisión.

Fuente: Elaboración propia en base a MAGERIT

5.2.1.4.3. Valoración de activos de información

a) Valoración de activos de acuerdo al impacto

Tabla 5.4

Valoración cualitativa de activos de información.

Impacto	Nomenclatura	Valor	Descripción
10	MA	Muy alto	daño muy grave
7-9	A	Alto	daño grave
4-6	M	Medio	daño importante
1-3	B	Bajo	daño menor
0	MB	Muy bajo	irrelevante a efectos prácticos

Fuente: MAGERIT

Tabla 5.5

Valoración cualitativa de activos de información de la OGAD.

Clasificación	Código	Descripción	Impacto	Razón
[D] Datos/ Información	D_BCK	Copias de seguridad	MA	Los archivos de copias de seguridad son determinantes para la recuperación.
	D_SRC	Códigos fuentes	MA	Los archivos de código fuente contienen información de cómo se ejecutan los procesos internos en los Sistemas de Información desarrollados para la oficina.
	D_PSW	Credenciales	MA	Son credenciales de acceso.
	D_FPO	File postulantes	A	Archivos de los postulantes, donde están datos personales y boucher de pago.
	D_EXA	Examen de admisión	MA	Es el examen que se elaboró y que posterior se le entrega al postulante para que desarrolle.
	D_RES	Resultados examen	A	Es el procesamiento digital de la ficha de respuestas

Clasificación	Código	Descripción	Impacto	Razón
[S] Servicios	S_WWW	Página web	A	Acceso a la página web de la oficina.
	S_MAI	Correo electrónico	A	Es el medio por la cual se transmite información
	S_ASW	Alojamiento de servidor web	A	Servicio de internet que provee un sistema para poder almacenar información, imágenes, vídeo, o cualquier contenido accesible vía web
	S_AAP	Alojamiento de aplicaciones	A	Servicio de administración de alojamiento de aplicaciones Apache en la nube.
[SW] Software	SW_SWP	Software de desarrollo propio	MA	Utilizados para el normal desarrollo de los procesos de la oficina.
	SW_DBS	Gestores de Bases de Datos	MA	Almacena toda la información de los diferentes Sistemas de Información y desarrollo normal de los procesos.
	SW_OFM	Ofimática	B	Utilizado para la ejecución de tareas.
	SW_AVS	Software de antivirus	M	Utilizado para la prevención y eliminación de software malintencionado,
	SW_OPS	Sistemas operativos	M	Administra los recursos de software y hardware de las diferentes computadoras
	SW_NW	Navegador web	A	Navegador web
[HW] Hardware	HW_BCK	Dispositivos de respaldo	MA	Dispositivos que almacenan los archivos de las copias de seguridad necesarios para la recuperación.
	HW_PCM	Computadoras portátiles	B	Dispositivos para la ejecución de tareas.
	HW_PCP	Computadoras de escritorio	B	Dispositivos para la ejecución de tareas.
	HW_PRT	Impresoras	MB	Dispositivo para realizar impresiones en papel.
	HW_SCN	Escáner	MB	Dispositivo para digitalizar documentos.
	HW_SWH	Switch	M	Expandir la conexión de las computadoras
	HW_TIP	Teléfono IP	M	Es la encargada de transformar la voz en paquetes de datos para que se puedan enviar a través de Internet.

Clasificación	Código	Descripción	Impacto	Razón
[COM] Comunicación	COM_INT	Internet	M	Esencial para tener acceso a redes externas.
	COM_LAN	Red de área local	A	Esencial para la transmisión de datos y dar soporte al normal funcionamiento de los servicios internos institucionales.
	COM_WIF	Conectividad inalámbrica	B	Amplía la cobertura y otorga acceso inalámbrico a estos tipos de dispositivos
[AUX] Equipo auxiliar	AUX_FBO	Fibra óptica	A	Otorga alta velocidad de transmisión en el tráfico de datos interno. Da soporte de conectividad a toda la institución.
	AUX_WIR	Cableado eléctrico	MA	Cableado esencial para mantener en funcionamiento los dispositivos y el normal desarrollo de los procesos institucionales.
[L] Instalaciones	L_SIT	Oficina General de Admisión	MA	Oficina donde se desarrollas las actividades
[P] Personal	P_ADSI	Administradores de sistemas	A	Administrador de sistema, personal técnico de procesos de admisión.

Fuente: Elaboración propia en base a MAGERIT

b) Valoración de activos de acuerdo a las dimensiones de seguridad

Tabla 5.6

Dimensiones de seguridad de valoración en MAGERIT.

Dimensión de seguridad	Nomen clatura	Definición
Disponibilidad	[D]	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008].
Integridad	[I]	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004].
Confidencialidad	[C]	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007].

Dimensión de seguridad	Nomen clatura	Definición
Autenticidad	[A]	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008].
Trazabilidad	[T]	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008].

Fuente: MAGERIT – Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro II.

Tabla 5.7

Valoración de activos Datos/Información de acuerdo a las dimensiones de seguridad - MAGERIT

[D] Datos/Información							
Código	**Descripción**	**Dimensión de seguridad**					
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
D_BCK	Copias de seguridad	3		2		
D_SRC	Códigos fuentes		3	5		
D_PSW	Credenciales		3	5		
D_FPO	File postulantes		2			
D_EXA	Examen de admisión		4	7	4	4
D_RES	Resultados examen		4	7	6	6

Código	**Dimensión**	**Descripción**
D_BCK	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización
D_SRC	[I]	3.olm: Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
	[C]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
D_PSW	[I]	3.olm: Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
	[C]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
D_FPO	[I]	2.pi1: Pudiera causar molestias a un individuo
D_EXA	[I][A][T]	4.pi2: Probablemente quebrante leyes o regulaciones
	[C]	7.lro: Probablemente cause un incumplimiento grave de una ley o regulación
D_RES	[I]	3.lro: Probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización

Fuente: Elaboración propia en base a MAGERIT

Tabla 5.8

Valoración de activos Servicios de acuerdo a las dimensiones de seguridad – MAGERIT

[S] Servicios							
Código	**Descripción**		**Dimensión de seguridad**				
			[D]	**[I]**	**[C]**	**[A]**	**[T]**
S_WWW	Página Web		3				
S_MAI	Correo electrónico		3		2		
S_ASW	Alojamiento de servidor web		5	2	2		
S_AAP	Alojamiento de aplicaciones		5	2	2		
Código	**Dimensión**	**Descripción**					
S_WWW	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización					
S_MAI	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización					
	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización					
S_ASW	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización					
	[I]	2.pi1: Pudiera causar molestias a un individuo					
	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización					
S_AAP	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización					
	[I]	2.pi1: Pudiera causar molestias a un individuo					
	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización					

Fuente: Elaboración propia en base a MAGERIT

Tabla 5.9

Valoración de activos Software de acuerdo a las dimensiones de seguridad – MAGERIT

[SW] Software							
Código	**Descripción**	**Dimensión de seguridad**					
		[D]	**[I]**	**[C]**	**[A]**	**[T]**	
SW_SWP	Software de desarrollo propio	3		4	7	4	
SW_DBS	Gestores de Bases de Datos	7	7	7	7		
SW_OFM	Ofimática	1					
SW_AVS	Software de antivirus			7			
SW_OPS	Sistemas operativos	5	7				
SW_NW	Navegador web	1					
Código	**Dimensión**	**Descripción**					
SW_SWP	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización					
	[C]	4.pi1: Probablemente afecte a un grupo de individuos					
	[A]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves					
	[T]	4.crm: Dificulte la investigación o facilite la comisión de delitos					
SW_DBS	[D][I][A]	7.adm: Probablemente impediría la operación efectiva de la Organización					
	[C]	7.lro: Probablemente cause un incumplimiento grave de una ley o regulación					
SW_OFM	[D]	1.adm: Pudiera impedir la operación efectiva de una parte de la Organización					
SW_AVS	[C]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves					
SW_OPS	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización					
	[I]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves					
SW_NW	[D]	1.adm: Pudiera impedir la operación efectiva de una parte de la Organización					

Fuente: Elaboración propia en base a MAGERIT

Tabla 5.10

Valoración de activos Hardware de acuerdo a las dimensiones de seguridad – MAGERIT

[HW] Hardware							
Código	**Descripción**	**Dimensión de seguridad**					
		[D]	**[I]**	**[C]**	**[A]**	**[T]**	
HW_BCK	Dispositivos de respaldo			2		3	
HW_PCM	Computadoras portátiles.	1					
HW_PCP	Computadoras de escritorio.	1					
HW_PRT	Impresoras	1					
HW_SCN	Escáner	1					
HW_SWH	Switch	5			7		
Código	**Dimensión**	**Descripción**					
HW_BCK	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización					
	[T]	3.si: Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente					
HW_PCM	[D]	1.adm: Pudiera impedir la operación efectiva de una parte de la Organización					
HW_PCP	[D]	1.adm: Pudiera impedir la operación efectiva de una parte de la Organización					
HW_PRT	[D]	1.pi1: Pudiera causar molestias a un individuo					
HW_SCN	[D]	1.pi1: Pudiera causar molestias a un individuo					
HW_SWH	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización					
	[T]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves					

Fuente: Elaboración propia en base a MAGERIT

Tabla 5.11

Valoración de activos Comunicación de acuerdo a las dimensiones de seguridad – MAGERIT

[COM] Comunicación							
Código	**Descripción**	**Dimensión de seguridad**					
		[D]	**[I]**	**[C]**	**[A]**	**[T]**	
COM_INT	Internet	3		2		3	
COM_LAN	Red de área local	5					
COM_WIF	Conectividad inalámbrica	1					
Código	**Dimensión**	**Descripción**					
COM_INT	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización					
COM_LAN	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización					
COM_WIF	[D]	1.adm: Pudiera impedir la operación efectiva de una parte de la Organización					

Fuente: Elaboración propia en base a MAGERIT

Tabla 5.12

Valoración de activos Equipo auxiliar de acuerdo a las dimensiones de seguridad – MAGERIT

[AUX] Equipo auxiliar							
Código	**Descripción**	**Dimensión de seguridad**					
		[D]	**[I]**	**[C]**	**[A]**	**[T]**	
AUX_FBO	Fibra óptica	5					
AUX_WIR	Cableado eléctrico	5					
Código	**Dimensión**	**Descripción**					
AUX_FBO	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización					
AUX_WIR	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización					

Fuente: Elaboración propia en base a MAGERIT

Tabla 5.13

Valoración de activos Instalaciones de acuerdo a las dimensiones de seguridad – MAGERIT

[L] Instalaciones							
Código	**Descripción**		**Dimensión de seguridad**				
			[D]	**[I]**	**[C]**	**[A]**	**[T]**
L_SIT	Oficina General de Admisión de la UNASAM		7				
Código	**Dimensión**	**Descripción**					
L_SIT	[D]	7.adm: Probablemente impediría la operación efectiva de la Organización					

Fuente: Elaboración propia en base a MAGERIT

Tabla 5.14

Valoración de activos Personal de acuerdo a las dimensiones de seguridad – MAGERIT

[P] Personal							
Código	**Descripción**		**Dimensión de seguridad**				
			[D]	**[I]**	**[C]**	**[A]**	**[T]**
P_ADSI	Administradores de sistemas		5				
Código	**Dimensión**	**Descripción**					
P_ADSI	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización					

Fuente: Elaboración propia en base a MAGERIT

5.2.1.4.4. Identificación de amenazas

Tabla 5.15

Catálogo de amenazas sobre los activos de información

Tipo de amenaza	Nomenclatura	Definición
Desastres naturales	[N]	Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
De origen industrial	[I]	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.
Errores y fallos no intencionados	[E]	Fallos no intencionales causados por las personas.
Ataques intencionados	[A]	Fallos deliberados causados por las personas.

Fuente: MAGERIT – Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro II - Catálogo de Elementos.

5.2.1.4.5. Valoración de amenazas

Tabla 5.16

Probabilidad o frecuencia de ocurrencia de amenazas - MAGERIT.

Probabilidad o frecuencia	Rango	Valor
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada 1 semanas	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

Fuente: MAGERIT – Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro II - Catálogo de Elementos.

