UNIVERSIDAD NACIONAL
SANTIAGO ANTÚNEZ DE MAYOLO

FACULTAD DE CIENCIAS
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

"MODELO BASADO EN LA NORMA TÉCNICA PERUANA 17799 PARA MEJORAR LA GESTIÓN DE SEGURIDAD DE LA INFRAESTRUCTURA DE TECNOLOGÍAS DIGITALES DE LA OFICINA GENERAL DE ADMISIÓN DE LA UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO"

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS E INFORMATICA

PRESENTADO POR:

Bachiller ANDY JUNIOR BONILLA RIVERA

ASESOR:

Mag. Ing. MIGUEL ÁNGEL SILVA ZAPATA

HUARAZ - PERU

2022

N° Registro: T139

DEDICATORIA

A mis padres, por el apoyo incondicional que me brindan cada día en mi desarrollo profesional y personal, que son la fuerza y razón que me impulsa a seguir adelante para hacer realidad mis metas.

A mis hermanos por el constante apoyo que me brindan para seguir adelante en mis proyectos.

A mis familiares y amigos, por los consejos brindados para seguir adelante en mi desarrollo como profesional.

A mi asesor por el constante apoyo y guía en el desarrollo de la tesis.

AGRADECIMIENTO

Estoy agradecido con mis padres porque han sido el motor de mis sueños, han estado a mi lado en mi formación profesional, han sido mis guías en la vida, y hoy estoy terminando una etapa más de mis estudios, la cual voy a lograr. se dedica como uno de mis objetivos.

Los consejos y palabras de mis maestros fueron sabios, sus conocimientos y requerimientos durante mis estudios moldearon mi responsabilidad y amor por la materia que elegí estudiar, y los llevaré conmigo en mi camino como profesional, gracias por su paciencia y compartiendo mis conocimientos.

Gracias a mi asesor, sin tus conocimientos, sin tu paciencia y perseverancia no lo hubiera logrado y tus consejos son muy útiles cuando no pensé en escribir lo que logré hoy.

RESUMEN

El presente Informe Final de Tesis, titulado “Modelo Basado En La Norma Técnica Peruana 17799 Para Mejorar La Gestión De Seguridad De La Infraestructura De Tecnologías Digitales De La Oficina General De Admisión De La Universidad Nacional Santiago Antúnez De Mayolo”. Tiene como objetivo principal Mejorar la gestión de seguridad de la infraestructura de las tecnologías digitales, mediante un modelo basado en la norma técnica peruana 17799 de la Oficina General de Admisión de la Universidad Nacional Santiago Antúnez De Mayolo.

Puesto que en la actualidad la Oficina General de Admisión carece de controles o políticas de gestión de seguridad de la información, lo cual ha sido demostrado en la investigación, sabiendo que la Oficina General de Admisión trata toda la información de los postulantes de los procesos llevados a cabo en la UNASAM.

Para solucionar la problemática en la Oficina General de Admisión se desarrolló un Modelo Basado En La Norma Técnica Peruana 17799 Para Mejorar La Gestión De Seguridad De La Infraestructura De Tecnologías Digitales.

Para la investigación se definió como variable Independiente como Modelo Basado en la Norma Técnica Peruana 17799 y la variable dependiente como Gestión de Seguridad de la Infraestructura de las Tecnologías Digitales.

En la presente investigación se utilizó la metodología de tipo experimental para el desarrollo de la investigación, teniendo como población de 354 postulantes.

Al finalizar la investigación se llegaron a las siguientes conclusiones, el modelo basado en la norma técnica peruana 17799 mejora la gestión de seguridad de la infraestructura de tecnologías digitales de la oficina general de admisión de la universidad nacional Santiago Antúnez de Mayolo – Huaraz, lo cual se contrasto con la aplicación de la prueba de normalidad de Kolmogorov Smirnov obteniendo el resultado de 0.007, siendo menor al nivel de significancia al 5%.

ABSTRACT

This Final Thesis Report, entitled Model Based On The Peruvian Technical Standard 17799 To Improve Security Management Of The Digital Technology Infrastructure Of The General Admissions Office Of The Santiago Antúnez De Mayolo National University. Its main objective is to improve the security management of the digital technology infrastructure, through a model based on the Peruvian technical standard 17799 of the General Admission Office of the Santiago Antúnez De Mayolo National University.

Since currently the General Admissions Office lacks an information security management model or policies, which has been demonstrated in the investigation, knowing that the General Admissions Office handles all the information of the applicants of the processes held at UNASAM.

To solve the problem in the General Admissions Office, a Model Based on the Peruvian Technical Standard 17799 was developed to Improve the Security Management of the Digital Technology Infrastructure.

For the investigation, the Independent variable was defined as a Model Based on the Peruvian Technical Standard 17799 and the dependent variable as Security Management of the Digital Technologies Infrastructure.

In the present investigation, the experimental type methodology was used for the development of the investigation, having a population of 354 applicants.

At the end of the investigation, the following conclusions were reached: the model based on the Peruvian technical standard 17799 improves the security management of the digital technology infrastructure of the general admission office of the Santiago Antúnez de Mayolo - Huaraz National University, which It was contrasted with the application of the Kolmogorov Smirnov normality test, obtaining the result of 0.007, being less than the level of significance at 5%.

INDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

“MODELO BASADO EN LA NORMA TÉCNICA PERUANA 17799 PARA MEJORAR LA GESTIÓN DE SEGURIDAD DE LA INFRAESTRUCTURA DE TECNOLOGÍAS DIGITALES DE LA OFICINA GENERAL DE ADMISIÓN DE LA UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO”

I. INTRODUCCIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA

La Oficina General de Admisión (OGAD), es un órgano autónomo de la UNASAM, encargada de organizar y conducir los procesos de Admisión a nivel de pregrado y postgrado, depende del Vicerrectorado Académico. Tiene potestad sobre el personal docente y administrativo, nombrado y contratado de Las Comisiones Centrales de Admisión de Pregrado y Postgrado; así como, del personal administrativo.

En la oficina general de admisión se realizan 4 procesos fundamentales:

- **PROCESO DE CONSIGNACIÓN DE VACANTES:** En este proceso la OGAD se encarga de solicitar a todas las facultades las vacantes que ofertaran durante todo el año, información que es analizada por el jefe encargado de hacer una propuesta de vacantes para el proceso que luego se somete a la aprobación por consejo universitario, una vez que las vacantes son aprobadas con resolución el jefe de la OGAD entrega las vacantes al presidente de la comisión para que inicie las acciones del nuevo proceso.
- **PROCESO DE PLANIFICACIÓN Y/O ORGANIZACIÓN:** Dentro de este proceso la comisión central de admisión elabora el plan de trabajo y presupuesto que necesita y lo somete a la aprobación por consejo UNIVERSITARIO.
- **PROCESO DE INSCRIPCIÓN:** En este proceso se publican de manera oficial las fechas de examen e inicio de inscripción al proceso de admisión en curso, así como también los requisitos para postular y se da inicio a las inscripciones, que se llevan a cabo mediante la página web de admisión disponible al público en general.
- **PROCESO DE ELABORACIÓN:** El responsable encargado de llevar a cabo el proceso conforma un equipo de docentes especializados en los temas que contiene el temario de examen de admisión, para que cumplan la función de elaborar las preguntas del examen con sus respectivas respuestas y alternativas, elaboradas las preguntas estas son entregadas al encargado de digitar el examen, por lo que el digitador transcribe todas las preguntas en el formato oficial del examen, una vez digitadas las preguntas del examen se procede a su revisión minuciosa con sus respectivas

respuestas correctas, finalizada la revisión todas las claves son llenadas manualmente en una tarjeta OMR para ser entregada al responsable de calificación.

- **PROCESO DE APLICACIÓN:** En este proceso el responsable gestiona y organiza las actividades relacionadas con la aplicación del examen de admisión, coordina con los decanos de las facultades con el fin de verificar las aulas y realizar la proyección de cuantas se requieren para llevar a cabo el examen. En otro momento el responsable solicita de manera oficial los ambientes que se utilizaran para el examen, también se encarga de realizar las coordinaciones con la policía para que brinden el servicio de resguardo policial y control biométrico, se preparan los equipos que utilizara la policía para el control biométrico en la aplicación del examen. Hace la convocatoria para la selección de vigilantes de aulas y personal de apoyo para el examen, una vez realizadas todas las coordinaciones y llegado el día de examen el responsable se encarga realizar la verificación de los ambientes a utilizar antes de que ingrese cualquier personal de la comisión. Se encarga del control de ingreso de los vigilantes de aula y coordinadores para esto cuenta con la relación y datos personales de cada vigilante de aula; así mismo en paralelo designa a un miembro de la comisión para que se encargue de hacer las instalaciones de control electrónico de postulantes y controlar el ingreso del personal de apoyo. Llegada la hora indicada de ingreso de los postulantes el responsable espera en el centro de acopio al presidente de la comisión para hacerle entrega de los exámenes de admisión y materiales que se utilizaran durante la evaluación; así también llena las actas de entregas de exámenes, según la guía del postulante se procede a cumplir con las indicaciones del examen, una vez iniciado el examen se le da un tiempo prudente a cada vigilante para que pueda indicar a los postulantes como deben de llenar correctamente la tarjeta OMR (Identificación y Respuesta), cada coordinador de pabellón o local es el encargado de recoger y verificar que todas las tarjetas estén completas y bien llenadas antes de ser entregas al responsable de aplicación, quien realiza una verificación de todas las tarjetas junto a su equipo especializado en revisión de tarjetas OMR, si se detecta algún error o deterioro de tarjeta OMR se informa al coordinador para que pueda subsanar el inconveniente,

cuando se tiene todas las tarjetas OMR de los postulantes el responsable las entrega al presidente de la comisión para que sea conducido al lugar donde se realizara la calificación del examen, todo esto sucede en un primer momento al iniciar el examen. Un segundo momento es cuando termina el examen y los coordinadores recogen las tarjetas de respuestas de todos los postulantes para así repetir el proceso de entrega y verificación al responsable de aplicación, culminada la revisión de las tarjetas de respuesta se genera la última entrega de tarjetas de respuestas al presidente de la comisión, el presidente se encarga de llevar las tarjetas de respuestas al centro de calificación.

- **PROCESO DE CALIFICACIÓN:** En el proceso de calificación el responsable de calificar los exámenes de admisión recibe por parte de la oficina general de admisión las vacantes oficiales para que pueda realizar la calificación.

  El presidente de la comisión hace entrega de las tarjetas de identificación en un primer momento para que sean leídas mediante el Escanear de calificación y así generar una base de datos de los postulantes en el software de calificación, en un segundo momento el presidente entrega las tarjetas de respuestas al calificador es ahí donde el calificador procede a la lectura de las tarjetas de respuestas y realiza una combinación entre las tarjetas de identificación y respuestas, ya cuando se tiene la base de datos oficial de los postulantes con sus respuestas leídas, el notario y el fedatario entregan al calificador las claves de los exámenes para que pueda iniciar con la calificación.

  El calificador notifica al presidente de la comisión que se concluyó la calificación del examen, es ahí donde el presidente de la comisión toma 2 tarjetas OMR al azar para que realice una verificación manual de los resultados, una vez contrastado el presidente informa al calificador que genere los reportes correspondientes para su publicación y validación del notario, jefe de la OGAD y el presidente.

- **PROCESO DE ACREDITACIÓN DEL INGRESANTE:** En el proceso de acreditación de postulantes, la oficina general de admisión recibe la documentación requerida (requisitos para acreditar el ingreso) según

cronograma, luego que todos los ingresantes formalicen sus documentos, se procede de manera manual al llenado en el sistema web todos los requisitos que presento el ingresante para luego de ello poder asignarles el código de estudiante y su número de expediente, cuando se generan los códigos y números de expediente se sacan los reportes oficiales de ingresantes por cada carrera profesional para luego ser entregados a las respectivas facultades.

En este proceso se maneja toda la información sensible de los ingresantes, es aquí cuando se les entrega la constancia de ingreso de manera virtual mediante la página web de admisión, dicha información está de manera pública y puede ser revisada por el ingresante en todo momento, cabe resaltar que las constancias de ingreso cuentan con un código QR que cumple la función de verificación de autenticada de la constancia de ingreso.

En todos estos procesos se genera y utiliza información sensible que está estrechamente relacionada con la imagen y prestigio institucional que se proyecta hacia la sociedad. Sin embargo, actualmente existen problemas que atentan contra la seguridad de la infraestructura digital que gestiona toda esta información, que se generan por la falta de seguridad reflejada en los diferentes aspectos:

- No existe políticas de seguridad de la información.
- No se sabe si hay vulneración, ataques, extracción de datos.
- No se tiene un control de seguridad de la información adecuado en la oficina.
- No se tiene un test de seguridad de información
- Los equipos informáticos están desfasados lo cual los hace más vulnerables.
- Toda la información de los postulantes se encuentra alojado en un hosting, pero no sabe si cuenta con protección de datos.
- Centralización de toda la base de datos en un solo ordenador, sin contar con las réplicas necesarias.
- No se cuenta con un control en el proceso de calificación de exámenes.
- No se tiene una correcta evaluación de la información

- Posibilidades de filtración de información.

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1. PROBLEMA GENERAL

¿En qué medida mejora la gestión de la seguridad de la infraestructura de las tecnologías digitales de la Oficina General de Admisión de la universidad nacional Santiago Antúnez de Mayolo con el Modelo basado en la norma técnica peruana 17799?

1.2.2. PROBLEMAS ESPECIFICOS

- ¿Reducir las alertas mejorará la gestión de seguridad de la infraestructura de las Tecnologías Digitales de la OGAD?

- ¿Limitar los ataques mejorará la gestión de seguridad de la infraestructura de las Tecnologías Digitales de la OGAD?

- ¿Minimizar las vulnerabilidades mejorará la gestión de seguridad de la infraestructura de las Tecnologías Digitales de la OGAD?

1.3. OBJETIVOS DE LA INVESTIGACIÓN

1.3.1. OBJETIVO GENERAL

Mejorar la gestión de seguridad de la infraestructura de las tecnologías digitales, mediante un modelo basado en la norma técnica peruana 17799 de la Oficina General de Admisión de la Universidad Nacional Santiago Antúnez De Mayolo.

1.3.2. OBJETIVOS ESPECIFICOS

- Reducir las alertas que influyen en la gestión de seguridad de la infraestructura de las Tecnologías Digitales de la OGAD.
- Limitar los ataques en la gestión de seguridad de la infraestructura de las Tecnologías Digitales de la OGAD.
- Minimizar las vulnerabilidades que intervienen en la gestión de seguridad de la infraestructura de las Tecnologías Digitales de la OGAD.

1.4. JUSTIFICACIÓN DE LA INVESTIGACIÓN

1.4.1. JUSTIFICACIÓN SOCIAL

Se justifica socialmente porque el modelo basado en la norma técnica peruana 17799, el análisis y el tratamiento que se le da a los riesgos son puntos importantes y críticos, por lo que tratamos de generar conciencia a la población comprendida por profesionales que labora en la Oficina General de Admisión y dar la importancia que se merece ya que la Oficina General de Admisión tiene datos sensibles para ello es importante tener un modelo basado en la norma técnica peruana 17799 para identificar, analizar y evaluar los riesgos que enfrentan para garantizar que las personas reciban servicios de alta calidad y que las personas se sientan seguras al iniciar cualquier procedimiento en la Oficina General de Admisión.

1.4.2. JUSTIFICACIÓN ECONOMICA

El presente proyecto económicamente es viable porque llega hasta el proceso de desarrollo, teniendo como producto final una propuesta que dependerá de las autoridades si se llega a dar su aplicación.

1.4.3. JUSTIFICACIÓN TECNOLOGICA

El presente proyecto es técnicamente factible porque la tecnología evoluciona a pasos agitanados, en la actualidad la Norma Técnica Peruana 17799 es una Norma de uso obligatorio y en la presente investigación se pretende crear un modelo que permite su implementación en OGAD.

En el diario El Peruano, menciona lo siguiente (Peruano, 2016) “Aprueban el uso obligatorio de la Norma Técnica Peruana (NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición), en todas las entidades integrantes del Sistema Nacional de Informática”.

A demás se cuenta con el conocimiento y los recursos para poder realizar el modelo basado en la norma técnica peruana 17799, lo cual el proyecto traerá beneficios a la Oficina General de Admisión UNASAM y a la Institución.

1.4.4. JUSTIFICACIÓN OPERATIVA

La Oficina General de Admisión es la encargada de realizar Procesos de Exámenes de Admisión siendo la Oficina la encargada de manejar información sensible de los postulantes e ingresantes a la Universidad Nacional Santiago Antúnez de Mayolo y que vela por el correcto funcionamiento de los sistemas. La Oficina General de Admisión cuenta con personal especializado por lo que no será un problema capacitarlo para garantizar el cumplimiento del modelo que se establecerá en cuanto a la seguridad de información.

1.4.5. JUSTIFICACIÓN LEGAL

El proyecto tiene justificación legal en el diario El Peruano (Peruano, 2016) la cual menciona que la "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

(Peruano, 2016) dicha norma tiene Resolución Ministerial Nº 197-2011-PCM, al ser aprobado con la Resolución Ministerial, se fijaron tiempos para que las entidades públicas implementen el Plan de Seguridad de la Información dispuesto en la NTP; posteriormente, con la Resolución Ministerial Nº 129-2012-PCM se realizó 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.

(Peruano, 2016) Que, la Norma Técnica Peruana "NTP ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos", aprobada mediante Resolución Nº 42-2008/INDECOPI-CNB, por la Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias del Instituto Nacional de Defensa de la Competencia y de Protección de la Propiedad Intelectual (INDECOPI) ha sido reemplazada por la nueva versión de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información.

Requisitos.2da Edición" aprobada por Resolución Nº 129-2014/DNB-INDECOPI.

II. MARCO TEORICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN INTERNACIONAL

(Guerra, Neira, Díaz, & Patiño, 2021) **en su artículo titulado Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias, Colombia.** Los autores definen como objetivo principal Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias, para ello implementarán la metodología MAGERIT para la gestión de riesgos. En su estudio utilizan la metodología de tipo aplicada para el desarrollo de su investigación, teniendo como población la Biblioteca de una Institución Universitaria. Los resultados obtenidos de los cálculos de riesgos intrínseco y efectivo demuestran la presencia de salvaguardas y la evaluación de los impactos. Se establece el porcentaje de afectación en cada riesgo por proceso de calidad, se identifica la medida correctiva, y se incorporan formatos de registros. (Guerra, Neira, Díaz, & Patiño, 2021) concluye que "la incorporación de los formatos propuestos para desarrollar el control y auditorías a los indicadores de calidad permite la optimización del sistema de gestión de la seguridad de la información (SGSI) para los procesos de la biblioteca universitaria".

(Marlon Altamirano, 2019) **en su artículo titulado Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso, Ecuador.** El objetivo principal del autor es evaluar los factores que aumentan la eficacia de la gestión de la seguridad de la información y reducen la complejidad de la gestión de la seguridad informática. En el estudio se utilizaron métodos empíricos y teóricos. Incluye una lógica histórica que nos permite analizar varios estándares y abordar desarrollos, tendencias y generalizaciones en el desarrollo de sistemas de gestión de seguridad de la

información. El instrumento que utilizo en su investigación fue la encuesta y su población enfocado a directivos y especialistas de la Universidad Estatal Península de Santa Elena. Al terminar su investigación llega a la siguiente conclusión: A través de una encuesta aplicada a directivos y especialistas de la Universidad Estatal Península de Santa Elena, la cual tuvo como objetivo evaluar los factores que contribuyen a aumentar la efectividad de la gestión de la seguridad de la información y a disminuir la complejidad de la gestión de la seguridad informática se constató el efecto positivo que tiene la automatización y la gestión integrada de los controles, a la vez que se reconoce la importancia de medir la eficacia del sistema, de manera que se pueda corregir a tiempo y disminuir los riesgos de la información. Con respecto al empleo de algún sistema de indicadores para evaluar la efectividad de los controles de seguridad informática, el 75% de los encuestados respondió afirmativamente su uso. En la presente investigación se realiza un análisis integrador, donde se tienen en cuenta todos los controles de seguridad de la información propuestos por las principales guías y estándares internacionales (ISO/IEC 27001:2016 y NIST SP 800-53), puestos en práctica en la Universidad Estatal península de Santa Elena en el Ecuador.

(Cappellozza, Salati Marcondes de Moraes, Perez, & Lourenço Simões, 2022) **en su Artículo titulado Antecedent factors of violation of information security rules, Brasil.** Los autores plantean como objetivo principal la influencia de la desvinculación moral, la pena percibida, las experiencias negativas y la intención de rotación sobre la intención de violar las reglas de seguridad establecidas. Este estudio se desarrolló con un único enfoque cuantitativo transversal y se llevó a cabo a través de un cuestionario que busca, entre otros objetivos, identificar las opiniones y la distribución del fenómeno en la población utilizando técnicas estadísticas de análisis de datos. Utiliza el cuestionario como una técnica de recolección de datos para su investigación. El cuestionario fue impreso y aplicado a 338 personas que trabajaban en empresas con ISP establecidas hace más de un año para componer la muestra final. Después de analizar la integridad de las respuestas, 20 cuestionarios incompletos fueron descartados de los análisis finales. Por lo tanto, la muestra final utilizada para analizar las hipótesis fue de 318 participantes. Los

resultados de la investigación enfatizan que la certeza y la severidad del castigo afectan significativamente las decisiones de los empleados en su intención de cometer un delito. Comparando los factores analizados en este estudio, los resultados confirmaron la desvinculación moral como la principal influencia en la decisión de violar la PSI, seguida por la sanción percibida. Con base en esta evidencia, la primera recomendación práctica de este estudio es mejorar la comunicación organizacional con el objetivo de mitigar las vulnerabilidades de seguridad de la información. Esta mejora de la comunicación se puede implementar de varias formas, por ejemplo, con acciones de formación que simulen rutinas de trabajo diarias y situaciones que ofrezcan oportunidades para violar las políticas de la organización, para que los profesionales puedan tener un sentido real de la susceptibilidad de las fallas en la protección de datos y mitigar las fallas individuales. tendencias que pueden favorecer conductas no deseadas.