Tabla 5.17

Valor cuantitativo de amenazas – MAGERIT

Impacto	Valor cualitativo
Muy alto	**100%**
Alto	**75%**
Medio	**50%**
Bajo	**20%**
Muy Bajo	**5%**

Fuente: MAGERIT

Tabla 5.17

Relación de amenazas por activo identificado, su frecuencia de ocurrencia y el impacto.

Activo	Frecuencia de amenaza	[D]	[I]	[C]	[A]	[T]
[D] Datos/Información						
Copias de seguridad						
5.3.1. [E.1] Errores de los usuarios	5	5%	50%	75%		
5.3.10. [E.15] Alteración accidental de la información	5		100%	75%		
5.3.11. [E.18] Destrucción de información	5	100%				
5.3.12. [E.19] Fugas de información	5			100%		
5.3.2. [E.2] Errores del administrador	5	50%	50%	75%		
5.3.9. [E.14] Escapes de información	5			100%		
5.4.13. [A.15] Modificación deliberada de la información	5		100%			
5.4.14. [A.18] Destrucción de información	5	100%				
5.4.15. [A.19] Divulgación de información	5			100%		
5.4.4. [A.6] Abuso de privilegios de acceso	5	100%	100%	100%		
5.4.9. [A.11] Acceso no autorizado	5	75%	75%	75%		
Códigos fuentes						
5.3.10. [E.15] Alteración accidental de la información	5		50%			
5.3.11. [E.18] Destrucción de información	5	100%				
5.3.12. [E.19] Fugas de información	5			100%		

Activo	Frecuencia de amenaza	[D]	[I]	[C]	[A]	[T]
5.3.4. [E.4] Errores de configuración	10	20%				
5.3.9. [E.14] Escapes de información	5			100%		
5.4.13. [A.15] Modificación deliberada de la información	5		100%	20%	100%	
5.4.14. [A.18] Destrucción de información	5	100%				
5.4.15. [A.19] Divulgación de información	5			100%		
5.4.4. [A.6] Abuso de privilegios de acceso	5	100%	100%	100%		
5.4.9. [A.11] Acceso no autorizado	5	100%	100%	100%		
Credenciales						
5.3.10. [E.15] Alteración accidental de la información	5		50%			
5.3.11. [E.18] Destrucción de información	5	100%				
5.3.12. [E.19] Fugas de información	5	20%		100%		
5.3.4. [E.4] Errores de configuración	10	20%				
5.3.9. [E.14] Escapes de información	5			100%		
5.4.13. [A.15] Modificación deliberada de la información	5		100%		100%	
5.4.14. [A.18] Destrucción de información	5	100%				
5.4.15. [A.19] Divulgación de información	5			100%		
5.4.4. [A.6] Abuso de privilegios de acceso	5	100%	100%	100%		
5.4.9. [A.11] Acceso no autorizado	5	100%	100%	100%		
File postulantes						
5.3.1. [E.1] Errores de los usuarios	50		50%			
5.3.10. [E.15] Alteración accidental de la información	10		50%	75%		
5.3.11. [E.18] Destrucción de información	5	100%				
5.3.12. [E.19] Fugas de información	5		100%			
5.3.9. [E.14] Escapes de información	10			100%		
5.4.13. [A.15] Modificación deliberada de la información	5		75%			
5.4.14. [A.18] Destrucción de información	5	100%				
5.4.15. [A.19] Divulgación de información	10			100%		
5.4.4. [A.6] Abuso de privilegios de acceso	5	100%	100%	100%		
Examen de admisión						
5.3.11. [E.18] Destrucción de información	5	100%				
5.3.12. [E.19] Fugas de información	10			75%		
5.3.9. [E.14] Escapes de información	10		50%	50%		

Activo	Frecuencia de amenaza	[D]	[I]	[C]	[A]	[T]
5.4.13. [A.15] Modificación deliberada de la información	5		100%			
5.4.14. [A.18] Destrucción de información	5	100%				
5.4.15. [A.19] Divulgación de información	10			100%		
5.4.3. [A.5] Suplantación de la identidad del usuario	5	75%	75%	75%		
5.4.4. [A.6] Abuso de privilegios de acceso	5	100%	100%	100%		
5.4.9. [A.11] Acceso no autorizado	5	100%	100%	100%		
Resultados examen						
5.3.11. [E.18] Destrucción de información	5	100%				
5.3.12. [E.19] Fugas de información	10			75%		
5.3.9. [E.14] Escapes de información	10		50%	50%		
5.4.13. [A.15] Modificación deliberada de la información	5		100%			
5.4.14. [A.18] Destrucción de información	5	100%				
5.4.15. [A.19] Divulgación de información	10			100%		
5.4.3. [A.5] Suplantación de la identidad del usuario	5	75%	75%	75%		
5.4.4. [A.6] Abuso de privilegios de acceso	5	100%	100%	100%		
5.4.9. [A.11] Acceso no autorizado	5	100%	100%	100%		
[S] Servicios						
Página Web						
5.3.10.[E.15] Alteración accidental de la información	10			50%		
5.3.16 [E.24] Caída del sistema por agotamiento de recursos	50	100%				
5.4.14[A.18]Destrucción de información	5	100%				
5.4.18[A.24]denegación de servicio	5	100%				
Correo electrónico						
5.3.1. [E.1] Errores de los usuarios	50					
5.3.10. [E.15] Alteración accidental de la información	10		75%			
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	50	100%		20%		
5.3.9. [E.14] Escapes de información	50			100%		
5.4.11. [A.13] Repudio	5				100%	20%
5.4.13. [A.15] Modificación deliberada de la información	5		100%			
5.4.14. [A.18] Destrucción de información	5	100%				
5.4.15. [A.19] Divulgación de información	10			100%		

Activo	Frecuencia de amenaza	[D]	[I]	[C]	[A]	[T]
5.4.18. [A.24] Denegación de servicio	5	100%				
5.4.3. [A.5] Suplantación de la identidad del usuario	5			75%	75%	20%
5.4.4. [A.6] Abuso de privilegios de acceso	5		100%	75%		
5.4.8. [A.10] Alteración de secuencia	5		100%		100%	
5.4.9. [A.11] Acceso no autorizado	10			100%		
Alojamiento de servidor web						
5.3.10. [E.15] Alteración accidental de la información	5		100%		100%	20%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	50	100%				
5.3.9. [E.14] Escapes de información	50			50%		
5.4.11. [A.13] Repudio	5				50%	
5.4.13. [A.15] Modificación deliberada de la información	10		100%	100%		
5.4.14. [A.18] Destrucción de información	5	100%				
5.4.15. [A.19] Divulgación de información	5			100%		
5.4.18. [A.24] Denegación de servicio	5	100%				
5.4.3. [A.5] Suplantación de la identidad del usuario	5			100%	75%	20%
5.4.4. [A.6] Abuso de privilegios de acceso	5		100%	75%	100%	20%
5.4.9. [A.11] Acceso no autorizado	10			100%		
Alojamiento de aplicaciones						
5.3.10. [E.15] Alteración accidental de la información	5		100%		100%	20%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	50	100%				
5.3.9. [E.14] Escapes de información	50			50%		
5.4.11. [A.13] Repudio	5				50%	
5.4.13. [A.15] Modificación deliberada de la información	10		100%	100%		
5.4.14. [A.18] Destrucción de información	5	100%				
5.4.15. [A.19] Divulgación de información	5			100%		
5.4.18. [A.24] Denegación de servicio	5	100%				
5.4.3. [A.5] Suplantación de la identidad del usuario	5			100%	75%	20%
5.4.4. [A.6] Abuso de privilegios de acceso	5		100%	75%	100%	20%
5.4.9. [A.11] Acceso no autorizado	10			100%		
[SW] Software						
Gestores de Bases de Datos						

Activo	Frecuencia de amenaza	[D]	[I]	[C]	[A]	[T]
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	75%	75%		75%
5.3.1. [E.1] Errores de los usuarios	10	5%	5%	5%		
5.3.10. [E.15] Alteración accidental de la información	5	75%	75%		75%	
5.3.11. [E.18] Destrucción de información	5	100%				
5.3.12. [E.19] Fugas de información	5		100%	100%		
5.3.13. [E.20] Vulnerabilidades de los programas (software)	10	50%	75%	75%		
5.3.2. [E.2] Errores del administrador	10	50%	50%	50%		
5.3.6. [E.8] Difusión de software dañino	5	5%	5%	5%		
5.3.9. [E.14] Escapes de información	5			75%		
5.4.13. [A.15] Modificación deliberada de la información	5		100%	100%	100%	
5.4.14. [A.18] Destrucción de información	5	100%				
5.4.15. [A.19] Divulgación de información	5		75%	100%		
5.4.16. [A.22] Manipulación de programas	5		50%	50%		
5.4.3. [A.5] Suplantación de la identidad del usuario	10			50/		
5.4.4. [A.6] Abuso de privilegios de acceso	5	100%	100%	100%	100%	
5.4.5. [A.7] Uso no previsto	5	75%	75%	75%	75%	
5.4.6. [A.8] Difusión de software dañino	5	5%	5%	5%		
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5		10%			
5.4.8. [A.10] Alteración de secuencia	5	50%				
5.4.9. [A.11] Acceso no autorizado	5	100%	100%	100%	100%	
Software de desarrollo propio						
5.2.6. [I.5] Avería de origen físico o lógico	5	20%				
5.3.1. [E.1] Errores de los usuarios	50			5%		
5.3.10. [E.15] Alteración accidental de la información	5		50%			
5.3.11. [E.18] Destrucción de información	5	100%				
5.3.12. [E.19] Fugas de información	5			50%		
5.3.13. [E.20] Vulnerabilidades de los programas (software)	50	20%				20%
5.3.2. [E.2] Errores del administrador	10	20%	20%	20%		
5.3.6. [E.8] Difusión de software dañino	10	20%				
5.3.9. [E.14] Escapes de información	10		20%	20%		
5.4.13. [A.15] Modificación deliberada de la información	5		50%	100%	100%	
5.4.14. [A.18] Destrucción de información	5	100%				

Activo	Frecuencia de amenaza	[D]	[I]	[C]	[A]	[T]
5.4.15. [A.19] Divulgación de información	5		5%	5%		
5.4.16. [A.22] Manipulación de programas	5		75%	75%	75%	20%
5.4.3. [A.5] Suplantación de la identidad del usuario	5		50%			
5.4.4. [A.6] Abuso de privilegios de acceso	5		100%	100%	100%	
5.4.5. [A.7] Uso no previsto	5	5%				
5.4.6. [A.8] Difusión de software dañino	10	50%				
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5	50%				
5.4.8. [A.10] Alteración de secuencia	5	100%				
5.4.8. [A.10] Alteración de secuencia	5	100%	100%	100%		
Ofimática						
5.2.6. [I.5] Avería de origen físico o lógico	5	5%				
5.3.1. [E.1] Errores de los usuarios	50	5%				
5.3.13. [E.20] Vulnerabilidades de los programas (software)	50	50%				
5.3.6. [E.8] Difusión de software dañino	10	50%			75%	
5.4.5. [A.7] Uso no previsto	50	20%				
5.4.6. [A.8] Difusión de software dañino	5	50%		50%		
5.4.9. [A.11] Acceso no autorizado	5	50%				
Software de Antivirus						
5.2.6. [I.5] Avería de origen físico o lógico	5	75%				
5.3.1. [E.1] Errores de los usuarios	50	50%				
5.3.13. [E.20] Vulnerabilidades de los programas (software)	10	50%				
5.3.6. [E.8] Difusión de software dañino	10	75%			75%	
5.4.5. [A.7] Uso no previsto	5	20%				
5.4.6. [A.8] Difusión de software dañino	5	50%				
5.4.9. [A.11] Acceso no autorizado	5	100%				
Sistemas operativos						
5.2.6. [I.5] Avería de origen físico o lógico	5	75%				
5.3.1. [E.1] Errores de los usuarios	10	75%				20%
5.3.10. [E.15] Alteración accidental de la información	10	50%	20%	20%		
5.3.11. [E.18] Destrucción de información	5	100%				
5.3.12. [E.19] Fugas de información	5			75%		
5.3.13. [E.20] Vulnerabilidades de los programas (software)	5	50%				

Activo	Frecuencia de amenaza	[D]	[I]	[C]	[A]	[T]
5.3.2. [E.2] Errores del administrador	10	75%				20%
5.3.6. [E.8] Difusión de software dañino	10	75%	50%			
5.3.9. [E.14] Escapes de información	5			5%		
5.4.13. [A.15] Modificación deliberada de la información	5	75%	100%	100%		
5.4.14. [A.18] Destrucción de información	5	100%				
5.4.15. [A.19] Divulgación de información	5			100%		
5.4.16. [A.22] Manipulación de programas	5			50%		50%
5.4.3. [A.5] Suplantación de la identidad del usuario	5	100%	100%	100%		20%
5.4.4. [A.6] Abuso de privilegios de acceso	5	100%	100%	100%		20%
5.4.5. [A.7] Uso no previsto	5	50%				
5.4.6. [A.8] Difusión de software dañino	5	75%				
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5	50%				
5.4.8. [A.10] Alteración de secuencia	5	50%				
5.4.9. [A.11] Acceso no autorizado	5	75%	75%	75%		20%
Navegador web						
5.2.6. [I.5] Avería de origen físico o lógico	5	5%				
5.3.1. [E.1] Errores de los usuarios	10	5%				
5.3.13. [E.20] Vulnerabilidades de los programas (software)	50	50%				
5.3.6. [E.8] Difusión de software dañino	10	50%			75%	
5.4.5. [A.7] Uso no previsto	50			20%		
5.4.6. [A.8] Difusión de software dañino	5	50%		50%		
5.4.9. [A.11] Acceso no autorizado	5	50%				
[HW] Hardware						
Dispositivos de respaldo						
5.2.1. [I.1] Fuego	5	100%				
5.2.2. [I.2] Daños por agua	5	100%				
5.2.6. [I.5] Avería de origen físico o lógico	5	75%				
5.2.7. [I.6] Corte del suministro eléctrico	50	100%				
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad.	10	75%				
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	50%				
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5	75%				

Activo	Frecuencia de amenaza	[D]	[I]	[C]	[A]	[T]
5.3.17. [E.25] Pérdida de equipos	5	100%				
5.3.2. [E.2] Errores del administrador	5	50%				
5.4.17. [A.23] Manipulación de los equipos	5		50%			20%
5.4.18. [A.24] Denegación de servicio	5	100%				
5.4.19. [A.25] Robo	5	100%				
5.4.4. [A.6] Abuso de privilegios de acceso	5			75%		
5.4.5. [A.7] Uso no previsto	5	75%				
5.4.9. [A.11] Acceso no autorizado	5	75%		75%	75%	
Computadoras portátiles.						
5.2.1. [I.1] Fuego	5	100%				
5.2.2. [I.2] Daños por agua	5	100%				
5.2.6. [I.5] Avería de origen físico o lógico	5	75%				
5.2.7. [I.6] Corte del suministro eléctrico	50	20%				
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad.	10	75%				
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	10	75%				
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5	100%				
5.3.17. [E.25] Pérdida de equipos	5	100%				
5.3.2. [E.2] Errores del administrador	50	50%				
5.4.17. [A.23] Manipulación de los equipos	5		75%			20%
5.4.18. [A.24] Denegación de servicio	5	100%				
5.4.19. [A.25] Robo	5	100%				
5.4.4. [A.6] Abuso de privilegios de acceso	5			75%		
5.4.5. [A.7] Uso no previsto	5	75%				
5.4.9. [A.11] Acceso no autorizado	5	75%		75%	75%	
Computadoras de escritorio.						
5.2.1. [I.1] Fuego	5	100%				
5.2.2. [I.2] Daños por agua	5	100%				
5.2.6. [I.5] Avería de origen físico o lógico	5	75%				
5.2.7. [I.6] Corte del suministro eléctrico	50	100%				
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad.	10	75%				
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	10	75%				
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5	100%				

Activo	Frecuencia de amenaza	[D]	[I]	[C]	[A]	[T]
5.3.17. [E.25] Pérdida de equipos	5	100%				
5.3.2. [E.2] Errores del administrador	50	50%				
5.4.17. [A.23] Manipulación de los equipos	5		75%			20%
5.4.18. [A.24] Denegación de servicio	5	100%				
5.4.19. [A.25] Robo	5	100%				
5.4.4. [A.6] Abuso de privilegios de acceso	5			75%		
5.4.5. [A.7] Uso no previsto	5	75%				
5.4.9. [A.11] Acceso no autorizado	5	75%		75%	75%	
Impresoras						
5.2.1. [I.1] Fuego	5	100%				
5.2.2. [I.2] Daños por agua	5	100%				
5.2.6. [I.5] Avería de origen físico o lógico	5	75%				
5.2.7. [I.6] Corte del suministro eléctrico	50	100%				
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad.	10	75%				
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	10	75%				
5.3.17. [E.25] Pérdida de equipos	5	100%				
5.4.19. [A.25] Robo	5	100%				
Escáner						
5.2.1. [I.1] Fuego	5	100%				
5.2.2. [I.2] Daños por agua	5	100%				
5.2.6. [I.5] Avería de origen físico o lógico	5	75%				
5.2.7. [I.6] Corte del suministro eléctrico	50	100%				
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad.	10	75%				
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	10	75%				
5.3.17. [E.25] Pérdida de equipos	5	100%				
5.4.19. [A.25] Robo	5	100%				
Switch						
5.2.1. [I.1] Fuego	5	100%				
5.2.2. [I.2] Daños por agua	5	100%				
5.2.6. [I.5] Avería de origen físico o lógico	5	75%				
5.2.7. [I.6] Corte del suministro eléctrico	50	100%				
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad.	10	75%				

Activo	Frecuencia de amenaza	[D]	[I]	[C]	[A]	[T]
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	75%				
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5	100%				
5.3.17. [E.25] Pérdida de equipos	5	100%				
5.3.2. [E.2] Errores del administrador	50	75%				
5.4.17. [A.23] Manipulación de los equipos	5		75%			20%
5.4.18. [A.24] Denegación de servicio	5	100%				
5.4.19. [A.25] Robo	5	100%				
5.4.4. [A.6] Abuso de privilegios de acceso	5				75%	
5.4.5. [A.7] Uso no previsto	5	75%				
5.4.9. [A.11] Acceso no autorizado	5	75%		75%	75%	
[COM] Comunicación						
Internet						
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	10	100%				
5.3.2. [E.2] Errores del administrador	5	20%				
5.3.7. [E.9] Errores de [re-]encaminamiento	5		20%			
5.4.10. [A.12] Análisis de tráfico	5		50%	50%		
5.4.12. [A.14] Interceptación de información (escucha)	5			100%		
5.4.18. [A.24] Denegación de servicio	10	100%				
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5			75%	75%	20%
5.4.8. [A.10] Alteración de secuencia	5			75%	75%	20%
5.4.9. [A.11] Acceso no autorizado	10	50%				
Red de área local						
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	70	100%				
5.3.2. [E.2] Errores del administrador	10	20%				
5.3.7. [E.9] Errores de [re-]encaminamiento	5		20%			
5.4.10. [A.12] Análisis de tráfico	5		50%	50%		
5.4.12. [A.14] Interceptación de información (escucha)	5			100%		
5.4.18. [A.24] Denegación de servicio	70	100%				
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5			75%	75%	
5.4.8. [A.10] Alteración de secuencia	5			75%	75%	
5.4.9. [A.11] Acceso no autorizado	50	50%				

Activo	Frecuencia de amenaza	[D]	[I]	[C]	[A]	[T]
Conectividad inalámbrica						
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	70	100%				
5.3.2. [E.2] Errores del administrador	10	20%				
5.3.7. [E.9] Errores de [re-]encaminamiento	5		20%			
5.4.10. [A.12] Análisis de tráfico	5		50%	50%		
5.4.12. [A.14] Interceptación de información (escucha)	5			100%		
5.4.18. [A.24] Denegación de servicio	70	100%				
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5			75%	75%	20%
5.4.8. [A.10] Alteración de secuencia	5			75%	75%	20%
5.4.9. [A.11] Acceso no autorizado	50	50%				
[AUX] Equipo auxiliar						
Cableado eléctrico						
5.2.1. [I.1] Fuego	5	100%				
5.2.2. [I.2] Daños por agua	5	100%				
5.2.6. [I.5] Avería de origen físico o lógico	5	75%				
5.2.7. [I.6] Corte del suministro eléctrico	50	100%				
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	5	5%				
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	20%				
5.4.19. [A.25] Robo	5	100%				
5.4.20. [A.26] Ataque destructivo	5	100%				
Fibra óptica						
5.2.1. [I.1] Fuego	5	100%				
5.2.2. [I.2] Daños por agua	5	100%				
5.2.6. [I.5] Avería de origen físico o lógico	5	75%				
5.2.7. [I.6] Corte del suministro eléctrico	50	100%				
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	50	5%				
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	20%				
5.4.19. [A.25] Robo	5	100%				
5.4.20. [A.26] Ataque destructivo	5	100%				
[L] Instalaciones						
Oficina General de Admisión de la UNASAM						

Activo	Frecuencia de amenaza	[D]	[I]	[C]	[A]	[T]
5.1.3. [N.*] Desastres Naturales	5	100%				
5.3.10. [E.15] Alteración accidental de la información	5	20%	100%			
5.3.11. [E.18] Destrucción de información	5	100%				
5.3.12. [E.19] Fugas de información	5			100%		
5.4.13. [A.15] Modificación deliberada de la información	5		100%	100%	100%	
5.4.14. [A.18] Destrucción de información	5	100%		100%		
5.4.15. [A.19] Divulgación de información	5		100%	100%		
5.4.20. [A.26] Ataque destructivo	5	100%				
5.4.5. [A.7] Uso no previsto	5	50%				
5.4.9. [A.11] Acceso no autorizado	5	75%				
[P] Personal						
Administradores de sistemas						
5.3.12. [E.19] Fugas de información	5				75%	
5.3.18. [E.28] Indisponibilidad del personal	10	50%				
5.3.5. [E.7] Deficiencias en la organización	5	75%				
5.4.22. [A.28] Indisponibilidad del personal	5	50%				

Fuente: Elaboración con MAGERIT

5.2.1.4.6. Impacto potencial

Se determina el nivel de daño o impacto que tendría un activo si se llegara a materializar una amenaza determinada en cada una de sus dimensiones de seguridad.

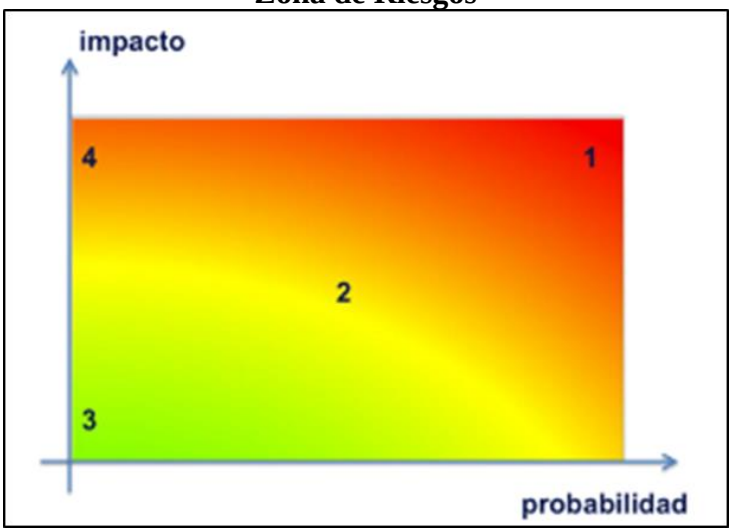
5.2.1.4.7. Riesgo potencial

El riesgo es la medida probable de daño sobre un sistema el cual es posible determinar directamente conociendo la probabilidad de ocurrencia de una amenaza sobre un activo y el impacto. Por ende, el riesgo es calculado como:

Riesgo = Probabilidad x Impacto.

El riesgo crece con el impacto y con la probabilidad como se muestra en la siguiente ilustración:

Figura 5.2
Zona de Riesgos



Fuente: MAGERIT, Libro I – Método.

Donde las zonas identifican lo siguiente:

- Zona 1: Riesgos muy probables y de muy alto impacto (MA: Críticos).
- Zona 2: Riesgos que varían desde situaciones improbables y con impacto medio hasta situaciones muy probables pero de impacto bajo o muy bajo (M: Apreciables).
- Zona 3: Riesgos improbables y de bajo impacto (MB, B: Despreciables o Bajos).
- Zona 4: Riesgos improbables pero de muy alto impacto (A: Importantes).