NACIONAL

(Olivos Guerra & Guevara Saldaña, 2017) **en su tesis titulado Formulación de políticas de control de accesos y seguridad física y del entorno basado en la norma técnica peruana NTP-ISO/IEC 17799 para la mejora de la gestión en la oficina central de cómputo – Universidad de Lambayeque, Lambayeque.** Los autores de la tesis plantean como objetivo general Formulación de Políticas de Control de Accesos y Seguridad Física y del entorno basado en la Norma Peruana NTP/IEC 17799 para mejorar la gestión de seguridad de la Oficina Central de Computo de la Universidad de Lambayeque, los autores realizaron la metodología de análisis y evaluación de riesgos desarrollada y diseñada, el autor define la Variable Independiente como formulación de políticas de control de accesos y seguridad física y del entorno basado en la norma peruana NTP-ISO/IEC 17799 y su Variable Dependiente como gestión de la seguridad en la Oficina Central de Cómputo (OCC) de la Universidad de Lambayeque y el tipo de investigación que usaron fue de tipo pre-Experimental. Teniendo como población 47 personas entre el personal directivo y personal administrativo, para ello utilizaron la encuentra como técnica de recolección de datos. (Olivos Guerra & Guevara Saldaña, 2017) Al finalizar la investigación llegaron a la siguiente conclusión: El

diagnóstico del estado de seguridad de la información muestra el nivel de cumplimiento de la UDL con los requisitos NTP ISO/IEC 17799:2007, es del 30%, lo que significa que la implementación del Sistema de Gestión de Seguridad de la información le implicará a la institución un refuerzo considerable debido a la ausencia de controles o al bajo grado de cumplimiento de muchos de ellos.

(Aguirre Abanto & Lopez Ynostroza, 2018) **en su tesis Implementación de una guía referencial para gestionar los riesgos informáticos en la Universidad Autónoma del Perú, Lima.** Los autores de la tesis plantean como objetivo principal Determinar en qué medida un Plan de contingencia disminuirá los riesgos informáticos en la Universidad Autónoma del Perú, Este trabajo muestra la norma técnica peruana ISO 17799 la cual establece recomendaciones para la gestión de la seguridad de la información, la cual nos basaremos en la cláusula de gestión de la continuidad del negocio. En la tesis los autores definen la Variable Independiente como Plan de Contingencia y la Variable Dependiente como Guía referencial para mitigar los riesgos informáticos, el tipo de investigación que se empleó para esta investigación fue aplicada y el nivel de la investigación Explicativa, teniendo como población a Todos las Guías Referenciales en la Universidad Autónoma del Perú y como muestra al Proceso para mitigar riesgos informáticos (30 usuarios), la técnica que se utilizó en esta investigación fue: la observación, entrevista y cuestionario. El investigador llega a la conclusión que la identificación de los riesgos, que podrían darse sobre los activos críticos de la universidad, fue realizada en base a los principales perfiles de amenazas a los que estos se ven expuestos y al nivel de impacto que dichas amenazas podrían causar sobre los activos, con lo cual se realizó la respectiva propuesta del plan de mitigación para tratar de minimizar al máximo el impacto que estas amenazas podrían causar en la universidad.

(Calisaya Sana & Tarrillo Villegas, 2018) **en su tesis titulada Implementación de controles de seguridad para la protección de datos personales en una Universidad Privada para el cumplimiento parcial de la Ley 29733 basado en los controles de seguridad de la NTP-ISO/IEC 17799:2007, Lima.** Los autores de la tesis tienen como objetivo Implementar

controles de seguridad basado en la NTP-ISO/IEC 17799:2007 para el cumplimiento parcial de la Ley de Protección de Datos Personales nro. 29733 en una Universidad Privada, el investigador define la variable dependiente como artículos del Capítulo V Medidas de Seguridad del Reglamento de la LPDP y la variable independiente como los controles de seguridad de la NTP-ISO/IEC 17799:2007, el nivel de investigación es descriptivo y experimental, el tipo de investigación es exploratoria y el enfoque de la investigación es mixto (Cuantitativo y Cualitativo), el investigador tiene como población al personal de DIGETI y Secretaría General que labora dentro de la UPeU y como muestra a las personas encargadas de cada sub área perteneciente al lugar de aplicación, para esta investigación utilizaron la entrevista y listado de chequeo. Al finalizar la investigación llegaron a la siguiente conclusión:

- Se realizó una evaluación preliminar de cumplimiento del Reglamento de la LPDP a las áreas comprometidas. En DIGETI se evidenció un 54,2 % de cumplimiento y en Secretaría General un 43,8%.
- Se realizó una evaluación al área comprometida para identificar el nivel de cumplimiento post implementación. En DIGETI se demostró 78,55% de cumplimiento, y en Secretaría General un 80,37%.

(Hernández Mechate, 2020) **en su tesis titulada Vulnerabilidades informáticas en el portal web de la Universidad Andina del Cusco, Cusco.** El autor de la tesis tiene como objetivo Identificar vulnerabilidades informáticas mediante la aplicación de las herramientas de detección de vulnerabilidades en el portal Web de la Universidad Andina del Cusco. El investigador utilizo el tipo de investigación descriptivo y el diseño de la investigación cuantitativo, teniendo como población al personal de la Dirección de Tecnologías de Información (DTI), quien tiene la información y conoce los procesos actuales dentro de la Universidad Andina del Cusco y como muestra a la Dirección de Tecnologías de Información está conformada por tres unidades; pero la que se encarga de administrar el portal Web de Universidad Andina del Cusco es la Unidad de Diseño y Programación. Los resultados obtenidos por el investigador afirman que el portal Web de la

Universidad Andina del Cusco es vulnerable. Y qué Para la vulnerabilidad de implementación se utilizó el software Acunetix Web Vulnerability Scanner 10.5 para ataques de Inyección de código SQL, Cross-site Scripting (XSS) y Cross-site request reference forgery (CSRF), se encontró deficiencia en cuanto a: nivel de vulnerabilidad (media), lista de archivos con entradas Get y Post, enlaces rotos y contraseñas con autocompletado habilitado; un hacker black hat, podría eliminar información de la base de datos, inyectar códigos y ejecutar scripts maliciosos, entre muchas cosas más, afectando la integridad del sistema informático.

(Poma & Vargas, 2019) **en su artículo titulado Problemática en Ciberseguridad como protección de sistemas informáticos y redes sociales en el Perú y en el Mundo, Trujillo.** El autor tiene como objetivo investigar si la Ciberseguridad protege los sistemas informáticos y redes sociales en el Perú y el mundo. El investigador indica que su investigación es cuantitativa y su diseño es experimental y descriptivo, los resultados obtenidos por el investigador fueron favorables, en el sentido que se pudo apreciar que, mediante la adopción de medidas rígidas, los sistemas informáticos; así como las redes sociales, se vuelven potencialmente seguros en un 70%. En tal sentido se concluye que la Ciberseguridad como protección de medios informáticos potencializa las buenas prácticas en las empresas y protege la información.

REGIONAL

(Asencios Carbajal, 2017) **en su tesis de maestría titulada Guía metodológica de sistema de gestión de seguridad de la información basada en la NTP-ISO/IEC 17799, 27001 y COBIT 5 para minimizar los riesgos de gestión de la información en el poder judicial de Carhuaz, 2014, Huaraz.** El autor define su objetivo como Formular una guía metodológica de sistema de gestión de seguridad de la información basada en la NTP-ISO/IEC 17799, 27001 y COBIT 5 para minimizar los riesgos de gestión de la información asociados a confidencialidad, integridad, disponibilidad del poder judicial de Carhuaz.

El investigador define su variable Independiente como Guía metodológica de sistema de gestión de seguridad de la información basada en la NTP.ISO/IEC 17799, 27001 y Cobit 5 y su Variable dependiente como Riesgos de gestión de la información. La investigación es aplicada y descriptiva y su diseño es de tipo no experimental, transversal, tomando una población de 45 trabajadores de lo cual se extrajo una muestra de 45 trabajadores, debido a tener una población menor, el investigador utiliza instrumentos para recabar información tales como fichas textuales, resúmenes, etc. Al término de su investigación se tuvo el siguiente resultado, que la implementación de la metodología mostro que se tiene un riesgo muy bajo, con un promedio de 2.4, con este resultado el investigador concluye lo siguiente la implementación del sistema de gestión de seguridad de la información, se minimizó los riesgos en la gestión de información asociados a confidencialidad, integridad, disponibilidad.

(Guardia Tamara, 2020) **en su tesis de maestría titulada Diseño de un modelo de seguridad de la información para minimizar los riesgos informáticos en la gestión académica del Instituto de Educación Superior Tecnológico Publico Eleazar Guzmán Barrón – Huaraz – 2018, Huaraz.** El autor define como objetivo Diseñar un modelo de seguridad de la información para minimizar los riegos informáticos en la gestión académica del Instituto de Educación Superior Tecnológico Público Eleazar Guzmán Barrón. Para su investigación define la variable Independiente como Diseño De Un Modelo De Seguridad De La Información y la variable Dependiente como Minimizar los Riesgos Informáticos. El investigador define el tipo de investigación correlacional, con un enfoque cuantitativo de tipo aplicada, el diseño de su investigación es experimental, Para el presente estudio se tomó como población al Área de secretaria para fijar la muestra se empleó el método no probabilístico (no aleatoria) de tipo intencional; que es el más conveniente para el propósito del estudio de 20 colaboradores del Área de secretaria Académica del Instituto de educación superior tecnológico Público Eleazar Guzmán Barrón, del Distrito de Independencia, Provincia de Huaraz, Región de Ancash Académica del Instituto de educación superior tecnológico Público Eleazar Guzmán Barrón, del Distrito de Independencia, Provincia de Huaraz,

Región de Ancash. El investigador utiliza como instrumento de recolección de datos: Las fichas de recolección de datos de Internet, Fichas de resumen, el resultado obtenido por el investigador dice como la hipótesis nula ha sido rechazada, se confirma que hay diferencia estadísticamente significativa con el diseño un modelo de seguridad de la información se minimizará los riegos informáticos en la gestión académica del Instituto de Educación Superior Tecnológico Público Eleazar Guzmán Barrón- Huaraz., antes y después del diseño del modelo. Así el investigador llega a la conclusión que el diseño del modelo permitió afirmar con la hipótesis planteada, dado que con el diseño un modelo de seguridad de la información se optimizo los riegos informáticos en la gestión académica del Instituto de Educación Superior Tecnológico Público Eleazar Guzmán Barrón- Huaraz y con lo que se logró los objetivos planteados.

(Carrión Apéstegui, 2015) **en tu tesis titulada diagnóstico y propuesta de mejora para la gestión de riesgos basado en la ISO/IEC 27002:2008 para la oficina general de estudios UNASAM - Huaraz 2014, Huaraz.** El autor tiene como objetivo de investigación Realizar el diagnóstico de la gestión de riesgos para la mejora de los procesos académicos de la Oficina General de Estudios de la UNASAM. La tesis tiene como variable independiente el Diagnostico de la situación actual y la variable dependiente a los Controles contenidos en la ISO/IEC 27002:008 para la seguridad de la información. Se está considerando el criterio de población beneficiaria a todos los alumnos de la UNASAM que hacen uso del SIGA WEB UNASAM, el cual es administrado directamente por la OGE. Además, también se está considerando a los docentes y administrativos de todas las facultades que hacen uso del mismo. Se está tomando esta población ya que son los mayores beneficiarios al ser los usuarios principales del SIGA WEB. Y su muestra tendremos un total de 3 muestras, ya que cada uno de ellos hace un uso distinto del SIGA WEB. Es por ello que tendremos la Muestra 1 conformada por los alumnos de la UNASAM, la Muestra 2 conformada por el personal docente y la Muestra 3 conformada por el personal administrativo. Además, cada una de las muestras se diferenciará por facultades. Muestra 1: Tamaño de muestra para una proporción; siendo el tamaño de muestra igual a 362 para la población 1,

teniendo en cuenta un nivel de confianza del 95%, error de muestreo de 5% y uso de la fórmula general, Muestra 2: Muestreo estratificado para la proporción, siendo el tamaño de muestra obtenido de 212, para lo cual se tuvo en cuenta un nivel de confianza del 95% y error de muestreo del 5% y Muestra 3: Muestreo estratificado para la proporción, siendo el tamaño de muestra obtenido de 50, para lo cual se tuvo en cuenta un nivel de confianza del 95% y error de muestreo del 5% UNASAM. El tipo de investigación de acuerdo a la orientación es Investigación Básica, De acuerdo a la técnica de contrastación es Descriptiva simple. Es un enfoque no experimental y transversal, también indica que para la investigación se usó entrevista, encuestas y observación. Llegando a la conclusión que, al evaluar el nivel de riesgo de los activos de la OGE, se aprecia que en su mayoría de ellos están entre un estado de intolerable y extremo riesgo. Gracias a la metodología Magerit se siguió una serie de puntos para el análisis y gestión de riesgos, fase fundamental en este estudio ya que se obtuvo resultados realistas del estado de riesgo actual en la OGE donde se supo escoger que medidas serán necesarias para mitigar el riesgo.

(Brito Rodríguez, 2020) **en su tesis titulada Gestión de incidentes de seguridad de la información en la facultad de Ciencias de la universidad nacional Santiago Antúnez de Mayolo, 2017, Huaraz.** El objetivo planteado por el autor es Diseñar la Gestión de Incidentes para establecer los controles de Seguridad de la Información en la Facultad de Ciencias de la UNASAM. La tesis tiene como variable independiente la Gestión de incidentes y la variable dependiente la Seguridad de la Información en la facultad de ciencias de la UNASAM. El tesista indica que su tipo de investigación es aplicada y descriptiva, también utiliza la observación y la encuesta como técnicas de procesamiento de datos, La población en la cual se aplicó los instrumentos de recolección de datos está conformada por el personal administrativo responsable de la seguridad de los activos de información y activos informáticos de la facultad de Ciencias de la Universidad Nacional Santiago Antúnez de Mayolo y la muestra será igual a la población, ya que la población objetivo está delimitada a un solo grupo de estudio. El tesista llega a la siguiente conclusión al finalizar la investigación: es importante la gestión de

incidentes de seguridad de la información para administrar de manera eficaz los sucesos críticos que afectan los activos de información y recursos informáticos de la facultad de ciencias de la UNASAM.

2.2. BASES TEORICAS

NORMA TECNICA PERUANA 17799:

(conexiónesan, 2022) menciona que el 23 de julio del 2004 la Presidencia del Consejo de ministros a través de la ONGEI, dispone el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 17799:2004 EDI Tecnología de la Información: Código de buenas prácticas para la gestión de la seguridad de la información en entidades del Sistema Nacional de Informática.

(conexiónesan, 2022) dice que la NTP-ISO 17799 es una compilación de recomendaciones para las prácticas exitosas de seguridad, que toda organización puede aplicar independientemente de su tamaño o sector. Esta norma técnica se caracteriza por su flexibilidad, pues no induce a las organizaciones a cumplirla al pie de la letra sino les permite encontrar soluciones de seguridad de acuerdo a sus necesidades, señala el especialista Max Lázaro, de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI).

Para (ISOTools Excellence, 2015) indica que “la norma NTP-ISO/IEC 17799 es una norma técnica peruana que ayuda a implementar también medidas de seguridad en las organizaciones, mejorando el rendimiento de la organización y aumenta su valor añadido ante las demás organizaciones del mismo sector”.

SEGURIDAD DE LA INFORMACIÓN:

En la actualidad la seguridad de la información se ha convertido en uno de los puntos más importantes en toda organización debido a que cada organización trabaja con base de datos sensible en su organización.

(EALDE, 2022) menciona que la norma ISO 27001 es el estándar internacional para la gestión de la seguridad de la información en las organizaciones, tanto para la información física como para la digital. Es parte de la familia de estándares ISO 27000, las cuales ayudan a las organizaciones a mantener sus bienes de información seguros.

Según (EALDE, 2022) dice La implementación de esta normativa, adoptada por miles de empresas, públicas y privadas alrededor del mundo, establece un enfoque sistemático para la gestión de la información organizacional confidencial y asegura que se mantenga protegida y disponible. En general, es un estándar amplio que cubre la seguridad técnica, física, de personal y de procesos en la compañía.

Según (ISO, 2022) indica que un sistema de gestión de la seguridad de la información protege la confidencialidad, la integridad y la disponibilidad de la información a través de los procesos de gestión de riesgos y brinda a las partes interesadas la confianza de que los riesgos se gestionan adecuadamente.

Otro dato muy importante que menciona (ISO, 2022) es que "El orden en que se presentan los requisitos en esta Norma Internacional no refleja su importancia ni implica el orden en que deben implementarse. Los elementos de la lista se enumeran solo con fines de referencia."

ELEMENTOS DE GESTIÓN DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

(Areitio Bertolín, 2008) menciona que hay varios elementos como:

- Identificación de todos los activos: el autor (Areitio Bertolín, 2008) dice "los activos incluyen personas, equipos de hardware y software, materiales, etc. Así como activos intangibles como la imagen organizacional, la reputación, que también indican que los activos vulnerables requieren una evaluación de riesgo aceptable".
- Identificación de amenazas a los activos: para (Areitio Bertolín, 2008) las amenazas pueden ocasionar eventos no deseados que pueden ocasionar pérdidas o daños a una organización, lo que indica que las amenazas pueden estar relacionadas con el entorno de la organización, pueden ser ambientales y culturales, y también tienen ciertas características que pueden surgir de forma interna o externa, hay ciertos tipos de motivos, como alguna forma de ganancia financiera, sabotaje de empleados, robo de contraseña, etc, y también tienen frecuencias y gravedades.
- Identificación de vulnerabilidades: Para (Areitio Bertolín, 2008) "la vulnerabilidad es la capacidad de materializar una amenaza a un recurso,

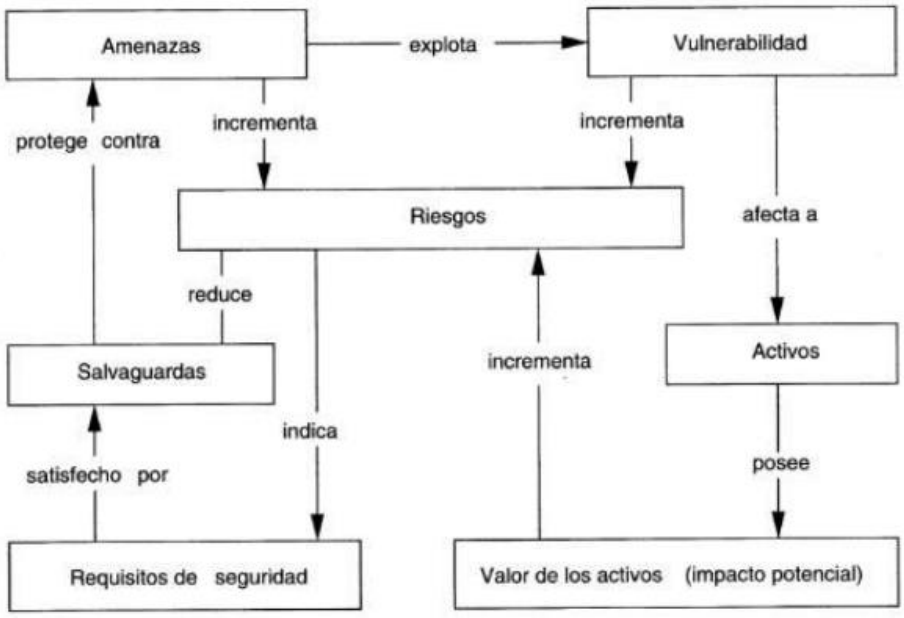
también indica que una vulnerabilidad en sí misma no causa ningún daño, una vulnerabilidad es una debilidad que puede ser aprovechada y llevar a consecuencias no deseadas".

- Identificación de impactos: (Areitio Bertolín, 2008) menciona que los efectos son las consecuencias de la realización de una amenaza a los bienes, como pérdida de información, pérdida de seguridad y disponibilidad, que amenaza la integridad de los sistemas de información, mientras que esas acciones tienen efectos indirectos, ya que pueden generar pérdidas económicas, daños a la imagen de la empresa, sanciones legales, etc. La evaluación de impacto permite determinar la proporción de impactos y el costo de las actividades de control.
- Identificación del riesgo: (Areitio Bertolín, 2008) indica que el riesgo se caracteriza por dos factores: 1) la probabilidad de un evento adverso y 2) su impacto, también indica que existe un ambiente de riesgo cuando una amenaza o grupo de amenazas pueden aprovechar la debilidad o vulnerabilidades de un activo o grupo de activos, causando así pérdida o daño al negocio.
- Aplicación de salvaguardas: Para el autor (Areitio Bertolín, 2008) También se conocen como controles o contramedidas, que pueden ser procesos o algún dispositivo físico o lógico que de alguna manera protege un activo de alguna amenaza con el fin de reducir su vulnerabilidad, daño y minimizar el impacto del incidente. El entorno en el que opera la empresa afecta la elección de los controles, es importante elegir controles o medidas de seguridad que no afecte a la sociedad o cultura en la que opera la empresa. es importante sensibilizar a los empleados para que puedan comprender la importancia de los controles que se consideran seguros.
- Identificación de riesgos residuales: Para el autor (Areitio Bertolín, 2008) Esto significa saber qué riesgos permanecen a pesar de que se han implementado medidas de seguridad o controles para reducir ese riesgo, entendiendo que los controles reducen solo una parte de los riesgos, si hay riesgos residuales deben analizarse. Si son aceptados por la empresa y cuanto mayor sea el nivel de protección, mayores serán los costos incurridos, entonces si se toma la decisión de asumir el riesgo residual, esa

decisión debe ser asumida por el propietario del activo, quien, en consecuencia, toma el control.

- Limitaciones: Para el autor (Areitio Bertolín, 2008) es saber que limitaciones existen en el ambiente que pueden afectar los peligros, riesgos, control y seguridad, limitaciones que deben ser reconocidas y establecidas por la dirección de la organización, pueden ser organizacionales, financieras, legales, ambientales, técnicas, personales, provisionales y otros también indican que estos factores deben ser considerados en la selección e implementación de medidas de control. Las restricciones nuevas y existentes deben revisarse periódicamente para identificar posibles cambios, y estas restricciones pueden cambiar con el tiempo, debido a desarrollos sociales o culturales organizacionales.

Figura 1 *Relaciones entre componentes de la Gestión de la Seguridad.*



NOTA: (Areitio Bertolín, 2008). Seguridad de la información. Redes, informática y sistemas de información. p.22

EL autor (Escrivá, Romero, Ramada, & Onrubio, 2015) teniendo en cuenta los principios básicos de la seguridad de la información: integridad, confidencialidad y disponibilidad.

MAGERIT:

MAGERIT (2012), indica que dicha metodología es "utilizada para analizar los riesgos derivados del uso de las tecnologías de la Información y comunicaciones para así implementar medidas de control adecuadas que permitan tener riesgos controlados." Por lo que esta metodología, permite conocer el estado actual de una organización en relación a los riesgos al que están expuestos los activos de información y poder tomar decisiones de seguridad para contrarrestarlos.

Escrivá (2013), indica "Hay que tener en cuenta qué activos hay que proteger, sus vulnerabilidades y amenazas, así como la probabilidad de que estas se produzcan junto con el impacto de las mismas". El resultado de un análisis de riesgos permite recomendar medidas para la protección de los activos de información.