A su vez, la relación de la probabilidad e impacto para determinar el riesgo de forma cualitativa se muestra en la siguiente tabla:

Tabla 5.18

Estimación cualitativa del riesgo.

Riesgo		Probabilidad				
		MB	B	M	A	MA
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: MAGERIT – Libro II - Catálogo de Elementos

Tabla 6.19

Riesgo potencial

Código	Activo	Im_ pacto	Proba_ bilidad	Ame naza	Riesgo _Id	Ries_ go
[D] Datos/Información						
D_BCK	Copias de seguridad	MA	MB	E*, A*	R_D_B CK	A
D_SRC	Códigos fuentes	MA	B	E*, A*	R_D_S RC	MB
D_PSW	Credenciales	MA	B	E*, A*	R_D_PS W	MB
D_FPO	File postulantes	A	M	E*, A*	R_D_FP O	A
D_EXA	Examen de admisión	MA	B	E*, A*	R_D_E XA	MA
D_RES	Resultados examen	A	B	E*, A*	R_D_R ES	MA
[S] Servicios						
S_WWW	Página Web	A	M	E*, A*	R_S_W WW	A
S_MAI	Correo electrónico	A	M	E*, A*	R_S_M AI	MA
S_ASW	Alojamiento de servidor web	A	M	E*, A*	R_S_AS W	A
S_AAP	Alojamiento de aplicaciones	A	M	E*, A*	R_S_A AP	A
[SW] Software						
SW_DBS	Gestores de Bases de Datos	MA	B	I*, E*, A*	R_SW_ DBS	MA
SW_SWP	Software de desarrollo propio	MA	M	I*, E*, A*	R_SW_ SWP	MA
SW_OFM	Ofimática	B	M	I*, E*, A*	R_SW_ OFM	B
SW_AVS	Software de antivirus	M	M	I*, E*, A*	R_SW_ AVS	M
SW_OPS	Sistemas operativos	M	B	I*, E*, A*	R_SW_ OPS	M
SW_NW	Navegador web	A	M	I*, E*, A*	R_SW_ NW	B
[HW] Hardware						
HW_BCK	Dispositivos de respaldo	MA	M	I*, E*, A*	R_HW_ BCK	MA
HW_PCM	Computadoras portátiles.	B	M	I*, E*, A*	R_HW_ PCM	B
HW_PCP	Computadoras de escritorio.	B	M	I*, E*, A*	R_HW_ PCP	B
HW_PRT	Impresoras	MB	M	I*, E*, A*	R_HW_ PRT	MB
HW_SCN	Escáner	MB	M	I*, E*, A*	R_HW_ SCN	MB
HW_SWH	Switch	A	M	I*, E*, A*	R_HW_ SWH	A
[COM] Comunicación						
COM_INT	Internet	A	A	E*, A*	R_COM _INT	MA

COM_LAN	Red de área local	MA	A	E*, A*	R_COM_LAN	MA
COM_WIF	Conectividad inalámbrica	B	A	E*, A*	R_COM_WIF	M
[AUX] Equipo auxiliar						
AUX_WIR	Cableado eléctrico	MA	M	I*, E*, A*	R_AUX_WIR	MA
AUX_FBO	Fibra óptica	MA	M	I*, E*, A*	R_AUX_FBO	MA
[L] Instalaciones						
L_SIT	Oficina General de Admisión	MB	MB	N*, I*, E*, A*	R_L_SIT	A
[P] Personal						
P_ADSI	Administradores de sistemas	MA	B	E*, A*	R_P_ADSI	MA

Fuente: Elaboración con MAGERIT

Se clasifican los riesgos de acuerdo a las zonas establecidas en MAGERIT:

Tabla 6.20

Clasificación de los riegos según la zona de riesgos

RIESGO		**Probabilidad**				
		MB	**B**	**M**	**A**	**MA**
Impacto	**MA**	R_D_BCK	R_D_SRC, R_SW_DBS, P_ADSI, R_D_PSW, R_D_EXA	R_SW_SWP, R_HW_BCK, R_AUX_WIR, R_AUX_FBO	R_COM_LAN	
	A		R_D_RES R_SW_NW	R_S_WWW, R_HW_SWH, R_D_FPO, R_S_MAI	R_COM_INT R_S_ASW R_S_AAP	
	M		R_SW_OPS	R_SW_AVS		
	B			R_SW_OFM, R_HW_PCM, R_HW_PCP	R_COM_WIF	
	MB	R_L_SIT		R_HW_PRT, R_HW_SCN		

Fuente: Elaboración con MAGERIT

Figura 5.3

Cantidad de riesgo según la zona de riesgo

Fuente: Elaboración propia

CAPÍTULO VI: CONSTRUCCIÓN DE LA SOLUCIÓN

6.1. Construcción

6.1.1. Declaración de aplicabilidad

En el presente capítulo habiendo ya realizado el proceso de análisis de riesgos por la metodología MAGERIT, en el cual se identificaron los activos de información críticos y los riesgos a los que se encuentran expuestos actualmente con la finalidad de determinar las estrategias a seguir para su mitigación.

Sin embargo, estas estrategias no definen explícitamente las acciones a realizar puesto que son generales. Es por este motivo que la norma ISO/IEC 27001:2013 exige que se desarrolle el documento denominado “Declaración de aplicabilidad” en el que se detalla la selección de los controles a implementarse para mitigar los riesgos identificados. Este documento debe presentar la selección de los controles incluidos en el Anexo, detallando qué controles ya se encuentran implementados, cuáles se debe implementar (detallando de manera general las pautas que se debe tener en cuenta en su implementación) y cuáles de ellos no se implementarán (detallando el motivo de su exclusión).

En la presente Declaración de aplicabilidad se presenta una explicación contextualizada de los controles presentados en la norma en relación a su aplicación en la Oficina General de Admisión de la UNASAM. Para ello se

ha hecho uso del detalle de los controles que se encuentra en la ISO/IEC 27001:2013.

La declaración de aplicabilidad desarrollada como entregable final del proyecto se encuentra en la sección “Anexo: Declaración de Aplicabilidad” en el documento de anexos que acompaña al presente proyecto.

6.1.2. Políticas y objetivos de seguridad

En el Anexo se observa la descripción de controles a implementar de acuerdo a la ISO/IEC 27001:2013. La cual contiene 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES, además como producto final de la tesis en el Anexo se tiene la Declaración de aplicabilidad junto con sus guías de implementación.

CAPÍTULO VII: IMPLEMENTACIÓN

7.1. Monitoreo y evaluación de la solución

7.1.1. Elementos de monitoreo y evaluación

Las acciones de monitoreo se realizarán más eficientemente cuando las actividades, recursos y activos relacionados se gestionen como un proceso, para ello se debe tener identificado la interacción entre los mismos. Además, se deberá tener en cuenta las medidas preventivas a tomar y llevar un registro de los mismos. Para llevar un control de todo esto, se propone realizarlo a través del ciclo de Deming (de Edwards Deming), también conocido como círculo PDCA (del inglés plan-do-check-act, = planificar-hacer-verificar-actuar). Es una estrategia de mejora continua de la calidad en cuatro pasos, que tienen por función:

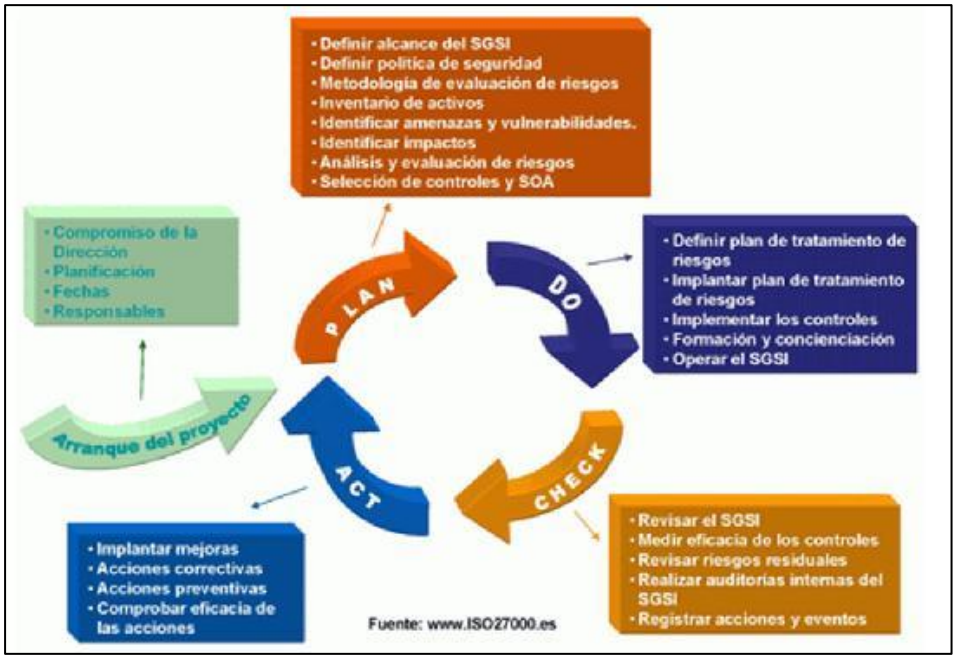
1) Toma de datos y registro en las Tablas y anexos respectivos.

2) Contrastación de los datos contra el nivel esperado de cumplimiento

3) Decisión respecto de las acciones correctivas o de retroalimentación necesarias de acuerdo a la información obtenida

4) Implementación de las acciones correctivas o de retroalimentación.

Figura 7.1
Ciclo de DEMING



Fuente: http://www.pearltrees.com/fernandotrujillo

7.1.2. Plan de monitoreo y evaluación

El Plan de monitoreo y evaluación debe necesariamente dar respuesta al menos a las siguientes interrogantes: ¿Cómo se va a recoger la información?, ¿Quién va a recogerla?, ¿Cuándo se va a obtener?, ¿Cómo se va a analizar la información recogida?, ¿Quién la va a analizar?, ¿Cuándo se va a hacer el análisis?, ¿Quién va a recibir los resultados?, ¿En qué formato se van a distribuir?

7.2. Bitácora y puesta a punto

Para el registro de las observaciones, ideas, datos, avances y obstáculos en el desarrollo de las actividades que se llevan a cabo durante el proyecto, se empleó

la siguiente Tabla para consolidar las condiciones bajo las cuales se desarrolló el proyecto.

Tabla 7.1
Bitácora para el diseño del proyecto

Fecha	Etapa	Actividad	Observación
Del 01/02/2018 Al 30/04/2018	Análisis	Identificar fuentes de información	Se realizó de acuerdo a lo planificado
		Recopilar información	Se realizó de acuerdo a lo planificado
		Organizar información	Se realizó de acuerdo a lo planificado
		Analizar la información	Se realizó de acuerdo a lo planificado
Del 01/05/2018 Al 01/07/2018	Diseño	Plantear controles de seguridad	Se realizó de acuerdo a lo planificado
		Identificar Salvaguardas	Se realizó de acuerdo a lo planificado
		Gestión de Riesgos	Se realizó de acuerdo a lo planificado
		Establecer la Declaración de aplicabilidad	Se realizó de acuerdo a lo planificado

Fuente: Elaboración propia

Una vez realizada la propuesta de mejora para el Sistema de seguridad de la Información, la puesta en operatividad dependerá de la adaptación al cambio de los actores principales.

CAPÍTULO VIII: RESULTADOS

Al finalizar la aplicación de nuestros instrumentos para la recolección de información y nuestras herramientas en el procesamiento de la misma, se pudo evidenciar por medio de los resultados la realidad que vive la Oficina General de Admisión de la UNASAM en cuanto refiere al tema de seguridad de la información.

Los resultados que se muestran van de acorde al planteamiento de nuestros objetivos los cuales se plasman a continuación:

Resultado 1: Para este resultado se realizó el diagnóstico de la situación actual de la Oficina General de Admisión, de acuerdo al Anexo A de la ISO/IEC 27001:2013 y que se muestra en el Anexo 02.

Resultado 2: Para este resultado se procedió a la identificar y valorización de los activos de la información de los procesos de negocio que se identificaron en la Oficina General de Admisión, la cual se detallan en el Capítulo V, Inventario, clasificación y valoración de activos de la información.

Resultado 3: Para este resultado en base a la identificación y valoración de los activos de la información se pasó a evaluar y tratar los riesgos a los que están expuestos los activos de la información, la cual se detalla en Capítulo V, Relación de amenazas por activo identificado, su frecuencia de ocurrencia y el impacto.

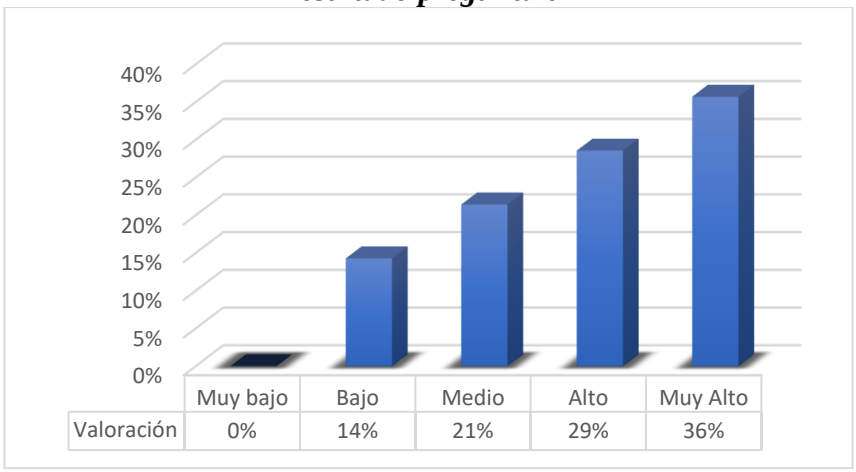
Resultado 4: Para este resultado se diseñó la declaración de aplicabilidad que son los controles aplicables a la Oficina General de Admisión, la cual se muestra en el Anexo 06.

Del mismo modo mostramos de manera detallada la consolidación de la respuesta de la encuesta aplicada y los resultados obtenidos al procesar la información:

Diseño de un Sistema de Gestión de Seguridad de la información mediante la aplicación de la norma ISO/IEC 27001:2013 para mejorar la seguridad de la información en la en la Oficina General de Admisión de la UNASAM.

Pregunta 01: ¿Cómo evalúa usted las políticas de seguridad dadas en el Diseño de un Sistema de Gestión de Seguridad de la Información mediante la aplicación de la norma ISO/IEC 27001:2013 para la OGAD de la UNASAM?

Figura 8.1
Resultado pregunta 01

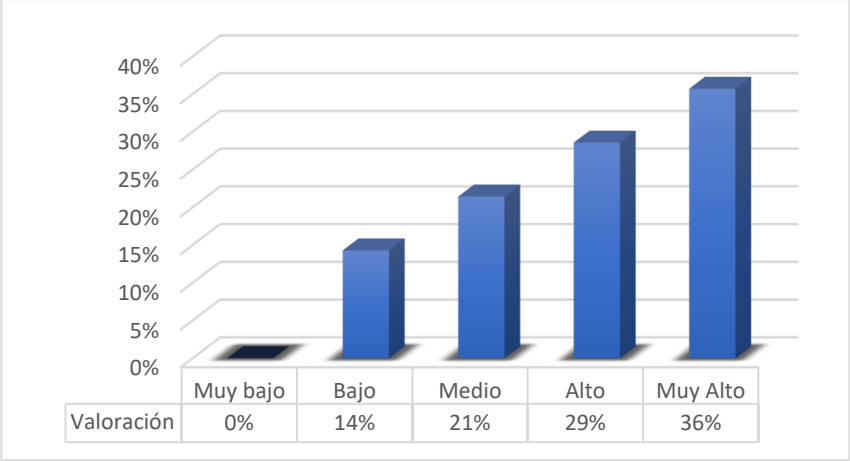


Fuente: Elaboración propia

El 72% de los encuestados calificaron como Muy Alto y Alto sobre las políticas de seguridad en el Diseño de un SGSI mediante la aplicación de la norma ISO/IEC 27001:2013 de la OGAD de la UNASAM, el 21% califico medio y el 7% como bajo.

Pregunta 02: ¿Cómo califica usted el inventario de los activos en el Diseño de un Sistema de Gestión de Seguridad de la Información mediante la aplicación de la norma ISO/IEC 27001:2013 para la OGAD de la UNASAM?

Figura 8.2
Resultado pregunta 02

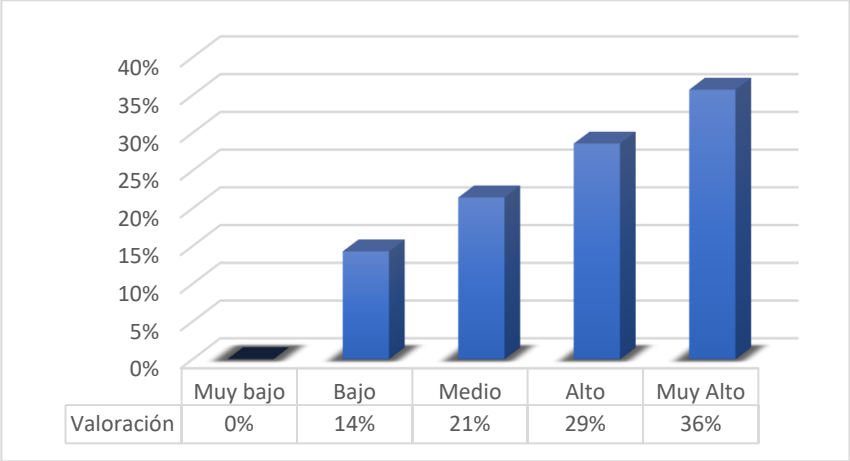


Fuente: Elaboración propia

De los encuestados, sobre el inventario de activos en el Diseño de un SGSI mediante la aplicación de la norma ISO/IEC 27001:2013, el 79% calificaron como Muy Alto y Alto, el 14% califico medio y el 7% como bajo.

Pregunta 03: ¿Cómo evalúa usted la identificación y valoración de amenazas en el Diseño de un Sistema de Gestión de Seguridad de la Información mediante la aplicación de la norma ISO/IEC 27001:2013 para la OGAD de la UNASAM?

Figura 8.3
Resultado pregunta 03

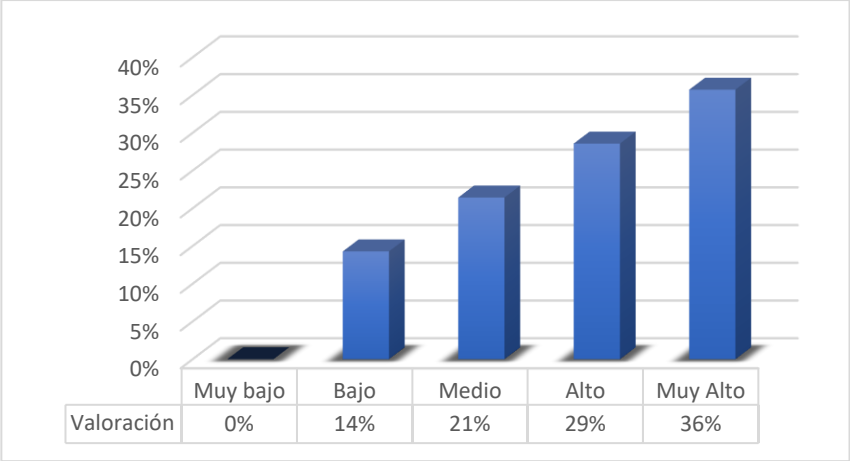


Fuente: Elaboración propia

De los encuestados, Sobre la identificación y valoración de amenazas en el Diseño de un Sistema de Gestión de Seguridad de la Información mediante la aplicación de la norma ISO/IEC 27001:2013, el 72% calificaron como Muy Alto y Alto, el 21% califico medio y el 7% como bajo.

Pregunta 04: ¿Cómo califica usted, en el Diseño de un Sistema de Gestión de Seguridad de la Información mediante la aplicación de la norma ISO/IEC 27001:2013, mejorar la seguridad de la información en los niveles de riesgos de la OGAD de la UNASAM?

Figura 8.4
Resultado pregunta 04



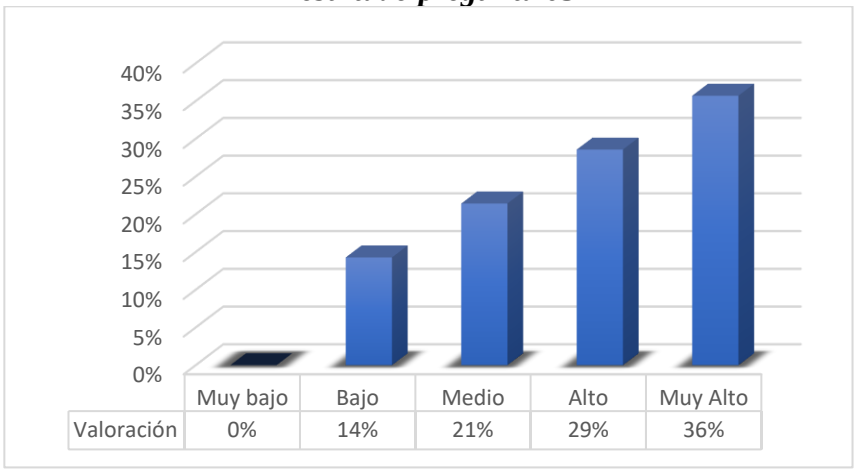
Fuente: Elaboración propia

De los encuestados, en el Diseño de un Sistema de Gestión de Seguridad de la Información mediante la aplicación de la norma ISO/IEC 27001:2013, mejorar la seguridad de la información en los niveles de riesgos de la OGAD de la UNASAM, el 69% calificaron como Muy Alto y Alto, el 21% califico medio y el 7% como bajo.

Pregunta 05: ¿Cómo califica usted, en el Diseño de un Sistema de Gestión de Seguridad de la Información mediante la aplicación de la norma ISO/IEC 27001:2013

para la OGAD de la UNASAM, el tratamiento de los riegos de la información mejora considerablemente la oficina?

Figura 8.5
Resultado pregunta 05

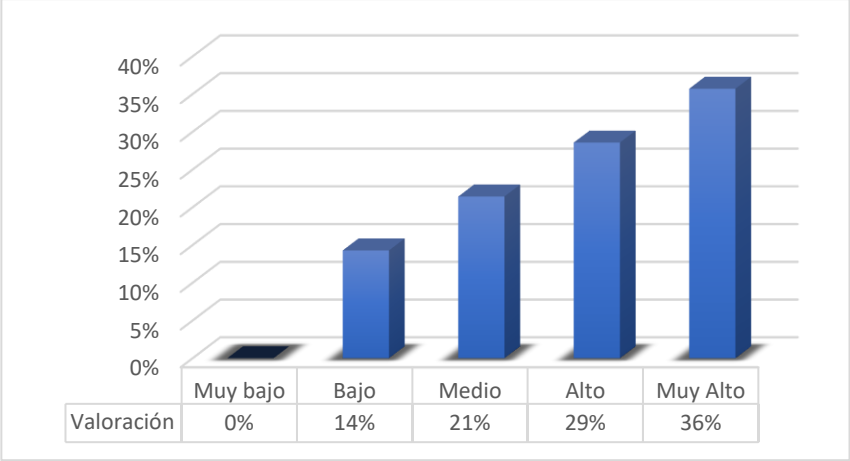


Fuente: Elaboración propia

De los encuestados, en el Diseño de un Sistema de Gestión de Seguridad de la Información mediante la aplicación de la norma ISO/IEC 27001:2013 para la OGAD de la UNASAM, el tratamiento de los riegos de la información el 86% calificaron como Muy Alto y Alto, el 14% califico medio.

Pregunta 06: ¿Cómo evalúa usted, en el Diseño de un Sistema de Gestión de Seguridad de la Información mediante la aplicación de la norma ISO/IEC 27001:2013 para la OGAD de la UNASAM, la declaración de aplicabilidad?

Figura 8.6
Resultado pregunta 06



Fuente: Elaboración propia

De los encuestados, en el Diseño de un Sistema de Gestión de Seguridad de la Información mediante la aplicación de la norma ISO/IEC 27001:2013 para la OGAD de la UNASAM, en la declaración de aplicabilidad el 65% calificaron como Muy Alto y Alto, el 21% califico medio y 14% bajo.