RIESGO:

El autor MAGERIT (2012) define el riesgo como una evaluación de la exposición a una amenaza planteada a uno o más activos que causan daños o perjuicios a la Organización. Los riesgos muestran lo que puede pasar con los activos si no se protegen adecuadamente. Es importante saber qué características son de interés para cada activo y también saber en qué medida estas características están en riesgo, es decir, analizar el sistema.

ANÁLISIS DE RIESGOS

El autor MAGERIT (2012) define, proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

Para el autor MAGERIT (2012) menciona que los sistemas de gestión de la seguridad de la información (SGSI) [ISO 27001] formalizan cuatro etapas cíclicas:

Figura 2 *Ciclo PDCA.*

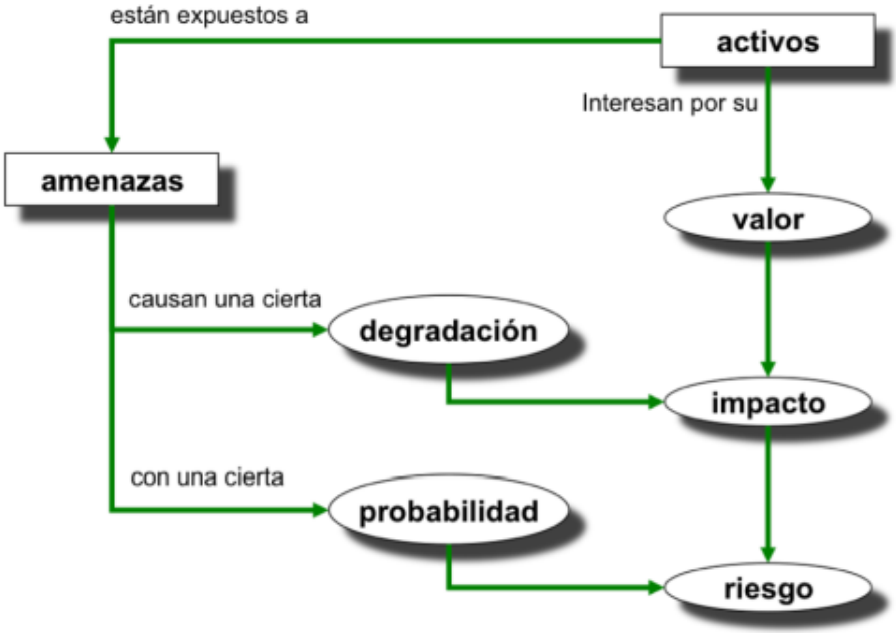
NOTA: MAGERIT 2012, MAGERIT – versión 3.0. p.11.

METODO DE ANALISIS DE RIESGO:

El autor MAGERIT (2012) define lo siguiente, El análisis de riesgos es un enfoque metódico para la identificación de riesgos que incluye varios pasos:

- Identificar los activos relevantes para la Organización, sus relaciones y su valor en términos del daño (valor) que supondrá su degradación.
- Identificar las amenazas a las que se enfrentan estos recursos.
- Determine qué precauciones existen y qué tan efectivas son para los peligros.
- Estimación de impacto, definido como el daño causado a la propiedad como consecuencia de la materialización de la amenaza.
- Estimación del riesgo, definida como el impacto ponderado con la frecuencia (o expectativa de actualización) del peligro.

Figura 3 *Elementos del análisis de riesgos potenciales.*



NOTA: MAGERIT 2012, MAGERIT – versión 3.0. p.22.

POLITICAS DE SEGURIDAD:

(IBM, 2021) La política de seguridad define qué es lo que desea proteger y qué espera de los usuarios del sistema. Proporciona una base para la planificación de la seguridad al diseñar nuevas aplicaciones o ampliar la red actual. Describe responsabilidades del usuario como las de proteger información confidencial y crear contraseñas no triviales. La política de seguridad también debe describir cómo se va a supervisar la efectividad de las medidas de seguridad. Esta supervisión le ayudará a determinar si alguna persona podría intentar burlar sus defensas.

OBJETIVOS DE SEGURIDAD:

(IBM, 2021) indica, cuando cree y desarrolle una política de seguridad, deberá tener claros los objetivos. Los objetivos de seguridad entran dentro de una o más de estas categorías:

- **PROTECCIÓN DE RECURSOS:** (IBM, 2021) El esquema de protección de recursos garantiza que solo los usuarios autorizados podrán acceder a los objetos del sistema. La capacidad de asegurar

todo tipo de recursos del sistema es una de las fortalezas del IBM® i. Primero deberá definir con precisión las distintas categorías de usuarios que pueden acceder al sistema. Asimismo, cuando cree la política de seguridad, deberá definir qué tipo de autorización de acceso desea otorgar a estos grupos de usuarios.

- **AUTENTICACIÓN:** (IBM, 2021) Una autenticación convincente defiende el sistema contra riesgos de seguridad como las limitaciones, en las que el remitente o el destinatario Utilice un nombre falso para acceder al sistema. Los sistemas han utilizado tradicionalmente contraseñas y nombres de usuario para la autenticación; los certificados digitales pueden ofrecer un método más seguro de autenticación, a la vez que proporcionan otras ventajas de seguridad. Cuando enlaza su sistema con una red pública como Internet, la autenticación de usuario toma nuevas dimensiones. Una diferencia importante entre Internet y una intranet es la capacidad de confiar en la identidad del usuario que inicia la sesión. Por lo tanto, debe considerar seriamente la posibilidad de utilizar unos métodos más potentes de autenticación que los que proporcionan los procedimientos tradicionales de conexión mediante nombre de usuario y contraseña. Los usuarios autenticados podrían tener distintos tipos de permisos, según su nivel de autorización.

- **AUTORIZACIÓN:** (IBM, 2021) La autorización es el proceso de determinar quién o qué puede acceder a los recursos del sistema o ejecutar determinadas actividades en un sistema.

- **INTEGRIDAD:** (IBM, 2021) Es la seguridad de que la información entrante es la misma que la que se ha enviado. Para entender la integridad, primero deberá comprender los conceptos de integridad de los datos e integridad del sistema.

- **INTEGRIDAD DE LOS DATOS:** (IBM, 2021) La integridad de los datos los defiende contra riesgos de seguridad como la manipulación, donde alguien intercepta y modifica la información sin estar autorizado para ello. Además de proteger los datos que están almacenados en la red, podría necesitar medidas de seguridad adicionales para garantizar la integridad de los datos cuando estos entran en su sistema procedentes de fuentes que no sean de confianza.

- **INTEGRIDAD DEL SISTEMA:** (IBM, 2021) el sistema proporciona resultados coherentes con el rendimiento esperado.

- **NO REPUDIO:** (IBM, 2021) El uso de certificados digitales y de la criptografía de claves públicas para firmar transacciones, mensajes y documentos es la base del no repudio. El remitente y el destinatario están ambos de acuerdo en que el intercambio tiene lugar. La firma digital de los datos es una prueba suficiente.

- **CONFIDENCIALIDAD:** (IBM, 2021) La confidencialidad es fundamental para la seguridad total de los datos. El cifrado de los datos con certificados digitales y la capa de sockets segura (SSL) o con una conexión de redes privadas virtuales (VPN) permite asegurar la confidencialidad al transmitir datos entre varias redes que no sean de confianza. La política de seguridad debe indicar qué métodos se emplearán para proporcionar la confidencialidad de la información dentro de la red y de la información que sale de ella.

- **ACTIVIDADES DE SEGURIDAD DE AUDITORÍA:** (IBM, 2021) Consisten en supervisar los eventos relacionados con la seguridad para proporcionar un archivo de anotaciones de los accesos satisfactorios y de los no satisfactorios (denegados). Los

registros de accesos satisfactorios indican quién está haciendo cada tarea en los sistemas. Los registros de accesos no satisfactorios (denegados) indican que alguien está intentando abrirse paso a través de las barreras de seguridad del sistema o que alguien tiene dificultades para acceder al sistema.

2.3. DEFINICIÓN DE TERMINOS

VULNERABILIDAD:

El autor (Gabriel Baca, 2016) significa un evento o acción que permite que un peligro se materialice. Se es tan vulnerable que no tienes suficientes protecciones para evitar que ocurra la amenaza. Ahora se cree que hay ataques intencionales y no intencionales a los que una empresa siempre es más o menos vulnerable. Cuando hay una falla en una computadora, generalmente se considera una falla en el diseño, implementación u operación del sistema.

AMENAZA:

El autor (Gabriel Baca, 2016) establece que una amenaza es el estado ambiental de un sistema, área o dispositivo que contiene información crítica (persona, dispositivo, evento o idea), que en estas circunstancias podría conducir a una brecha de seguridad (no cumple con ninguno de los aspectos enumerados), afecta a un departamento de TI y a una organización de TI.

ATAQUES:

El autor (Purificación Aguilar, 2010) define, se dice que cuando la amenaza se materializa, se ha producido un ataque accidental o intencionado al sistema.

ACTIVOS:

El autor (Purificación Aguilar, 2010) activos identificados, son recursos propiedad del propio sistema de información o vinculados al mismo. La presencia de activos que facilitan el funcionamiento de una empresa u organización y el logro de sus objetivos. Al examinar los activos existentes, es importante considerar la relación entre ellos y su impacto: cómo el daño causado a otros afectará a uno de ellos.

RIESGOS:

El autor (Purificación Aguilar, 2010) define el riesgo como la posibilidad de que una amenaza se materialice o no como resultado de la explotación de una vulnerabilidad. Una amenaza no es un riesgo cuando no hay vulnerabilidad, ni es una vulnerabilidad cuando no hay amenaza para ella.

RIESGOS TECNOLOGICOS:

El autor (Gabriel Baca, 2016) define a los riesgos de origen tecnológico; suelen ser cometidos por usuarios con muy poca experiencia, quienes no miden la magnitud de las consecuencias.

SISTEMA DE INFORMACIÓN:

El autor (Purificación Aguilar, 2010) define un sistema de información (SI) como un conjunto de elementos organizados, interconectados y coordinados encargados de asegurar el funcionamiento global de una empresa o cualquier otra actividad humana para lograr su objeto.

SEGURIDAD:

El autor (Purificación Aguilar, 2010) La seguridad informática es una disciplina relacionada con el desarrollo de estándares, procesos, métodos y prácticas para crear un sistema de información seguro y confiable.

2.4. HIPÓTESIS

2.4.1. HIPÓTESIS GENERAL

La gestión de la seguridad de la infraestructura de las tecnologías digitales de la Oficina General de Admisión mejora de manera importante con el modelo basado en la norma técnica peruana 17799.

2.4.2. HIPÓTESIS ESPECIFICAS

- El modelo basado en la norma técnica peruana 17799 reduce las alertas en la gestión de seguridad de la infraestructura de las TD de la OGAD.
- El modelo basado en la norma técnica peruana 17799 limita los ataques en la gestión de seguridad de la infraestructura de las TD de la OGAD.

- El modelo basado en la norma técnica peruana 17799 minimiza las vulnerabilidades que intervienen en la gestión de seguridad de la infraestructura de las TD de la OGAD.

2.5. VARIABLES

2.5.1. VARIABLE INDEPENDIENTE

MODELO BASADO EN LA NORMA TECNICA PERUANA 17799

2.5.2. VARIABLE DEPENDIENTE

GESTIÓN DE SEGURIDAD DE LA INFRAESTRUCTURA DE LAS TECNOLOGIAS DIGITALES

2.5.3. OPERACIONALIZACIÓN DE VARIABLES

Tabla 1 Operacionalización de Variables

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES
Variable Dependiente: Gestión de seguridad de la infraestructura de las TD	Gestión de la seguridad: Proceso de establecer y mantener la seguridad de un ordenador o sistema de red **(ISACA, 2015,p.60)** Las TIC: Conjunto de servicios telemáticos, redes, software y dispositivos de hardware que se integran en sistemas de información interconectadas y complementarias cuyo fin es la de gestionar datos, información y procesos **(CONCYTEC, 2016, p.8)** La infraestructura: Capacidad informática y de procesamiento, conexión de red y dispositivos conectados **(HUAWEI,2018,p.8)**	A partir de la definición conceptual en la realidad de la UNASAM, específicamente en la OGAD, se observará y evaluará las bases de datos para identificar y registrar la existencia de las dimensiones e indicadores.	Confidencialidad Integridad	Presencia
			Disponibilidad	Presencia
Variable Independiente: Modelo basado en la norma	Instrumento predictivo, cuya función es predecir las interacciones como variable y dar soporte de los sistemas para que desde esta perspectiva el profesional observador pueda describir el	Al finalizar el modelo basado en la norma técnica peruana 17799, se registrarán los datos	Autoevaluación	Alertas
				Ataques

técnica peruana 17799	comportamiento de los sistemas de la institución a lo largo del tiempo **(Matthew & Zheng, 2017)**.	obtenidos para realizar una evaluación objetiva de los resultados.	Vulnerabilidades

III. METODOLOGÍA

3.1. TIPO DE ESTUDIO

ENFOQUE DE INVESTIGACIÓN:

Se utilizará el enfoque cuantitativo porque recopilaremos y analizaremos los datos.

NIVEL:

Sera de nivel Aplicativo porque se supervisará y controlará.

TIPO DE INVESTIGACIÓN:

- Según la Intervención del sujeto: Experimental
- De la planificación: Retrospectivo
- Mide: Longitudinal
- Variable de Interés: Analítica

3.2. EL DISEÑO DE LA INVESTIGACIÓN

Para el proyecto se utilizará el Diseño Cuasi Experimental con dos grupos experimental y de control, con medición pre y post test.

3.3. DESCRIPCIÓN DE LA UNIDAD DE ANÁLISIS, POBLACIÓN Y MUESTRA (CUANTITATIVO).

Nuestra unidad de análisis será los postulantes al proceso de admisión en la Universidad Nacional Santiago Antúnez de Mayolo.

POBLACIÓN:

La población estará determinada por el promedio de los 3 últimos procesos de admisión de la Universidad Nacional Santiago Antúnez de Mayolo, que hacen uso y que confían la seguridad de sus datos almacenados o procesados mediante la infraestructura digital de la Oficina General de Admisión que es un total de:

Tabla 2 Postulantes de los últimos 3 procesos que se inscribieron virtualmente

PROCESO	POSTULANTES
2022 – I	1500
2021- II	1500
2021-I	1500
TOTAL	4500

NOTA: Información extraída de la Base de Datos de la OGAD.

MUESTRA:

La muestra es de 354 postulantes, para determinar la muestra se utilizará el método no probabilístico, teniendo en cuenta la disponibilidad de la información.

3.4. TÉCNICAS DE INSTRUMENTOS DE RECOLECCIÓN DE DATOS.

ENCUESTA:

(Encuestas probabilísticas vs. no probabilísticas, 2000) En una encuesta, la población es el agregado o colección de elementos que poseen las características que se desean investigar; ésta puede delimitarse espacial y temporalmente, la población a investigar será únicamente los elementos a estudiar.

INSTRUMENTO:

Para el proyecto se utilizará el cuestionario como medio de recolección de datos.

3.5. TÉCNICAS DE ANÁLISIS Y PRUEBA DE HIPÓTESIS (ESTUDIO CUANTITATIVO).

TÉCNICA DE ANÁLISIS:

Con la presente investigación se espera demostrar la hipótesis planteada para ello utilizaremos el análisis estadístico inferencial (análisis).

PRUEBA DE HIPÓTESIS:

Para realizar la prueba de hipótesis se elaborará una base de datos y para contrastar la hipótesis se aplicará la prueba de Wilcoxon.

IV. RESULTADOS DE LA INVESTIGACIÓN

4.1. Descripción del trabajo de campo

4.1.1. Contexto de la organización

La oficina general de admisión (OGAD), es un órgano autónomo de la UNASAM, encargada de organizar y conducir los procesos de admisión a nivel de pregrado y posgrado.

La oficina general de admisión cuenta con procesos, cada una de ellas es indispensable para poder llevar a cabo el Examen de Admisión:

- Proceso de consignación de vacantes
- Proceso de planificación y/o organización
- Proceso de inscripción
- Proceso de elaboración
- Proceso de aplicación
- Proceso de calificación
- Proceso de acreditación del ingresante

De todos los procesos que tiene la Oficina General de Admisión nos enfocaremos en el proceso de inscripción y calificación debido a que en cada uno de los procesos se maneja gran cantidad de información sensible.

PROCESO DE INSCRIPCIÓN

En el proceso de inscripción de postulante, es un proceso el cual se lleva a cabo de dos formas:

- Inscripciones de manera presencial: Las inscripciones de manera presencial es llevado a cabo por un personal especializado y capacitado en el manejo de la plataforma de admisión, este personal está preparado para poder dar solución inmediata si se produjera algún inconveniente durante la inscripción del postulante.
- Inscripciones de manera virtual: Las inscripciones de manera virtual, es llevado a cabo por el propio postulante para ello se desarrolló un manual y un video instructivo donde se detalla paso a paso como se debe de realizar una buena inscripción, en el caso de que se produjera

algún imprevisto el postulante debe de comunicarse con la Oficina General de Admisión para que puedan solucionar el inconveniente.

Cuando se inician las inscripciones, se apertura la plataforma que se encuentra de manera pública para el público, para que puedan interactuar e inscribirse al Examen de Admisión, cabe resaltar que en nuestra plataforma de admisión se encuentra toda la información de los procesos llevados a cabos hasta la fecha, el cual está expuesto a cualquier tipo de vulneración.

El proceso de inscripción es un proceso muy delicado y sensible debido a que no solo se maneja información de los postulantes si no también se almacenan los pagos realizados en el banco de la nación y de tesorería de la UNASAM, por ello se debe de tener mucho cuidado cuando se cargan los pagos a la plataforma de admisión ya que algunos pagos se realizan de manera errónea por parte de los postulantes.

Se debe de manejar la información de todos los inscritos al Examen de Admisión de manera adecuada ya que si se produjera el caso de que un postulante se inscribió, pero en la validación y contrastación de pagos no existirá su pago, se tendría que eliminar su inscripción y ser retirado del listado de postulantes y padrón.

PROCESO DE CALIFICACIÓN

El proceso de calificación es otro de los puntos importantes de la Oficina General de Admisión ya que ahí es donde se procesó los exámenes de todos los postulantes, lo cual conlleva a ser un proceso muy sensible.

Para este proceso se cuenta con un lector óptico y una computadora de escritorio, cuya función principal es procesar las respuestas de los postulantes, debido a que este proceso es manejado por una personal especialidad en calificación de exámenes, en el ordenador donde se procesa los resultados se almacena la información de cada uno de los postulantes con su respectivo puntaje, porque este proceso es sensible porque se debe de velar y salvaguardar la información recolectada de cada postulante y no debe ser alterada.

Luego de ser procesada toda la información se procede a realizar la calificación manual de postulantes de manera aleatoria tomando 2 o 3 postulantes que obtuvieron el puntaje más alto y más bajo para así el presidente de la comisión que está llevando a cabo el proceso pueda dar conformidad y garantizar que la calificación fue transparente.

Una vez finalizado el proceso se entrega en un USB todos los resultados al especialista de la OGAD para ser resguardado y cargado a la plataforma de inscripciones los resultados finales.

4.1.2. Liderazgo

El jefe de la Oficina General de Admisión tiene como compromiso gestionar la seguridad de la información para garantizar que la información sea confiable, debido a que es de carácter sensible, y así avalar la integridad de los datos y no sean alterados durante los procesos de inscripción y calificación por lo que también asume el compromiso de tener la información disponible en todo momento.

a) Política

La política de seguridad de la información busca adoptar una serie de medidas para mantener la confidencialidad, integridad y disponibilidad de la información, declarando que estos son los tres componentes básicos de la seguridad de la información y tiene como finalidad establecer requisitos para la protección de la información, equipos, tecnología de servicio. Para ayudar con el proceso de registro y calificación de la Oficina General de Admisión.

La Política sobre privacidad de la Información es muy importante y regirá el aspecto legal de la seguridad de la Oficina General de Admisión.

La tecnología digital confronta actualmente a un número cada vez mayor de vulnerabilidades y amenazas, esto hace que la adaptación y la gestión de riesgos sean esenciales.

Objetivo

El propósito principal es detallar los principios y reglas fundamentales de la gestión de la seguridad y el propósito es garantizar la seguridad y se reduzca el riesgo.

Alcance

La política se aplica a todos los miembros de la Oficina General de Admisión, quienes deben acatarla sin perjuicio y para perfeccionar la seguridad en lo posible.

El alcance cubre los procesos de inscripción y calificación llevados a cabo por la Oficina General de Admisión, tanto en forma impresa como digital.

Se publicará y será al alcance de todos en el portal web admision.unasam.edu.pe y en todas las oficinas que comprende la Oficina General de Admisión, de forma accesible por todos los trabajadores que laboran.

Adaptación y Desarrollo

La política debe ser ajustada y elaborada por cada oficina, cada oficina decidirá cómo aplicar esta política a su trabajo a través de la documentación adecuada, la cual debe cumplir con los principios de seguridad de la información.

En este sentido, cada oficina constituyente de OGAD debe adoptar la política aquí identificada como un requisito mínimo y debe adaptar esa política a las necesidades requeridas, a los tipos de diferentes conjuntos de datos, a fin de detallar los requisitos para la fase operativa a nivel operacional.

- ALCANCE ESTRATEGICO: Debe ser responsabilidad de la agencia responsable de la sede para que las estrategias puedan coordinarse e integrarse para crear un trabajo totalmente coordinado.
- SEGURIDAD INTEGRAL: Sera entendida como un proceso global, que incluye factores técnicos, humanos, físicos y organizacionales, la seguridad de la información debe ser considerada como una parte regular del trabajo, presente y aplicada durante todo el proceso.
- GESTIÓN DE RIESGOS: Serán fundamentales para los procesos de seguridad de la información. La gestión de riesgos le permitirá mantener un entorno controlado al limitar los riesgos a un nivel aceptable.
- PROPORCIONALIDAD: Las medidas de resguardo, detección y restauración deben corresponder a los riesgos potenciales y los costos de información relacionados con los servicios involucrados.
- MEJORA CONTINUA: Los controles de seguridad deben actualizarse habitualmente para mantener su efectividad relevante para la evolución de los sistemas de protección y amenazas.
- SEGURIDAD POR DEFECTO: Los sistemas deben estar diseñados, configurados para proporcionar un nivel suficiente de seguridad por defecto.

La Oficina General de Admisión estima que la seguridad de la información debe integrarse en la jerarquía de los empleados.

Dado que la confidencialidad concierne a todos los empleados de la Oficina General de Admisión, esta política debe ser socializada, entendida y aceptada responsablemente por todos los empleados.

Compromiso De La Dirección

La Oficina General de Admisión, entendiendo lo valioso que es garantizar la seguridad para lograr sus propósitos, se compromete a:

- Promover roles y compromiso para garantizar la seguridad de la información.
- Proporcionar los recursos necesarios para lograr las metas de seguridad de la información.
- Incitar, promover y sensibilizar en materia de política de seguridad de la información.
- Tenga en cuenta los riesgos de seguridad de la información al tomar decisiones.