CAPÍTULO IX: DISCUSIÓN DE RESULTADOS

Este proyecto abarcó lo que es un Diseño de Sistema de Gestión de la Seguridad de la Información en la Oficina General de Admisión, por ser una de las dependencias con activos de información importantes para la institución, es por ello que al presentar alguna falla en cualquier momento puede ocasionar problemas e inconvenientes en el desarrollo normal de los procesos. A pesar de ello se ha observado que hasta el momento no se ha puesto mayor esfuerzo en lo que respecta a la seguridad de la información.

En el desarrollo del presente proyecto se han observado estudios e información sobre el tema en cuestión, en la tesis de Benites Arango, ha logrado implementar de una Guía Metodología Basada en la NTP ISO/IEC 27001:2008, NTP ISO/IEC 17799:2007 y COBIT 5 para Mejorar la Seguridad de la Información, la cual no es certificada debido a que ahora se cuenta con la actualización al estándar internacional ISO/IEC 27001:2013, estas investigaciones se realizaron antes del cambio contractual por lo que fueron a grandes rasgos puesto que su aplicación de todo o en parte se está imponiendo de manera necesaria y obligatoria para la institución pública.

En base a nuestros antecedentes vemos que a pesar de que nos encontramos en una etapa donde la información es importante, poco o nada se hace para salvaguardarlo y protegerla de los riesgos y amenazas a los que se ven expuestos diariamente ya que varios estudios confirman lo dicho.

Esperamos que a partir de este proyecto se tome conciencia sobre los riesgos a los que están expuestos los activos y se empiece por implantar políticas de seguridad,

salvaguardas y controles, empezando por cosas que pueden parecer pequeñas al inicio pero que pueden formar parte de un cambio dentro de la institución permitiendo preservar la confidencialidad, integridad y disponibilidad de la información aplicando las Políticas de seguridad y la Declaración de aplicabilidad el cual contiene la cláusula, la sección, el objetivo del control y la visión general de la implementación.

CONCLUSIONES

- En el estudio realizado el diagnóstico de la situación actual que se desarrolló mediante las entrevistas y la recopilación bibliográfica permitió formular los requerimientos y directrices necesarios para el diseño de un Sistema de Gestión de Seguridad de la Información.

- Según el análisis realizado, el diseñar un Sistema de Gestión de Seguridad de Información mediante la aplicación de la norma ISO/IEC 27001:2013 mejorara la seguridad de la información en la Oficina General de Admisión de la UNASAM, sin embargo este diseño por motivos académicos aún no puede ser implementada.

- Se logró incrementar los conocimientos sobre seguridad de la información y permitieron plasmar en el diseño de un Sistema de Gestión de Seguridad de Información mediante la aplicación de la norma ISO/IEC 27001:2013.

- La Oficina General de Admisión no cuenta con medidas de seguridad guiados y documentados, por lo cual el proyecto será de gran aporte como punto de partida a la minimización de los riesgos existentes y los que afectaran en el futuro a la oficina.

- Se estableció la declaración de aplicabilidad mediante el ISO/IEC 27002:2013 la cual cuenta con 14 dominios, 35 objetivos de control y 114 controles, los cuales fueron adaptados al alcance de la solución del proyecto.

RECOMENDACIONES

Se recomiendo que este diseño de un Sistema de Gestión de Seguridad de Información mediante la aplicación de la norma ISO/IEC 27001:2013 para la Oficina General de Admisión de la UNASAM, se lleve a la implementación para mejorar la seguridad de la información y preservar la confidencialidad, integridad y disponibilidad.

Se recomienda sensibilizar al personal involucrado de la Oficina General de Admisión en el proceso de Seguridad de la Información ya que se evidencia actividades que ocasionan latencia en dicho procesos.

REFERENCIAS BIBLIOGRAFICAS

Ardila Navarrete, J. A. (2016). *Diseño de un Sistema de Gestiòn de Seguridad de la Informaciòn (SGSI) basado en la Norma ISO/IEC 27001 para Positiva Compañía de Seguros S.A en la Ciudad de Bogotá.* Proyecto de Grado, Universidad Nacional Abierta y a Distancia, Bogotá - Colombia.

Atalaya Vasquez, O. (2016). *Propuesta de un Sistema de Seguridad de la Informacion para la Oficina de Admisión y Regristro Académico de la Uversidad Antonio Urrelo, 2016.* Grado de Maestro, UPAGU, Cajamarca - Perú.

Benites Arango, R. R. (2017). *Implementación de una Guía Metodológica basada en NTP ISO/IEC 27001:2008, NTP ISO/IEC 17799:2007 y COBIT 5 PARA mejorar la Seguridad de la Información en la Municipalidad Distrital de Tarica-2014.* Grado de Maestro, Universidad Nacional Santiago Antunez de Mayolo, Huaraz - Perú.

Bermúdez Molina, K. G., & Bailón Sánchez, E. R. (2015). *Análisis en Seguridad Informática y Seguridad de la Información basado en la Norma ISO/IEC 27001- Sistemas de Gestión de Seguridad de la Información dirigido a una Empresa de Servicios Financieros.* Título Profesional, Universidad Politécnica Salesiana, Guayaquil - Colombia.

España, G. d. (2012). *MAGERIT - Metodologia de Analisis y Gestion de Riegos de los Sistemas de Informacion.* España.

Hernández Sampieri, R., Fernández collado, C., & Baptista Lucio, P. (2014). *Metodologia de la Investigación* (Vol. Sexta Edición). México: Mc Graw Hill.

iso27000.es. (20 de 03 de 2018). *El Portal de ISO 27001 en Español*. Obtenido de www.iso27000.es

isotools. (06 de 04 de 2018). *ISO/IEC 27001:2013*. Obtenido de ISO 27001: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Mory Garay, A. C. (2015). *Aplicación de la Norma ISO 27001 para mejorar la Seguridad de la Información en la Empresa HM Contratistas S.A.* Titulo Profesional, UNASAM, Huaraz - Perú.

Moyano Orjuela, L. A., & Suárez Cárdenas, Y. E. (2017). *Plan de Implementación del SGSI Basado en la Norma ISO 27001:2013 para la empresa Interfaces y Soluciones.* Título Profesional, Universidad Distrital Francisco José de Caldas, Bogotá - Colombia.

Narváez Barreiros, I. R. (2013). *Aplicación de la Norma ISO 27001 para la Implementación de un SGSI en la Fiscalía General del Estado.* Título Profesional, Pontificia Universidad Catolica del Ecuador, Quito - Ecuador.

Santos Llanos, D. E. (2016). *Establecimiento, Implementación, Mantenimiento y Mejora de un Sistema de Gestión de Seguridad de la Información, basado en la ISO/IEC 27001:2013, para una Empresa de Consultoría de Software.* Título Profesional, Pontificia Universidad Católica del Perú, Lima - Perú.

Talavera Álvarez, V. R. (2015). *Diseño de un Sistema de Gestión de Seguridad de la Información para una Entidad Estatal de Salud de acuerdo a la ISO/IEC 27001:2013* . Título Profesional, Pontificia Universidad Católica del Perú, Lima - Perú.

Vilca Mosquera, E. C. (2017). *Diseño e Implementación de un SGSI ISO 27001 para la mejora de la Seguridad de Humanos de Lima.* Título Profesional, Universidad de Huánuco, Huánuco - Perú.

Zavaleta Rodriguez, D. (2016). *Implementación de un Sistema de Gestión de Seguridad de la Información aplicando NTP ISO/IEC 27001:2014 en el sector Hospitalario, 2016.* Título Profesional, Universidad Norbert Wiener, Lima - Peru.

ANEXOS

Anexo 01

ENCUESTA

Diseño de un Sistema de Seguridad de la Información mediante la aplicación de la norma ISO/IEC 27001:2013

1. ¿Cómo evalúa usted las políticas de seguridad dadas en el Diseño de un Sistema de Gestión de Seguridad de la Información mediante la aplicación de la norma ISO/IEC 27001:2013 para la OGAD de la UNASAM?

   Muy Bajo ( ) Bajo ( ) Medio ( ) Alto ( ) Muy Alto ( )

2. ¿Cómo califica usted el inventario de los activos en el Diseño de un Sistema de Gestión de Seguridad de la Información mediante la aplicación de la norma ISO/IEC 27001:2013 para la OGAD de la UNASAM?

   Muy Bajo ( ) Bajo ( ) Medio ( ) Alto ( ) Muy Alto ( )

3. ¿Cómo evalúa usted la identificación y valoración de amenazas en el Diseño de un Sistema de Gestión de Seguridad de la Información mediante la aplicación de la norma ISO/IEC 27001:2013para la OGAD de la UNASAM?

   Muy Bajo ( ) Bajo ( ) Medio ( ) Alto ( ) Muy Alto ( )

4. ¿Cómo califica usted, en el Diseño de un Sistema de Gestión de Seguridad de la Información mediante la aplicación de la norma ISO/IEC 27001:2013, mejorar la seguridad de la información en los niveles de riesgos de la OGAD de la UNASAM?

   Muy Bajo ( ) Bajo ( ) Medio ( ) Alto ( ) Muy Alto ( )

5. ¿Cómo califica usted, en el Diseño de un Sistema de Gestión de Seguridad de la Información mediante la aplicación de la norma ISO/IEC 27001:2013 para la

OGAD de la UNASAM, el tratamiento de los riegos de la información mejora considerablemente la oficina?

Muy Bajo ( ) Bajo ( ) Medio ( ) Alto ( ) Muy Alto ( )

6. ¿Cómo evalúa usted, en el Diseño de un Sistema de Gestión de Seguridad de la Información mediante la aplicación de la norma ISO/IEC 27001:2013 para la OGAD de la UNASAM, la declaración de aplicabilidad?

Muy Bajo ( ) Bajo ( ) Medio ( ) Alto ( ) Muy Alto ( )

Anexo 02:

Nivel de Cumplimiento de los Dominios de Control de la Norma ISO/IEC 27001:2013.

Dominios de Control	Estado actual	Estado deseado
5 Políticas de Seguridad de la Información	5%	60%
6 Organización de la seguridad de la información	10%	60%
7 Seguridad de los recursos humanos	5%	60%
8 Gestión de activos	35%	60%
9 Control de acceso	13%	60%
10 Criptografía	5%	60%
11 Seguridad física y ambiental	10%	60%
12 Seguridad de las operaciones	5%	60%
13 Seguridad de las comunicaciones	8%	60%
14 Adquisición, desarrollo y mantenimiento de sistemas	5%	60%
15 Relaciones con los proveedores	0%	60%
16 Gestión de incidentes de seguridad de la información	6%	60%
17 Aspectos de seguridad de la información en la gestión de continuidad del negocio	23%	60%
18 Cumplimiento	13%	60%

Fuente: Elaboración propia en base a la Norma ISO/IEC 27001:2013.

Análisis de controles con el estado actual frente al estado esperado

Fuente: Elaboración propia en base a la Norma ISO/IEC 27001:2013.

Anexo 03: Encuesta a los trabajadores

Universidad Nacional Santiago Antúnez de Mayolo
Oficina General de Admisión
Encuesta al personal

Encueta a los trabajadores de la Oficina General de Admisión. (Marque con una X).

1) ¿Ha tenido en cuenta la posibilidad de perder información?
   a) Si
   b) No

2) ¿Ha tenido en cuenta la posibilidad de robo de sus datos?
   a) Si
   b) No

3) ¿Ha tenido en cuenta la posibilidad de fallos en sus discos duros?
   a) Si
   b) No

4) ¿Realiza copia de seguridad de sus datos?
   a) Si
   b) No

5) ¿Si hace copias de seguridad estas están Automatizadas?
   a) Si
   b) No

6) ¿Se almacenas las copias de seguridad en un lugar de acceso restringido?
   a) Si
   b) No

7) ¿Almacena una copia de seguridad semanal fuera de los edificios de trabajo?
   a) Si
   b) No

8) ¿Disponen de correo electrónico?
   a) Si
   b) No

9) ¿Protege su antivirus los e-mail, infracciones de seguridad y navegación web?
   a) Si
   b) No

10) ¿Existe algún control de sobre la navegación, correo y descarga de internet?
   a) Si
   b) No

11) ¿Se tiene una política en cuanto a seguridad?
   a) Si
   b) No

12) ¿Los equipos cuentan con un regulador?
   a) Si
   b) No

13) ¿Los cables están dentro de paneles y canaletas eléctricas?
   a) Si
   b) No

Anexo 04: formato de entrevista

Universidad Nacional Santiago Antúnez de Mayolo
Oficina General de Admisión
Entrevista

Personal de informática y sistemas de procesos de admisión

Nivel conocimiento de seguridad de la información por parte de su personal

1) Frente a cualquier desastre natural, provocado o humano ¿Su personal conoce cuales son los activos más importantes que debe proteger en relación a la información?

   SI ( )

   a. ¿Para ello existen procedimientos documentados para actuar antes, durante y después del desastre?_____

   b. ¿Ha realizado algún simulacro con defensa civil o tiene previsto hacerlo en el futuro?_____

   c. Lo cree necesario hacerlo con esta organización_____

   d. ¿Su área posee algún plan de contingencia, si no lo tiene ha motivado a sus trabajadores para elaborarlo?_____

   NO ( )

   e. ¿A qué se debe?_____

Backups y claves

1) La administración de todos los servicios de tecnología de información que están a su cargo se manejan a través de claves de autenticación_____

2) Cree usted necesario que la alta dirección deba poseer las claves (y su actualización de las mismas)_____

   Porqué_____

3) ¿Existe algún procedimiento para realizar backups, de la información que usted maneja?

   SI ( )

   a. ¿Están descritos en algún documento?_____

   b. ¿Se cumplen conforme están descritos?_____

   c. ¿Son depositados en algún lugar especial? _____

   4) Porqué_____

a. Cada que tiempo se hace y quién los realiza_____

NO ( )

b. Porqué_____

Problemas frecuentes

1) ¿Cuáles son los problemas más frecuentes con los que se enfrenta el área que Usted tiene a cargo?_____
2) Frente a las actividades de su área_____
3) Frente a los servicios que le brinda a los usuarios_____
4) ¿Se encuentran archivados esos problemas? _____
5) ¿Qué estrategia usa para disminuir esos problemas frecuentes? _____
6) Existe alguna estadística de la evolución de esos problemas_____
7) Emplean tarjetas o fichas de seguimiento de los equipos que se les brinda a los usuarios_____

Mantenimiento de los equipos

1) ¿Existe un plan de mantenimiento para todos los equipos?

   SI ( )

   a) Cada qué tiempo lo realizan_____
   b) ¿Qué aspectos son los que toman en cuenta para ese mantenimiento?_____
   c) Cómo se trata el tema de los antivirus _____

Adquisición de software y hardware

1) ¿Cuál es el procedimiento para la adquisición de un SW o HW?_____
2) Este procedimiento se encuentra debidamente identificado en un documento_____Porqué_____ _____
3) ¿Quién justifica la adquisición?_____
4) ¿Quién evalúa la adquisición?_____
5) ¿Quién evalúa los proveedores?_____

Anexo 05: Resultado de encuesta al personal de la Oficina General de Admisión

Preguntas:	Respuesta	Cantidad	(%)
1) ¿Ha tenido en cuenta la posibilidad de perder información?	SI	9	64%
	NO	5	26%
		Total	100%
2) ¿Ha tenido en cuenta la posibilidad de robo de sus datos?	SI	8	57%
	NO	6	43%
		Total	100%
3) ¿Ha tenido en cuenta la posibilidad de fallos en sus discos duros?	SI	5	26%
	NO	9	64%
		Total	100%
4) ¿Realiza copia de seguridad de sus datos?	SI	8	57%
	NO	6	43%
		Total	100%
5) ¿Si hace copias de seguridad estas están Automatizadas?	SI	2	14%
	NO	12	86%
		Total	100%
6) ¿Se almacenas las copias de seguridad en un lugar de acceso restringido?	SI	2	14%
	NO	12	86%
		Total	100%
7) ¿Almacena una copia de seguridad semanal fuera de los edificios de trabajo?	SI	1	7%
	NO	13	93%
		Total	100%
8) ¿Disponen de correo electrónico?	SI	13	93%
	NO	1	7%
		Total	100%
9) ¿Protege su antivirus los e-mail, infracciones de seguridad y navegación web?	SI	7	50%
	NO	7	50%
		Total	100%
10) ¿Existe algún control de sobre la navegación, correo y descarga de internet?	SI	5	26%
	NO	9	64%
		Total	100%
11) ¿Se tiene una política en cuanto a seguridad?	SI	4	29%
	NO	9	71%
		Total	100%
12) ¿Los equipos cuentan con un regulador?	SI	6	43%
	NO	8	57%
		Total	100%
13) ¿Los cables están dentro de paneles y canaletas eléctricas?	SI	8	57%
	NO	6	43%
		Total	100%

Anexo 06

Universidad Nacional Santiago Antúnez de Mayolo
Oficina General de Admisión
DECLARACIÓN DE APLICABILIDAD
(ISO/IEC 27001:2013 – NTP ISO/IEC 27001:2014)

Leyenda: (Razón de controles seleccionados)

Sec.	Objetivos de control y controles	Apli_ cable	Visión General de la Implementación
5	**Políticas de Seguridad de la Información**		
5.1	**Dirección de la gerencia para la seguridad de la información**		
5.1.1	Política para la seguridad de la información	SI	Redacción y documentación de las políticas de seguridad de la información acorde a los objetivos de seguridad acordados y niveles de riesgo tolerable y este documento poner a disposición de los empleados y público en general.
5.1.2	Revisión de las políticas para la seguridad de la información	SI	Las políticas de seguridad de la información se revisan y evalúan periódicamente y/o cuando sea necesario. Se documentan los cambios y las justificaciones de los mismos.
6	**Organización de la seguridad de la información**		
6.1	**Organización interna**		
6.1.1	Roles y responsabilidades para la seguridad de la información	SI	Se debe establecer los roles y responsabilidades de la seguridad de la información.
6.1.2	Segregación de funciones	SI	Al personal se le otorga acceso sólo a los activos y/o información estrictamente necesaria para la realización de su trabajo.
6.1.3	Contacto con autoridades	SI	Mantener los contactos actualizados para incidentes de seguridad.
6.1.4	Contacto con grupos especiales de interés	SI	Mantener contactos con los grupos de interés (Reniec, etc) para los incidentes de seguridad para informes en tiempo real y soluciones a implementar.

Sec.	Objetivos de control y controles	Apli_ cable	Visión General de la Implementación
6.1.5	Seguridad de la información en la gestión de proyectos	SI	Aplicación de una metodología de análisis y evaluación de riesgos y seguir los lineamientos de la seguridad de la información, con la finalidad de garantizar el cumplimiento de los requisitos de seguridad de la oficina.
6.2	**Dispositivos móviles y teletrabajo**		
6.2.1	Política de dispositivos móviles	SI	no aplica para nuestro estudio dado a que no se utilizan dispositivos móviles en los procesos del alcance del proyecto
6.2.2	Teletrabajo	NO	
7	**Seguridad de los recursos humanos**		
7.1	**Antes del empleo**		
7.1.1	Selección	SI	El personal es seleccionado cuidadosamente en base a su perfil y la idoneidad del trabajo a realizar.
7.1.2	Términos y condiciones del empleo	SI	Los acuerdos contractuales actualmente incluyen las responsabilidades asignadas relativas a la seguridad de la información.
7.2	**Durante el empleo**		
7.2.1	Responsabilidades de la gerencia	SI	La oficina comprende la importancia de la seguridad de la información y soporta el diseño del SGSI puesto que esto corresponde al plan estratégico de la oficina y a los intereses de los usuarios como parte activa en los requerimientos.
7.2.2	Conciencia, educación y capacitación sobre la seguridad de la información	SI	Se debe establecer un plan de capacitación para los colaboradores, acerca de la política de seguridad de la información, del mismo modo la evaluación que nos permitirá medir el nivel de conocimiento del tema.
7.2.3	Proceso disciplinario	SI	El personal debe ser sometido a procesos disciplinarios en caso de incumplimiento con las políticas de seguridad de la información de forma deliberada.
7.3	**Terminación y cambio de empleo**		
7.3.1	Terminación o cambio de responsabilidades del empleo.	SI	El periodo de tiempo al cual se encuentra sujeta el colaborador debe cumplir con los términos y condiciones de seguridad de la información establecido en el momento de incorporarse, lo que permitirá a la oficina protegerse de posibles filtraciones realizadas por personal que ya no labora en un proceso de admisión.
8	**Gestión de activos**		
8.1	**Responsabilidad por los activos**		
8.1.1	Inventario de activos	SI	Realizar el inventario de activos y se documentan con su clasificación y responsable
8.1.2	Propiedad de los activos	SI	Los activos inventariados tienen asignados a los personales responsables.

Sec.	Objetivos de control y controles	Apli_ cable	Visión General de la Implementación
8.1.3	Uso aceptable de los activos	SI	Debe especificarse, documentar y comprometerse a utilizar los activos de forma aceptable teniendo en cuenta las políticas de seguridad de la información.
8.1.4	Retorno de activos	SI	Se mantienen registros de la devolución de los activos entregados al personal de la oficina.
8.2	**Clasificación de la información**		
8.2.1	Clasificación de la información	SI	Cada uno de los activos inventariados contiene la clasificación de la información asociada de acuerdo a los niveles de seguridad establecidos
8.2.2	Etiquetado de la información	SI	La clasificación de la información debe ser dependiendo del contexto, por este motivo se debe revisar la clasificación periódicamente.
8.2.3	Manejo de activos	SI	Documentar los procedimientos para el manejo de los activos de acuerdo a la clasificación de cada uno.
8.3	**Manejo de los medios**		
8.3.1	Gestión de medios removibles	SI	Debe existir una política para la gestión de los medios removibles y clasificar, proteger de acuerdo a su tipo.
8.3.2	Disposición de medios	SI	Los medio removibles son dispuestos en lugares seguros y su información es almacenada en medios seguros.
8.3.3	Transferencia de medios físicos	NO	
9	**Control de acceso**		
9.1	**Requisitos de la empresa para el control de acceso**		
9.1.1	Política de control de acceso	SI	La política de control de acceso debe estar documentada en las políticas de la seguridad de información y debe ser de conocimiento del personal.
9.1.2	Acceso a redes y servicios de red	SI	Los niveles de control de acceso deben ser establecidos según los lineamientos de uso del personal y al acceso que van a tener tanto interna y externamente.
9.2	**Gestión de acceso de usuario**		
9.2.1	Registro y baja de usuarios	SI	Para poder mitigar el riesgo de acceso no autorizado, se debe mantener un procedimiento de altas y sobre todo bajas de usuarios de los sistemas que maneja la oficina.
9.2.2	Aprovisionamiento de acceso a usuario	NO	
9.2.3	Gestión de derechos de acceso privilegiados	SI	Se debe establecer la segregación de funciones en base al cargo del personal, de este modo se puede diseñar un control de privilegio de accesos.

Sec.	Objetivos de control y controles	Apli_ cable	Visión General de la Implementación
9.2.4	Gestión de información de autentificación secreta de usuarios	SI	La asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado que permitirá tener una trazabilidad de las acciones realizadas por los usuarios.
9.2.5	Revisión de derechos de acceso de usuarios	SI	Verificar que los permisos y derechos de acceso de los usuarios son los que en realidad tiene asignados.
9.2.6	Remoción o ajuste de derechos de acceso	SI	Verificar y eliminan los permisos asignados al personal que sea retirado.
9.3	**Responsabilidades de los usuarios**		
9.3.1	Uso de información de autentificación secreta	SI	La información de autenticación del personal en los sistemas y acceso a información es confidencial.
9.4	**Control de acceso a sistema y aplicación**		
9.4.1	Restricción de acceso a la información	SI	Los derechos de acceso a los sistemas e información son controlados de acuerdo a rol y responsabilidad del personal en la organización.
9.4.2	Procedimientos de ingreso seguro	SI	Los sistemas deben estar protegidos mediante un mecanismo de inicio de sesión seguro.
9.4.3	Sistema de gestión de contraseñas	SI	Se implementarían mecanismos de recuperación de contraseñas de forma automática
9.4.4	Uso de programas utilitarios privilegiados	SI	Verificar que los sistemas y activos críticos sólo se les instalan los programas estrictamente necesarios y licenciados
9.4.5	Control de acceso al código fuente de los programas		Verificar que los códigos fuentes de los programas permanecen de forma confidencial restringiendo su acceso.
10	**Criptografía**		
10.1	**Controles criptográficos**		
10.1.1	Política sobre el uso de controles criptográficos	SI	Debe manejarse y activar controles criptográficos que garanticen que la información debe mantenerse bajo custodia para tener la integridad de la información y evitar que se pueda transferir la información
10.1.2	Gestión de claves	SI	Debería existir una política de seguridad que documente el proceso y ciclo de vida de las llaves criptográficas.
11	**Seguridad física y ambiental**		
11.1	**Áreas seguras**		
11.1.1	Perímetro de seguridad física	SI	Se deberían definir y utilizar perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica.