Roles y Responsabilidades

La Oficina General de Admisión, encabezado por el director, tiene el compromiso de garantizar la seguridad de los activos sensibles a cargo de sus funciones mediante la adopción de medidas para garantizar el cumplimiento de las normas.

Identificar quién es el responsable de implementar y monitorear las medidas de ciberseguridad y seguridad de la información. Esto debe ser determinado por el entorno de gestión y liderazgo o determinado por el comité de auditoría y debe incluir roles y responsabilidades.

Será responsable de desarrollar y mantener la política, asegurándose de que sea relevante y esté actualizada.

Gestión de la Seguridad de los Recursos Humanos

La oficina general de admisión debe gestionar sus actividades de acuerdo con los criterios de seguridad definidos en la política, la cual es clave para su ejecución.

Deben cubrir los requerimientos establecidos en la política, incluyendo el período de precontrato, el período de contrato y el período de retiro del empleado.

Formación Y Concienciación

La Oficina General de Admisión debe asegurarse de que todos los empleados actuales reciban el nivel adecuado de formación y concienciación en el área de seguridad de la información, particularmente en el área de seguridad de la información como también en prevención de fugas.

En este sentido, los empleados deben estar informados sobre las mejoras de las políticas y métodos de seguridad que les son de aplicación, así como de los riesgos existentes, de tal forma que se asegure el cumplimiento.

Los empleados tienen el deber y la obligación de actuar de manera responsable con respecto a la información que manejan, procurando que esta información no caiga en malas manos.

Política De Mesas Limpias

Establecer los requerimientos para garantizar la seguridad en el trabajo:

- La sesión del dispositivo debe bloquearse al instante que el empleado abandona el lugar de trabajo, esto se puede hacer de

forma manual o automática configurando un bloqueo del ordenador.

- Al final de la jornada laboral, los empleados deben conservar todos los documentos físicos y digitales que utilizan en el trabajo.
- Las computadoras de escritorio deben tener un mantenimiento adecuado y estar libres de papeles o soportes de computadora que otras personas puedan ver o acceder.

Gestión De Activos

Los activos de información necesarios para respaldar los procesos comerciales de la oficina de admisiones deben identificarse e inventariarse.

Se deberá clasificarse de acuerdo con el tipo de información que manejan.

Tiene que asignarse una persona responsable de la adecuada gestión de los recursos de información. La persona responsable debe registrar oficialmente al usuario autorizado al recurso especificado. Además, cada propiedad debe tener un responsable de asegurar que la propiedad esté inventariada, clasificada y protegida.

La configuración de recursos debe actualizarse periódicamente.

Gestión De Las Copias De Seguridad

La información, el software y los sistemas de seguridad deben respaldarse y revisarse habitualmente.

Se recomienda generar un respaldo de aplicaciones, archivos y bases de datos, esto debe ser programado dependiendo de la seguridad de la información, por ejemplo, las plataformas de inscripciones deben ser

respaldadas semanalmente debido a que es robada o manipulada por ataques o empleados no autorizados. en caso de que una gran cantidad de personas se registren todos los días, es posible realizar copias de seguridad diarias, lo que es ideal para la seguridad de la información.

Es importante tener en cuenta que las copias de seguridad deben tener las mismas protecciones que los datos originales, lo que garantiza un almacenamiento adecuado y un control de acceso adecuado. Se deben realizar pruebas de restauración de respaldo para garantizar que los procesos funcionen correctamente, esto debe hacerse periódicamente y todo el proceso debe documentarse en todo momento.

Los archivos de copia de seguridad, las aplicaciones y la información deben almacenarse y protegerse en una ubicación limitada y segura, al igual que las copias de seguridad no deben almacenarse en el mismo lugar.

Clasificación De La Información

El modelo de información debe clasificarse y definirse de manera que se conozcan e implementen medidas técnicas y organizativas para mantener su disponibilidad, el modelo debe contar con un responsable de actualización.

Tipos De Información

- Soporte logístico: información que los empleados utilizan a través de medios de oficina, correo electrónico o un sistema de TI evolucionado.
- Medios físicos: información que se encuentra en archivadores o en papel, USB, DVD, etc.

Niveles De Clasificación

La oficina general de admisión debería de categorizar la información en cinco niveles:

- Uso público.
- Difusión limitada.
- Información confidencial.
- Información reservada.
- Información secreta.

Tabla 3 Niveles de Clasificación

NIVEL	DETALLE NIVEL	EJEMPLOS
Uso público	Se trata de información que puede ser conocida por cualquier persona, y el uso de esta información de manera engañosa no amenaza los intereses de la Oficina General de Admisión.	La página web de admisión donde se publican los cronogramas de exámenes, numero de vacantes, montos de pagos para las inscripciones, tutoriales del proceso de inscripción
Difusión limitada	Se trata de información utilizada en el proceso de registro de postulantes, cuyo uso fraudulento atenta contra los intereses de la Oficina General de Admisión.	Los datos de los postulantes que se inscribieron al examen de admisión, modificación de las carreras que seleccionaron los postulantes o las modalidades a la que se presentan, también si manipulan los pagos

		que se cargan a dicha plataforma para validar su inscripción.
Información confidencial	Esta es información que puede ser conocida solo por unas pocas personas, se maneja información muy sensible durante el proceso de inscripción y la manipulación de esta información podría amenazar los intereses de la Oficina General de Admisión.	En el proceso de calificación solo tiene acceso el presidente, el calificador, el jefe de la OGAD y el notario, el que maneja dicha información es el calificador y los que supervisan es el presidente, el jefe de la ogad y el notario, si hubiera una alteración de un puntaje o se leyera mal la tarjeta de respuestas con la cual se va a calificar traerá riesgos para la oficina.
Información Reservada	Se trata de información que sólo debe conocer el titular de la OGAD, cuya divulgación podría perjudicar gravemente los intereses de la OGAD.	En el proceso de calificación, se entrega los solucionarios del examen de manera física, según el reglamento de admisión pregrado las claves de las respuestas no se deben de publicar y mucho menos alterar.
Información Secreta	Se trata de información cuya divulgación no autorizada podría	Las tarjetas OMR son aquella información donde se guardan las

	causar perjuicios de extrema gravedad a los intereses esenciales de OGAD.	respuestas de los postulantes, dicha información debe de ser secreta ya que si existiera alguna irregularidad solo en ese caso se sacaría la información para su investigación.

Etiquetado De La Información

La oficina de admisión conjunta debe etiquetar manualmente, para facilitar la correcta gestión de las medidas de seguridad. Los documentos, informes y copias deben estar numerados de acuerdo a su confidencialidad, excepto la información pública.

El procedimiento de etiquetado se definirá de acuerdo con los siguientes requisitos:

- La información debe etiquetarse de acuerdo con el esquema de clasificación.
- Asegúrese de que las etiquetas sean visibles y fácilmente reconocibles.
- Capacite al personal de la oficina sobre cómo colocar y usar etiquetas de acuerdo con los procedimientos de acceso a la información.
- Los activos físicos que contengan información confidencial o delicada deben marcarse cuidadosamente.

Manipulación De La Información

La Oficina General de Admisión es responsable de desarrollar un proceso apropiado para el manejo adecuado de la información, y se deben tomar las medidas necesarias para proteger la información.

Los activos sensibles deben custodiarse hasta que cumpla su ciclo de vida útil.

Privacidad De La Información

La Oficina General de Admisión deberá garantizar la confidencialidad de los activos con el propósito de salvaguardar los derechos de la persona, en consideración al derecho del honor, intimidad y la imagen, con el proceso para controlar el manejo de los activos. Se deben tomar las medidas apropiadas para garantizar la confidencialidad de la información.

Prevención De Fugas De Información

La fuga de información es la divulgación descontrolada de información, ya sea intencional o no, que pueden realizar personas no autorizadas o el propietario pierde el control de acceso.

Es necesario analizar dónde se producen las fugas de información, para ello es necesario identificar qué fugas suponen un mayor riesgo para cada proceso, para identificar las posibles rutas de fuga de cada activo.

- Uso adecuado de dispositivos extraíbles como USB, CD/DVD.
- Uso del correo electrónico.
- Transmisión de información de forma oral.
- Impresión de documentación.

- Salida de documentación.
- Uso de internet.
- Escritorios limpios y ordenadores.

Control De Acceso

Todos los sistemas informáticos gestionados por la Oficina General de Admisión deben contar con sistemas de control de acceso y control de acceso para garantizar que solo las personas autorizadas tengan acceso a la información almacenada.

Requisitos De Negocio Para El Control De Acceso

La Oficina General de Admisión debe aceptar una serie de requisitos para la gestión del control de acceso:

- Todos los usuarios deben ser únicos y no se pueden compartir con otros empleados, para esto cada usuario debe tener permisos.
- Si es posible, debería estar disponible una autenticación de doble factor para acceder a los sistemas de TI.

Derecho De Acceso

La Oficina Genera de Admisión deberá de implementar medidas para regular el acceso y garantizar que se asignen los privilegios necesarios a cada usuario.

- Control de acceso basado en roles: defina los roles que debe tener cada empleado que trabaja en la oficina, como gerente, administrador, empleado y candidato.
- Privilegios mínimos: Cada usuario tendrá privilegios de acuerdo a su función que realice en la oficina.

- Ningún usuario deberá de acceder a los sistemas de información sin la aprobación del responsable.

Control De Acceso Lógico

La oficina general de admisión tiene el deber de crear una política para gestionar las contraseñas, por ejemplo, cada contraseña deberá de contener como mínimo 1 letra mayúscula y números.

Seguridad Física Y Del Entorno

El lugar de alojamiento del sistema de información de la oficina general de admisión, tiene que estar resguardado a través de filtros de inicialización, dichos filtros deben ser perimetrales, sistemas de video vigilancia y accidentes como incendios o desastres naturales.

Cabe resaltar que para los archivos físicos se deberá de tener un control de acceso físico a la información, este registro se debe de realizar en un papel o formato adecuado de ingreso de personal.

Auditorias De Seguridad Y Gestión De Vulnerabilidades

Las vulnerabilidades técnicas en los sistemas de TI deben identificarse periódicamente. La información y aplicaciones utilizadas por la organización se expresan en términos de exposición, omisiones y acciones apropiadas tomadas para reducir los riesgos asociados a las mismas.

Una vez que se descubre una vulnerabilidad, la Oficina General de Admisión deben actuar y realizar las correcciones necesarias lo antes posible. Identificar, gestionar y corregir las vulnerabilidades deben abordarse de acuerdo con un enfoque basado en el riesgo Materialidad y riesgo de los activos.

Sanciones Disciplinarias

En el caso de detectarse vulneración de la política se deberá de tomar medidas correctivas de acuerdo al reglamento de la OGAD, es
Cualquier violación de la presente Política de seguridad de la información puede resultar en la toma de acciones disciplinarias de acuerdo con el proceso interno de la Oficina General de Admisión, es responsabilidad de todos los trabajadores en dar a conocer al responsable sobre las actividades malintencionadas que incumpla con las normativas

Revisión De La Política

La aprobación de esta política implica que la implantación debe de contar con el apoyo de la Dirección de la Oficina General de Admisión para lograr todos los objetivos establecidos.

La presente política de seguridad de la información, será revisado y aprobado anualmente por la Oficina General de Admisión, si se tuviera cambios o modificación de acuerdo a las normas vigentes de seguridad de la información o nuevas amenazas que aparecen se deberá de revisar y en caso de quesea necesario se procederá a una actualización.

Roles, Responsabilidades Y Autoridades Organizacionales

La oficina general de admisión definirá los roles de cada personal que labora en la oficina así mismo cada personal debe de cumplir con responsabilidad lo encomendado por la OGAD, la única autoridad autorizada para llevar a cabo el manejo de la seguridad de la información es el jefe de la OGAD.

4.1.3. Planificación

La oficina general de admisión mantiene sus activos seguros con protección física cuando sus activos de información tengan una protección razonable contra virus.

El proceso de tratamiento de los riesgos de la información requiere de un desarrollo de carácter preventivo, seleccionar y aplicar medidas de control apropiadas o medidas, de manera que se pueda comprender las implicaciones de los riesgos y así evitarlos.

La metodología magerit implementa el proceso de gestión de riesgos para que las autoridades realicen acciones tomando en cuenta los riesgos sobre las tecnologías de la información.

Según (Ortiz Aristizabal, 2021) Magerit tiene como objetivos:

- Sensibilizar a los responsables de las organizaciones de la información sobre la existencia de amenazas y la necesidad de gestionarlas, recomendando métodos sistemáticos de análisis de amenazas emergentes a partir del uso de tecnologías digitales (pág. 41).
- Proporcionar herramientas oportunas de detección, evaluación y planificación del tratamiento para controlar los riesgos (pág. 41).

Identificación de riesgos:

(Ortiz Aristizabal, 2021) menciona que el proceso de identificación de riesgos nos permite conocer y tener una idea de cuanto valor tiene la información y de cómo se está protegiendo los activos de la oficina general de admisión (pág. 53).

En tal sentido nos enfocaremos en analizar las amenazas son frecuentes y se guían por los principios del análisis de riesgos:

- El proceso de identificación de activos clave de la comisión de admisiones.
- El proceso de identificación de amenazas a los activos.

- Definir varios controles de seguridad definidos por recursos
- Implementar un proceso de evaluación si ocurre una amenaza en cualquier momento.

Para la oficina general de admisión los activos son:

  - La plataforma de inscripciones
  - El sistema de calificación de exámenes
  - Los equipos informáticos
  - Las instalaciones donde se encuentran los equipos informáticos
  - El personal que labora en la oficina

Tabla 4 Activos de la Oficina General de Admisión

DATOS/INFORMACIÓN	- Archivos - Credenciales - Datos de validación de credenciales - Registro de actividades
SOFTWARE	- Windows 10 el más utilizados, se encuentran los diversos sistemas operativos. -Sistema de inscripción
HARDWARE	-servidor de base de datos - Equipos informáticos
COMUNICACIONES	-Acceso a Internet -Red Telefónica básica -Wifi -Red LAN
EQUIPOS AUXILIARES	-Fuentes de suministro de energía -Sistema de alimentación interrumpidas. -Sistema de extinción de incendios

SERVICIOS	Correo electrónico Almacenamiento internet
PERSONAL	autoridad de la OGAD Especialista de Sistemas Asistente de sistemas secretaria personal de inscripción personal de inscripción personal de imagen de la OGAD personal de almacén
SOPORTES DE INFORMACIÓN	Almacenamiento en red

Valoración De Activos

(Ortiz Aristizabal, 2021) nos dice que el proceso de tasación de la propiedad está impulsado por los cambios que pueden ocurrir e impactar negativamente a la comisión de admisión en general al evitar los costos de tasación inicial, los costos de remodelación, el uso de la propiedad y la generación de oportunidades perdidas, asegurando siempre la disponibilidad, integridad, confidencialidad y disponibilidad de cada oportunidad (pág. 58).

Servicios de base de datos:

Los servidores almacenan los datos de todos los ingresantes y todos los procesos han sido y están siendo realizados por la Comisión Central de Admisión. (Ortiz Aristizabal, 2021) menciona que este servidor es básicamente útil para la captación y operación de estudiantes universitarios y la pérdida de datos se verá reflejada en información confidencial, poniendo en peligro la Autenticidad (A), Confiabilidad (C), Integridad (I) y Disponibilidad (D) de la información. Además, no hay evidencia de planes de respaldo para servidores externos, falta de comprensión de los sistemas de seguridad que protegen la información y el acceso físico y lógico donde se almacenan los

activos más importantes, es decir, la información y el código fuente del creador (pág. 59).

Identificación De Amenazas

Una vez realizado e identificado los activos más importantes de la Oficina General de Admisión, se tiene que proceder a identificar las posibles amenazas que puedan afectar al activo.

Tabla 5 Clasificación

[N] Desastres Naturales
[I] De origen industrial
[E] Errores y fallos no intencionados
[A] Ataques intencionados

Fuente: *PUBLICAS, M. D. (20 de 05 de 2006)*

Tabla 6 Clasificación de Amenazas

[N] Desastres Naturales
[N.1] Fuego
[N.2] Daños por agua
[N.3] Desastres Naturales
[I] De origen industrial
[I.1] Fuego
[I.2] Daños por agua
[I.3] Corte del Suministro Eléctrico
[I.4] Fallo de servicios de comunicaciones
[I.5] Interrupción de otros servicios y suministros esenciales
[E] Errores y fallos no intencionados
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.3] Errores de configuración
[E.4] Deficiencias en la organización
[E.5] Errores de [re-]encaminamiento

[E.6] Escapes de información
[E.7] Alteración accidental de la información
[E.8] Destrucción de información
[E.9] Fugas de información
[E.10] Vulnerabilidades de los programas (software)
[E.11] Caída del sistema por agotamiento de recursos
[E.12] Pérdida de equipos
[E.13] Indisponibilidad del personal
[A] Ataques intencionados
[A.1] Manipulación de la configuración
[A.2] Suplantación de la identidad del usuario
[A.3] Abuso de privilegios de acceso
[A.4] Acceso no autorizado
[A.5] Modificación deliberada de la información
[A.6] Destrucción de información
[A.7] Divulgación de información

Fuente: *PUBLICAS, M. D. (20 de 05 de 2006)*

Tabla 7 Identificación de las Amenazas

ACTIVOS
DATOS/INFORMACIÓN
Archivos, Credenciales, Datos de validación de credenciales, Registro de actividades
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.3] Errores de configuración
[E.4] Deficiencias en la organización
[E.5] Errores de [re-]encaminamiento
[E.6] Escapes de información
[E.7] Alteración accidental de la información
[E.8] Destrucción de información
[E.9] Fugas de información
[E.10] Vulnerabilidades de los programas (software)

[E.11] Caída del sistema por agotamiento de recursos
[E.12] Pérdida de equipos
[E.13] Indisponibilidad del personal
[A.1] Manipulación de la configuración
[A.2] Suplantación de la identidad del usuario
[A.3] Abuso de privilegios de acceso
[A.4] Acceso no autorizado
[A.5] Modificación deliberada de la información
[A.6] Destrucción de información
[A.7] Divulgación de información
[I.4] Fallo de servicios de comunicaciones
SERVICIOS
Correo electrónico, Almacenamiento, internet
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.6] Escapes de información
[E.7] Alteración accidental de la información
[A.4] Acceso no autorizado
[A.5] Modificación deliberada de la información
[A.6] Destrucción de información
[A.7] Divulgación de información
SOFTWARE
Diversos sistemas operativos entre los más utilizados **Microsoft Windows 10, Sistema de inscripción**
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.5] Errores de [re-]encaminamiento
[E.6] Escapes de información
[E.8] Destrucción de información
[E.9] Fugas de información
[E.10] Vulnerabilidades de los programas (software)
HARDWARE
Servidor de base de datos, Equipos informáticos

[N.1] Fuego
[N.3] Desastres Naturales
[I.1] Fuego
[I.2] Daños por agua
[I.3] Corte del Suministro Eléctrico
[E.2] Errores del administrador
[E.11] Caída del sistema por agotamiento de recursos
[E.12] Pérdida de equipos
[A.3] Abuso de privilegios de acceso
REDES Y COMUNICACIONES
Acceso a Internet, Red Telefónica básica, Wifi, Red LAN
[E.2] Errores del administrador
[E.5] Errores de [re-]encaminamiento
[E.9] Fugas de información
[E.11] Caída del sistema por agotamiento de recursos
[A.2] Suplantación de la identidad del usuario
[A.3] Abuso de privilegios de acceso
[A.4] Acceso no autorizado
EQUIPAMIENTO AUXILIAR
Fuentes de alimentación, Sistema de alimentación interrumpidas, Sistema de extinción de incendios
[N.1] Fuego
[N.3] Desastres Naturales
[I.1] Fuego
[I.2] Daños por agua
[I.5] Interrupción de otros servicios y suministros esenciales
[E.12] Pérdida de equipos
[A.4] Acceso no autorizado
SOPORTE DE INFORMACIÓN
Almacenamiento en red
[N.1] Fuego
[N.3] Desastres Naturales
[I.1] Fuego

[I.2] Daños por agua
[I.3] Corte del Suministro Eléctrico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.7] Alteración accidental de la información
[E.8] Destrucción de información
[E.9] Fugas de información
[E.12] Pérdida de equipos
[A.4] Acceso no autorizado
[A.5] Modificación deliberada de la información
[A.7] Divulgación de información
INSTALACIONES
Oficinas
[N.1] Fuego
[N.3] Desastres Naturales
[I.1] Fuego
[I.2] Daños por agua
[E.9] Fugas de información
[A.4] Acceso no autorizado
[A.5] Modificación deliberada de la información
[A.7] Divulgación de información
PERSONAL
Autoridad de la OGAD, Especialista de Sistemas, Asistente de sistemas, secretaria, personal de inscripción, personal de inscripción, personal de imagen de la OGAD, personal de almacén
[E.4] Deficiencias en la organización
[E.9] Fugas de información
[E.13] Indisponibilidad del personal
[A.2] Suplantación de la identidad del usuario
[A.3] Abuso de privilegios de acceso
[A.4] Acceso no autorizado
[A.5] Destrucción de la información.

Fuente: *PUBLICAS, M. D. (20 de 05 de 2006)*

Valoración De Las Amenazas

(Ortiz Aristizabal, 2021) explica que en esta etapa se evalúan todas las amenazas que puedan surgir en diferentes áreas, ya sea en funciones implementadas por el usuario o daños a la propiedad (pág. 66).

En el siguiente cuadro se indica los valores de identificación y calificación de las amenazas.

Tabla 8 Probabilidad de Ocurrencia

Alto (A)
Medio (M)
Bajo (B)

Tabla 9 Dimensión de Seguridad

Confiabilidad (C)
Integridad (I)
Disponibilidad (D)

Tabla 10 Escala de Rango porcentual dimensión de seguridad

Alto (A)
Medio (M)
Bajo (B)

Tabla 11 Identificación de Riesgo

ACTIVOS	PROBABILIDAD DE OCURRENCIA	[C]	[I]	[D]
DATOS/INFORMACIÓN				
Archivos, Credenciales, Datos de validación de credenciales, Registro de actividades				
[E.1] Errores de los usuarios	**A**	**M**	**A**	**M**
[E.2] Errores del administrador	**B**	**B**	**M**	**A**
[E.3] Errores de configuración	**M**	**A**		
[E.4] Deficiencias en la organización	**B**	**M**	**M**	**M**
[E.5] Errores de [re-]encaminamiento	**B**	**A**		
[E.6] Escapes de información	**M**	**M**	**M**	**B**
[E.7] Alteración accidental de la información	**B**	**M**	**A**	**B**
[E.8] Destrucción de información	**B**			**A**
[E.9] Fugas de información	**B**	**B**	**A**	**M**
[E.10] Vulnerabilidades de los programas (software)	**B**	**B**	**A**	**M**
[E.11] Caída del sistema por agotamiento de recursos	**M**			**A**
[E.12] Pérdida de equipos	**M**			**A**
[E.13] Indisponibilidad del personal	**M**			**M**
[A.1] Manipulación de la configuración	**B**		**A**	
[A.2] Suplantación de la identidad del usuario	**B**		**A**	
[A.3] Abuso de privilegios de acceso	**B**	**B**	**A**	**M**
[A.4] Acceso no autorizado	**B**	**A**	**A**	

[A.5] Modificación deliberada de la información	**B**		**A**	
[A.6] Destrucción de información	**M**			**A**
[A.7] Divulgación de información	**B**		**A**	**A**
[I.4] Fallo de servicios de comunicaciones	**A**	**A**	**M**	**B**
SERVICIOS				
Correo electrónico, Almacenamiento, internet				
[E.1] Errores de los usuarios	**B**		**B**	
[E.2] Errores del administrador	**B**		**B**	
[E.6] Escapes de información	**B**		**M**	**A**
[E.7] Alteración accidental de la información	**M**	**A**	**A**	**A**
[A.4] Acceso no autorizado	**B**		**M**	**M**
[A.5] Modificación deliberada de la información	**A**	**A**	**A**	**A**
[A.6] Destrucción de información	**B**			**B**
[A.7] Divulgación de información	**B**			**B**
SOFTWARE				
Diversos sistemas operativos entre los más utilizados Microsoft Windows 10, Sistema de inscripción				
[E.1] Errores de los usuarios	**B**	**A**	**A**	
[E.2] Errores del administrador	**B**			**M**
[E.5] Errores de [re-]encaminamiento	**B**			**B**
[E.6] Escapes de información	**M**	**A**	**A**	**A**
[E.8] Destrucción de información	**B**			**M**
[E.9] Fugas de información	**M**		**A**	**A**
[E.10] Vulnerabilidades de los programas (software)	**B**		**A**	**M**
HARDWARE				

Servidor de base de datos, Equipos informáticos				
[N.1] Fuego	**B**			**A**
[N.3] Desastres Naturales	**B**			**A**
[I.1] Fuego	**B**			**A**
[I.2] Daños por agua	**B**			**A**
[I.3] Corte del Suministro Eléctrico	**B**			**A**
[E.2] Errores del administrador	**B**	**B**	**M**	**A**
[E.11] Caída del sistema por agotamiento de recursos	**M**			**A**
[E.12] Pérdida de equipos	**B**			**A**
[A.3] Abuso de privilegios de acceso	**B**	**B**	**M**	**A**
REDES Y COMUNICACIONES				
Acceso a Internet, Red Telefónica básica, Wifi, Red LAN				
[E.2] Errores del administrador	**B**	**B**	**M**	**A**
[E.5] Errores de [re-]encaminamiento	**B**			**A**
[E.9] Fugas de información	**B**	**M**	**A**	**A**
[E.11] Caída del sistema por agotamiento de recursos	**B**			**A**
[A.2] Suplantación de la identidad del usuario	**B**		**B**	**M**
[A.3] Abuso de privilegios de acceso	**B**	**B**	**B**	**A**
[A.4] Acceso no autorizado	**B**		**M**	**A**
EQUIPAMIENTO AUXILIAR				
Fuentes de alimentación, Sistema de alimentación interrumpidas, Sistema de extinción de incendios				
[N.1] Fuego	**B**			**A**
[N.3] Desastres Naturales	**B**			**A**
[I.1] Fuego	**B**			**A**
[I.2] Daños por agua	**B**			**A**

[I.5] Interrupción de otros servicios y suministros esenciales	**B**			**A**
[E.12] Pérdida de equipos	**B**			**A**
[A.4] Acceso no autorizado	**B**		**M**	**A**
SOPORTE DE INFORMACIÓN				
Almacenamiento en red				
[N.1] Fuego	**B**			**A**
[N.3] Desastres Naturales	**B**			**A**
[I.1] Fuego	**B**			**A**
[I.2] Daños por agua	**B**			**A**
[I.3] Corte del Suministro Eléctrico	**B**			**A**
[E.1] Errores de los usuarios	**B**	**B**	**M**	**A**
[E.2] Errores del administrador	**B**	**M**	**A**	**B**
[E.7] Alteración accidental de la información	**B**	**A**	**A**	**B**
[E.8] Destrucción de información	**B**			**A**
[E.9] Fugas de información	**B**	**A**	**A**	**M**
[E.12] Pérdida de equipos	**B**			**A**
[A.4] Acceso no autorizado	**B**		**B**	**M**
[A.5] Modificación deliberada de la información	**B**	**A**	**A**	**M**
[A.7] Divulgación de información	**B**	**M**	**M**	**B**
INSTALACIONES				
Oficinas				
[N.1] Fuego	**B**			**A**
[N.3] Desastres Naturales	**B**			**A**
[I.1] Fuego	**B**			**A**
[I.2] Daños por agua	**B**			**A**
[E.9] Fugas de información	**B**	**A**	**A**	**M**
[A.4] Acceso no autorizado	**B**		**B**	**M**
[A.5] Modificación deliberada de la información	**B**	**A**	**A**	**B**

[A.7] Divulgación de información	**B**	**M**	**M**	**B**
PERSONAL				
Autoridad de la OGAD, Especialista de Sistemas, Asistente de sistemas, secretaria, personal de inscripción, personal de inscripción, personal de imagen de la OGAD, personal de almacén				
[E.4] Deficiencias en la organización	**B**			**B**
[E.9] Fugas de información	**B**	**A**	**A**	**M**
[E.13] Indisponibilidad del personal	**B**			**B**
[A.2] Suplantación de la identidad del usuario	**B**	**A**	**A**	**A**
[A.3] Abuso de privilegios de acceso	**B**	**A**	**A**	**A**
[A.4] Acceso no autorizado	**B**		**B**	**M**
[A.5] Destrucción de la información	**B**			**A**

Análisis de riesgos según su impacto

Analizaremos el impacto de los riesgos identificados según la siguiente tabla:

Tabla 12 Cuadro de análisis de impacto y probabilidad

		PROBABILIDAD				
		MUY RARO	POCO PROBABLE	POSIBLE	PROBABLE	CASI SEGURO
IMPACTO	MUY ALTO	A	MA	MA	MA	MA
	ALTO	M	A	A	MA	MA
	MEDIO	B	M	M	A	A
	BAJO	MB	B	B	M	M
	MUY BAJO	MB	MB	MB	B	B

Fuente: Magerit 3.0

Teniendo la tabla para medir el impacto del riesgo, clasificaremos por colores para tener nuestro mapa de calor.

Tabla 13 Mapa de calor de impacto y probabilidad

		PROBABILIDAD				
		MUY RARO	POCO PROBABLE	POSIBLE	PROBABLE	CASI SEGURO
IMPACTO	MUY ALTO	A	MA	MA	MA	MA
	ALTO	M	A	A	MA	MA
	MEDIO	B	M	M	A	A
	BAJO	MB	B	B	M	M
	MUY BAJO	MB	MB	MB	B	B

Fuente: Elaboración propia.

Analizaremos según el mapa de calor el impacto de cada uno de los riesgos identificados anteriormente, para poder identificar de manera rápida el grado de riesgo que presenta dicho activo.

Tabla 14 Mapa de calor de datos/información

ACTIVOS	PROBABILIDAD DE OCURRENCIA	[C]	[I]	[D]
DATOS/INFORMACIÓN				
[E.1] Errores de los usuarios	**A**	**M**	**A**	**M**
[E.2] Errores del administrador	**B**	**B**	**M**	**A**
[E.3] Errores de configuración	**M**	**A**	**B**	**B**
[E.4] Deficiencias en la organización	**B**	**M**	**M**	**M**
[E.5] Errores de [re-]encaminamiento	**B**	**A**	**B**	**B**
[E.6] Escapes de información	**M**	**M**	**M**	**B**
[E.7] Alteración accidental de la información	**B**	**M**	**A**	**B**
[E.8] Destrucción de información	**B**	**B**	**B**	**A**
[E.9] Fugas de información	**B**	**B**	**A**	**M**
[E.10] Vulnerabilidades de los programas (software)	**B**	**B**	**A**	**M**
[E.11] Caída del sistema por agotamiento de recursos	**M**	**B**	**B**	**A**
[E.12] Pérdida de equipos	**M**	**B**	**B**	**A**
[E.13] Indisponibilidad del personal	**M**	**B**	**B**	**M**
[A.1] Manipulación de la configuración	**B**	**B**	**A**	**B**
[A.2] Suplantación de la identidad del usuario	**B**	**B**	**A**	**B**
[A.3] Abuso de privilegios de acceso	**B**	**B**	**A**	**M**
[A.4] Acceso no autorizado	**B**	**A**	**A**	**B**

[A.5] Modificación deliberada de la información	B	B	A	B
[A.6] Destrucción de información	M	B	B	A
[A.7] Divulgación de información	B	B	A	A
[I.4] Fallo de servicios de comunicaciones	A	A	M	B

Fuente: Elaboración propia.

Tabla 15 Mapa de calor de servicios

ACTIVOS	PROBABILIDAD DE OCURRENCIA	[C]	[I]	[D]
SERVICIOS				
[E.1] Errores de los usuarios	B	B	B	B
[E.2] Errores del administrador	B	B	B	B
[E.6] Escapes de información	B	B	M	A
[E.7] Alteración accidental de la información	M	A	A	A
[A.4] Acceso no autorizado	B	B	M	M
[A.5] Modificación deliberada de la información	A	A	A	A
[A.6] Destrucción de información	B	B	B	B
[A.7] Divulgación de información	B	B	B	B

Fuente: Elaboración propia.

Tabla 16 Mapa de calor de software

ACTIVOS	PROBABILIDAD DE OCURRENCIA	[C]	[I]	[D]
SOFTWARE				
[E.1] Errores de los usuarios	B	A	A	B
[E.2] Errores del administrador	B	B	B	M
[E.5] Errores de [re-]encaminamiento	B	B	B	B
[E.6] Escapes de información	M	A	A	A
[E.8] Destrucción de información	B	B	B	M
[E.9] Fugas de información	M	B	A	A
[E.10] Vulnerabilidades de los programas (software)	B	B	A	M

Fuente: Elaboración propia.

Tabla 17 Mapa de calor de hardware

ACTIVOS	PROBABILIDAD DE OCURRENCIA	[C]	[I]	[D]
HARDWARE				
[N.1] Fuego	B	B	B	A
[N.3] Desastres Naturales	B	B	B	A
[I.1] Fuego	B	B	B	A
[I.2] Daños por agua	B	B	B	A
[I.3] Corte del Suministro Eléctrico	B	B	B	A
[E.2] Errores del administrador	B	B	M	A
[E.11] Caída del sistema por agotamiento de recursos	M	B	B	A
[E.12] Pérdida de equipos	B	B	B	A
[A.3] Abuso de privilegios de acceso	B	B	M	A

Fuente: Elaboración propia.

Tabla 18 Mapa de calor de redes y comunicaciones

ACTIVOS	PROBABILIDAD DE OCURRENCIA	[C]	[I]	[D]
REDES Y COMUNICACIONES				
[E.2] Errores del administrador	B	B	M	A
[E.5] Errores de [re-]encaminamiento	B	B	B	A
[E.9] Fugas de información	B	M	A	A
[E.11] Caída del sistema por agotamiento de recursos	B	B	B	A
[A.2] Suplantación de la identidad del usuario	B	B	B	M
[A.3] Abuso de privilegios de acceso	B	B	B	A
[A.4] Acceso no autorizado	B	B	M	A

Fuente: Elaboración propia.

Tabla 19 Mapa de calor de equipamiento auxiliar

ACTIVOS	PROBABILIDAD DE OCURRENCIA	[C]	[I]	[D]
EQUIPAMIENTO AUXILIAR				
[N.1] Fuego	B	B	B	A
[N.3] Desastres Naturales	B	B	B	A
[I.1] Fuego	B	B	B	A
[I.2] Daños por agua	B	B	B	A

[I.5] Interrupción de otros servicios y suministros esenciales	B	B	B	A
[E.12] Pérdida de equipos	B	B	B	A
[A.4] Acceso no autorizado	B	B	M	A

Fuente: Elaboración propia.

Tabla 20 Mapa de calor de soporte de información

ACTIVOS	PROBABILIDAD DE OCURRENCIA	[C]	[I]	[D]
SOPORTE DE INFORMACIÓN				
[N.1] Fuego	B	B	B	A
[N.3] Desastres Naturales	B	B	B	A
[I.1] Fuego	B	B	B	A
[I.2] Daños por agua	B	B	B	A
[I.3] Corte del Suministro Eléctrico	B	B	B	A
[E.1] Errores de los usuarios	B	B	M	A
[E.2] Errores del administrador	B	M	A	B
[E.7] Alteración accidental de la información	B	A	A	B
[E.8] Destrucción de información	B	B	B	A
[E.9] Fugas de información	B	A	A	M
[E.12] Pérdida de equipos	B	B	B	A
[A.4] Acceso no autorizado	B	B	B	M
[A.5] Modificación deliberada de la información	B	A	A	M
[A.7] Divulgación de información	B	M	M	B

Fuente: Elaboración propia.

Tabla 21 Mapa de calor de instalaciones

ACTIVOS	PROBABILIDAD DE OCURRENCIA	[C]	[I]	[D]
INSTALACIONES				
[N.1] Fuego	B	B	B	A
[N.3] Desastres Naturales	B	B	B	A
[I.1] Fuego	B	B	B	A
[I.2] Daños por agua	B	B	B	A
[E.9] Fugas de información	B	A	A	M
[A.4] Acceso no autorizado	B	B	B	M
[A.5] Modificación deliberada de la información	B	A	A	B

[A.7] Divulgación de información	B	M	M	B

Fuente: Elaboración propia.

Tabla 22 Mapa de calor del personal

ACTIVOS	PROBABILIDAD DE OCURRENCIA	[C]	[I]	[D]
PERSONAL				
[E.4] Deficiencias en la organización	B	B	B	B
[E.9] Fugas de información	B	A	A	M
[E.13] Indisponibilidad del personal	B	B	B	B
[A.2] Suplantación de la identidad del usuario	B	A	A	A
[A.3] Abuso de privilegios de acceso	B	A	A	A
[A.4] Acceso no autorizado	B	B	B	M
[A.5] Destrucción de la información	B	B	B	A

Fuente: Elaboración propia.

4.1.4. Soporte

Recursos

En la oficina general de admisión se identificaron los recursos con las que cuenta para poder llevar a cabo la gestión de seguridad de la información.

La oficina general de admisión cuenta con recurso de personal, tecnológico y de procesos.

Cuenta con un personal especialista de sistemas, personal de calificación, personal que lleva a cabo el proceso y una autoridad que en este caso es el jefe de la oficina general de admisión.

Competencias

La oficina general de admisión debe de contratar personal con conocimientos en seguridad de la información, que respete y trabaje con responsabilidad el cargo que se le va a encomendar.

La autoridad (jefe de la OGAD), debe de planificar capacitaciones sobre seguridad de la información no solo al encargado de custodiar la información sensible sino también a todo el personal que labore en dicha oficina.

El personal debe ser responsable, comprometido con las actividades que desarrollará dentro de la oficina general de admisión así mismo deberá de aplicar las políticas que maneja la OGAD, para poder proteger la información y no tener vulneraciones.

El personal a cargo de manejar la información sensible debe de documentar toda acción que realice siempre con la autorización y supervisión de la autoridad (jefe de la OGAD).

Concientización

Se debe de concientizar no solo al personal que labora en la oficina sino también a la autoridad (jefe de la OGAD), porque es muy importante tener el apoyo de la autoridad correspondiente debido a que será más factible la aplicación de las políticas de seguridad de la información.

En este punto se debe dar a conocer a la autoridad porque es importante salvaguardar la información, ya que en la actualidad encontramos que las tecnologías van cambiadas y debe de estar capacitando al personal sobre las nuevas amenazas o riesgos que aparezcan en el camino.

La oficina general de admisión es uno de los puntos más importantes de la UNASAM ya que es la encargada de llevar a cabo el proceso de examen de admisión y por ende es una de las oficinas que maneja gran cantidad de datos e información sensible que debe de estar bien resguardado por la autoridad correspondiente de dicha oficina.

Se plantea que se debe de salvaguardar la información en los dos procesos identificados de la OGAD, el proceso de inscripción y el proceso de calificación es ahí donde se debe de tener mucho cuidado con el manejo de la información.

Si durante las inscripciones se vulnera la seguridad de la plataforma web la persona o personal no autorizado podrá modificar los datos como carrera profesional inscrita, modalidad y pagos realizados, muy aparte como se trabaja con un ordenador de escritorio para la calificación la cual no debe de tener acceso a internet para evitar fuga o vulneraciones durante el proceso de calificación, es ahí donde es el otro punto fundamental que debemos de tener

mucho cuidado como Oficina porque si se vulnera o hay fugas de información la OGAD tendría problemas grandes ya que se estaría adulterando la información.

Debido a eso es que se debe de garantizar que toda información que brinde la OGAD sea transparente y de confiabilidad, esto garantizara la confianza de la población y de los postulantes.

Comunicación

La autoridad de la OGAD es la encargada de comunicar a todo el personal que labora sobre las políticas que se maneja dentro de la organización y también se debe de sociabilizar esta política con cada uno de los trabajadores de acuerdo al rol que va a desempeñar en la OGAD.

Las políticas de seguridad de la información deben ser canalizado y entregado de manera digital mediante los correos institucionales y se debe de colocar en lugares estratégicos de fácil visibilidad para que todo el personal pueda identificarlo en todo momento de su desarrollo laboral.

Se debe de evaluar al personal sobre las políticas que tiene la Oficina General de Admisión, para poder capacitarlos y reforzar los puntos débiles que tiene cada uno de ellos sobre las políticas y seguridad de la información.

También se debe de comunicar cada vez que se actualicen o modifiquen las políticas de seguridad de la información.

Toda acción o modificación de las políticas debe estar correctamente documentado para que el personal pueda identificar cuáles fueron las actualizaciones o modificaciones.

4.1.5. Operación

En base al resultado del análisis de los riesgos, (Ortiz Aristizabal, 2021) propone acciones de mejora sugeridas, que pueden ser implementadas a través de planes de acción o gestión de riesgos, para que la información conserve siempre sus características de confidencialidad, integridad y disponibilidad (pág. 78).

Con el desarrollo de la tecnología (Ortiz Aristizabal, 2021) indica que se ve obligado a cambiar según el progreso tecnológico, cuando aparecen nuevas tecnologías, desaparecen las viejas tecnologías, se crean nuevas fuentes de información y se desarrollan nuevos métodos de protección de la información (pág. 79).

El proceso de tratamiento de riesgos de seguridad de la información, debe estar orientado a las estrategias que se requiere para lograr una cultura de prevención y así aplicar los controles y medidas adecuadas, de tal forma comprender lo que significan los riesgos, para plantear mecanismos que reduzcan la afectación de la información, con el único fin de tener un control sobre los riesgos, la Oficina General de Admisión debe garantizar como mínimo:

- El correcto funcionamiento de los sistemas de información.
- Mecanismos de control de seguridad de la información física y digital.
- Implementar nuevos mecanismos de seguridad

(Ortiz Aristizabal, 2021) nos dice que debemos de realizará un análisis de costos de las diferentes acciones que se pueden tomar de manera muy efectiva, atendiendo las posibles pérdidas por no tomar acción frente al riesgo, identificando riesgos, amenazas, etc. Amenazas y violaciones, se pueden seleccionar medidas de control para reducir el nivel de riesgo del enfoque administrativo o no requieren tiempo y recursos (pág. 78).

Para ello se define los siguiente:

- Un nivel bajo de riesgo puede ser aceptado por OGAD porque la probabilidad es baja y el impacto es insignificante, no se requieren acciones adicionales, es decir, no se requieren acciones de control y mejora.
- Los riesgos de nivel medio tienen que ser tratados con el análisis de costo beneficio, para tomar la decisión de asumir, reducir o aceptar, dependiendo de la estrategia de la OGAD.

- Los niveles de riesgo alto, se debe de generar controles de riesgos más rigurosos, para reducir el impacto y mejorar las posibles consecuencias.

4.1.6. Evaluación del desempeño

La evaluación del desempeño comprende en evaluar la seguridad de la información, cuya actividad debe ser desarrollado por la Oficina General de Admisión.

La OGAD es la encargada de determinar lo que se va a monitorear y medir los controles de la seguridad de la información.

El proceso de monitoreo de riesgos nos da a conocer si las acciones implementadas fueron efectivos y si los riesgos siguen igual o sufrieron una modificación, también sirve para ver en el transcurso del periodo cuantos riesgos importantes siguen activos y si se han concretado o no para ver la eficacia de los mismos.

El monitoreo es uno de los procesos que se debe de realizar tantas veces sea conveniente por la Oficina General de Admisión.

Para monitorear los riesgos se debería de tener en cuenta lo siguiente:

- Conformar un equipo de trabajo para la revisión de los estados de riesgos, esto conlleva a tener una estructura definida por la OGAD, la cual debe de contener lo siguiente, un objetivo y tiempo, para lograrlo se debe de plantear algunas preguntas como:
    - ¿Qué riesgos identificados son de mayor prioridad en cuanto a tratamiento?
    - ¿Existen cambios en la prioridad de tratamiento de riesgos, correspondientes a su última evaluación?
    - ¿Los planes de acción fueron efectivos?
    - ¿Es necesario alguna implementación adicional para tratar los riesgos?
- Indicadores claves de riesgos, los indicadores de riesgos de la OGAD, nos brindan información sobre los niveles a los cual esta expuesto los

riesgos en un determinado periodo (Oficinas en zonas de riesgo alto, Número de postulantes que utilizan las herramientas en el último periodo).

- Indicadores calve de rendimiento, los indicadores no brindan información de los procesos operativos (Porcentaje de consultas en la plataforma de inscripciones, cantidad de inscritos mensualmente).
- Auditorias de riesgos, determinaran la efectividad del proceso de gestión de riesgos.
- Análisis de tendencia y varianza, los resultados serán comparados para verificar si los riesgos siguen existiendo.

Las herramientas de monitoreo son definidas por la Oficina General de Admisión de acuerdo a las necesidades que se requiera.

Auditoría interna

La Oficina General de Admisión es la encargada de llevar las auditorías internas en periodos, para ello se debe de planificar, establecer e implementar las acciones necesarias para llevar a cabo, los programas de auditoria esto conlleva considerar los procesos donde se maneje la información sensible.

Toda auditoria que se lleve a cabo se debe de documentar en un archivo físico o digital para su posterior tratamiento y evaluación de los resultados obtenidos de la auditoria.

Revisión por la gerencia

La Oficina General de Admisión es la encargada de planificar periódicamente la supervisión de los sistemas de seguridad de la información, para garantizar su continuidad.

Las revisiones programadas deben de contener los siguientes aspectos:

- Revisiones realizadas anteriormente.
- Realizar una retroalimentación respecto al rendimiento de seguridad de la información (acciones correctivas, resultados de los monitoreos, resultados de las auditorias) y cumplir con los objetivos establecidos en la seguridad de la información.

La Oficina General de Admisión es la encargada de documentar los productos obtenidos de las revisiones, para luego incluir decisiones relacionadas a la oportunidad de mejora continua, dicha información debe ser almacenada y custodiada por la autoridad correspondiente.

4.1.7. Mejoras

El tratamiento de las no conformidades y las acciones correctivas, es uno de los factores importantes dentro de la Oficina General de Admisión para la mejora continua de todos los sistemas utilizados, las no conformidades es el no cumplimiento de los requisitos establecidos.

(Ortiz Aristizabal, 2021) dice que las no conformidades pueden ser externas (incumplimiento de la norma ISO) como también internas (incumplimientos de procedimientos de la OGAD).

Las no conformidades no tienen un origen único debido a que pueden ser detectadas en diversas situaciones de la Oficina General de Admisión.

A continuación, se mencionará algunas de las razones para detectar una no conformidad:

- En la gestión interna de procesos.
- En las inspecciones que están mencionados en la documentación de los sistemas de gestión.
- En las auditorias que se llevan con el fin de cumplir los requisitos legales.

Las no conformidades se pueden clasificar por su gravedad:

- No conformidad mayor, es el incumplimiento de los requisitos normativos que vulneran la integridad.
- No conformidad menor, son esporádicas y no dañan la eficiencia e integridad.
- Observación, constituye la oportunidad de una mejora, como por ejemplo optimizar procedimientos del sistema.

4.2. Presentación de resultado y prueba de hipótesis

Análisis Descriptivo

Resultados pre test

Respecto a la evaluación para medir el nivel de seguridad de la información en la oficina general de admisión – Huaraz, se aplicó una encuesta a 380 postulantes que son los actores principales en el proceso que se lleva a cabo en la Oficina General de Admisión.

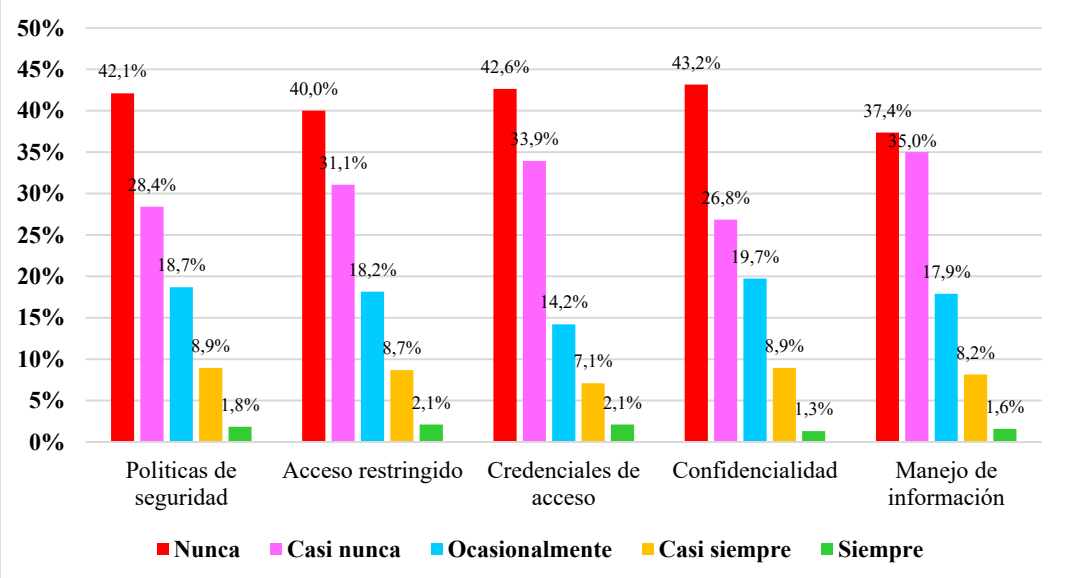
Las alternativas que se utilizó en la encuesta fueron nunca (1), casi nunca (2), ocasionalmente (3), casi siempre (4) y siempre (5), los resultados estuvieron de acuerdo a las dimensiones y variables para poder determinar el nivel de seguridad de la información de la Oficina General de Admisión.

Tabla 23 Dimensión de Confiabilidad

Escala de Medición	Políticas de seguridad	Acceso restringido	Credenciales de acceso	Confidencialidad	Manejo de información
Nunca	160	152	162	164	142
Casi nunca	108	118	129	102	133
Ocasionalmente	71	69	54	75	68
Casi siempre	34	33	27	34	31
Siempre	7	8	8	5	6
Total, general	380	380	380	380	380

Fuente: Elaboración propia

Figura 4 Grafico de Barras de la dimensión de Confiabilidad



Fuente: Elaboración propia

Políticas de seguridad

Como podemos observar en el grafico de barras el 42.1% de postulantes desconoce de las políticas de seguridad de la Oficina General de Admisión y solo un 1.8% tiene conocimiento de ellas.

Acceso restringido

El grafico de barras nos muestra que un 40% de postulantes desconoce sobre las limitaciones que tiene su cuenta de postulante en la plataforma de inscripciones y 2.1% de los postulantes encuestados conoce las limitaciones que tiene.

Credenciales de Acceso

El 42.6% de los postulantes no comparte sus credenciales de acceso a la plataforma de inscripciones, mientras que un 2.1% desconoce de las políticas de seguridad y no protege su credencial de acceso (comparte con otras personas sus credenciales).

Confidencialidad

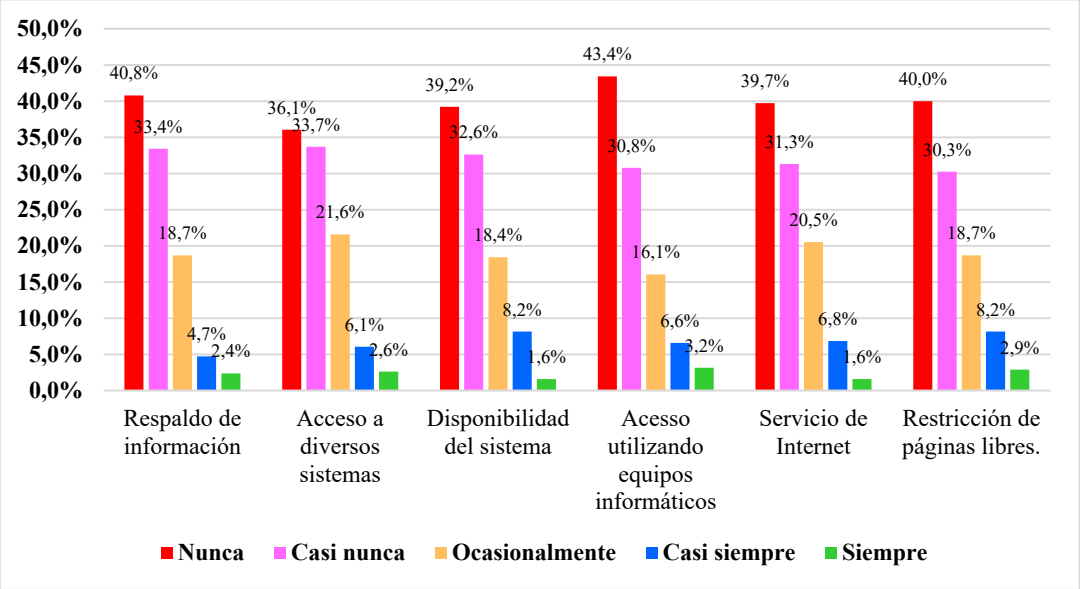
El 43.2% de los postulantes desconoce el tratamiento que le puedan dar a su información que deja al momento de su inscripción y solo el 1.3% tiene conocimiento sobre la confidencialidad de sus datos.

Tabla 24 Dimensión de Disponibilidad

Escala de Medición	Respaldo de información	Acceso a diversos sistemas	Disponibilidad del sistema	Acceso utilizando equipos informáticos	Servicio de Internet	Restricción de páginas libres.
Nunca	155	137	149	165	151	152
Casi nunca	127	128	124	117	119	115
Ocasionalmente	71	82	70	61	78	71
Casi siempre	18	23	31	25	26	31
Siempre	9	10	6	12	6	11
Total general	380	380	380	380	380	380

FUENTE: Elaboración propia

Figura 5 Grafico de barras de la dimensión de Disponibilidad



FUENTE: Elaboración propia

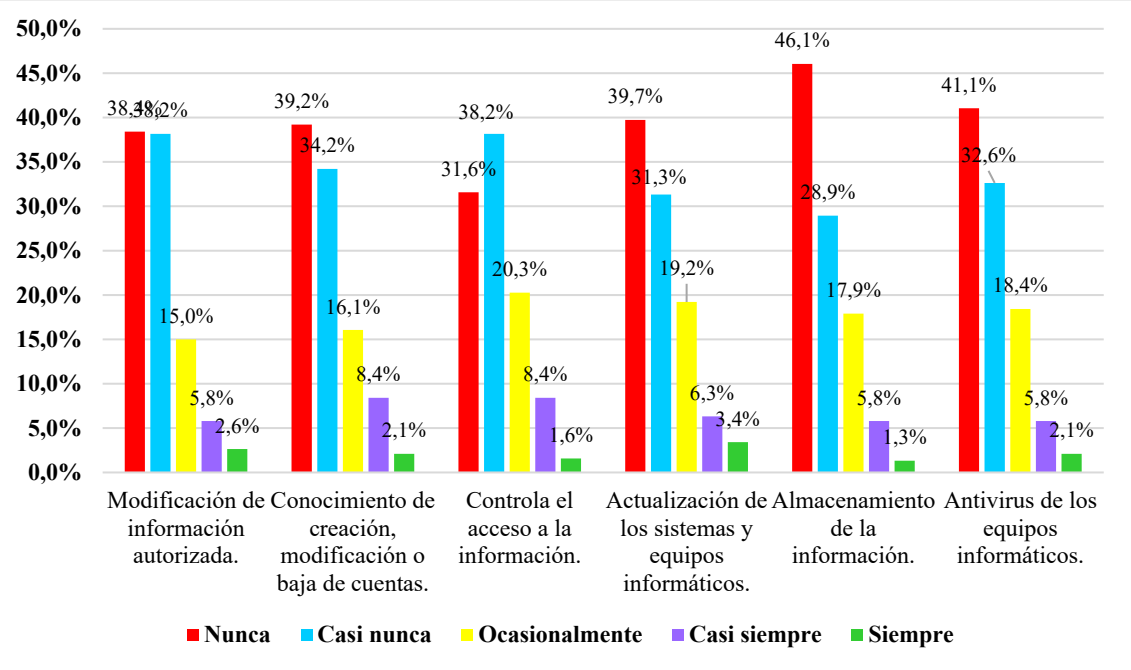
El 43.4% de los postulantes utilizan los equipos informáticos de la Oficina General de Admisión para realizar su inscripción a los exámenes de admisión y un 3.2% realiza su inscripción de manera virtual.

Tabla 25 Dimensión de Integridad

Escala de Medición	Modificación de información autorizada	Conocimiento de creación, modificación o baja de cuentas	Controla el acceso a la información	Actualización de los sistemas y equipos informáticos	Almacenamiento de la información.	Antivirus de los equipos informáticos
Nunca	146	149	120	151	175	156
Casi nunca	145	130	145	119	110	124
Ocasionalmente	57	61	77	73	68	70
Casi siempre	22	32	32	24	22	22
Siempre	10	8	6	13	5	8
Total general	380	380	380	380	380	380

FUENTE: Elaboración propia

Figura 6 Grafico de Barras de la dimensión de Integridad



FUENTE: Elaboración propia

El 46.1% del postulante desconoce donde se almacenan sus datos que dejan en su inscripción mientras que solo el 1.3% de los postulantes tiene conocimiento del lugar donde se almacenara su información.

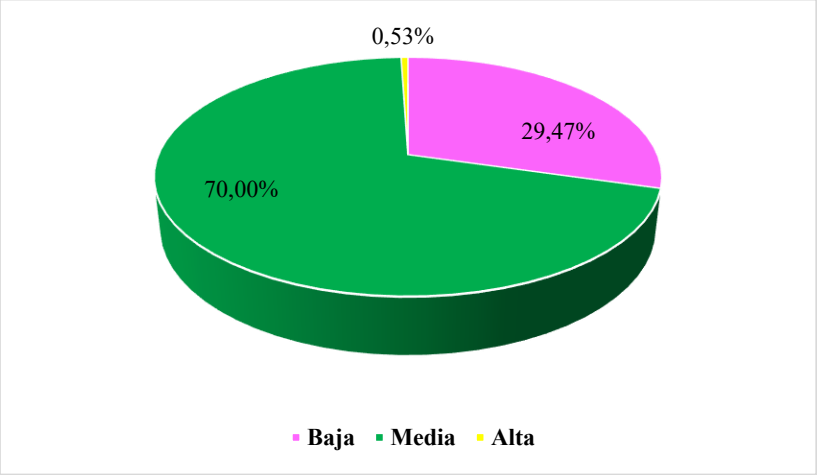
- Respecto al nivel de seguridad se obtuvieron los siguientes resultados:

Tabla 26 Resultados de la dimensión Confidencialidad

Nivel de Seguridad	Frecuencia	Porcentaje
Baja	112	29.47%
Media	266	70.00%
Alta	2	0.53%
Total	380	100%

FUENTE: Elaboración propia

Figura 7 Resultados de la dimensión Confidencialidad



Fuente: Elaboración propia

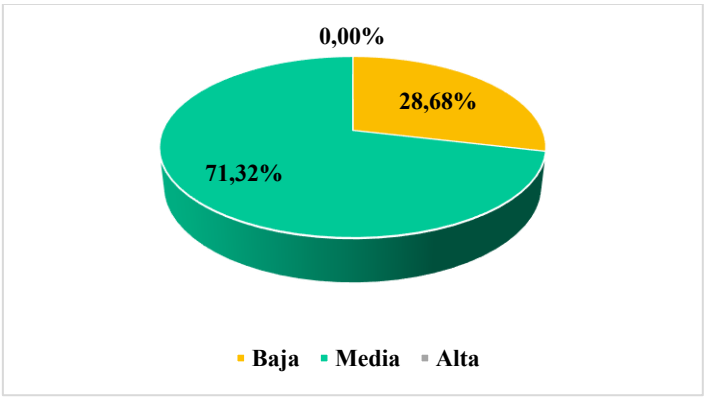
En el cuadro 15 y figura 7 se observa que la confiabilidad de la información, conformado por un 70%, califican como media y un 0.53% considera que es alto la confiabilidad de la información.

Tabla 27 Resultados de la dimensión Disponibilidad

Nivel de Seguridad	Frecuencia	Porcentaje
Baja	109	28.68%
Media	271	71.32%
Alta	0	0.00%
Total	380	100%

FUENTE: Elaboración propia

Figura 8 Resultados de la dimensión Disponibilidad



FUENTE: Elaboración propia.

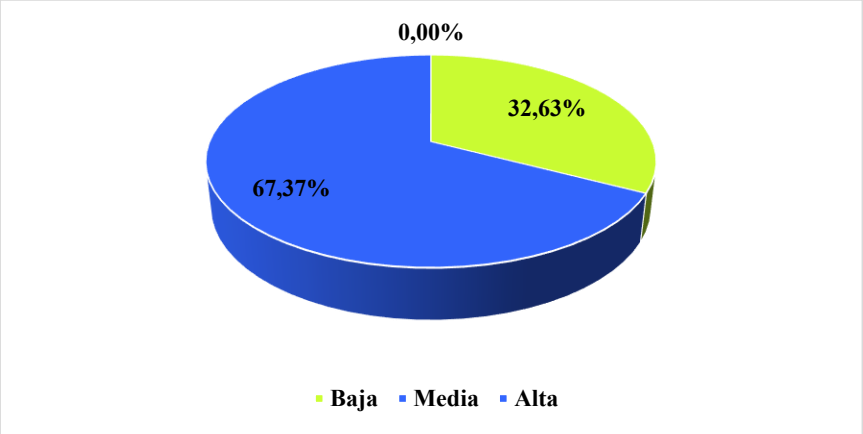
En el cuadro 16 y figura 8 se observa que la disponibilidad de la información, conformado por un 71.32%, califican como media y un 0% considera que es alto la disponibilidad de la información.

Tabla 28 Resultados de la dimensión Integridad

Nivel de Seguridad	Frecuencia	Porcentaje
Baja	124	32.63%
Media	256	67.37%
Alta	0	0.00%
Total	380	100%

FUENTE: Elaboración propia

Figura 9 Resultados de la dimensión Integridad



FUENTE: Elaboración propia

En el cuadro 17 y figura 9 se observa que la integridad de la información, conformado por un 67.37%, califican como media y un 0% considera que es alto la integridad de la información.

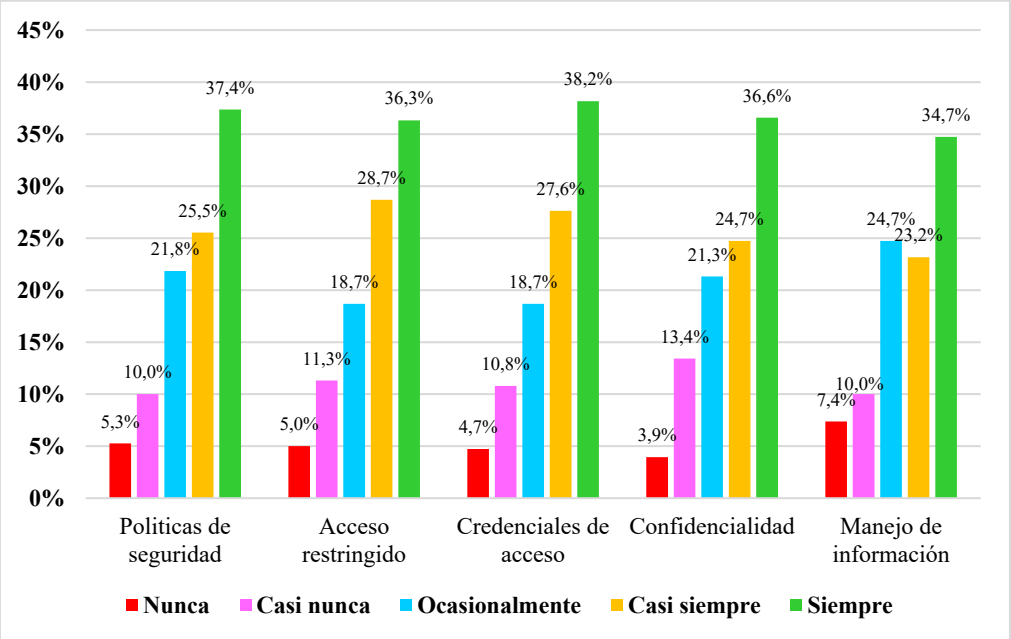
Resultados post test

Tabla 29 Dimensión de Confiabilidad

Escala de Medición	Politicas de seguridad	Acceso restringido	Credenciales de acceso	Confidencialidad	Manejo de información
Nunca	20	19	18	15	28
Casi nunca	38	43	41	51	38
Ocasionalmente	83	71	71	81	94
Casi siempre	97	109	105	94	88
Siempre	142	138	145	139	132
Total general	380	380	380	380	380

ELABORACIÓN: Fuente propia

Figura 10 Grafico de Barras de la dimensión de Confiabilidad



FUENTE: Elaboración propia

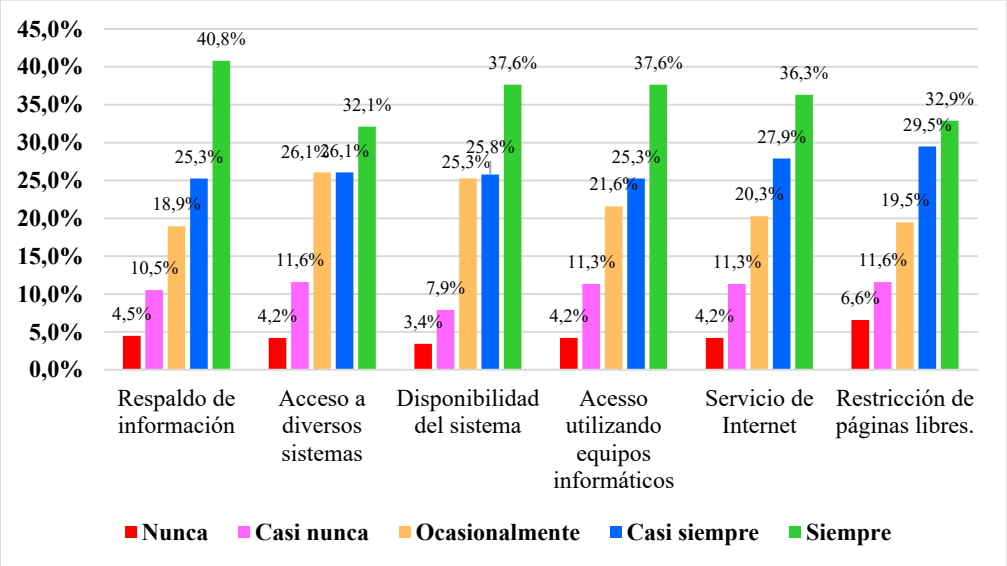
El 36.6% de los postulantes desconoce el tratamiento que le puedan dar a su información que deja al momento de su inscripción y solo el 3.9% tiene conocimiento sobre la confidencialidad de sus datos.

Tabla 30 Dimensión de Disponibilidad

Escala de Medición	Respaldo de información	Acceso a diversos sistemas	Disponibilidad del sistema	Acceso utilizando equipos informáticos	Servicio de Internet	Restricción de páginas libres.
Nunca	17	16	13	16	16	25
Casi nunca	40	44	30	43	43	44
Ocasionalmente	72	99	96	82	77	74
Casi siempre	96	99	98	96	106	112
Siempre	155	122	143	143	138	125
Total general	380	380	380	380	380	380

FUENTE: Elaboración propia

Figura 11 Grafico de barras de la dimensión de Disponibilidad



FUENTE: Elaboración propia

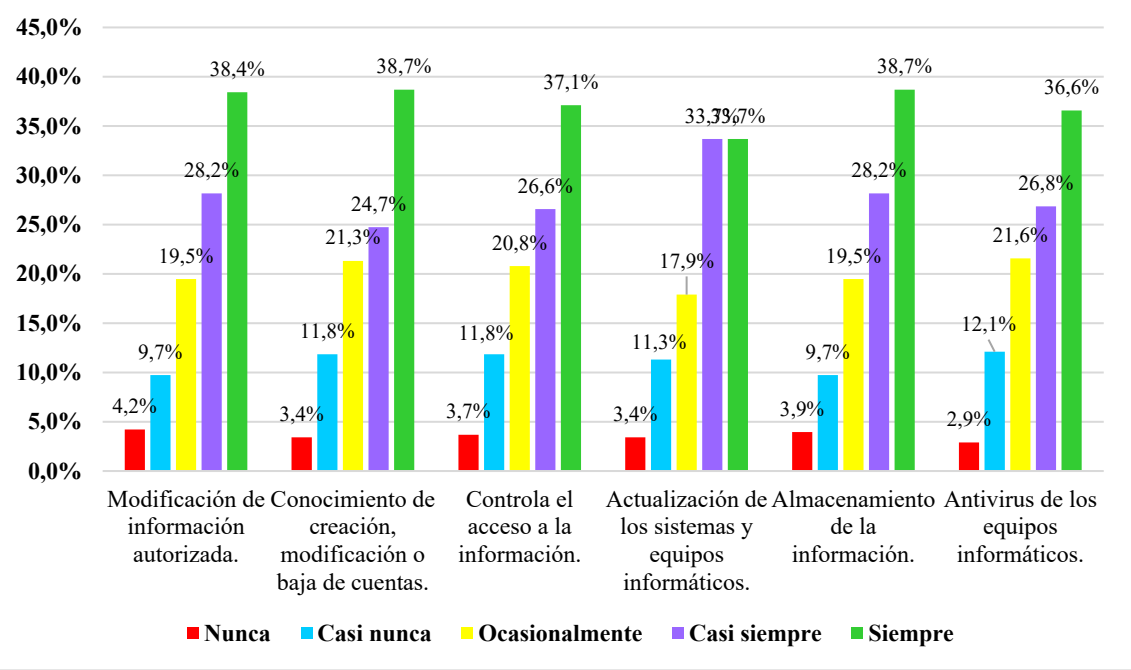
El 37.6% de los postulantes utilizan los equipos informáticos de la Oficina General de Admisión para realizar su inscripción a los exámenes de admisión y un 4.2% realiza su inscripción de manera virtual.

Tabla 31 Dimensión de Integridad

Escala de Medición	Modificación de información autorizada	Conocimiento de creación, modificación o baja de cuentas	Controla el acceso a la información	Actualización de los sistemas y equipos informáticos	Almacenamiento de la información.	Antivirus de los equipos informáticos
Nunca	16	13	14	13	15	11
Casi nunca	37	45	45	43	37	46
Ocasionalmente	74	81	79	68	74	82
Casi siempre	107	94	101	128	107	102
Siempre	146	147	141	128	147	139
Total general	380	380	380	380	380	380

ELABORACIÓN: Fuente propia

Figura 12 Grafico de Barras de la dimensión de Integridad



ELABORACIÓN: Fuente propia

El 38.7% del postulante desconoce donde se almacenan sus datos que dejan en su inscripción mientras que solo el 3.9% de los postulantes tiene conocimiento del lugar donde se almacenara su información.

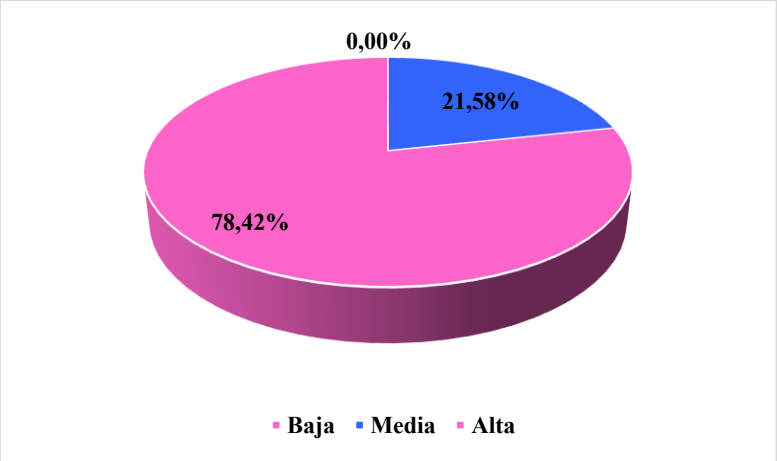
Respecto al nivel de seguridad se obtuvieron los siguientes resultados:

Tabla 32 Resultados de la dimensión Confidencialidad

Nivel de Seguridad	Frecuencia	Porcentaje
Baja	0	0.00%
Media	82	21.58%
Alta	298	78.42%
Total	380	100%

FUENTE: Elaboración propia

Figura 13 Resultados de la dimensión Confidencialidad



FUENTE: Elaboración propia

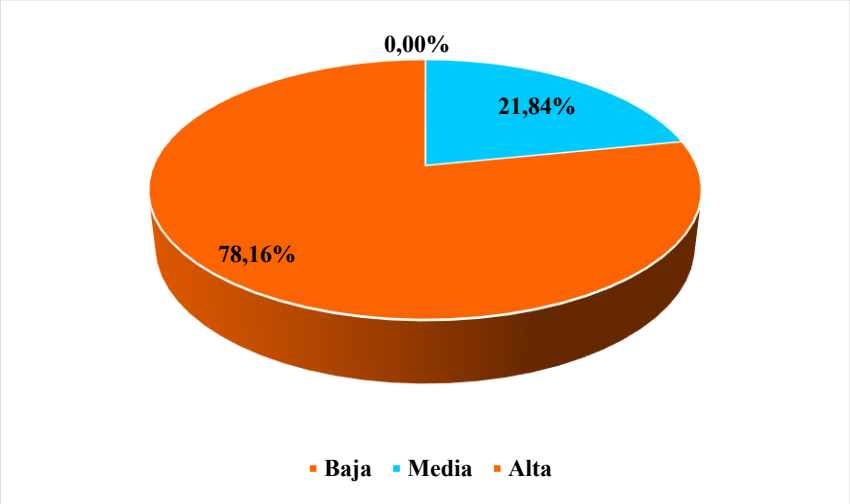
En el cuadro 21 y figura 13 se observa que la confiabilidad de la información, conformado por un 78.42%, califican como alta y un 21.58% considera que es media la confiabilidad de la información.

Tabla 33 Resultados de la dimensión Disponibilidad

Nivel de Seguridad	Frecuencia	Porcentaje
Baja	0	0.00%
Media	83	21.84%
Alta	297	78.16%
Total	380	100%

FUENTE: Elaboración propia

Figura 14 Resultados de la dimensión Disponibilidad



FUENTE: Elaboración propia

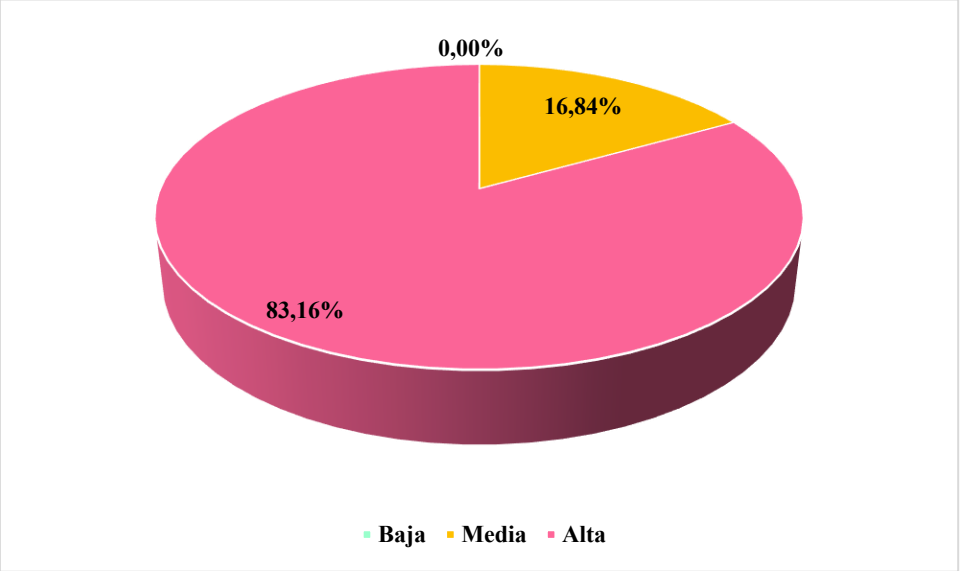
En el cuadro 22 y figura 14 se observa que la disponibilidad de la información, conformado por un 78.16%, califican como alta y un 21.84% considera que es media la disponibilidad de la información.

Tabla 34 Resultados de la dimensión Integridad

Nivel de Seguridad	Frecuencia	Porcentaje
Baja	0	0.00%
Media	64	16.84%
Alta	316	83.16%
Total	380	100%

FUENTE: Elaboración propia

Figura 15 Resultados de la dimensión Integridad



FUENTE: Elaboración propia

En el cuadro 23 y figura 15 se observa que la integridad de la información, conformado por un 83.16%, califican como alta y un 16.84% considera que es media la integridad de la información.

Análisis Inferencial

Para la contrastación de hipótesis planteada en la presente investigación, se recolectó información pre test y post test. A continuación, se mostrará el análisis descriptivo respecto a la gestión de seguridad de la infraestructura de las tecnologías digitales antes y después de implementar el modelo basado en la norma técnica peruana 17799.

Tabla 35 Análisis descriptivo de la gestión de seguridad de la infraestructura de las tecnologías digitales antes y después de implementar el modelo basado en la norma técnica peruana 17799.

Descriptivos			Estadístico	Error estándar
Pre-Test	Media		34,15	,226
	95% de intervalo de confianza para la media	Límite inferior	33,71	
		Límite superior	34,59	
	Media recortada al 5%		34,14	
	Mediana		34,00	
	Varianza		19,378	
	Desviación estándar		4,402	
	Mínimo		21	
	Máximo		48	
	Rango		27	
	Rango intercuartil		6	
	Asimetría		,061	,125
	Curtosis		-,069	,250
Post-Test	Media		68,66	,324
	95% de intervalo de confianza para la media	Límite inferior	68,03	
		Límite superior	69,30	
	Media recortada al 5%		68,77	
	Mediana		69,00	
	Varianza		39,965	
	Desviación estándar		6,322	
	Mínimo		50	
	Máximo		82	
	Rango		32	
	Rango intercuartil		8	
	Asimetría		-,180	,125
	Curtosis		-,084	,250

De la tabla 24, se observa que existe una diferencia en el pre test y post test; respecto a la gestión de seguridad de la infraestructura de las tecnologías digitales inicialmente se tiene una media de 34,15, a comparación del resultado post test, es decir; después de implementar el modelo basado en la norma técnica peruana 17799 se tiene una media de 68,66; claramente se

observa un incremento lo que nos lleva a la conclusión que el modelo basado en la norma técnica peruana 17799 mejora de manera importante la gestión de seguridad de la infraestructura de las tecnologías digitales.

A partir de ello, dado que nuestra muestra es representativa y superior a 30 registros, se realiza la prueba de normalidad de Kolmogorov Smirnov, con el propositico de evaluar si el pre test y post test respecto a la gestión de seguridad de la infraestructura de las tecnologías digitales tienen un comportamiento paramétrico. El cual plantea como hipótesis nula, lo siguiente:

H0: Los datos tienen un comportamiento paramétrico.

H1: Los datos tienen un comportamiento no paramétrico.

Tabla 36 Prueba estadística de normalidad de los datos.

	Estadístico	Grados de Libertad	Significancia
Gestión de seguridad – Pre Test	0.076	380	0.000
Gestión de seguridad – Post Test	0.056	380	0.007

De la tabla 25, se puede comprobar que la significación del pre test tiene un valor de 0.000, siendo menor al nivel de significancia al 5%, por lo que rechazamos la hipótesis nula, por lo que concluimos que los datos del pre test respecto a la gestión de seguridad tienen un comportamiento no paramétrico. Asimismo, la significación del post test tiene un valor de 0.007, siendo menor al nivel de significancia al 5%, por lo que rechazamos la hipótesis nula de que no hay diferencia significativa por lo que concluimos que los datos del post test respecto a la gestión de seguridad tienen un comportamiento no paramétrico.

Por consecuente, se contrastará la hipótesis mediante la prueba no paramétrica de los rangos con signo de Wilcoxon, se procederá con el análisis para saber si el modelo ha causado mejoras en la gestión de seguridad.

H_0: La gestión de la seguridad de la infraestructura de las tecnologías digitales de la Oficina General de Admisión no mejora con el modelo basado en la norma técnica peruana 17799.

H_1: La gestión de la seguridad de la infraestructura de las tecnologías digitales de la Oficina General de Admisión mejora de manera importante con el modelo basado en la norma técnica peruana 17799.

Tabla 37 Prueba estadística de rangos con signo de Wilcoxon para muestras relacionadas.

	Estadístico de prueba	Error estándar	Estadístico de prueba Estandarizado	Significancia
Gestión de seguridad Pre Test y Post Test	72390.00	2142.191	16.896	0.000

De la tabla, se tiene una significancia de 0.000, siendo menor al nivel de significancia al 5%, rechazamos la hipótesis nula, por lo que estadísticamente podemos concluir que la implementación del modelo basado en la norma técnica peruana 17799 mejora de manera importante y significativa la gestión de la seguridad de la infraestructura de las tecnologías digitales de la Oficina General de Admisión en la universidad nacional Santiago Antúnez de Mayolo.

Prueba de Hipótesis Especifica 1

H0: El modelo basado en la norma técnica peruana 17799 no reduce las alertas en la gestión de seguridad de la infraestructura de las TD de la OGAD.

H1: El modelo basado en la norma técnica peruana 17799 reduce las alertas en la gestión de seguridad de la infraestructura de las TD de la OGAD.

Tabla 38 Prueba estadística de rangos con signo de Wilcoxon para muestras relacionadas.

	Estadístico de prueba (Z)	Significancia
Confidencialidad Pre Test y Post Test	-16,893	0.000

De la tabla 38, se tiene una significancia de 0.000, siendo menor al nivel de significancia al 5%, rechazamos la hipótesis nula, por lo que estadísticamente podemos concluir que la implementación del modelo basado en la norma técnica peruana 17799 reduce las alertas en la gestión de seguridad de la infraestructura de las tecnologías digitales de la Oficina General de Admisión en la universidad nacional Santiago Antúnez de Mayolo.

Prueba de Hipótesis Especifica 2

H0: El modelo basado en la norma técnica peruana 17799 no limita los ataques en la gestión de seguridad de la infraestructura de las TD de la OGAD.

H1: El modelo basado en la norma técnica peruana 17799 limita los ataques en la gestión de seguridad de la infraestructura de las TD de la OGAD.

Tabla 39 Prueba estadística de rangos con signo de Wilcoxon para muestras relacionadas.

	Estadístico de prueba (Z)	Significancia
Disponibilidad Pre Test y Post Test	-16,907	0.000

De la tabla 39, se tiene una significancia de 0.000, siendo menor al nivel de significancia al 5%, rechazamos la hipótesis nula, por lo que estadísticamente podemos concluir que la implementación del modelo basado en la norma técnica peruana 17799 limita los ataques en la gestión de seguridad de la infraestructura de las tecnologías digitales de la Oficina General de Admisión en la universidad nacional Santiago Antúnez de Mayolo.

Prueba de Hipótesis Especifica 3

H0: El modelo basado en la norma técnica peruana 17799 no minimiza las vulnerabilidades que intervienen en la gestión de seguridad de la infraestructura de las TD de la OGAD.

H1: El modelo basado en la norma técnica peruana 17799 minimiza las vulnerabilidades que intervienen en la gestión de seguridad de la infraestructura de las TD de la OGAD.

Tabla 40 Prueba estadística de rangos con signo de Wilcoxon para muestras relacionadas.

	Estadístico de prueba (Z)	Significancia
Integridad Pre Test y Post Test	-16,841	0.000

De la tabla 40, se tiene una significancia de 0.000, siendo menor al nivel de significancia al 5%, rechazamos la hipótesis nula, por lo que estadísticamente podemos concluir que la implementación del modelo basado en la norma técnica peruana 17799 minimiza las vulnerabilidades que intervienen en la gestión de seguridad de la infraestructura de las tecnologías digitales de la Oficina General de Admisión en la universidad nacional Santiago Antúnez de Mayolo.

4.3. Discusión de resultados

Con relación a nuestro objetivo general: Mejorar la gestión de seguridad de la infraestructura de las tecnologías digitales, mediante un modelo basado en la norma técnica peruana 17799 de la Oficina General de Admisión de la Universidad Nacional Santiago Antúnez De Mayolo, se obtuvo como resultado la implementación del modelo basado en la norma técnica peruana 17799 mejora de manera importante y significativa la gestión de la seguridad de la infraestructura de las tecnologías digitales de la Oficina General de Admisión en la universidad nacional Santiago Antúnez de Mayolo, esto fue verificado con un valor de 0.007, siendo menor al nivel de significancia al 5%, lo manifestado tiene una relación con lo que indica (Guerra, Neira, Díaz, & Patiño, 2021) donde se encontró que la inclusión de los formatos de desarrollo de auditoría y control propuestos en los indicadores de calidad permite optimizar el sistema de gestión de seguridad de la información (SGSI), los resultados optenidos en la investigación tiene relación con (Marlon Altamirano, 2019) que a través de una encuesta aplicada a directivos y especialistas de la Universidad Estatal Península de Santa Elena, la cual tuvo como objetivo evaluar los factores que contribuyen a aumentar la efectividad de la gestión de la seguridad de la información y a disminuir la complejidad de

la gestión de la seguridad informática se constató el efecto positivo que tiene la automatización y la gestión integrada de los controles, a la vez que se reconoce la importancia de medir la eficacia del sistema, de manera que se pueda corregir a tiempo y disminuir los riesgos de la información, en cuanto al aspecto teorico, los resultados obtenidos se fortalece con la teoria de MAGERIT (2012), donde nos indica que dicha metodología es "utilizada para analizar los riesgos derivados del uso de las tecnologías de la Información y comunicaciones para así implementar medidas de control adecuadas que permitan tener riesgos controlados." Por lo que esta metodología, permite conocer el estado actual de una organización en relación a los riesgos al que están expuestos los activos de información y poder tomar decisiones de seguridad para contrarrestarlos.

En base a los resultados obtenidos, antecedentes y marco teórico se puede indicar que si se implementa el modelo basado en la norma técnica peruana 17799 mejoraría la gestión de seguridad de la información.

V. CONCLUSIONES

1. El modelo, basado en la norma técnica peruana 17799, mejora la gestión de seguridad de la infraestructura de tecnologías digitales de la oficina general de admisión de la universidad nacional Santiago Antúnez de Mayolo – Huaraz, lo cual se contrasto con la aplicación de la prueba de normalidad de Kolmogorov Smirnov obteniendo el resultado de 0.007, siendo menor al nivel de significancia al 5%.
2. El nivel de seguridad de la información en la oficina general de admisión de la UNASAM, fue calificada en la dimensión de confiabilidad como media con un 70%, mientras que con el post test se consideró alto con un 78.42%.
3. El nivel de seguridad de la información en la oficina general de admisión de la UNASAM, fue calificada en la dimensión de disponibilidad como media con un 71.32%, mientras que con el post test se consideró alto con un 78.16%.
4. El nivel de seguridad de la información en la oficina general de admisión de la UNASAM, fue calificada en la dimensión de integridad como media con un 67.37%, mientras que con el post test se consideró alto con un 85.16%.
5. Se realizo el modelo basado en la norma técnica peruana 17799 de acuerdo a las necesidades de la Oficina General de Admisión de la UNASAM, estructurando y priorizando la seguridad de los activos más sensibles del área.

VI. RECOMENDACIONES

1. Se recomienda actualizar todos los recursos informáticos de la Oficina General de Admisión para mejorar el procesamiento del proceso de inscripción de los postulantes al examen de admisión.

2. Se recomienda generar y guardar en un ordenador o disco duro externo los backups de los sistemas de información que utiliza la Oficina General de Admisión.

3. El personal que labora en la Oficina General de Admisión debe de estar en constante capacitación sobre los recursos tecnológicos debido a que se maneja información sensible.

4. La autoridad de la Oficina General de Admisión debe de promover y concientizar sobre las políticas de Seguridad de la Información a todo el personal que labora en dicha área.

5. Crear un área específica donde se manejará y almacenará los activos físicos y digitales más importantes de la Oficina General de Admisión.

VII. REFERENCIAS BIBLIOGRAFICAS

Aguirre Abanto, M. A., & Lopez Ynostroza, G. A. (2018). Implementación de una guía referencial para gestionar los riesgos informáticos en la Universidad Autónoma del Perú. *Tesis Grado*. Universidad Autónoma del Perú, Lima, Perú.

Areitio Bertolín, J. (2008). Seguridad de la información. Redes, informática y sistemas de información. Madrid: Ediciones paraninfo.

Asencios Carbajal, H. C. (2017). Guía metodológica de sistema de gestión de seguridad de la información basada en la NTP-ISO/IEC 17799, 27001 y COBIT 5 para minimizar los riesgos de gestión de la información en el poder judicial de Carhuaz, 2014. *Tesis Post Grado*. Universidad Nacional Santiago Antúnez de Mayolo, Huaraz, Perú.

Brito Rodríguez, R. E. (2020). Gestión de incidentes de seguridad de la información en la facultad de Ciencias de la universidad nacional Santiago Antúnez de Mayolo, 2017. *Tesis de Grado*. Universidad Nacional Santiago Antúnez de Mayolo, Huaraz, Perú.

Calisaya Sana, C. Y., & Tarrillo Villegas, M. (2018). Implementación de controles de seguridad para la protección de datos personales en una Universidad Privada para el cumplimiento parcial de la Ley 29733 basado en los controles de seguridad de la NTP-ISO/IEC 17799:2007. *Tesis Grado*. Universidad Peruana Unión, Lima, Perú.

Cappellozza, A., Salati Marcondes de Moraes, G. H., Perez, G., & Lourenço Simões, A. (2022). Antecedent factors of violation of information security rules. *Articulo Cientifico*. Universidade de São Paulo, São Paulo, Brasil.

Carrión Apéstegui, S. G. (2015). Diagnóstico y propuesta de mejora para la gestión de riesgos basado en la ISO/IEC 27002:2008 para la oficina general de estudios UNASAM - Huaraz 2014. *Tesis de Grado*. Universidad Nacional Santiago Antúnez de Mayolo, Huaraz, Perú.

conexiónesan. (01 de 08 de 2022). Obtenido de conexiónesan: https://www.esan.edu.pe/conexion-esan/norma-tecnica-peruana-politicas-procedimientos-seguridad-informacion#:~:text=La%20NTP%2DISO%2017799%20es,de%20su%20tama%C3%B1o%20o%20sector.

EALDE. (01 de 08 de 2022). Obtenido de EALDE: https://www.ealde.es/iso-27001-para-que-sirve/#:~:text=La%20norma%20ISO%2027001%20es,sus%20bienes%20de%20informaci%C3%B3n%20seguros.

Encuestas probabilísticas vs. no probabilísticas. (2000). En R. P. Lastra, *Encuestas probabilísticas vs. no probabilísticas* (pág. 3). Universidad Autónoma Metropolitana Unidad Xochimilco.

Escrivá, G. G., Romero, S. R., Ramada, D. J., & Onrubio, P. R. (2015). Seguridad Informatica. España: Macmillan Profesional., España.

Gabriel Baca, U. (2016). Introducción a la Seguridad Informática. *Libro*. Mexico: Grupo Editorial Patria.

Guardia Tamara, R. V. (2020). Diseño de un modelo de seguridad de la información para minimizar los riesgos informáticos en la gestión académica del Instituto de Educacion Superior Tecnologico Publico Eleazar Guzman Barron – Huaraz – 2018. *Tesis de Maestria*. Universidad Nacional Santiago Antúnez de Mayolo, Huaraz, Perú.

Guerra, E., Neira, H., Díaz, J., & Patiño, J. (10 de 2021). Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias. *Articulo*. Universidad de la costa, Barranquilla - Colombia, Colombia.

Hernández Mechate, E. J. (2020). Vulnerabilidades informáticas en el portal web de la Universidad Andina del Cusco. *Tesis de Grado*. Universidad Andina del Cusco, Cusco, Perú.

IBM. (14 de 04 de 2021). *Política y objetivos de seguridad*. Obtenido de https://www.ibm.com/docs/es/i/7.5?topic=ssw_ibm_i_75/rzaj4/rzaj40j0securitypolco.htm

ISO. (01 de 08 de 2022). *ISO*. Obtenido de ISO: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

ISOTools Excellence. (01 de 04 de 2015). Obtenido de ISOTools Excellence: https://www.pmg-ssi.com/2015/04/isoiec-17799-politica-de-seguridad/

Machín, N., & Gazapo, M. (2016). LA CIBERSEGURIDAD COMO FACTOR CRÍTICO EN LA SEGURIDAD DE LA UNIÓN EUROPEA. *Revista UNISCI*. Universidad Complutense de Madrid, España.

Marlon Altamirano, D. (2019). Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso. *Articulo Cientifico*. Instituto de Información Científica y Tecnológica, Cuba.

Merino Rosas, C. A. (2021). Implementación de un plan de seguridad informática con la norma ISO/IEC 27001 en la empresa RANSA Comercial S.A. - Piura; 2021. *Tesis de Grado*. Universidad Católica los Ángeles de Chimbote, Piura, Perú.

Olivos Guerra, F., & Guevara Saldaña, E. W. (2017). Formulación de políticas de control de accesos y seguridad física y del entorno basado en la norma técnica peruana NTP-ISO/IEC 17799 para la mejora de la gestión en la oficina central de cómputo – Universidad de Lambayeque. *Tesis de Grado*. Universidad de Lambayeque, Chiclayo, Perú.

Ortiz Aristizabal, A. (2021). ANÁLISIS DE RIESGOS BASADO EN LA NORMA MAGERIT V3 DE LA RED WLAN DE LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR DEL TOLIMA. Colombia.

Pazmiño Flores, C. D., & Contero Ramos, W. M. (2019). Diseño de una política de seguridad de la información basada en la norma ISO 27002:2013, para el sistema de botones de seguridad del Ministerio del Interior. *Tesis Post Grado*. Universidad Internacional SEK, Quito, Ecuador.

Peruano, E. (08 de 01 de 2016). *Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Siste*, pág. 575410.

Poma, A., & Vargas, R. (2019). Problemática en Ciberseguridad como protección de sistemas informáticos y redes sociales en el Perú y en el Mundo. *Articulo*. Sciendo, Perú.

PUBLICAS, M. D. (20 de 05 de 2006). *Metodología de Análisis y Gestión de Riesgos (CATALOGO DE ELEMENTOS - MAGERIT)*. Obtenido de https://www.pilar-tools.com/doc/magerit/v2/cat-es-v11.pdf

Purificación Aguilar, L. (2010). Seguridad Informática. *Libro*. Editex.

Romero Galicia, J. (2018). CONCEPTUALIZACIÓN DE UNA ESTRATEGIA DE CIBERSEGURIDAD PARA LA SEGURIDAD NACIONAL DE MÉXICO. *Articulo Cientifico*. Secretaría de Gobernación, México, Mexico, Mexico.

VIII. ANEXOS

MATRIZ DE CONSISTENCIA DE LA INVESTIGACIÓN:

Tabla 41 Matriz de consistencia del proyecto de investigación

Problema	Objetivos	Hipótesis	Variables	Metodología
General			**Variable Dependiente:** Gestión de seguridad de la infraestructura de las TD**.** **Dimensiones:** Confidencialidad **integridad disponibilidad**	**TIPO DE INVESTIGACIÓN:** Según el enfoque es cuantitativo con nivel de investigación correlacional - corte transversal. **DISEÑO DE LA INVESTIGACIÓN:** Corresponde al diseño Cuasi - experimental. **POBLACIÓN** La población estará determinada por el promedio de los 3 últimos procesos de admisión de la Universidad Nacional Santiago Antúnez de Mayolo, que hacen uso y que confían la seguridad de sus datos almacenados o procesados mediante la infraestructura digital de la Oficina General de Admisión
¿En qué medida mejora el Modelo basado en la norma técnica peruana 17799 con la gestión de seguridad de la infraestructura de las tecnologías de digitales de la Oficina General de Admisión?	Mejorar la gestión de seguridad de la infraestructura de las tecnologías de digitales, mediante un modelo basado en la norma técnica peruana 17799 de la Oficina General de Admisión.	El modelo basado en la norma técnica peruana 17799 mejora la gestión de seguridad de la infraestructura de las tecnologías de digitales de la Oficina General de Admisión.		
Específico				
P1: ¿Al reducir las alertas mejorará la gestión de seguridad de la infraestructura de las TD de la OGAD?	**O1:** Reducir las alertas que influyen en la gestión de seguridad de la infraestructura de las TD de la OGAD.	**H1:** El modelo basado en la norma técnica peruana 17799 reduce las alertas en la gestión de seguridad de la infraestructura de las TD de la OGAD.	**Variable Independiente:** Modelo basado en la norma técnica peruana 17799. **Dimensiones:** Autoevaluación	
P2: ¿Limitar los ataques mejorará la gestión de seguridad de la infraestructura de las TD de la OGAD?	**O2:** Limitar los ataques en la gestión de seguridad de la infraestructura de las TD de la OGAD.	**H2:** El modelo basado en la norma técnica peruana 17799 limita los ataques en la gestión de seguridad de la infraestructura de las TD de la OGAD.		
P3: ¿Minimizar las vulnerabilidades mejorará la gestión de seguridad de la infraestructura de las TD de la OGAD?	**O3:** Minimizar las vulnerabilidades que intervienen en la gestión de seguridad de la infraestructura de las TD de la OGAD.	**H3:** El modelo basado en la norma técnica peruana 17799 minimiza las vulnerabilidades que intervienen en la gestión de seguridad de la infraestructura de las TD de la OGAD.		

“INSTRUMENTO DE RECOLECCION DE DATOS”

UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO

Escuela profesional de ingeniería de sistemas e informática

ENCUESTA PARA MEDIR EL NIVEL DE SEGURIDAD DE LA INFORMACIÓN EN LA OFICINA GENERAL DE ADMISIÓN – HUARAZ.

Objetivo: Recopilar información sobre el nivel de seguridad de la información en la oficina general de admisión de la UNASAM-Huaraz, Por favor se solicita su participación y apoyo a responder el siguiente cuestionario, dirigido a los postulantes del proceso de admisión.

Instrucciones: Marque con una “X” en el recuadro correspondiente de acuerdo a su percepción en cada una de las preguntas, cuya escala de apreciación es el siguiente:

Nunca	Casi nunca	Ocasionalmente	Casi siempre	Siempre
1	2	3	4	5

Dimensiones	Ítems	Nunca	Casi nunca	Ocasionalmente	Casi siempre	Siempre
CONFIDENCIALIDAD	Se le informó al postulante sobre las políticas de seguridad de la información de la Oficina General de Admisión.	1	2	3	4	5
	El postulante tiene acceso restringido a los sistemas e instalaciones que alojen información que no sea relevante para sus funciones.	1	2	3	4	5
	El postulante comparte sus credenciales de acceso a la plataforma de admisión con sus compañeros.	1	2	3	4	5
	El postulante firma algún documento de confidencialidad sobre el manejo de su información personal.	1	2	3	4	5
	Ítems	**Nunca**	**Casi nunca**	**Ocasionalmente**	**Casi siempre**	**Siempre**

	El postulante maneja cuidadosamente la información personal considerada privada/confidencial durante el proceso de inscripción.	1	2	3	4	5
DISPONIBILIDAD	Al postulante se le brinda respaldo de información física o digital (ficha de inscripción) ante cualquier falla del sistema o inconveniente con el documento.	1	2	3	4	5
	El postulante accede a los diversos sistemas haciendo uso de su credencial de acceso (usuario y contraseña) por ejemplo, al sistema web de ingresantes, sistema de calificación, etc.	1	2	3	4	5
	Los sistemas y equipos informáticos utilizados por el postulante en el proceso de inscripción (presencial) están disponibles para su uso incluso ante un corte de fluido eléctrico.	1	2	3	4	5
	Los equipos informáticos utilizados por el postulante le permiten acceder a los diversos sistemas y repositorios de información necesarios para su inscripción, sin presentar inconvenientes.	1	2	3	4	5
	El servicio de Internet que tiene la Oficina General de Admisión, le permite acceder a los diversos sistemas web necesarios para el proceso de inscripción del postulante.	1	2	3	4	5
	El servicio de Internet que tiene la Oficina General de Admisión, le restringe el acceso libre a las diversas páginas que no son relevantes para la inscripción del postulante.	1	2	3	4	5
	Ítems	**Nunca**	**Casi nunca**	**Ocasionalmente**	**Casi siempre**	**Siempre**
INTEGRIDAD	Toda modificación de la información del postulante es autorizada por el área o jefatura correspondiente. (por ejemplo, cambio de carrera o modalidad a la que se inscribió el postulante)	1	2	3	4	5

	Conoce algún tipo de procedimiento para la creación, modificación o baja de las cuentas de usuario de la plataforma de inscripción.	1	2	3	4	5
	La Oficina General de Admisión controla y restringe el acceso de personas no autorizadas a las instalaciones o sistemas que alojen información (física/digital) considerada de importancia para el desarrollo de su inscripción.	1	2	3	4	5
	Los sistemas y equipos informáticos utilizados en el desarrollo de su inscripción son actualizados constantemente.	1	2	3	4	5
	El área encargada del proceso de inscripción, almacena la información generada luego de ser realizado la inscripción (ficha de inscripción) en repositorios adecuados que le aseguren que la información está protegida.	1	2	3	4	5
	Los equipos informáticos utilizados por el postulante en el proceso de inscripción cuentan con antivirus instalado.	1	2	3	4	5

UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS E INFORMÁTICA

Huaraz 03 de noviembre del 2022

SEÑOR: Ing. Joseph Darwin Alvarado Tolentino

Yo, Andy Junior Bonilla Rivera, identificado con DNI N° 70137923, Bachiller en Ingeniería de Sistemas e Informática, me dirijo a usted con la finalidad de solicitar su valiosa colaboración en la validación de contenido de los ítems que conforman el instrumento de recolección de datos que utilizaré para recabar la información requerida en la investigación titulada "MODELO BASADO EN LA NORMA TECNICA PERUANA 17799 PARA MEJORAR LA GESTION DE SEGURIDAD DE LA INFRAESTRUCTURA DE TECNOLOGIAS DIGITALES DE LA OFICINA GENERAL DE ADMISIÓN DE LA UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO". Por lo cual, facilito la documentación pertinente:

1. Matriz de Operacionalización de Variables.
2. Matriz de Consistencia
3. Instrumento de Recolección de Datos.

Por su experiencia profesional y méritos académicos me permito para la validación de dicho instrumento.

Agradezco de antemano su valioso aporte.

Atentamente

Andy Junior Bonilla Rivera
DNI N°: 70137923

1. Matriz de operacionalización de Variables:

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES
Variable Dependiente: Gestión de seguridad de la infraestructura de las TD	Gestión de la seguridad: Proceso de establecer y mantener la seguridad de un ordenador o sistema de red **(ISACA, 2015,p.60)** Las TIC: Conjunto de servicios telemáticos, redes, software y dispositivos de hardware que se integran en sistemas de información interconectadas y complementarias cuyo fin es la de gestionar datos, información y procesos **(CONCYTEC, 2016, p.8)** La infraestructura: Capacidad informática y de procesamiento, conexión de red y dispositivos conectados **(HUAWEI,2018,p.8)**	A partir de la definición conceptual en la realidad de la UNASAM, específicamente en la OGAD, se observará y evaluará las bases de datos para identificar y registrar la existencia de las dimensiones e indicadores.	Confidencialidad Integridad	Presencia
			Disponibilidad	Presencia
Variable Independiente: Modelo basado en la norma	Instrumento predictivo, cuya función es predecir las interacciones como variable y dar soporte de los sistemas para que desde esta perspectiva el profesional observador pueda describir el	Al finalizar el modelo basado en la norma técnica peruana 17799, se registrarán los datos obtenidos para realizar	Autoevaluación	Alertas
				Ataques

técnica peruana 17799	comportamiento de los sistemas de la institución a lo largo del tiempo **(Matthew & Zheng, 2017)**.	una evaluación objetiva de los resultados.	Vulnerabilidades

2. Matriz de Consistencia:

Problema	Objetivos	Hipótesis	Variables	Metodología
General			**Variable Dependiente:** Gestión de seguridad de la infraestructura de las TD. **Dimensiones:** Confidencialidad **integridad disponibilidad**	**TIPO DE INVESTIGACIÓN:** Según el enfoque es cuantitativo con nivel de investigación correlacional - corte transversal. **DISEÑO DE LA INVESTIGACIÓN:** Corresponde al diseño Cuasi - experimental. **POBLACIÓN** La población estará determinada por el promedio de los 3 últimos procesos de admisión de la Universidad Nacional Santiago Antúnez de Mayolo, que hacen uso y que confían la seguridad de sus datos almacenados o procesados mediante la infraestructura digital de la Oficina General de Admisión
¿En qué medida mejora el Modelo basado en la norma técnica peruana 17799 con la gestión de seguridad de la infraestructura de las tecnologías de digitales de la Oficina General de Admisión?	Mejorar la gestión de seguridad de la infraestructura de las tecnologías de digitales, mediante un modelo basado en la norma técnica peruana 17799 de la Oficina General de Admisión.	El modelo basado en la norma técnica peruana 17799 mejora la gestión de seguridad de la infraestructura de las tecnologías de digitales de la Oficina General de Admisión.		
Específico				
P1: ¿Al reducir las alertas mejorará la gestión de seguridad de la infraestructura de las TD de la OGAD?	**O1:** Reducir las alertas que influyen en la gestión de seguridad de la infraestructura de las TD de la OGAD.	**H1:** El modelo basado en la norma técnica peruana 17799 reduce las alertas en la gestión de seguridad de la infraestructura de las TD de la OGAD.	**Variable Independiente:** Modelo basado en la norma técnica peruana 17799. **Dimensiones:** Autoevaluación	
P2: ¿Limitar los ataques mejorará la gestión de seguridad de la infraestructura de las TD de la OGAD?	**O2:** Limitar los ataques en la gestión de seguridad de la infraestructura de las TD de la OGAD.	**H2:** El modelo basado en la norma técnica peruana 17799 limita los ataques en la gestión de seguridad de la infraestructura de las TD de la OGAD.		
P3: ¿Minimizar las vulnerabilidades mejorará la gestión de seguridad de la infraestructura de las TD de la OGAD?	**O3:** Minimizar las vulnerabilidades que intervienen en la gestión de seguridad de la infraestructura de las TD de la OGAD.	**H3:** El modelo basado en la norma técnica peruana 17799 minimiza las vulnerabilidades que intervienen en la gestión de seguridad de la infraestructura de las TD de la OGAD.		

3. Instrumento de Recolección de Datos

"INSTRUMENTO DE RECOLECCION DE DATOS"

UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO

Escuela profesional de ingeniería de sistemas e informática

ENCUESTA PARA MEDIR EL NIVEL DE SEGURIDAD DE LA INFORMACIÓN EN LA OFICINA GENERAL DE ADMISIÓN – HUARAZ.

Objetivo: Recopilar información sobre el nivel de seguridad de la información en la oficina general de admisión de la UNASAM-Huaraz, Por favor se solicita su participación y apoyo a responder el siguiente cuestionario, dirigido a los postulantes del proceso de admisión.

Instrucciones: Marque con una "X" en el recuadro correspondiente de acuerdo a su percepción en cada una de las preguntas, cuya escala de apreciación es el siguiente:

Nunca	Casi nunca	Ocasionalmente	Casi siempre	Siempre
1	2	3	4	5

Dimensiones	Ítems	Nunca	Casi nunca	Ocasionalmente	Casi siempre	Siempre
CONFIDENCIALIDAD	Se le informó al postulante sobre las políticas de seguridad de la información de la Oficina General de Admisión.	1	2	3	4	5
	El postulante tiene acceso restringido a los sistemas e instalaciones que alojen información que no sea relevante para sus funciones.	1	2	3	4	5
	El postulante comparte sus credenciales de acceso a la plataforma de admisión con sus compañeros.	1	2	3	4	5
	El postulante firma algún documento de confidencialidad sobre el manejo de su información personal.	1	2	3	4	5

	Ítems	Nunca	Casi nunca	Ocasionalmente	Casi siempre	Siempre
	El postulante maneja cuidadosamente la información personal considerada privada/confidencial durante el proceso de inscripción.	1	2	3	4	5
DISPONIBILIDAD	Al postulante se le brinda respaldo de información física o digital (ficha de inscripción) ante cualquier falla del sistema o inconveniente con el documento.	1	2	3	4	5
	El postulante accede a los diversos sistemas haciendo uso de su credencial de acceso (usuario y contraseña) por ejemplo, al sistema web de ingresantes, sistema de calificación, etc.	1	2	3	4	5
	Los sistemas y equipos informáticos utilizados por el postulante en el proceso de inscripción (presencial) están disponibles para su uso incluso ante un corte de fluido eléctrico.	1	2	3	4	5
	Los equipos informáticos utilizados por el postulante le permiten acceder a los diversos sistemas y repositorios de información necesarios para su inscripción, sin presentar inconvenientes.	1	2	3	4	5
	El servicio de Internet que tiene la Oficina General de Admisión, le permite acceder a los diversos sistemas web necesarios para el proceso de inscripción del postulante.	1	2	3	4	5
	El servicio de Internet que tiene la Oficina General de Admisión, le restringe el acceso libre a las diversas páginas que no son relevantes para la inscripción del postulante.	1	2	3	4	5

	Ítems	Nunca	Casi nunca	Ocasionalmente	Casi siempre	Siempre
INTEGRIDAD	Toda modificación de la información del postulante es autorizada por el área o jefatura correspondiente. (por ejemplo, cambio de carrera o modalidad a la que se inscribió el postulante)	1	2	3	4	5
	Conoce algún tipo de procedimiento para la creación, modificación o baja de las cuentas de usuario de la plataforma de inscripción.	1	2	3	4	5
	La Oficina General de Admisión controla y restringe el acceso de personas no autorizadas a las instalaciones o sistemas que alojen información (física/digital) considerada de importancia para el desarrollo de su inscripción.	1	2	3	4	5
	Los sistemas y equipos informáticos utilizados en el desarrollo de su inscripción son actualizados constantemente.	1	2	3	4	5
	El área encargada del proceso de inscripción, almacena la información generada luego de ser realizado la inscripción (ficha de inscripción) en repositorios adecuados que le aseguren que la información está protegida.	1	2	3	4	5
	Los equipos informáticos utilizados por el postulante en el proceso de inscripción cuentan con antivirus instalado.	1	2	3	4	5

INFORME DE OPINIÓN DE EXPERTO

I. DATOS DEL EXPERTO

APELLIDOS Y NOMBRES: ALVARADO TOLENTINO JOSEPH DARWIN

PROFESIÓN: INGENIERO DE SISTEMAS E INFORMÁTICA

GRADO ACADÉMICO: MAESTRO EN CIENCIAS E INGENIERÍA

MENCIÓN: AUDITORIA Y SEGURIDAD INFORMÁTICA

CENTRO LABORAL: UNASAM

CARGO: DOCENTE

II. MATRIZ DE EVALUACIÓN DEL INSTRUMENTO DE RECOLECCIÓN DE DATOS

Indicador	Criterio	Deficiente 0 - 20	Regular 21 - 40	Bueno 41 - 60	Muy Bueno 61 - 80	Excelente 81 - 100
Claridad	Está formulado con un lenguaje claro.					X
Objetividad	No presenta sesgo ni induce a respuestas.				X	
Actualidad	Está de acuerdo con los avances de la teoría, ciencia y tecnología.					X
Organización	Existe una organización lógica y coherente de los ítems.				X	
Suficiencia	Comprende las dimensiones de la investigación en cantidad y calidad.					X
Intencionalidad	Adecuado para establecer asociación.				X	
Consistencia	Basado en aspectos teóricos y científicos.					X
Coherencia	Hay relación entre variables, dimensiones e indicadores.					X
Metodología	El instrumento se relaciona con el método planteado en el proyecto.				X	

Huaraz, 03 de noviembre del 2022

Ing. Joseph Darwin Alvarado Tolentino
N° de DNI: 46022813

Clasificación de Niveles de Fiabilidad

Tabla 42 Clasificación de los niveles de fiabilidad según el Alfa de Cronbach.

Índice	Nivel de Fiabilidad	Valor de Alfa de Cronbach
1	Excelente	] 0.9, 1]
2	Muy bueno	] 0.7, 0.9]
3	Bueno	] 0.5, 0.7]
4	Regular	] 0.3, 0.5]
5	Deficiente	[0, 0.3]

Nota: Clasificación de los niveles de fiabilidad. Fuente: elaborado por Tuapanta et al. (2017)

ANALISIS DE FIABILIDAD DEL INSTRUMENTO

Tabla 43 Análisis de fiabilidad de la variable Gestión de seguridad de la infraestructura de las tecnologías digitales.

Variable	Alfa de Cronbach	Número de Elementos
Gestión de seguridad de la infraestructura de las tecnologías digitales.	0.728	17

Nota: Coeficiente de Cronbach.