Sec.	Objetivos de control y controles	Apli_ cable	Visión General de la Implementación
11.1.2	Controles de ingreso físico	SI	Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado.
11.1.3	Asegurar oficinas, áreas e instalaciones	SI	Se debería diseñar y aplicar un sistema de seguridad física.
11.1.4	Protección contra amenazas externas y ambientales	SI	Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes, que puedan afectar tanto natural como provocados (incendios).
11.1.5	Trabajo en áreas seguras	SI	Se deberían diseñar y aplicar procedimientos para el desarrollo de trabajos y actividades en áreas seguras.
11.1.6	Áreas de despacho y carga	NO	
11.2	**Equipos**		
11.2.1	Emplazamiento y protección de los equipos	SI	Los equipos deben estar protegidos físicamente contra amenazas ambientales tales como fuego, incendio, agua, humo, etc.
11.2.2	Servicios de suministro	SI	Los servicios de suministros como energía deben ser protegidos.
11.2.3	Seguridad del cableado	SI	El cableado eléctrico debería estar separado del cableado de datos previniendo así interferencias.
11.2.4	Mantenimiento de equipos	SI	Los equipos que cuenten con acceso a información crítica deberán seguir un procedimiento de mantenimiento adecuado de manera que loa información que contienen no sea comprometida.
11.2.5	Remoción de activos	NO	
11.2.6	Seguridad de equipos y activos fuera de las instalaciones	SI	La oficina debe asegurar que cualquier uso externo de equipos que maneje información tenga la autorización correspondiente.
11.2.7	Disposición o reutilización segura de equipos	SI	Los equipos informáticos que se den de baja o se cambien de ambiente deben haber pasado por un proceso de eliminación de la información que puedan contener.
11.2.8	Equipos de usuario desatendidos	SI	Los usuarios deberán mantener la seguridad de sus equipos incluso cuando no estén trabajando con los mismos
11.2.9	Política de escritorio limpio y pantalla limpia	SI	Los usuarios deberán mantener sus escritorios libres de cualquier información sensible que pueda usar un agente externo como consecuencia de sus exposición como parte de un olvido o mala gestión
12	**Seguridad de las operaciones**		
12.1	**Procedimientos y responsabilidades operativas**		
12.1.1	Procedimientos operativos documentados	SI	Documentar los procedimientos de las operaciones relativas a la seguridad de la información de cada uno de los activos.

Sec.	Objetivos de control y controles	Apli_ cable	Visión General de la Implementación
12.1.2	Gestión del cambio	SI	Se deberá realizar el control de los cambios que afectan a la seguridad de la información y procesos de negocio, las instalaciones y sistemas de procesamiento de información.
12.1.3	Gestión de la capacidad	SI	Se necesitará monitorear y ajustar el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas.
12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	SI	Cada entorno de desarrollo, pruebas y operacionales deberían permanecer separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional.
12.2	**Protección contra códigos maliciosos**		
12.2.1	Controles contra códigos maliciosos	SI	Verificar que el software está protegido con antivirus y existe una política documentada de actualización de todo el software utilizado, antivirus y sistema operativo.
12.3	**Respaldo**		
12.3.1	Respaldo de la información	SI	Realizan las copias de seguridad de toda la información a intervalos programados y de acuerdo a las políticas de seguridad.
12.4	**Registros y monitoreo**		
12.4.1	Registro de eventos	SI	Se tiene que producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información.
12.4.2	Protección de información de registros.	SI	Se debería proteger contra posibles alteraciones y accesos no autorizados la información de los registros.
12.4.3	Registros del administrador y del operador	SI	Se deberían registrar las actividades del administrador y del operador del sistema y los registros asociados se deberían proteger y revisar de manera regular.
12.4.4	Sincronización de reloj		Se deberían sincronizar los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una oficina.
12.5	**Control del software operacional**		
12.5.1	Instalación de software en sistemas operacionales	SI	Se deberían implementar procedimiento de instalación de los sistemas operativos y software, que cumpla con las políticas de seguridad de la información.
12.6	**Gestión de vulnerabilidad técnica**		

Sec.	Objetivos de control y controles	Apli_ cable	Visión General de la Implementación
12.6.1	Gestión de vulnerabilidades técnicas	SI	Se debería obtener información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna para evaluar el grado de exposición de la organización y tomar las medidas necesarias para abordar los riesgos asociados.
12.6.2	Restricciones sobre la instalación de software	SI	Se deberían establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.
12.7	**Consideraciones para la auditoría de los sistemas de información.**		
12.7.1	Controles de auditoría de sistemas de información	SI	Se deberían planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.
13	**Seguridad de las comunicaciones**		
13.1	**Gestión de seguridad de la red**		
13.1.1	Controles de la red	SI	Se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones.
13.1.2	Seguridad de servicios de red	SI	Se deberían identificar e incluir los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados.
13.1.3	Segregación en redes	SI	Se deberían segregar las redes en función de los grupos de servicios, usuarios y sistemas de información.
13.2	**Transferencia de información**		
13.2.1	Políticas y procedimientos de transferencia de la información	SI	La seguridad necesaria para garantizar la confidencialidad e integridad de la información.
13.2.2	Acuerdo sobre transferencia de información	SI	Deberían existir acuerdos que abordar la transferencia segura de información entre la oficina y las partes externas.
13.2.3	Mensajes electrónicos	SI	Debería garanticen la confidencialidad e integridad de la información que se transmite a través de las redes.
13.2.4	Acuerdos de confidencialidad o no divulgación	SI	En los documentos y acuerdos contractuales del personal que labora en la oficina o participa del proceso de admisión se estipula el compromiso con la confidencialidad de la información.
14	**Adquisición, desarrollo y mantenimiento de sistemas**		

Sec.	Objetivos de control y controles	Apli_ cable	Visión General de la Implementación
14.1	**Requisitos de seguridad de los sistemas de información**		
14.1.1	Análisis y especificación de requisitos de seguridad de la información	SI	Los requisitos relacionados con la seguridad de la información se deberían incluir en los requisitos para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes.
14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas	SI	La información de los servicios de aplicación que pasan a través de redes públicas se debería proteger contra actividades fraudulentas y modificación no autorizada.
14.1.3	Protección de transacciones en servicios de aplicación	SI	La información en transacciones de servicios de aplicación se debería proteger para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción.
14.2	**Seguridad en los procesos de desarrollo y soporte**		
14.2.1	Política de desarrollo seguro	NO	
14.2.2	Procedimientos de control de cambio del sistema	NO	
14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	SI	Debería existir documentación sobre la implementación de las nuevas aplicaciones y son sometidas a pruebas para garantizar que no haya impactos adversos en la seguridad de la información.
14.2.4	Restricciones sobre cambios a los paquetes de software	SI	Se deberían evitar modificaciones en los paquetes de software suministrados por terceros, limitándose a cambios realmente necesarios. Todos los cambios se deberían controlar estrictamente.
14.2.5	Principios de ingeniería de sistemas seguros	SI	Se deberían establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información.
14.2.6	Ambiente de desarrollo seguro	SI	La oficina debería establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de DEMING de desarrollo del sistema.
14.2.7	Desarrollo contratado externamente	SI	La oficina debería supervisar y monitorear las actividades de desarrollo del sistema que se hayan externalizado.
14.2.8	Pruebas de seguridad del sistema	SI	Se deberían realizar pruebas de seguridad a los sistemas y documentan los procedimientos.
14.2.9	Pruebas de aceptación del sistema	SI	Se deberían establecer programas de prueba y criterios relacionados para la aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones.
14.3	**Datos de prueba**		

Sec.	Objetivos de control y controles	Apli_ cable	Visión General de la Implementación
14.3.1	Protección de datos de prueba	SI	Los datos de pruebas se deberían seleccionar cuidadosamente y se deberían proteger y controlar.
15	**Relaciones con los proveedores**		
15.1	**Seguridad de la información en las relaciones con los proveedores**		
15.1.1	Política de seguridad de la información para las relaciones con los proveedores	SI	Se deberían acordar y documentar adecuadamente los requisitos de seguridad de la información requeridos por los activos de la organización con el objetivo de mitigar los riesgos asociados al acceso por parte de terceras personas.
15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	NO	
15.1.3	Cadena de suministro de tecnología de información y comunicación	NO	
15.2	**Gestión de entrega de servicios del proveedor**		
15.2.1	Monitoreo y revisión de servicios de los proveedores	NO	
15.2.2	Gestión de cambios a los servicios de proveedores	NO	
16	**Gestión de incidentes de seguridad de la información**		
16.1	**Gestión de incidentes de seguridad de la información y mejoras**		
16.1.1	Responsabilidades y procedimientos	SI	Documentar los procesos y procedimientos para los incidentes de la seguridad de la información
16.1.2	Reporte de eventos de seguridad de la información	SI	Los incidentes deberían ser reportados, evaluados y documentados. Se establecen los procedimientos a seguir.
16.1.3	Reporte de debilidades de seguridad de la información	SI	Deberían existir los formatos documentados disponibles para que los funcionarios reporten las debilidades de la seguridad de la información.
16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	SI	Deberían existir los formatos documentados disponibles para que los funcionarios reporten las debilidades de la seguridad de la información.

Sec.	Objetivos de control y controles	Apli_ cable	Visión General de la Implementación
16.1.5	Respuesta a incidentes de seguridad de la información	SI	Se debería documentar los procesos y procedimientos para los incidentes de la seguridad de la información.
16.1.6	Aprendizaje de los incidentes de seguridad de la información	SI	Los incidentes de la seguridad de la información son documentados especificando las vulnerabilidades, amenazas, riesgos y los posibles controles de seguridad a implementar constituyendo así una base de conocimiento.
16.1.7	Recolección de evidencia	SI	Deberían existir formatos y documentos para recolectar la evidencia y emitirlos a las autoridades competentes.
17	**Aspectos de seguridad de la información en la gestión de continuidad del negocio**		
17.1	**Continuidad de seguridad de la información**		
17.1.1	Planificación de continuidad de seguridad de la información	SI	La organización debería determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre.
17.1.2	Implementación de continuidad de seguridad de la información	SI	La organización debería establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas.
17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información	SI	La organización debería verificar regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas.
17.2	**Redundancias**		
17.2.1	Instalaciones de procesamiento de la información	SI	Se debería implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad.
18	**Cumplimiento**		
18.1	**Cumplimiento con requisitos legales y contractuales**		
18.1.1	Identificación de requisitos contractuales y de legislación aplicables	SI	Los requisitos contractuales están identificados y se cumplen con los requerimientos exigidos por la ley.

Sec.	Objetivos de control y controles	Apli_ cable	Visión General de la Implementación
18.1.2	Derechos de propiedad intelectual	NO	
18.1.3	Protección de registros	SI	Los registros deberían estar protegidos físicamente contra alteración, modificación, pérdida y acceso de usuarios no autorizados.
18.1.4	Privacidad y protección de datos personales.	SI	Los datos personales deberían ser almacenados y protegidos de acuerdo de la ley.
18.1.5	Regulación de controles criptográficos	SI	Se deberían utilizar controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.
18.2	**Revisiones de seguridad de la información**		
18.2.1	Revisión independiente de la seguridad de la información	SI	Se debería revisar el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) y gestión de la seguridad de la información en base a revisiones independientes e intervalos planificados o cuando tengan lugar cambios significativos.
18.2.2	Cumplimiento de políticas y normas de seguridad	SI	Los jefes y responsables deberían revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente.
18.2.3	Revisión del cumplimiento técnico	SI	Los sistemas de información se deberían revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización.