UNIVERSIDAD NACIONAL

SANTIAGO ANTÚNEZ DE MAYOLO

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE

INGENIERÍA DE SISTEMAS E INFORMÁTICA

POLÍTICAS DE SEGURIDAD Y RIESGOS DE LA INFORMACIÓN EN LA FACULTAD DE CIENCIAS DE LA UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO, HUARAZ-2022

TESIS PARA OPTAR EL TÍTULO DE:

INGENIERO DE SISTEMAS E INFORMÁTICA

PRESENTADO POR:

Bachiller Roger Evelio Sanchez Herrera

ASESOR:

Mag. Elizabeth Gladys Arias Lazarte

HUARAZ-PERU

2022

N° Registro: T174

DEDICATORIA

Mis padres que han estado en todas las etapas de mi vida apoyándome y acompañándome y buscando que sea mejor cada día y nunca será suficiente para compensar todos los esfuerzos y confianza que brindaron a mi persona. Siempre mi amor y gratitud hacia ellos.

Mis hermanos que me apoyaron siempre con sus consejos y cariño, que siempre son un impulso más para lograr mis objetivos.

Mis abuelos que siempre estuvieron presentes en mi vida como unos padres más, brindándome su amor y esperanza. Y a toda mi familia que siempre confío en mi persona y a los que no también.

AGRADECIMIENTOS

Agradecer a mis padres por su apoyo incondicional y por brindarme el sustento necesario para poder alcanzar mis metas y objetivos que tengo en la vida.

Un agradecimiento especial a mis hermanos y abuelos que estuvieron para mi persona, siempre que los he necesitado.

Un agradecimiento especial a los docentes de la UNASAM, que con sus conocimientos y experiencias me guiaron por el camino del aprendizaje y los buenos valores.

RESUMEN

La presente investigación tuvo como objetivo determinar la relación que existe entre políticas de seguridad y riesgos de la información en la Facultad de Ciencias de la UNASAM en el año 2022. La investigación fue de tipo aplicada, el diseño tuvo un enfoque cuantitativo, de diseño no experimental y correlacional, la técnica que se empleará para la recolección de datos fue la encuesta, para la investigación se aplicó dos instrumentos, el primer instrumento enfocado a medir la variable políticas de seguridad y el según instrumento para medir la variable riesgos de la información , cuyos ítems estuvieron basados en el escala de Likert, estudiándose la muestra de 48 empleados (Administrativo y docentes) de la Facultad de Ciencias de la UNASAM. De manera complementaria se analizó la validez como la confiabilidad, mediante Alpha de Cronbach para ambos instrumentos. Se concluyó que las Políticas de Seguridad y Riesgos de la Información tienen una relación inversamente proporcional, debido a que el Rho de Spearman arrojo un valor de (-0.422**) y la significancia p=0.003 (p<5), con la cual se determinó la relación significativa

Palabras clave: Políticas de seguridad, riesgos de la información

ABSTRACT

The objective of this investigation was to determine the relationship that exists between security policies and information risks in the Faculty of Sciences of UNASAM in the year 2022. The research was of an applied type, the design had a quantitative approach, of a non-specific design. experimental and correlational, the technique that will be used for data collection was the survey, for the investigation two instruments were applied, the first instrument focused on measuring the security policy variable and the second instrument to measure the information risk variable, whose elements were based on the Likert scale, studying the sample of 48 employees (Administrative and teachers) of the Faculty of Sciences of UNASAM. In a complementary way, validity and reliability were analyzed using Cronbach's Alpha for both instruments. It was concluded that the Information Security and Risk Policies have an inversely proportional relationship, since Spearman's Rho yielded a value of (-0.422**) and the significance p=0.003 (p<0.05), with which the significant relationship is concluded

Keywords: Security policies, Information risks

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

1.1. Planteamiento del problema

Actualmente, la dependencia de las organizaciones en cuanto al uso de las tecnologías de la información está en aumento, y el valor dependerán de los objetivos organizaciones que se proponen a lograr, pues estas juegan un papel importante en el manejo de la información como el activo más importante para ser competitivos y lograr su continuidad en el mercado actual. Para Alvarado y Acosta, (2018) la accesibilidad en tiempo real a la información dentro de las organizaciones es una ventaja competitiva primordial, para un adecuado uso del recurso que repercuten en la toma de decisiones y la atención a demandas principales.

En un estudio aplicado en Latinoamérica en el año 2022, en la que participaron 539 personas tanto directores, gerentes y analistas de riesgos, gestores de seguridad de la información, auditores, entre otros. En la que se obtuvo que el 43.6 % consideran que el área de gestión de riesgos en la actualidad tiene mucha relevancia en sus empresas, cabe decir que lo consideran como un área principal que contribuye al logro de sus objetivos y a la continuidad de negocio. A pesar de la importancia que esta ganado la gestión de riesgos en las empresas actualmente, aún falta trabajar en la concientización del personal sobre el beneficio que estas representan. Para el 53.8 % la dificultad está en la gestión de riesgos debido a la falta de cultura para gestionar los riesgos, en cuanto al resto consideran que hay poco compromiso por parte de la gerencia y ello repercute en la falta de conocimiento de los trabadores. Solamente el 1.3 % asegura no tener dificultades al gestionar los riesgos (Pirani, 2022)

Según, Noreña, (2018), considera que proteger la seguridad y la estabilidad del país (España), está en la protección de su información, de manera que la información es la clave sobre la cual se debe priorizar en cuando salvaguardar la marca y la imagen

institucional del país se refiere. También que para proteger el país se debe establecer la contrainteligencia como una estrategia para contrarrestar los riesgos y amenazas que ciernen al país. Para Vilca, (2018), las empresas que cuentan con jerarquía deben contar con mecanismos que gestiones los posibles riesgos, para así garantizar la protección y la defensa de los datos, para lo cual se debe cumplir las etapas de PHVA (Planificar, Hacer, Verificar y Actuar).

Para Altamirano, /2017), las Instituciones deben enmarcase hacia un enfoque multifacético agrupando personas, tecnologías y procesos, en la que cuenten con comunidades para la confianza en supervisión y análisis. No solo basta con garantizar la seguridad de la información, sino que también se debe tener en cuenta los aspectos humanos de la seguridad de la información. Es por ese motivo que las amenazas a la seguridad no pueden prevenirse, evitarse, detectarse o eliminarse concentrándose únicamente en soluciones tecnológicas

Las políticas de seguridad de la información son primordiales para los enfoques de muchas organizaciones para reforzar las conductas deseables de seguridad de la información y reforzar las restricciones contra los comportamientos de seguridad no deseables. En cuanto a las universidades tanto nacionales como particulares manejan una gran cantidad de información, con respecto a sus alumnos, docentes, personal administrativo, cursos; por esta razón es necesario aplicar una Política para la gestión adecuada de riesgos de la información, esto debido a las múltiples amenazas a las que se expone la información de las organizaciones, pueden ser tanto internas como externas. De esta manera se puede evidenciar que los riesgos en la seguridad de información tales como datos erróneos, usuarios con accesos no autorizados, modificaciones no autorizadas a los sistemas, robo de información, etc. Generan consecuencias significativas para las la facultad de ciencias de la UNASAM, dañando

la imagen institucional y conllevando a futuras huelgas de alumnos, trabajadores y docentes, además denuncias o reclamos por parte de los proveedores, es por estos motivos que para las universidades en general es de suma importancia proteger la información crítica.

Para las universidades, los proceso de tramites, solicitudes y requerimiento, donde la información es su activo principal, debe ser prioridad proteger la confidencialidad, integridad y disponibilidad de las mismas. El valor de la información es relativamente alto en comparación con otros activos, como tal es una base fundamental para el logro de los objetivos y la continuidad de las mismas, por lo tanto, la universidad está expuesta a una serie de riesgos mientras no se garantice una protección adecuada de su información.

1.2. Formulación del problema

1.2.1. Problema general

¿Qué relación existe entre Políticas de Seguridad y Riesgos de la Información en la Facultad de Ciencias de la UNASAM?

1.2.2. Problemas específicos

- ¿Qué relación existe entre Políticas de Seguridad y el análisis de riesgos de la información en la Facultad de Ciencias de la UNASAM?
- ¿Qué relación existe entre Políticas de Seguridad y la evaluación de riesgos de la información en la Facultad de Ciencias de la UNASAM?
- ¿Qué relación existe entre Políticas de Seguridad y el tratamiento de riesgos de la información en la Facultad de Ciencias de la UNASAM?

1.3. Objetivos de la investigación:

1.3.1. Objetivo general

Determinar la relación que existe entre Políticas de Seguridad y Riesgos de la Información en la Facultad de Ciencias de la UNASAM

1.3.2. Objetivos específicos

- Determinar la relación que existe entre Políticas de Seguridad y el análisis de riesgos de la información en la Facultad de Ciencias de la UNASAM
- Determinar la relación que existe entre Políticas de Seguridad y la evaluación de riesgos de la información en la Facultad de Ciencias de la UNASAM
- Determinar la relación que existe entre Políticas de Seguridad y el tratamiento de riesgos de la información en la Facultad de Ciencias de la UNASAM

1.4. Justificación de la investigación

1.4.1. Justificación económica

La recolección de datos de la presente investigación permitirá brindar conocimiento a las autoridades de la dirección de escuela, la decanatura y los centros de cómputo de la UNASAM; con respecto a la calidad de gastos, invertidos en las instalaciones de la Universidad. Además, de realizarse una gestión de riesgos de la información es posible ampliar implementación al resto de áreas de la universidad logrando así un ahorro en posibles incidencias o emergencias.

1.4.2. Justificación operativa

La presente investigación recomienda una o varias medidas de solución al problema planteado anteriormente. Es decir, de qué manera se debe de gestionar la seguridad de la información, elaborando un plan que permita la gestión de riesgos de la información.

1.4.3. Justificación tecnológica

La recolección de datos de la presente investigación permitirá brindar conocimiento a las autoridades de la dirección de escuela, la decanatura y los centros de cómputo de la UNASAM; si es necesario o no, realizar mejoras o correcciones con respecto al uso de su infraestructura tecnológica.

1.4.4. Justificación legal

La presente investigación se justifica legalmente, mediante las siguientes leyes y decretos.

- Resolución Directoral N° 056-2017-INACAL/DN, que aprueba la "NTP-ISO/IEC 27002:2017, Tecnología de la información. Técnicas de seguridad.
- Reglamento de ley N° 29733 ley de protección de datos personales, decreto supremo N°003-2013-JUS
- Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- LEY Nº 27806.- Ley de Transparencia y Acceso a la Información Pública
- Ley Nº 30096, ley de delitos informáticos

1.4.5. Justificación social

El implementar un marco de referencia para la política de seguridad de la información y la gestión de riesgos de la información traería como consecuencia un aumento en la cultura de seguridad, consecuentemente menor información se verá en riesgo y se prevendrían problemas como la perdida de información personal (contraseñas, documentos privados, etc.)

MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1. Antecedentes Internacionales

Según, Cordero (2022) en su investigación, “Políticas de seguridad de la información basadas en normas internacionales para garantizar controles ante amenazas y vulnerabilidades en el departamento de tecnología de la cooperativa de ahorro y crédito San Francisco LTDA”. Presentado en la Universidad Técnica de Ambato de Ecuador. Donde su objetivo fue implementar políticas de seguridad de la información basadas en las normas internacionales que garanticen controles ante amenazas y vulnerabilidades en el departamento de tecnología de la cooperativa de ahorro y crédito San Francisco Ltda. Donde aplicó una metodología cuali-cuantitaiva y utilizó el instrumento de la encuesta y la entrevista, para determinar en nivel de seguridad de la información. Mediante la aplicación de la encuesta y la entrevista pudo determinar que es importante la creación de políticas de seguridad de la información dentro de la organización basado en las normativas internacionales, las cuales nos permitirán tener un mejor control de los activos de información, así como su disponibilidad, integridad y confidencialidad.

Según, Alvares y Llulluna (2021) en su investigación “Diseño de una política de seguridad de la información para la dirección de tecnologías de la información de la Universidad Técnica de Cotopaxi, basado en la norma ISO 27000”, presentado en la Universidad Técnica de Cotopaxi (UTC) de Ecuador. Donde su objetivo fue diseñar políticas de seguridad de la información para la gestión de la información y las herramientas informáticas en la dirección de tecnologías de la información de la Universidad Técnica de Cotopaxi, basado en la norma ISO 27000. En la cual aplicó una investigación bibliográfica y de campo se

utilizando el instrumento de la entrevista. Con el cual, se determinó que la institución podrá poseer una guía para neutralizar los riesgos a los cuales podrían estar expuestas, para ello es importante contar con el diseño de políticas de seguridad informática,

Según, Guerra at al. (2021) en su artículo de investigación titulada, "Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias", desarrollada en el Departamento de Ciencias de la Computación y Electrónica de la Universidad de la Costa, Barranquilla de Colombia. En el que planteó un objetivo de aplicar un sistema de gestión de la información basado en la metodología de identificación y análisis de riesgos para los procesos de bibliotecas universitarias. Para ello se adaptó la norma ISO/IEC 27001:2013, aplicando la metodología MARGERIT. El diseño de investigación fue de tipo aplicada. Los resultados obtenidos de los cálculos de riesgos intrínseco y efectivo demuestran la presencia de salvaguardas y la evaluación de los impactos. Concluyendo así, 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.

2.1.2. Antecedentes Nacionales

Según, García et al., (2021) es su estudio "Políticas basadas en la ISO 27001:2013 y su incidencia en la gestión de seguridad de la información en Municipalidades del Perú", aplicada en la Universidad Peruana Unión, Tarapoto de Perú. Donde su objetivo fue de mejorar la gestión de seguridad de la información en una municipalidad distrital peruana, mediante la implantación de un modelo de

políticas basado en la ISO 27001:2013. Desarrolló una investigación preexperimental con una muestra de 30 trabajadores a quienes se les aplicó un cuestionario para medir el grado de satisfacción con el modelo implantado. Donde encontró que más del 90 % de los encuestados reconoció mejoras en la municipalidad, lo que marca una gran diferencia entre el pre y postest, de 49 % a 96 %. Llegando a la conclusión de que el modelo de políticas de seguridad basado en tres pilares fundamentales: confidencialidad, integridad y disponibilidad mejora significativamente la gestión de seguridad de la información.

Según, Taboada, (2021), en su investigación "Modelo de seguridad de la información para contribuir en una mejora de la seguridad de los activos de información financiera de las unidades de gestión educativa local de Lambayeque", presentado en la Escuela de Posgrado de la Universidad Católica Santo Toribio de Mogrovejo de Lambayeque. Donde tuvo por objetivo de contribuir en la mejora de la seguridad de los activos de información financiera de las unidades de gestión. En el que aplicó una investigación cuasi experimental, donde su instrumento de recolección de datos fue la encuesta basada en la Norma ISO/IEC 27001:2013 de salvaguardas de seguridad de la información, al encargado del centro de Sistemas de información por cada unidad. Donde llegó a la conclusión de que el modelo propuesto de seguridad, contiene etapas que se encuentran enmarcadas en el ciclo Deming, cumpliendo con el enfoque de planear reflejadas en las fases de contexto de la organización, análisis de riesgos; implementar en la fase de implementación; verificar en la fase de comunicación y mejoras.

Según, Calderón, (2019) en su investigación sobre "Seguridad de la Información y la gestión de riesgos en los trabajos de la DIGERE del ministerio de educación, 2018", presentada en la Universidad Privada César Vallejo de Lima. Donde su objetivo fue determinar la relación que existe entre la seguridad de la información y la gestión de riesgos en los trabajadores de la Dirección de Gestión de Recursos Educativos del Ministerio de Educación, 2018. Aplicando una investigación de tipo básico, con un diseño no experimental, correlacional y transversal, la población elegida fue de 106 trabajadores de la Dirección de Gestión de Recursos Educativos del Ministerio de Educación. Donde llegó a la conclusión positiva, si existe un vínculo directo entre ambas variables en los empleados de la DIGERE del MINEDU, debido a que se logró un valor de significancia igual a cero con un Rho de Spearman de (0.886).

2.1.3. Antecedentes Locales

Según, Quispe, (2018) en su tesis "Declaración de aplicabilidad mediante la NTPISO/IEC27001:2014 para reducir los siniestros de la información en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash, 2018", desarrollada en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash. Donde su objetivo fue determinar cómo la declaración de aplicabilidad mediante la NTP-ISO/IEC 27001:2014 reducirá los siniestros de los activos en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Áncash. Aplicó una investigación de tipo no experimental de alcance descriptivo correlacional y de corte transversal con una muestra conformada por trabajadores y usuarios se utilizó la técnica de las encuestas y el instrumento el cuestionario posterior se hizo un análisis y procesamiento de datos para poder contrastar la

hipótesis. Llegando a la conclusión de que para proponer la declaración de aplicabilidad es fundamental el apoyo de la alta gerencia ya que hace un llamado de conciencia y dota de responsabilidades a los trabajadores que perteneces en el proceso de licencias de conducir quienes aportaron con gran información en el momento de evaluar los activos de información.

2.2. Bases teóricas

2.2.1. Políticas de seguridad

Las políticas de seguridad son documentos tangibles que se actualizan y cambian continuamente a medida que avanza las tecnologías, las vulnerabilidades y los requisitos de seguridad. La política de una organización está enmarcado a proteger sus activos físicos y de tecnología de la información (TI). Las políticas de seguridad pueden presentar una política de uso aceptable. Donde describen la planificación que hacen las organizaciones para educar a sus empleados sobre la protección de los activos. Donde se explican todo el proceso que aborda y también el procedimiento para evaluar la efectividad de la política para garantizar que se realicen las correcciones necesarias (Holtkamp, 2018).

Según, Rostami, (2022), las políticas de seguridad de la información (PSI), son las reglas establecidas que están orientados la protección de los activos de unas empresas. La seguridad de la información aborda las áreas de gestión de la seguridad de la información, informática, datos, y seguridad de la red. Cuando hablamos de seguridad, debemos abordar el tema de concientización, la capacitación educación y las tecnologías que son imprescindibles para la protección de datos. Las políticas de seguridad de la información están diseñadas para salvaguardar los recursos de la red de las infracciones de seguridad.

Las políticas de seguridad describen los lineamientos en el que se establecen los objetivos de la protección, es decir, que se desea proteger y el porqué, a través de normativas, reglamentos y protocolos, determinando responsabilidades, funciones de la organización y controlando su correcto funcionamiento. (Escudero, 2021)

2.2.1.1. Seguridad de la información

Para Vega, (2021) seguridad significa proteger los activos, de atacantes que invaden nuestras redes, desastres naturales, condiciones ambientales adversas, cortes de energía, robo u otros estados indeseables. También es la disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y esquemas normativos, que nos exigen niveles de protección de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación de la información.

Para la ISO/IEC (2013) la seguridad de la información son aquellos procesos, buenas prácticas y metodologías que busquen salvaguardar la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada. Es decir que debemos de proteger nuestros datos y nuestros recursos de infraestructura tecnológica de aquellos quiénes intentarían hacer un mal uso de ellos.

Según, Cano (2013) la Seguridad de la Información es la disciplina que se encarga de garantizar la confidencialidad, integridad y disponibilidad de la información. para alcanzar el objetivo se apoya en la seguridad informática, es decir que ambas disciplinas van de la mano.

a. **Confidencialidad**

Para Buenaño, (2013), la confidencialidad es dar el acceso a la información a todos aquellos que se encuentre autorizados sin ninguna excepción. Por tanto, la confidencialidad de la información nos asegura que solo aquellos con suficientes privilegios puedan acceder a cierta información.

b. Integridad

Para, Maureira, (2017) la integridad es el permitir que la información sea la adecuada y que no haya sido modificada por usuarios, entidades o procesos no autorizados. También, la integridad se refiere a la capacidad de evitar que nuestros datos se modifiquen de manera no autorizada o indeseable. Para las universidades la conservación la integridad de la información en su totalidad es muy importante tanto los datos institucionales y los datos sensibles que se maneja del personal y de los universitarios.

c. Disponibilidad

La disponibilidad está relacionada con la accesibilidad a la información en el momento que sea requerido. Hace referencia a la posibilidad de poder acceder a la información y sistemas cuando sea requerido. Según, Mosquera (2017). La pérdida de disponibilidad puede referirse a una amplia variedad de interrupciones en cualquier parte de la cadena de comunicaciones que nos permite acceder a nuestros datos. Tales problemas pueden ser el resultado de pérdida de energía, problemas del sistema operativo o de la aplicación, ataques a la red de datos, compromiso de un sistema u otros problemas que impidan a los usuarios acceder a su información. (Wang et al., 2017).

2.2.1.2. Seguridad informática

Esta disciplina es la encarga de implementar técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, de las tecnologías de información, establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo. (Cano, 2013)

Figura 1

Seguridad de la información vs. Seguridad informática

Fuente: https://seguridadetica.wordpress.com

2.2.1.3. Política de seguridad según la ISO 27001

Para la norma ISO 27001 es primordial definir una política de seguridad de la información adecuadas a las necesidades de la organización. Esto hace que, en muchas ocasiones erronaemente, se defina una política de seguridad únicamente para cumplir dicho requisito. Lo cual es un error, ya que puede ser utilizado como una herramienta de liderazgo de la dirección y de concienciación para los empleados.

Conforme a la norma ISO 27001, la política de seguridad de la información deberá cumplir unos requisitos básicos.

- Ser apropiada a la organización: La política de seguridad de la información debe de ser coherente con los activos de información de la empresa, así como con los riesgos y amenazas de su entorno.
- Servir de referencia a los objetivos: Las políticas de seguridad de la información deben estar alineados a los objetivos. De tal forma, que, si se indica la prioridad de garantizar la seguridad de los datos de los clientes, un objetivo coherente será reducir el número de incidencias de este tipo.
- Cumplir los compromisos aplicables: En la política de seguridad de la información se deberá indicar el compromiso de la dirección en cumplir los requisitos que le apliquen en esta materia. Tanto los requisitos legales que nos afecten o los compromisos adquiridos con sus clientes u otras partes interesadas.
- Garantizar la mejora continua: La dirección tiene que comprometerse a aplicar acciones de mejora continua en la política de seguridad de la información.

Otros de los requisitos de la norma ISO 27001, es el deber de comunicar correctamente la política de seguridad de la información dentro de organización, y de ponerla a disposición del resto de las partes interesadas cuando se considere necesario.

Según, la ISO 27001 los canales que se pueden utilizar para la comunicación son los siguientes:

- Sitio web corporativo: Utilizar la intranet de la organización para realizar la comunicación interna, y publicarla en el sitio web de la organización para su

puesta a disposición de las partes interesadas, suele ser la solución más sencilla y eficiente.

- Tablón de anuncios: Si no disponemos de intranet, es la solución más clásica para la consulta de los empleados. Lo malo es que la falta de espacio en el tablón de anuncios, puede hacer que esta quede tapada o sea eliminada por error.
- Formaciones internas: Las nuevas incorporaciones de la empresa, suelen recibir una formación básica sobre la seguridad de la información, y es donde se explica la política de seguridad. Para el resto de empleados: las formaciones de reciclaje, charlas de concienciación o reuniones departamentales, son buenas ocasiones para recordar su contenido e importancia.
- Comunicados de la Dirección: Los canales habituales utilizados por la dirección para la comunicación con los empleados (circulares, cartas, comunicados), son perfectos para la notificación de una versión de la política de seguridad de la información. Además, reforzará el liderazgo de la dirección en la gestión de la seguridad.
- Newsletters, revistas, catálogo de productos: Cuando la comunicación va dirigida a clientes, proveedores, colaboradores, accionistas... se pueden utilizar estos otros canales para difundir la política de seguridad de la información entre estas otras partes interesadas.
- La política de seguridad de la información debe ser conocida por todos los empleados de la institución. y no sólo deben saber cómo localizarla, sino que deben entenderla y ser capaces de explicar cómo influye en su trabajo.

2.2.2. Riesgos de la información

Los riesgos son las incidencias o hechos que ocurren en un momento dado, que estas repercuten en consecuencias negativas o positivas que podrían afectar el logro de los objetivos de toda organización.

El riesgo es la probabilidad de pérdidas y daños futuros, que genera incertidumbre de obstaculizar el logró de los objetivos y la continuidad de negocio. Según, Lavell, (1998), es una condición latente que capta la posibilidad de perdidas futuras físicas, económicas, sicosociales, culturales que están sujetas al análisis y medición de términos cualitativos y cuantitativos.

Tal es así que, el proceso de análisis de riesgos debe ser el más importa de la gestión de riesgos. La gestión de riesgos es el proceso que se encarga de identificar y cuantificar la probabilidad de que se produzcan amenazas y de establecer un nivel aceptable de riesgo para las instituciones, considerando el impacto potencial de una incidencia no deseado. La valoración de riesgo es el proceso de identificar los problemas antes de que aparezcan. Una incidencia tiene tres componentes: amenaza, vulnerabilidad e impacto. Las vulnerabilidades son debilidades en los activos que pueden ser explotadas por amenazas. Sin estos componentes, es posible que no se produzcan incidentes o riesgos de seguridad. (Areito, 2008).

Para mitigar los riesgos se debe implementar medidas, controles y contramedidas de seguridad, las propias medidas de seguridad pueden afectar a las amenazas, vulnerabilidades, impactos o riesgos

2.2.2.1. Riesgos en el manejo de la información

El manejo de riesgo en cuanto a la seguridad de la información se trata implica lo siguiente:

- Evitar: No permitir ningún tipo de exposición, evitando en lo posible realizar acciones que impliquen riesgo.
- Reducir: Cuando no se puede evitar el riesgo, por varias dificultades de tipo operacional, La opción más económica y sencilla es reducir en lo más mínimo posible el riesgo.
- Retener, asumir o aceptar el riesgo: Asumir la consecuencia de la ocurrencia del evento, que puede ser voluntariamente que consiste en reconocer la existencia del riesgo o involuntario que es cuando se retine el riesgo inconscientemente
- Transferir: Consistente en buscar un respaldo y compartir el riesgo con otros controles o entidades. (Hernandez, 2009)

2.2.2.2. Análisis de riesgos de la información

Para de Freitas, (2009), el objetivo del análisis de riesgo es identificar los riesgos basados en la identificación de los activos, de sus amenazas y vulnerabilidades. xSegún, Paredes (2018) los activos se podrían ver afectados negativamente si no cuentan con una protección adecuada. Por esta razón, es importante conocer las características de cada activo y así poder determinar el riesgo asociado a cada una de ellas, para estimar en qué medida los activos estos expuestos a ellos.

Mediante el análisis se obtendrá una visión real y precisade los activos de la información, conocer vulnerabilidades y los riesgos para poder identificar el impacto y así reducir los tiempos de actuación y respuesta,

facilitando así a la toma de decisiones. Evaluar su estado actual de seguridad, para implementar mejoras o reforzar aspectos débiles en cuanto a sus medidas de protección, y así poder crear una cultura organizacional de prevención, que involucre y comprometa a todos los interesados.

a. Identificación de todos los activos

Para, Areito (2008) los activos son aquellos elementos relacionados con el entorno, como el personal, los edificios, las instalaciones, los equipos o los suministros; los relacionados con los sistemas de TIC, relacionados con la información, los relacionados con la funcionalidad de la organización, los activos intangibles, como la imagen de la organización, credibilidad, conocimiento adquirido; los activos no protegidos exigen una valoración de riesgo aceptable. entre los atributos de los activos se encuentra su valoración intrínseca y/o su valoración en función de la posible pérdida de confidencialidad, integridad y disponibilidad. Los requisitos de protección de los activos dependen de la vulnerabilidad que presentan ante determinadas amenazas.

b. Identificación de amenazas

Según, Areito (2008), una amenaza necesita explotar una vulnerabilidad del activo para producir un daño. Una amenaza puede materializarse desde el interior de una organización, como el sabotaje de un empleado, el robo de contraseñas con un sniffer (escuchas clandestinas), mediante acceso por Internet no autorizado o un DoS (denegación de servicios).

El daño causado por una amenaza puede ser temporal o permanente y se puede asociar con una escala de severidad como otros fenómenos. El origen, que puede ser interno o externo. La motivación, como son las ventajas competitivas, los beneficios económicos, etc. La frecuencia o periodicidad de los ataques. La severidad, dependiendo de si es o no irreversible. (Areito, 2008)

c. Identificación de vulnerabilidades

Según, Areito (2008) Las vulnerabilidades pueden ser permanentes, a no ser que se produzcan cambios en el activo, de forma que lo haga insensible a la vulnerabilidad, una vulnerabilidad puede entenderse también como la potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo. Las vulnerabilidades asociadas a los activos, incluyen las debilidades en el nivel físico sobre la organización, los procedimientos, el personal, la gestión, la administración, los equipos, el software o la información. Una vulnerabilidad, por sí misma, no causa daño alguno; es, simplemente, una condición o conjunto de condiciones que pueden permitir que una amenaza afecte a un activo.

2.2.2.3. Evaluación de riesgos

Según la ISO 27000 los auditores deben tener documentado de evaluación de riesgos que explique cómo se identifican, analizan, evalúan y priorizan los riesgos relacionados con los activos de información más relevantes del alcance.

Según, De Freitas (2009) la evaluación de riesgo es el proceso de hacer una comparativa entre los riesgos estimados y los criterios de riesgo

establecidos o dados, para determinar el grado de importancia del riesgo. El proceso de evaluación del riesgo permite a una organización alcanzar los requerimientos del estándar.

El riesgo se evalúa contemplando tres elementos básicos

a. Estimado del valor de los activos de riesgos

Este punto es fundamental para evaluar el riesgo. El objetivo es determinar el daño económico que el riesgo pudiera causar a los activos evaluados. En base a ello se le da un valor monetario a cada activo de acuerdo al valor de referencia en el mercado y de su importancia para la Universidad.

b. Probabilidad de ocurrencia de riesgos

El riesgo es la posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización. Este impacto se puede producir debido a que una amenaza explote vulnerabilidades para causar pérdidas o daños. Un entorno de riesgo es aquél en el que una amenaza concreta o un grupo de amenazas, pueden explotar una vulnerabilidad o grupo de vulnerabilidades determinado, exponiendo los activos a daños o pérdidas. El riesgo se caracteriza por una combinación de dos factores: la probabilidad de que ocurra el incidente no deseado y su impacto. Cualquier modificación en activos, amenazas, vulnerabilidades y salvaguardas puede tener efectos significativos en el riesgo.

c. Valoración de riesgos de los activos

La estimación del impacto permite establecer una proporcionalidad entre las consecuencias de la agresión y el coste de los controles o las

salvaguardas necesarias. Se debe tener en cuenta, también, la posible frecuencia de materialización de las amenazas; esto es particularmente importante cuando el daño causado por cada agresión es pequeño, pero donde el efecto global de muchas agresiones en el tiempo, puede dar lugar a considerables pérdidas o daños.

Figura 2

Evaluación de riesgo

Fuente: www.iso27000.es

2.2.2.4. Tratamiento de riesgos de la información

El tratamiento de riesgo se define según el ISO/IEC 27001 como el proceso de selección e implementación de medidas para modificar el riesgo tales como: evitar, optimizar, transferir o retener el riesgo.

Para Pacheco y Jara (2009) son métodos, procedimientos que minimizan los ataques y permiten proteger activos de más importancia para la organización, la exactitud y confiabilidad de sus registros. Los controles de Seguridad soportan los activos de seguridad (Disponibilidad, Integridad y

Confidencialidad) y abarcan las terminologías básicas (Vulnerabilidad, Riesgo, Amenaza y Control).

Para, Areitio, (2008), Las salvaguardas, denominadas contramedidas o controles, son dispositivos físicos, lógicos o procedimientos que pueden proteger contra una amenaza, reducir la vulnerabilidad, limitar el impacto de un incidente no deseado y facilitar la recuperación. Las salvaguardas pueden realizar una, o más, de las siguientes funciones: detección, disuasión, prevención, limitación, cocción, recuperación, seguimiento, y concienciación. Normalmente, resulta más económico seleccionar salvaguardas que satisfagan múltiples funciones:

Los controles tienen los siguientes niveles: Administrativo, Técnico y Físico.

- **Administrativo**: controles al administrar sistemas, documentos de confidencialidad, personal de seguridad y entrenamiento a personal.
- **Técnico**: Controles a nivel lógico en hardware y software, se considera también la configuración a nivel firewall, políticas de autenticación.
- **Físico**: Especifican el lugar donde el activo está siendo protegido, para ejemplificación guardias de seguridad, cerraduras, circuitos cerrados.

Las metodologías de gestión de riesgos categorizan los controles como:

- **Controles Preventivos:** controles que disminuyen la probabilidad de materialización del riesgo, proponiendo un margen de violaciones de seguridad, son más rentables y deben incorporarse en los sistemas, de esta manera evitar costos de corrección o reproceso.
- **Controles Detectivos:** Son los controles que ayudan a detecta antes de que se producto un riesgo. Son más costosos que los preventivos, se encargan de

medir la efectividad de los controles preventivos, aunque algunas amenazas no puedan evitarse durante una etapa preventiva.

- **Controles Correctivos:** Aporta a las causas de los riesgos y de esta manera nos permite estudiarlas para encontrar la corrección más adecuada. También ayuda a tomar decisiones en procedimientos para una corrección (la recurrencia). Generan reportes que son elevados a la gerencia, vigilando todo tipo de actividad hasta hallar con la solución.
- **Controles Disuasivos:** son aquellos que reducen la probabilidad intentando desalentar un potencial ataque y de esta manera desviar la intención del individuo perpetrador.
- **Controles Recuperativos**: toman un lugar posterior al ataque con la finalidad de intentar proveer una restauración de un sistema y volver a la operación regular.
- **Controles Compensatorios:** entrega otra medida de control cuando las empresas no pueden financiar o se vean limitadas en algún aspecto institucional, que no les permita implementar el control respecto a los riesgos identificados.

2.2.3. Serie ISO 27000

La ISO 27000 son estándares internacionales sobre la seguridad de la información, en que te sugiere un modelo de gestión de riesgos como es la ISO/IEC 27005 que contiene un conjunto de buenas prácticas para la implementación y mejora de SGSI

Tabla 1

Principales Normativas de la Serie ISO 27000

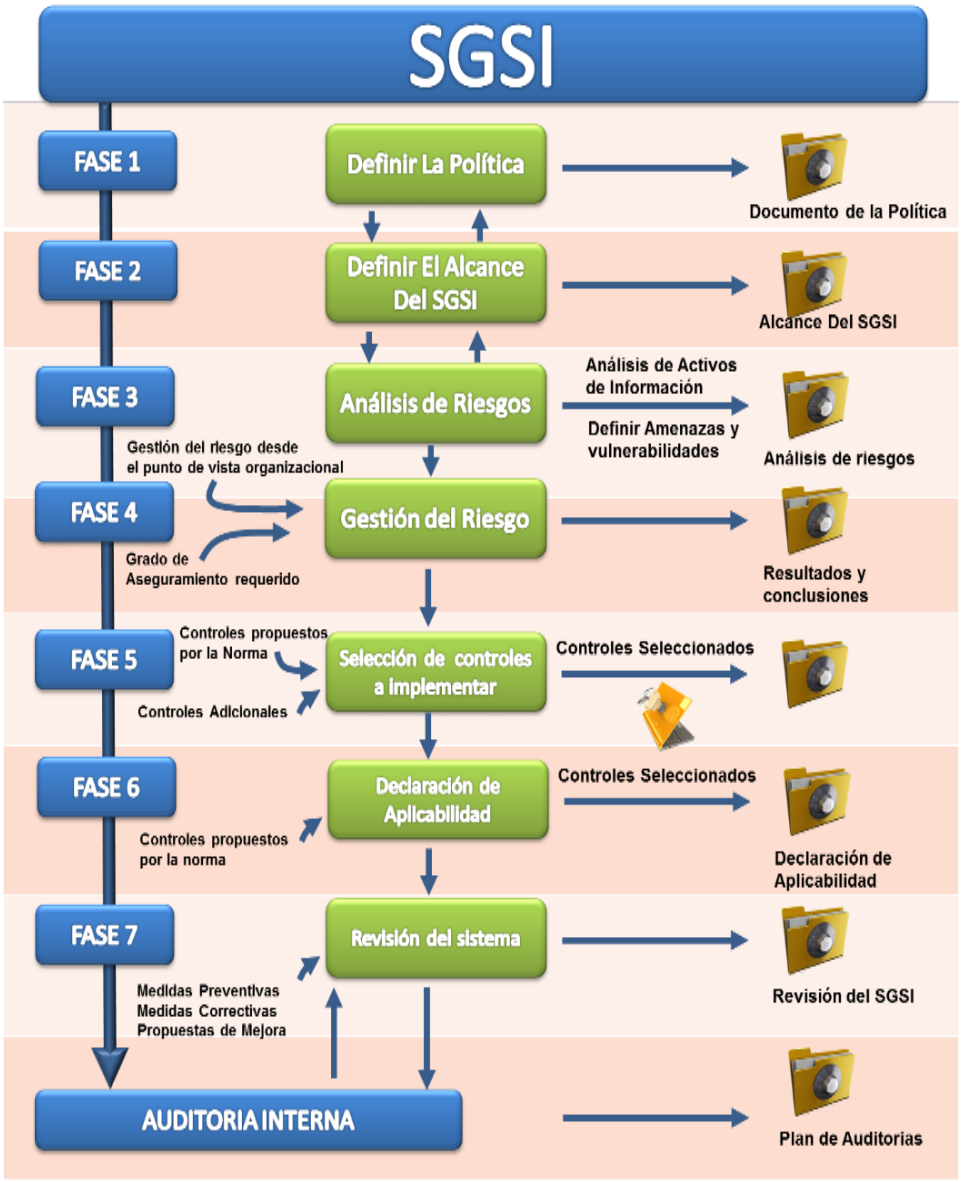
Norma ISO/IEC	Descripción
270000	Expone de forma general el alcance y propósito de las normativas que conforman la serie 27000. Además, aporta con una breve introducción a los conceptos relacionados con un Sistema de Gestión de Seguridad de la Información (SGSI).
27001	Recopila los requisitos para poner en marcha un SGSI. Su Anexo A incorpora 114 controles de seguridad, adaptables a las organizaciones (no son todos obligatorios). Es certificable
27002	Expone un conjunto de directrices y buenas prácticas que pretenden explicar y apoyar la implementación de los controles del Anexo A de ISO/IEC 27001
27003	Proporciona una serie de directrices que orientan la planificación y ejecución de un SGSI, según lo estipulado por la Norma ISO/IEC 27001.
27004	Provee una guía para la implementación de métricas que estimen el rendimiento y resultados de un SGSI.
27005	Establece el conjunto de tareas que se necesitan ejecutar, para una adecuada gestión de riesgos de TI, desde su análisis, evaluación y posterior tratamiento. Describe el proceso que debe cumplir una metodología de análisis del riesgo.
27006	Recoge los requisitos que acreditan a una entidad auditora y certificadora de SGSI.
27007	Es una guía para ejecutar planes de auditoría, que verifiquen el cumplimiento de la Norma ISO 27001. Orienta las tareas de los organismos de certificación acreditados y equipos de auditores internos o externos.
27008	Es una guía para la ejecución de programas de evaluación y revisión de los controles implementados, de acuerdo a la ISO 27001.
27009	Complementa la ISO 27001, en cuanto a la inclusión de requisitos y nuevos controles, aplicables a sectores específicos como: finanzas, transporte, salud, proyectos de infraestructura, telecomunicaciones, entre otros
27010	Especifica lineamientos para el intercambio seguro de información entre las distintas organizaciones, que buscan conformar un sistema de gestión comunitario.

Fuente: (Adaptación de ISO27000.ES)

2.2.3.1. La norma ISO/IEC 27001

Figura 3

El SGSI propuesto por la norma ISO 27001



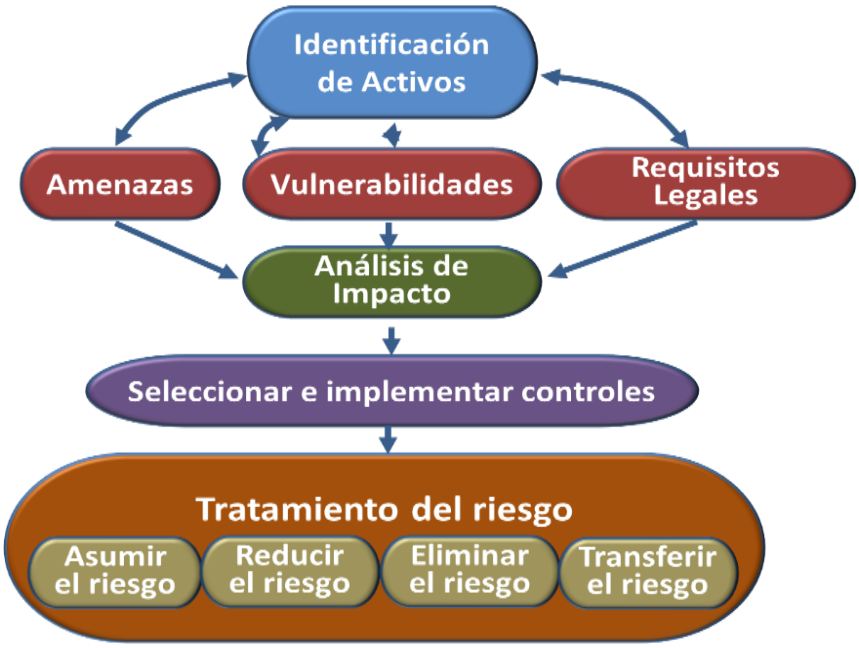
Fuente: https://www.normas-iso.com/iso-27001/

a. Metodología sugerida Norma ISO/IEC 27001

Existen muchas metodologías de evaluación de riesgos y se debe elegir la apropiada para el requerimiento de cada negocio. fases de la metodología sugerida en la norma (ISO/IEC 27001:2013).

Figura 4

Evaluación de riesgo según (ISO/IEC 27001:2013)



Fuente: https://www.normas-iso.com/iso-27001/

- **Identificar Activos:** Se entiende como activo lo que es de suma importancia para una empresa; incluye los soportes físicos e intelectuales o informáticos así también la manera en que pueda verse afectada una reputación en la organización, etc.
- **Vulnerabilidad:** Son activos susceptibles o que presentan debilidades para un determinado proceso, llegan a la posibilidad de permitir que un atacante comprometa, la integridad, disponibilidad o confidencialidad.
- **Amenazas:** Situaciones o fenómenos que atacan a los activos de la información. Ejemplo: Espionaje, Incendios.
- **Requisitos legales**: Normas o decretos que Empresa debe ejecutar en beneficio a su clientela, socios estratégicos y proveedores.

- **Identificar riesgos:** Resultado de evaluar la vulnerabilidad y amenaza de activos que al materializarse puedan afectar total o parcialmente la disponibilidad, confidencialidad e integridad.
- **Calcular riesgo:** Sirve para poder determinar el riesgo que tiene mayor prioridad, aplicando Riesgo = impacto de una amenaza x probabilidad que esta suceda.
- **Plan para tratamiento del riesgo:** Al definir este plan, ya se está preparado para identificar los controles que más se adecúen al riesgo estudiado según las definiciones mencionadas anteriormente, de esta manera se pueda cumplir con: Asumir, Reducir, Eliminar y Transferir los riesgos

2.2.4. Análisis de riesgos según ISO 27005:2018 e ISO 31000:2018

Esta norma proporciona las directrices para la gestión de riesgos en la seguridad de la información de una organización, apoyando los requisitos generales del SGSI definidos en la ISO 27001 y 27002 el conocimiento de los conceptos, modelos, procesos y términos descritos en estas normas es complemento necesario para el entendimiento de la norma ISO 27005:2018; fue diseñada para aplicar de forma satisfactoria la seguridad de la información con enfoque en gestión de riesgos (ISO/IEC 27005:2018)

La ISO 31000:2018 solo formula recomendaciones y eso significa que no permite la implementación de un sistema de gestión certificable. Sin embargo, los principales cambios en la ISO 31000:2018 resultan importante, ya que se alinean con el enfoque basado en el riesgo, presente en normas como ISO 9001 e ISO 14001.

Actividades del proceso de gestión de riesgos con el fin de identificar con claridad la situación de cada uno de sus activos: su valor, vulnerabilidades, y cómo están protegidos frente a amenazas.

Tabla 2

Actividades de la gestión de riesgo.

Identificar contexto	Analizar riesgo	Valorar riesgo	Tartar riesgo
• Identificar activos • Valorar los activos • Identificar amenazas • Identificar vulnerabilidades • identificar agentes generadores	• Estimar impacto por materialización • Estimar probabilidad de ocurrencia • Determinar riesgo • Identificar controles • Evaluar controles existentes	• Estimar estado del riesgo • Priorizar riesgo	• Toma de decisiones • Plan de tratamiento de riesgo

Fuente: Adaptación de ISO 27005:2018 e ISO 31000:2018

2.2.5. MAGERIT

La gestión de riesgos con la metodología Magerit, requiere dos fases importantes: el análisis y tratamiento de los riesgos que soportan los sistemas de información. La combinación del análisis y tratamiento, permitirá la gestión de los riesgos identificados. (Amutio et al. 2012).

Organización de las guías según MAGERIT versión 3, la cual se estructura en 3 libros.

2.2.5.1. Método

El capítulo 2 presenta los conceptos informalmente. En particular se enmarcan las actividades de análisis y tratamiento dentro de un proceso integral de gestión de riesgos.

El capítulo 3 concreta los pasos y formaliza las actividades de análisis de los riesgos.

El capítulo 4 describe opciones y criterios de tratamiento de los riesgos y formaliza las actividades de gestión de riesgos.

El capítulo 5 se centra en los proyectos de análisis de riesgos, proyectos en los que nos veremos inmersos para realizar el primer análisis de riesgos de un sistema y eventualmente cuando hay cambios sustanciales y hay que rehacer el modelo ampliamente.

El capítulo 6 formaliza las actividades de los planes de seguridad, a veces denominados planes directores o planes estratégicos.

El capítulo 7 se centra en el desarrollo de sistemas de información y cómo el análisis de riesgos sirve para gestionar la seguridad del producto final desde su concepción inicial hasta su puesta en producción, así como a la protección del propio proceso de desarrollo.

El capítulo 8 se anticipa a algunos problemas que aparecen recurrentemente cuando se realizan análisis de riesgos.

2.2.5.2. Catálogo de elementos

Nos marca unas pautas en cuanto a: Tipos de activos, dimensiones de valoración de los activos, criterios de valoración de los activos, amenazas típicas sobre los sistemas de información y salvaguardas a considerar para proteger sistemas de información.

Estas con el propósito de facilitar el trabajo de los ejecutores del proyecto, en el sentido de dotarlos de elementos estándar a los que puedan suscribirse rápidamente, centrándose en la especificidad del sistema que se analiza. Y Por otro lado, la estandarización de los resultados analíticos al promover una terminología y criterios comunes permite la comparación e incluso la integración de análisis realizados por diferentes grupos

2.2.5.3. Guía de Técnicas

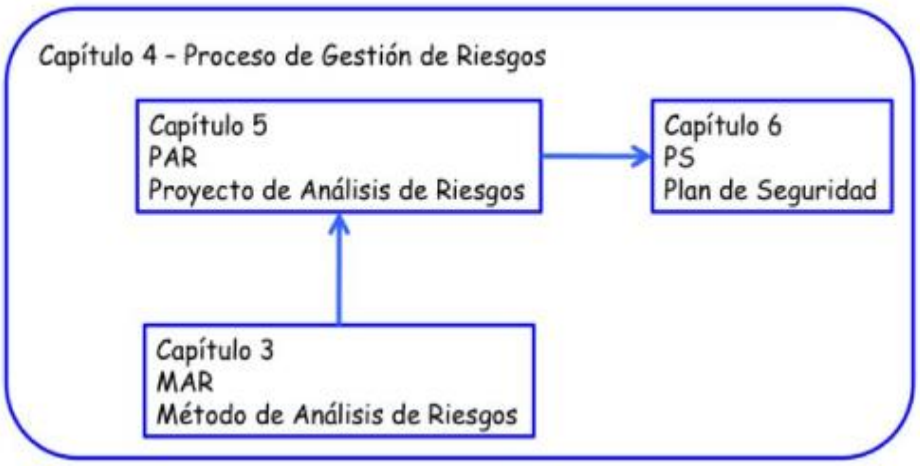
Más aclaraciones y proporciona orientación sobre algunos de los métodos comúnmente utilizados para llevar a cabo proyectos de análisis y gestión de riesgos:

Técnicas específicas para el análisis de riesgos, análisis mediante tablas, análisis algorítmico, árboles de ataque, técnicas generales, técnicas gráficas, sesiones de trabajo: entrevistas, reuniones y presentaciones

Estimación Delphi Esta es una guía de referencia. A medida que el lector avance a través de los objetivos del proyecto, se le pedirá que utilice varios métodos de los cuales esta guía será una introducción y le proporcionará enlaces para profundizar en el tema.

Figura 5

Pasos para el análisis de riesgos con Magerit



Fuente: (Magerit 3.0)

2.2.6. Metodología de análisis y gestión de riesgos

La metodología CRAMM (Metodología De Análisis Y Gestión De Riesgos Desarrollada Por El CCTA inglés). Esta metodología de Análisis de Riesgos fue desarrollada por el Centro de Informática y la Agencia Nacional de Telecomunicaciones (CCTA) del Gobierno del Reino Unido.

Se puede definir como un método analítico de la gestión de riesgos que aplica sus conceptos de cierta manera formal, disciplinado y organizado. Centrado en la protección de la confidencialidad, integridad y disponibilidad del sistema y de sus activos; que, aunque es considerado cuantitativo, utiliza evaluación cuantitativa y cualitativa y por ello se encuentra mixta.

Existen también la Metodología EBIOS que consta de cinco fases como son: Fase 1: Análisis del contexto, estudiando cuales son las dependencias de los procesos del negocio respecto a los sistemas de información. Fase 2 y 3: Análisis de las necesidades de seguridad y de las amenazas, determinando los puntos de conflicto. Fase 4 y 5: Resolución del conflicto, estableciendo los objetivos de seguridad necesarios y suficientes, con pruebas de cumplimiento y dejando claros cuáles son los riesgos residuales

La metodología OCTAVE: Este método, es una evaluación de amenazas. Operacionalmente críticas, activos y vulnerabilidades, se implementa con la conformación de un equipo mixto formado por personas del área de negocio y de TI. Esta configuración explica el hecho de que los representantes comerciales están mejor posicionados para determinar qué información es importante para los procesos y cómo se utiliza esa información; Por su parte, el equipo de TI conoce la configuración de la infraestructura y sus debilidades.

2.3. Definición de términos

- **Activo:** Es todo lo que tenga valor para lo organización. Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización, como la información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos" (ISO/IEC 27000, 2014).
- **Activos de Información:** Es todo activo que se usa dentro del sistema de gestión de seguridad de la información para que las entidades puedan cumplir con los objetivos propuestos desde la alta dirección, se consideran importantes o de alta validez que puede almacenar, procesar y transformar información. (MINAM, 2017)
- **ISO:** "Organización de Estandarización Internacional" (ISO/IEC 27000, 2014).
- **Norma:** Regla o conjunto de reglas que hay que seguir para llevar a cabo una acción, porque está establecido o ha sido ordenado de ese modo" (ISO/IEC 27000, 2014).
- **Amenaza:** Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización" (ISO/IEC 27000, 2014).
- **Vulnerabilidad:** Es la debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- **Riesgo:** Es el efecto que no ha sucedido, con una probabilidad de que suceda y que en caso de suceder tendrá una consecuencia (positiva o negativa) sobre los resultados esperados de la organización (ISO 9000:2015)
- **Análisis de riesgo:** Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización" (ISO/IEC 27000, 2014).

- **Control:** Herramienta de la gestión del riesgo, incluido: políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal" (ISO/IEC 27000, 2014).
- **Impacto:** Consecuencia que sobre un activo tiene la materialización de una amenaza (ISO/IEC 27000, 2014)
- **Gestión de riesgo:** Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos (MINTIC, 2015)
- **Evaluación de riesgos:** Etapa de la gestión del riesgo que busca controlar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (MINTIC, 2015)
- **Identificación del riesgo:** Solamente identificando los riesgos podremos proteger los activos adecuadamente (Flores, 2015)
- **Identificación del activo:** Todos los activos deben de estar claramente identificados e inventariados por la organización, para tener un tratamiento adecuado de los mismos. (MINTIC, 2016)
- **Clasificación del activo:** Los activos de información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. (MINTIC, 2016)
- **Probabilidad de ocurrencia:** Establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos, a fin de determinar la capacidad de la organización para su aceptación o manejo**. (**ISO 31000:2018)
- **Evaluación de riesgos:** Proceso de identificar, cuantificar y priorizar los riesgos en comparación con el criterio de aceptación de riesgo y los objetivos de la organización. (Flores, 2015)

- **Identificar amenazas:** Acción de identificar las distintas amenazas que puedan afectar a un activo y se clasificarlas. (Flores, 2018)
- **Tratamiento de riesgo:** Son las acciones que se tomaran después de la evaluación de los riesgos, tales como aplicar controles, aceptar los riesgos, evitar riesgos, eliminar riesgos. (Flores, 2015)
- **Control de riesgo:** Es el proceso diseñado para gestionar los riesgos de acuerdo a los objetivos de la empresa. (Flores, 2015)
- **Mitigar riesgos:** Reducir los riesgos a un nivel aceptable o eliminarlos, mediante la implantación de controles.
- **Elaborar estrategias:** Las estrategias de gestión de riesgos son la planificación y desarrollo de métodos eficaces para eliminar o reducir el impacto negativo de la probable ocurrencia de cada riesgo identificado. (Flores, 2015)
- **Efectividad del control de acceso:** Es una parte fundamental del tratamiento de datos de las personas que se manejan en la base de datos de las instalaciones para el ingreso o salida. (MINTIC, 2015)
- **Gestión de contingencias:** El Plan de contingencia determina las medidas que debemos adoptar, las labores, los recursos necesarios y las actuaciones con el objetivo principal de reducir los daños que se puedan producir. (ISO 9001:2015)
- **Causa:** Medios, circunstancias o agentes generadores del riesgo (MINTIC, 2015)
- **Consecuencias:** Efectos generadores por la ocurrencia de un riesgo que afecta los objetivos o un proceso de entidad. Pueden ser entre otros, una perdida, un daño, un perjuicio, un detrimento (MINTIC, 2015)
- **Salvaguarda:** Procedimiento o mecanismo tecnológico que reduce el riesgo (ISO/IEC 27000, 2014).

- **SGSI:** Sistema de Gestión de Seguridad de la Información. Es una herramienta de gestión" (ISO/IEC 27000, 2014).
- **Concientización:** Acción y efecto de crear conciencia entre la gente acerca de un problema o fenómeno que se juzga importante. (MINAM, 2017)
- **Cultura en Seguridad de la Información:** Es la creación de hábitos que la persona, institución o empresa debe tener en cuenta para las actividades y procesos que realice para la seguridad y protección de su información. (MINAM, 2017)
- **Gobernanza Digital:** Es el conjunto de procesos, estructuras, herramientas y normas que nos permiten dirigir, evaluar y supervisar el uso y adopción de las tecnologías digitales en la organización. (MINAM, 2017)
- **Incidentes de Seguridad de la Información:** Evento o serie de eventos que pueden comprometer la confianza, la prosperidad económica, la protección de las personas y sus datos personales, la información, entre otros activos de la organización, a través de tecnologías digitales. Por ejemplo, un acceso no autorizado, el robo de contraseñas, el robo de información, el borrado de información de terceros, etc. (MINAM, 2017)
- **Propietario del Activo de Información**: El propietario de activo proporciona la responsabilidad y rendición de cuentas por el activo. Tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad según corresponda. (MINAM, 2017)
- **Política de seguridad**: La política de seguridad consiste en desarrollar el marco de actuación apropiado para salvaguardar la información de la organización. El principal objetivo es indicar el propósito del Sistema de Gestión de Seguridad de la Información y del documento en sí mismo. (ISO/IEC 27000, 2014)
- **Seguridad de la Información**: Conjunto de actividades y prácticas orientadas a preservar la integridad, confidencialidad y disponibilidad de la información y los

activos asociados a su tratamiento, independiente de la forma en que esté se presente. (MINAM, 2017)

- **Sistema de Gestión de Seguridad de Información (SGSI)**: Es la parte del sistema integral de gestión, basado en un enfoque de riesgo del negocio para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. (MINAM, 2017)
- **Confidencialidad**: Propiedad o característica consistente en que la información ni se pone a disposición ni se revela a individuos, entidades o procesos no autorizados" (ISO/IEC 27000, 2014).
- **Disponibilidad**: Los activos de información deben estar disponibles para su uso, por parte de los usuarios autorizados cuando lo requieran, garantizando el acceso oportuno. (MINAM, 2017).
- Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados" (ISO/IEC 27000, 2014).
- **Integridad**: Propiedad o característica consistente en que el activo no ha sido alterado de manera no autorizada (ISO/IEC 27000, 2014).
- **Acción correctiva:** Acción para eliminar las causas de una no conformidad y prevenir su repetición" (ISO/IEC 27000, 2014).
- **Acción preventiva:** Medida de tipo pro-activo orientada a prevenir potenciales no conformidades" (ISO/IEC 27000, 2014).
- **Aceptación de riesgo:** Decisión informada de asumir un riesgo concreto" (ISO/IEC 27000, 2014).

2.4. Hipótesis

2.4.1. Hipótesis general

Existe una relación significativa entre Políticas de Seguridad y Riesgos de la Información en la Facultad de Ciencia de la UNASAM

2.4.2. Hipótesis especificas

- Existe una relación significativa entre Políticas de Seguridad y el análisis de riesgos de a información en la Facultad de Ciencias de la UNASAM
- Existe una relación significativa entre Políticas de Seguridad y la evaluación de riesgos de la información en la Facultad de Ciencias de la UNASAM
- Existe una relación significativa entre Políticas de Seguridad y el tratamiento de riesgos de la información en la Facultad de Ciencias de la UNASAM

2.5. Variables

2.5.1. Variable independiente

Políticas de seguridad

2.5.2. Variable dependiente

Riesgos de la información

Operacionalización de variables

Variables	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Ítems	Instrumento y Escala
V1: Políticas de Seguridad	Según, Vega (2008) las políticas de seguridad se desarrollan con el fin de proteger la información y los sistemas de una Institución, garantizando la integridad, confidencialidad y disponibilidad de la información. Los documentos relativos a las políticas de seguridad deben contemplar los procedimientos para hacer cumplir las reglas, las responsabilidades en todos los niveles. Todos ellos deben tener el apoyo gerencial de la organización.	Las políticas de seguridad estar enmarcadas a proteger la confidencialidad, integridad y la disponibilidad de la información, con la que cuenta la institución.	Seguridad de la información	Confidencialidad	Ítem 1, Ítem 2 y Ítem 3	Encuesta I Escala de Likert
				Integridad	Ítem 4, Ítem 5 y Ítem 6	
				Disponibilidad	Ítem 7 y Ítem 8	
V2: Riesgos de la Información	Según (Arteaga, 2018) menciona que todo proceso de análisis y gestión de riesgos, tiene como denominador común, la ejecución de las siguientes actividades: • Identificar los activos e información sensible, con el fin de asociarlos con los niveles de riesgo. • Evaluar las amenazas a que estas expuestos los Activos, y el potencial daño que pueden provocar en ellos. • Vincular el impacto que genera una amenaza, respecto a su probable ocurrencia, para encontrar el nivel de riesgo asociado. • Elaborar estrategias de tratamiento del riesgo, basadas en estándares y buenas prácticas.	En cuanto a los riesgos de la información se debe de analizar el riesgo identificado las amenazas y vulnerabilidades del activo, para poder evaluarlos respecto a su valor de dicho activo y la probabilidad de ocurrencia de la amenaza. Para así poder implementar controles y reducir riesgos.	Análisis de riesgos	Identificación del activo de información	Ítem 1 y Ítem 2	Encuesta II Escala de Likert
				Identificación de amenazas	Ítem 3, Ítem 4 y Ítem 5	
				Identificación de vulnerabilidades	Ítem 6 y Ítem 7	
			Evaluación de riesgos	Estimación del valor del activo	Ítem 8 y Ítem 9	
				Probabilidad de ocurrencia	Ítem 10	
				Valoración de riesgos	Ítem 11 y Ítem 12	
			Tratamiento de riesgos	Revisión de controles existentes	Ítem 13 y Ítem 14	
				Identificación de nuevos controles	Ítem 15	
				Implementación y reducción de riesgos	Ítem 16	

Fuente: Elaboración propia

METODOLOGÍA

3.1. Tipo de estudio

3.1.1. De acuerdo a la orientación

Aplicada: Este tipo de investigación se orienta al estudio de casos, en el cual busca profundizar el tema en cuestión de un grupo o una unidad de análisis en particular.

3.1.2. Según su enfoque

Cuantitativo: Este tipo de investigación evalúa el grado de asociación entre dos o más variables para luego cuantificar y analizar la vinculación.

3.2. El diseño de investigación

Diseño de investigación no experimental de corte transversal. puesto que el diseño de investigación no experimental consiste en observar fenómenos tal como se dan en un contexto natural para posteriormente analizarlos y no se realiza la manipulación deliberada de las variables. De corte transversal pues la recolección de los datos de los trabajadores se realizó en un solo momento.

3.3. Población y muestra

La población estuvo determinada por los trabajadores de la Facultad de Ciencias de la UNASAM, la cual asciende a 93 empleados entre administrativos y docentes.

Para la obtención de la muestra de la investigación, se utilizó el muestreo no probabilístico intencional a conveniencia; así la muestra estuvo conformada por 48 trabajadores (Administrativos y docentes) de la Facultad de Ciencias de la UNASAM. Según la representatividad y la conveniencia de la investigación.

3.4. Técnicas de instrumentos de recolección de datos.

Para la recolección de datos se utilizó la técnica de la encuesta para poder determinar las respuestas de una fuente primaria donde los encuestados tendrán conocimiento sobre los ítems a encuestar a través de preguntas cerradas y focalizada para la obtención de la información y su instrumento de aplicación será el cuestionario entiéndase como cuestionario un constructo de preguntas seleccionadas de ítems cerrado para obtener la respuesta de los datos requeridos para recabar una información o datos de las fuentes primarias de la información, el cual estará dirigido a 48 empleados de la Facultad de Ciencias de la UNASAM.

Para la confiabilidad de los instrumentos se realizó una prueba piloto a 8 empleados de la Institución objeto de estudio. Y los resultados serán procesados a través de la prueba Alpha de Cronbach para medir su confiabilidad teniendo como baremo la unidad de Medida de 0 a 1 siendo que entre más se acerque al coeficiente de 1 el nivel de confiabilidad sea más aceptable como una alta confiabilidad y siendo entre más cerca de 0 de muy baja confiabilidad. Así mismo, el instrumento se someterá al juicio de expertos para su validación, 3 expertos en dicha especialidad, metodólogos, estadísticos.

3.5. Técnicas de análisis y prueba de hipótesis

Para ejecutar el estudio se llevó a cabo el trámite administrativo, mediante una carta dirigido a la decanatura de la Facultad de Ciencias de la UNASAM, posteriormente la misma se realizó la aceptación del trabajo de campo, coordinando la aplicación del instrumento de recolección de datos para el mes de noviembre de 2022.

La aplicación de los instrumentos se realizó de manera presencial para los 6 administrativos y online para los docentes, para ello las escalas fueron digitalizadas en la aplicación Google Form. El formulario estuvo compuesto por 2 secciones: en la

primera sección se introdujo la presentación, el motivo y el objetivo de la investigación; en la segunda, la solicitud de sus datos, en la que se informa que su participación es anónima, voluntaria y confidencial; en la tercera, el primer instrumento Políticas de Seguridad, abreviada con sus instrucciones y preguntas respectivas y en la cuarta fue el segundo instrumento la Riesgos de la Información. Los resultados obtenidos fueron codificados empleando una tabla en Excel y se procedió con el respectivo análisis estadístico el Software SPSS 26, donde una vez tabulado los datos recabados por los instrumentos precisados se procedió a realizar una base de datos que presenten en cuadros y gráficos, que permitan la presentación de manera visual y estadística la prueba o rechazo de las hipótesis planteadas por el investigador.

Luego, el siguiente paso en la investigación fue la determinación a través de la tabulación estadística de sus respuestas para la creación de las tendencias estadística descriptiva de los resultados realzando la tendencia central de los mismos como lo son la frecuencia, la mediana, la moda, la desviación estándar, curtosis y asimetría.

Para la prueba de hipótesis se utilizó Rho de Spearman, por medio de la cual se realizará la contrastación de la hipótesis y determinar conclusiones. Mediante el proceso podremos ver si existe la relación entre Políticas de Seguridad y Riesgos de la Información, para el logro de nuestros objetivos. Seguidamente, se procederá a aceptar o rechazar la Hipótesis con la siguiente regla de decisión con un nivel de confianza del 95% y un margen de error admitido de 5% si producto de la prueba aplicada revela que significancia asintótica es menor 0.05 se procederá a aceptar la hipótesis del investigador y se rechaza la hipótesis nula; mientras que, si la significancia asintótica es mayor o igual a 0.05 se procederá a rechazar la hipótesis del investigador y se aceptara la hipótesis nula. aplicando los instrumentos diseñados para tales fines.

Tabla 3

Alfa de Cronbach de la encuesta I (V1: Políticas de Seguridad)

Encuesta I: Estadísticas de fiabilidad		
Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,865	,869	8

Como se observa, el instrumento cuenta con una confiabilidad alta.

Tabla 4

Alfa de Cronbach de la encuesta II (V2: Riesgos de la Información))

Encuesta II: Estadísticas de fiabilidad		
Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,822	,815	16

Como se observa, el instrumento cuenta con una confiabilidad alta.

RESULTADOS DE LA INVESTIGACIÓN

4.1. Descripción del trabajo de campo

Se ingresó al centro de trabajo con los protocolos de bioseguridad pertinente (lavado de manos y desinfección con alcohol gel) como si fuera un usuario más que ingresa, entrevistándonos con el encargado, a quien se le solicito la autorización para realizar la encuesta.

Previa autorización del encargado se procedió a realizar la encuesta para determinar primero la confiabilidad del instrumento. Obteniéndose un Alfa de Cronbach 0.86, siendo ésta, una alta confiabilidad. Lo que nos permitió seguir con el protocolo establecido para la recolección de datos correspondiente.

Tras verificar que el instrumento cuenta con alta confiabilidad, se siguió realizando la encuesta hasta completar los 48 empleados que conforman la muestra.

4.2. Presentación de resultados y prueba de hipótesis

Después de haber realizado el trabajo de campo, con la aplicación de instrumentos para la variable Políticas de Seguridad y Riesgos de la Información se ha llegado a los siguientes resultados.

Descripción de los resultados de la variable: Políticas de Seguridad

Tabla 5

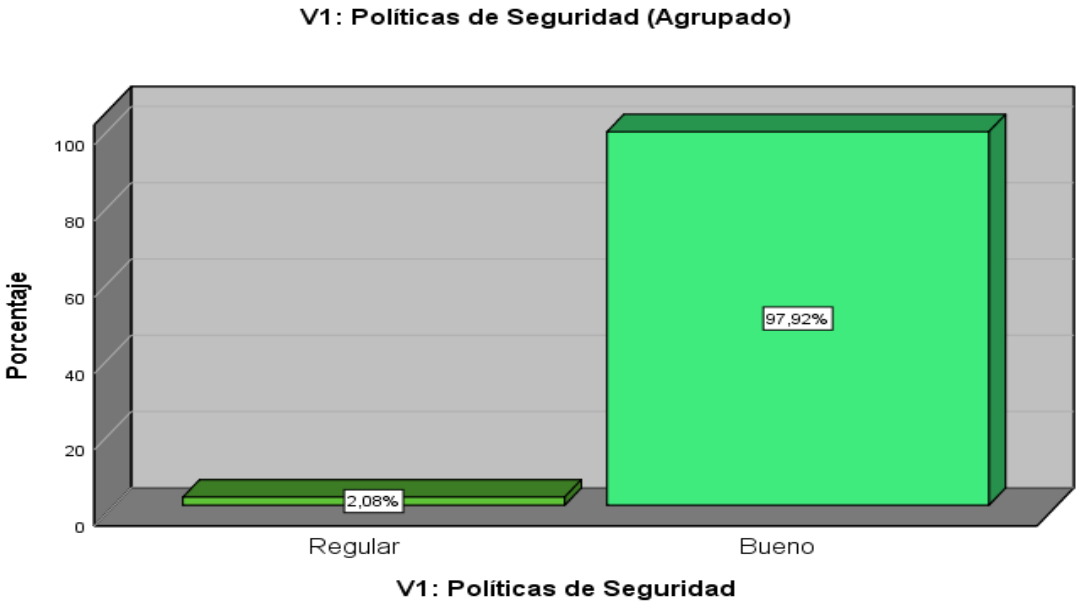
Distribución de frecuencia y porcentajes de encuestados según la V1: Políticas de Seguridad

V1: Políticas de Seguridad (Agrupado)					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	1	2,1	2,1	2,1
	Bueno	47	97,9	97,9	100,0
	Total	48	100,0	100,0	

Fuente: Base de datos (Elaboración propia)

Figura 6

Distribución porcentual de la variable Políticas de Seguridad



Fuente: Base de datos (Elaboración propia)

En la tabla 5 y figura 6, se observa el 97.92 % el cual representa 47 trabajadores de la Facultad de Ciencias de la UNASAM, que para ellos es bueno las Políticas de Seguridad, mientras que el 2.08% que representa 1 trabajador considera que es regular.

Descripción de la variable Riesgos de la Información

Tabla 6

Distribución de frecuencia y porcentajes de encuestados según V2: Riesgos de la Información

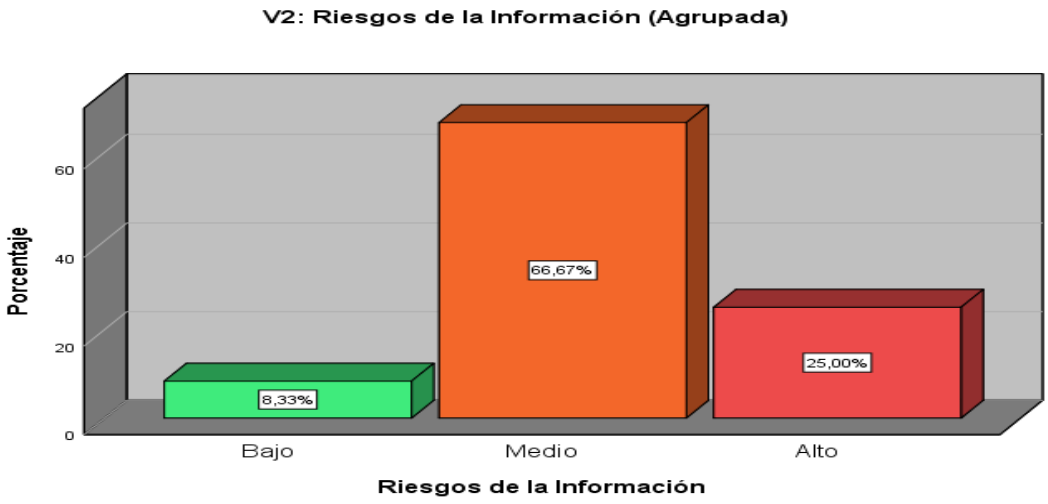
Riesgos de la Información (Agrupada)

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	4	8,3	8,3	8,3
	Medio	32	66,7	66,7	75,0
	Alto	12	25,0	25,0	100,0
	Total	48	100,0	100,0	

Fuente: Base de datos

Figura 7

Distribución porcentual de la variable Riesgos de la Información



Fuente: Base de datos (Elaboración propia)

En la tabla 6 y figura 7, se observa el 25 % el cual representa 12 trabajadores de la Facultad de Ciencias de la UNASAM, que para ellos es alto el nivel de Riesgos de la Información, mientras que el 66.67 % que representa 32 trabajadores considera que el nivel es medio, en cuanto al 8.33 % que representa 4 trabadores considera que es bajo el nivel de Riesgos de la Información.

Descripción de los resultados según las dimensiones de la variable Riesgos de la Información

Tabla 7

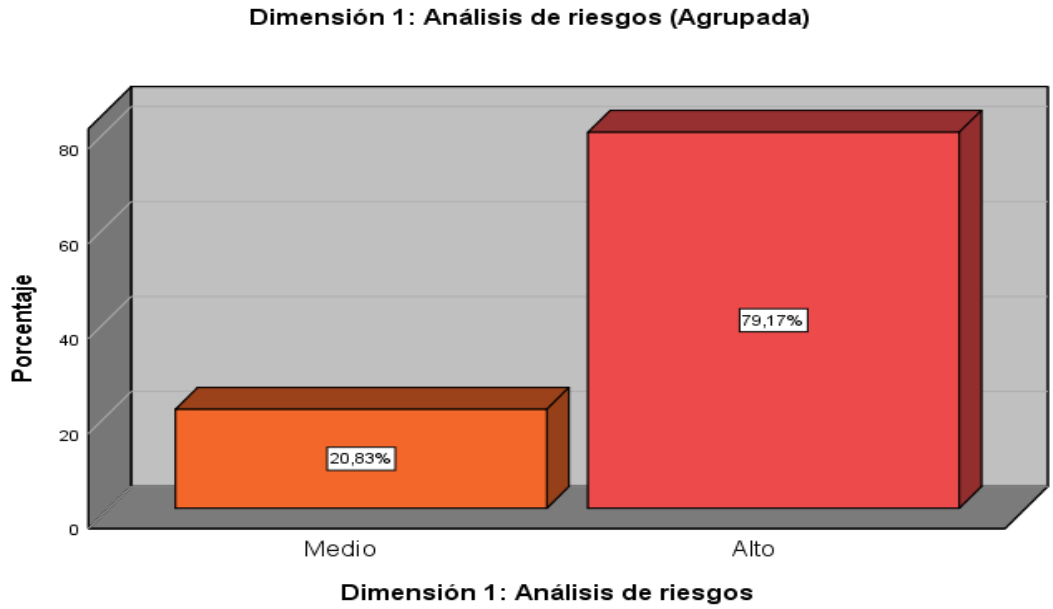
Distribución de frecuencia y porcentajes de encuestados según D1: Análisis de riesgos

Dimensión 1: Análisis de riesgos (Agrupada)					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	10	20,8	20,8	20,8
	Alto	38	79,2	79,2	100,0
	Total	48	100,0	100,0	

Fuente: Base de datos (Elaboración propia)

Figura 8

Distribución porcentual de la dimensión Análisis de riesgos



Fuente: Base de datos (Elaboración propia)

En la tabla 7 y figura 8, se observa el 79.17 % el cual representa 38 trabajadores de la Facultad de Ciencias de la UNASAM, que para ellos es alto el nivel de Análisis de riesgos de la información, mientras que el 20.83 % que representa 10 trabajadores considera que el nivel de Análisis de riesgos de la información, mientras que ninguno consideró un nivel bajo.

Tabla 8

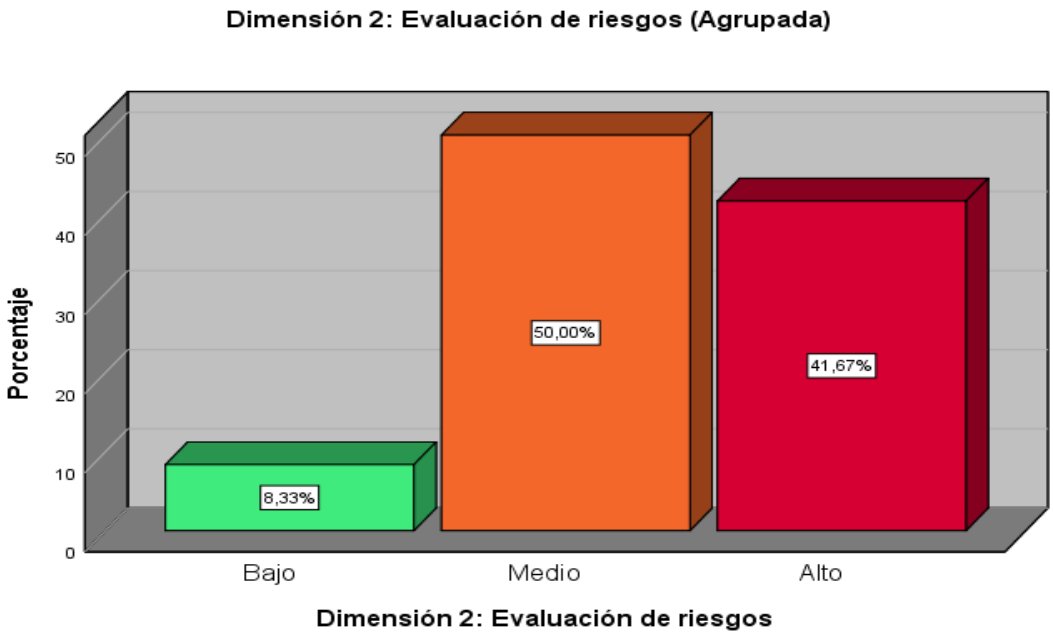
Distribución de frecuencia y porcentajes de encuestados según D2: Evaluación de riesgos

Dimensión 2: Evaluación de riesgos (Agrupada)					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	4	8,3	8,3	8,3
	Medio	24	50,0	50,0	58,3
	Alto	20	41,7	41,7	100,0
	Total	48	100,0	100,0	

Fuente: Base de datos (Elaboración propia)

Figura 9

Distribución porcentual de la dimensión Análisis de riesgos



Fuente: Base de datos (Elaboración propia)

En la tabla 8 y figura 9, se observa el 41.67 % el cual representa 20 trabajadores de la Facultad de Ciencias de la UNASAM, que para ellos es alto el nivel de Evaluación de riesgos, mientras que el 50 % que representa 24 trabajadores considera que el nivel es medio, en cuanto al 8.33 % que representa 4 trabadores considera que es bajo el nivel de Evaluación de riesgos.

Tabla 9

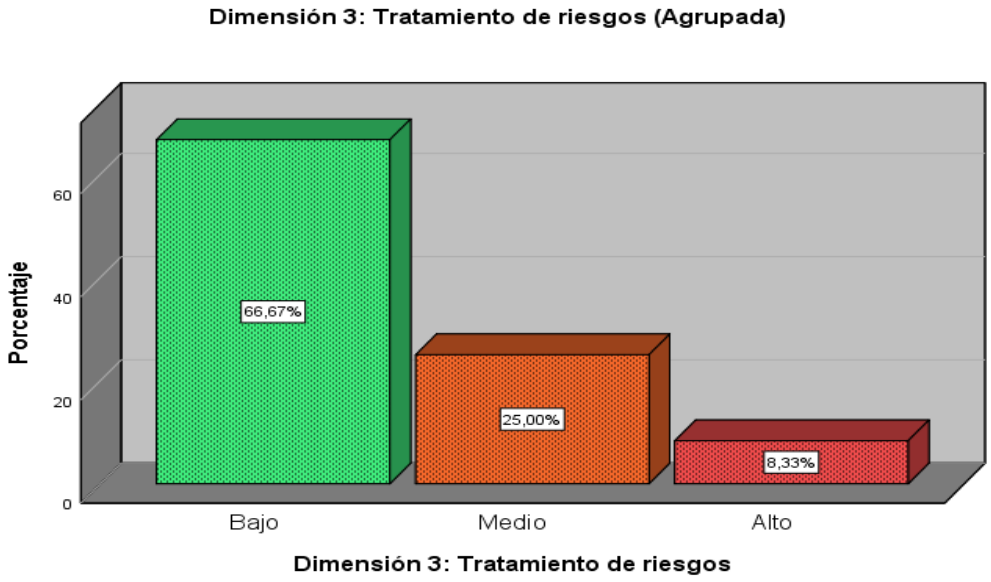
Distribución de frecuencia y porcentajes de encuestados según D3 Tratamiento de riesgos

Dimensión 3: Tratamiento de riesgos (Agrupada)					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	32	66,7	66,7	66,7
	Medio	12	25,0	25,0	91,7
	Alto	4	8,3	8,3	100,0
	Total	48	100,0	100,0	

Fuente: Base de datos (Elaboración propia)

Figura 10

Distribución porcentual de la dimensión Tratamiento de riesgos



Fuente: Base de datos (Elaboración propia)

En la tabla 9 y figura 10, se observa el 8.33 % el cual representa 4 trabajadores de la Facultad de Ciencias de la UNASAM, que para ellos es alto el nivel de Tratamiento de riesgos, mientras que el 25 % que representa 12 trabajadores considera que el nivel es medio, en cuanto al 66.67 % que representa 32 trabadores considera que es bajo el nivel de Tratamiento de riesgos.

RESULTADOS INFERENCIALES

Prueba de normalidad de la variable

Tabla 10
Prueba de estadística paramétrica Kolmogorov-Smirnov y Shapiro-Wilk

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
V1 Políticas de Seguridad	,151	48	,008	,936	48	,012
V2 Riesgos de la Información	,148	48	,011	,941	48	,017
D1 Análisis de riesgos	,217	48	,000	,891	48	,000
D2 Evaluación de riesgo	,140	48	,020	,954	48	,056
D3 Tratamiento del riesgo	,171	48	,001	,958	48	,084

a. Corrección de significación de Lilliefors

Fuente: Base de datos (Elaboración propia)

En la tabla 10 se presenta la prueba de la normalidad de las variables, se puede observar que el valor de probabilidad para V1, V2 y todas las dimensiones, tienen una significancia menor a 0,05 (Valor p < 0.05), en un diseño de asociación para usar la estadística paramétrica es necesario que las dos variables y las dimensiones cumplan la normalidad, en este caso las variables no cumplen con la normalidad, por lo que se realizará el análisis no paramétrico mediante el Coeficiente Rho de Spearman usando el software SPSSv26.

Prueba de hipótesis general

H1: Existe una relación significativa entre políticas de seguridad y riesgos de la información en la Facultad de Ciencia de la UNASAM

Tabla 11

Coeficiente de correlación y significancia entre las variables Políticas de Seguridad y la variable Riesgos de la Información

Correlaciones entre Variables				
			Políticas de Seguridad	Riesgos de la Información
Rho de Spearman	Políticas de Seguridad	Coeficiente de correlación	1,000	-,422**
		Sig. (bilateral)	.	,003
		N	48	48
	Riesgos de la Información	Coeficiente de correlación	-,422**	1,000
		Sig. (bilateral)	,003	.
		N	48	48

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Base de datos (Elaboración propia)

De los resultados se aprecia que en la tabla 11, el grado de correlación entre las variables es -0.422, lo cual significa que existe una correlación negativa media. Mientras la significancia se determina por la correlación rho de Spearman $p = 0.003$ y cuyo valor de $p < 0.05$; es decir, se acepta la hipótesis planteada. Por lo tanto, existe relación significativa entre Políticas de Seguridad y Riesgos de la Información en la Facultad de Ciencias de la UNASAM.

Prueba de la primera hipótesis especifica

H1: Existe una relación significativa entre Políticas de Seguridad y el análisis de riesgos de la información en la Facultad de Ciencias de la UNASAM

Tabla 12

Coeficiente de correlación y significancia entre las variables Políticas de Seguridad y la dimensión análisis de riesgos

Correlaciones de V1 con D1				
			V1: Políticas de Seguridad	D1: Análisis de riesgos
Rho de Spearman	Políticas de Seguridad	Coeficiente de correlación	1,000	-,346*
		Sig. (bilateral)	.	,016
		N	48	48
	Análisis de riesgos	Coeficiente de correlación	-,346*	1,000
		Sig. (bilateral)	,016	.
		N	48	48

*. La correlación es significativa en el nivel 0,05 (bilateral).

Fuente: Base de datos (Elaboración propia)

De los resultados se aprecia que en la tabla 12, el grado de correlación entre la variable Políticas de Seguridad y la dimensión análisis de riesgos de la información es -0.346, lo cual significa que existe una correlación negativa media. Mientras la significancia se determina por la correlación rho de Spearman p = 0.016 y cuyo valor de p < 0.05; es decir, se acepta la hipótesis planteada. Por lo tanto, existe relación significativa entre Políticas de Seguridad y el análisis de riesgos de la información en la Facultad de Ciencias de la UNASAM.

Prueba de la segunda hipótesis especifica

H1: Existe una relación significativa entre Políticas de Seguridad y el análisis de riesgos de la información en la Facultad de Ciencias de la UNASAM

Tabla 13

Coeficiente de correlación y significancia entre las variables Políticas de Seguridad y la dimensión evaluación de riesgos

Correlaciones entre V1 y D2				
			Políticas de Seguridad	Evaluación de riesgos
Rho de Spearman	Políticas de Seguridad	Coeficiente de correlación	1,000	-,302*
		Sig. (bilateral)	.	,037
		N	48	48
	Evaluación de riesgos	Coeficiente de correlación	-,302*	1,000
		Sig. (bilateral)	,037	.
		N	48	48

*. La correlación es significativa en el nivel 0,05 (bilateral).

Fuente: Base de datos (Elaboración propia)

De los resultados se aprecia que en la tabla 13, el grado de correlación entre la variable Políticas de Seguridad y la dimensión evaluación de riesgos de la información es -0.302, lo cual significa que existe una correlación negativa media. Mientras la significancia se determina por la correlación rho de Spearman p = 0.037 y cuyo valor de p < 0.05; es decir, se acepta la hipótesis planteada. Por lo tanto, existe relación significativa entre Políticas de Seguridad y el análisis de riesgos en la Facultad de Ciencias de la UNASAM.

Prueba de la tercera hipótesis especifica

H1: Existe una relación significativa entre políticas de seguridad y el tratamiento de riesgos de la información en la Facultad de Ciencias de la UNASAM

Tabla 14

Coeficiente de correlación y significancia entre las variables Políticas de Seguridad y la dimensión tratamiento de riesgos

Correlaciones entre V1 y D3				
			Políticas de Seguridad	Tratamiento de riesgos
Rho de Spearman	Políticas de Seguridad	Coeficiente de correlación	1,000	-,297*
		Sig. (bilateral)	.	,040
		N	48	48
	Tratamiento de riesgos	Coeficiente de correlación	-,297*	1,000
		Sig. (bilateral)	,040	.
		N	48	48

*. La correlación es significativa en el nivel 0,05 (bilateral).

Fuente: Base de datos (Elaboración propia)

De los resultados se aprecia que en la tabla 14, el grado de correlación entre la variable Políticas de Seguridad y la dimensión tratamiento de riesgos de la información es -0.297, lo cual significa que existe una correlación negativa media. Mientras la significancia se determina por la correlación rho de Spearman p = 0.040 y cuyo valor de p < 0.05; es decir, se acepta la hipótesis planteada. Por lo tanto, existe relación significativa entre Políticas de Seguridad y el análisis de riesgos en la Facultad de Ciencias de la UNASAM

4.3. Discusión de resultados

El objetivo general de esta investigación fue determinar la relación que existe entre Políticas de Seguridad y riesgos de la información en la Facultad de Ciencias de la UNASAM; los resultados permitieron confirmar las hipótesis de investigación.

La discusión se inicia con la presentación de los resultados descriptivos, así la implicancia teórica y empírica que permita comprender y discutir las hipótesis de la investigación. finalmente se presentan las limitaciones de la investigación.

Se encontró que 97.92 % el cual representa 47 trabajadores de la Facultad de Ciencias de la UNASAM, consideran que es bueno el nivel de Políticas de Seguridad. Por lo que se infiere que es importante contar con buenas Políticas de Seguridad en la Institución para la protección de nuestra información garantizando la confidencialidad, integridad y disponibilidad de las mismas. Sin embargo, no se puede dejar de considerar que 2.08% que representa 1 trabajador considera que es regular, que se entiende que no considera de importante ni poco importante contar con Políticas de seguridad.

Estos resultados se refuerzan a nivel internacional con los hallazgos de Cordero (2022) en Ecuador, donde encontró mediante los resultados de la aplicación de su encuesta y la entrevista pudo determinar que es importante la creación de políticas de seguridad de la información dentro de la Cooperativa de Ahorro y Crédito San Francisco basado en las normativas internacionales, las cuales permitieron tener un mejor control de los activos de información, así como su disponibilidad, integridad y confidencialidad.

También caso similar Alvares y Llulluna (2021) en Ecuador, donde determinó que, al contar con políticas de seguridad informática, la Universidad Técnica de Cotopaxi adaptó una guía para neutralizar los riesgos a los cuales se encuentran expuestas, además

de que servirá como pauta para el correcto uso de los recursos informáticos con los que cuenta la institución.

En el ámbito nacional García et al., (2021) en Tarapoto, donde el autor encontró que más del 90 % de los encuestados reconoció mejoras en la municipalidad, lo que marca una gran diferencia entre el pre y postest, de 49 % a 96 %. Determinando que el modelo de políticas de seguridad basado en tres pilares fundamentales: confidencialidad, integridad y disponibilidad mejoró la gestión de seguridad de la información, garantizando un adecuado resguardo de los datos.

Respecto a Riesgos de la Información, se encontró que el 25 % de colaboradores de la Facultad de Ciencias de la UNASAM, perciben un nivel alto de Riesgos de la Información, mientras que el 66.67 % consideran que el nivel es medio. Al respecto, es importante considerar que en la Institución no cuenta con un modelo de gestión de riesgos basados en las normas internaciones, mediante el cual se pueda analizar, evaluar y mitigar los riesgos de la información. En cuanto al 8.33 % de los trabadores considera que es bajo el nivel de Riesgos de la Información.

Estos resultados coinciden con el estudio de gestión de riesgos en aplicada en Latinoamérica 2022, Para el 43,6% de los directores y gerentes de riesgos, analistas de riesgos, oficiales de cumplimiento, gestores de seguridad de la información, auditores internos, entre otros., el área de gestión de riesgos actualmente tiene mucha importancia en sus empresas, la consideran como un área fundamental que contribuye al cumplimiento de los objetivos y a la continuidad del negocio. Para el 53,8% la principal dificultad que tienen al gestionar riesgos, es la falta de cultura en riesgos, esto demuestra que la mayoría de colaboradores de las empresas no tienen claridad sobre cómo pueden aportar a la

prevención, identificación, control y monitoreo de los riesgos que pueden presentarse en cada uno de los procesos.

Asimismo, Taboada, (2021), en Lambayeque concluyó que el modelo de seguridad de la información, contiene etapas que se encuentran enmarcadas en el ciclo Deming, cumpliendo con el enfoque de planear, reflejadas en las fases de contexto de la organización, liderazgo, evaluación de riesgos; implementar en la fase de implementación; verificar en la fase de comunicación y mejorar en la fase de mejoras. Apoyando la idea Calderón, (2019) determinó que si la seguridad de la información mejora la gestión de riesgos también lo hará, por ello no solo basta con implementar capacitaciones constantes, sino que precisa que es vital establecer políticas de seguridad, las cuales deberán ser aplicadas bajo responsabilidad por todo el personal de la empresa. En el ámbito local, Según Quispe, (2018) considera fundamental el apoyo de la gerencia en el llamado de conciencia y delegar responsabilidades a los trabajadores en cuanto concierne sus labores en la evaluación de los activos de información, vulnerabilidades y la información al personal para reducir y disminuir riesgos de perdida de datos.

4.3.1. Discusión de resultados de las hipótesis

Los datos obtenidos permitieron confirmar la hipótesis general de la investigación. La variable Políticas de Seguridad tiene una relación con la variable Riesgos de la Información percibido por los trabajadores (administrativos y docentes) de la Facultad de Ciencias de la UNASAM. Las pruebas estadísticas utilizadas nos indican que la correlación no paramétrica de Spearman es de -,422**, representando ésta una correlación negativa media de las variables y siendo negativo con un valor $p = 0.003$ ($p < 0.05$), de donde inferimos que tiene una relación inversamente proporcional, es decir que a

medida que las Políticas de Seguridad sean implementadas y aplicadas adecuadamente disminuirán los Riesgos de la Información.

Los resultados estadísticos también permitieron confirmar la hipótesis específica 1. Se encontró que existe una correlación negativa media entre la variable Políticas de Seguridad y la dimensión análisis de riesgos de la información; las pruebas estadísticas utilizadas nos indican que la correlación no paramétrica de Spearman de -,0.346, representando ésta una correlación negativa media de las variables y siendo negativo con un valor $p = 0.016$ ($p < 0.05$), de donde inferimos que tiene una relación inversamente proporcional. Es decir, que a medida que las Políticas de Seguridad sean implementadas y aplicadas adecuadamente en análisis de riesgos será baja debido que las políticas garantizan el control y disminución de los riesgos de la información.

Respecto a la hipótesis específica 2, se encontró que existe una correlación negativa media entre la variable Políticas de Seguridad y la dimensión evaluación de riesgos de la información; las pruebas estadísticas utilizadas nos indican que la correlación no paramétrica de Spearman de -,0.302, representando ésta una correlación negativa media de las variables y siendo negativo con un valor $p = 0.037$ ($p < 0.05$), de donde inferimos que tiene una relación inversamente proporcional. Evidenciando que a medida que las Políticas de Seguridad sean implementadas y aplicadas adecuadamente la evaluación de riesgos será baja debido que las políticas garantizan el control y disminución de los riesgos de la información.

La confirmación de la hipótesis específica 3, evidenció que existe una correlación negativa media entre la variable Políticas de Seguridad y la

dimensión tratamiento de riesgos de la información, las pruebas estadísticas utilizadas nos indican que la correlación no paramétrica de Spearman de -,0.297, representando ésta una correlación negativa media de las variables y siendo negativo con un valor $p = 0.040$ ($p < 0.05$), de donde inferimos que tiene una relación inversamente proporcional. evidenciando que a medida que las Políticas de Seguridad sean implementadas y aplicadas adecuadamente la Tratamiento de riesgos será baja debido que las políticas garantizan el control y disminución de los riesgos de la información.

4.3.2. Limitaciones de la investigación

A continuación, se presentan las principales limitaciones de la investigación. Una de las mayores limitaciones fue la dificultad de aplicar los instrumentos en forma presencial para la totalidad de la muestra; debido a que la población estuvo conformada por los docentes y administrativos de la Facultad de Ciencias de la UNASAM, y los docentes tienen un horario muy variado, y se optó conveniente aplicarlo de forma virtual, para lo cual se tuvo que virtualizar el instrumento, distribuirlos por sus correos institucionales y números de contactos. Asimismo, debido a que aún no está superado la pandemia del virus de Covid-19 en su totalidad, exigió la aplicación virtual del instrumento.

Otra limitación de la investigación fue la obtención de datos, debido a que la respuesta del cuestionario estuvo en la consideración de cada docente, por ello fue tardado la obtención de los datos. En cuanto a los antecedentes también se tuvo limitaciones ya que no encontramos muchas investigaciones enmarcadas a correlacionar las variables como lo son las Políticas de Seguridad y Riesgos de la Información

CONCLUSIONES

- Mediante la presente investigación se llegó a concluir que existe una relación inversamente proporcional entre Políticas de Seguridad y Riesgos de la Información en la Facultad de Ciencias de la UNASAM, en consecuencia, de los resultados obtenidos con Rho de Spearman de (-0.422**). Y la significancia se determina por la correlación rho de Spearman p = 0.003 y cuyo valor de p < 0.05; Por lo tanto, existe relación significativa.
- Mediante la presente investigación se corrobora que existe una relación inversamente proporcional entre Políticas de Seguridad y análisis de riesgos de la información, por el cual se llegó a la conclusión de que al contar con una buena política de seguridad los riesgos de los activos de información van a disminuir proporcionalmente.
- La investigación demostró que existe una relación inversamente proporcional entre Políticas de Seguridad y evaluación de riesgos de la Información, en consecuencia, de los resultados obtenidos con Rho de Spearman de (-0.302). Y la significancia se determina por la correlación rho de Spearman p = 0.037 y cuyo valor de p < 0.05; Por lo tanto, existe relación significativa.
- La investigación demostró que existe una relación inversamente proporcional entre Políticas de Seguridad y tratamiento de riesgos de la Información, ya que en nuestro resultado obtuvimos un p = 0.040 con Rho de Spearman de (-0.297). Y la significancia se determina por la correlación rho de Spearman p = 0.040 y cuyo valor de p < 0.05; Por lo tanto, existe relación significativa.

RECOMENDACIONES

- Mientras se cuente con buenas Políticas de la Seguridad se reducirán los Riesgos de la Información. Motivo por el cual el cual la alta dirección de las Instituciones mediante el área de tecnologías de la información debe reforzar la importancia de logar los objetivos estratégico, correspondientes a la seguridad de la información mediante la implementación y mejora continua de las políticas de la seguridad enfocados en las buenas prácticas de seguridad y un modelo de gestión de riesgos
- Las Políticas de Seguridad y análisis de riesgos de las informaciones relacionan inversamente proporcional de la cual inferimos que mientras se cuente con buenas Políticas de la Seguridad se reducirán los costos del análisis de riesgos de la información. Motivo por el cual el cual se recomienda que implemente una política de seguridad mediante la evaluación de las distintas mitologías de que existen para gestionar los riesgos con la cual se garantizan la protección de la información plasmados en las políticas.
- A la luz de los resultados, es necesario seguir investigando acerca de los modelos y normativas con certificaciones que actualmente existen para la gestión de riesgos de la información como los son la ISO 3100, ISO 27000 entre otros, que son una guía en la que nos dan pautas de cómo gestionar, analizar, evaluar y tartar los riesgos. Y que estas estén plasmadas dentro de una política en la que este comprometido la alta gerencia y los trabajadores que hacen manejo de la información dentro de la Institución.

REFERENCIAS BIBLIOGRÁFICAS

Bustamante, S. (2021). Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú. [Tesis de titulación, Universidad Peruana Unión]. https://doi.org/10.29019/enfoqueute.743

Cordero, M. (2022). Políticas de seguridad de la información basadas en Normas internacionales para garantizar controles ante Amenazas y vulnerabilidades en el departamento de Tecnología de la cooperativa de ahorro y crédito san Francisco ltda. [Tesis de titulación, Universidad técnica de Ambato]. https://repositorio.uta.edu.ec/bitstream/123456789/34814/1/t1959si.pdf

Ramirez, J. y Rodriguez, A. (2019). Seguridad de la información y la gestión de riesgos en los centros de cómputo de la Universidad Nacional del Callao, 2019. [Tesis de grado, Universidad César Vallejo]. https://hdl.handle.net/20.500.12692/49143

Álvares, W. y Llulluna, J. (2021). Diseño de una política de seguridad de la información para la Dirección de Tecnologías de la Información de la Universidad Técnica de Cotopaxi, basado en la Norma ISO 2700. [Tesis de titulación, Universidad Técnica de Cotopaxi]. http://repositorio.utc.edu.ec/handle/27000/8719

Vega, W. (2008). Políticas y seguridad de la información. Fides et Ratio - Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia, 2(2), 63-69. http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008&lng=es&tlng=es.

Noreña, D. (2018). Estrategia de seguridad de Estados Unidos y España [Archivo PDF]. https://repositorio.ulima.edu.pe/bitstream/handle/20.500.12724/7419/Nore%C3%B1a_%20seguridad_internacional.pdf?sequence=1&isAllowed=y

INACAL. (2017). Norma Técnica Peruana NTP-ISO/IEC 27002 Tecnología de la información. Código de prácticas para controles de seguridad de la información

De Freitas, V. (2009). Análisis y evaluación del riesgo de la información. http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1690-75152009000100004&lng=es&tlng=es

Whiting, K. (2022). Informe de Riesgos Globales 2022: Lo que necesitas saber. Foro Económico Mundial. https://es.weforum.org/agenda/2022/02/informe-de-riesgos-globales-2022-lo-que-debes-saber/

Hernández R., Fernández C. y Baptista P. (2010). Metodología de la investigación. (Quinta Edición).

Rodríguez S., (2003). Paradigmas, enfoques y métodos en la investigación educativa. Investigación Educativa. Vol 7 N°. 12. p 23-40. https://revistasinvestigacion.unmsm.edu.pe/index.php/educa/article/view/8177/7130

Hsu, C. T. Wang, and A. Lu, "The impact of ISO 27001 certification on firm performance," Proc. Annu. Hawaii Int. Conf. Syst. Sci., vol. 2016-March, pp. 4842–4848, 2016, doi: 10.1109/HICSS.2016.600.

Buenaño (2013). Análisis y solución de las vulnerabilidades de la seguridad informática y seguridad de la información de un medio de comunicación audio-visual.

Figueroa, J., Rodríguez, R., Bone, C. (2018). La seguridad informática y la seguridad de la información. Polo del Conoc., vol. 2, no. 12, p. 145. doi: 10.23857/pc.v2i12.420.

Alvarado, R., Acosta C. y Mata de buonaffina Y. (2018). Necesidad de los sistemas de información gerencial para la toma de decisiones en las organizaciones. InterSedes, vol. XIX, núm. 39, pp. 17-31, 2018. https://www.redalyc.org/journal/666/66658188002/html/

Pirani. (s/f). Estudio de Gestión de Riesgos 2022. Piranirisk.com. https://www.piranirisk.com/es/academia/especiales/estudio-de-gestion-de-riesgos-en-latinoamerica-2022

ANEXOS

MATRIZ DE CONSISTENCIA

Título	Problema de la investigación	Objetivos de la investigación	Hipótesis de la investigación	Método
	Problema general	Objetivo general	Hipótesis general	
"Políticas de seguridad y riesgos de la información en la Facultad de Ciencias de la Universidad Nacional Santiago Antúnez de Mayolo, Huaraz-2022"	¿Qué relación existe entre Políticas de Seguridad y Riesgos de la Información en la Facultad de Ciencias de la UNASAM?	Determinar la relación que existe entre Políticas de Seguridad y Riesgos de la Información en la Facultad de Ciencias de la UNASAM	Existe una relación significativa entre Políticas de Seguridad y Riesgos de la Información en la Facultad de Ciencia de la UNASAM	Tipo de investigación Correlacional Diseño de investigación No experimental Enfoque Cuantitativo Población: 93 (administrativos y docentes) Muestra: 48 (administrativos y docentes) Técnica Encuesta Instrumentos Cuestionario Método de análisis Análisis descriptivo e inferencial, SPSS26
	Problemas específicos	Objetivos específicos	Hipótesis específica	
	¿Qué relación existe entre Políticas de Seguridad y el análisis de riesgos de la información en la Facultad de Ciencias de la UNASAM?	Determinar la relación que existe entre Políticas de Seguridad y el análisis de riesgos de la información en la Facultad de Ciencias de la UNASAM	Existe una relación significativa entre Políticas de Seguridad y el análisis de riesgos de la información en la Facultad de Ciencias de la UNASAM	
	¿Qué relación existe entre Políticas de Seguridad y la evaluación de riesgos de la información en la Facultad de Ciencias de la UNASAM?	Determinar la relación que existe entre Políticas de Seguridad y la evaluación de riesgos de la información en la Facultad de Ciencias de la UNASAM	Existe una relación significativa entre Políticas de Seguridad y la evaluación de riesgos de la información en la Facultad de Ciencias de la UNASAM	
	¿Qué relación existe entre Políticas de Seguridad y el tratamiento de riesgos de la información en la Facultad de Ciencias de la UNASAM?	Determinar la relación que existe entre Políticas de Seguridad y el tratamiento de riesgos de la información en la Facultad de Ciencias de la UNASAM	Existe una relación significativa entre Políticas de Seguridad y el tratamiento de riesgos de la información en la Facultad de Ciencias de la UNASAM	

Fuente: Elaboración propia

Comparativa de las diferentes metodologías

Criterio / Metodología	Idioma	Enfoque	Procesos de gestión de riesgos	Apoyo de uso	Ayuda a la implementación	Elementos	Acceso	Tipos de empresa	Tipo de análisis	Complejidad
ISO 31000:2018	Español	General	Cuenta con la mayoría de los procesos principales	Documentación general de la norma	Plan de proyecto, técnicas, cuestionarios	Activos, recursos, amenazas, vulnerabilidades y controles	Pago	Mayoría de las empresas	Cualitativo y cuantitativa	Media
MARGERIT	Español	Seguridad de la información	Cuenta con la mayoría de los procesos principales	Cuenta con guías de apoyo en la implementación	Plan de proyecto, técnicas, roles, cuestionarios	Activos, amenazas y controles	Libre	Medianas y grandes	Cualitativo y cuantitativa	Media
OCTAVE	Ingles	Seguridad de la información	Cuenta con la mayoría de los procesos principales	Cuenta con guías de apoyo en la implementación	Plan de proyecto, técnicas, roles, cuestionarios	Procesos, activos, recursos, vulnerabilidades, amenazas y controles	Algunos materiales restringidos	Medianas y grandes	Cualitativo	Media
CRAMM	Ingles	Seguridad de la información	Cuenta con la mayoría de los procesos principales	Documentación general de la norma	Plan de proyecto, técnicas, roles, cuestionarios	Activos, procesos, amenazas, vulnerabilidades y controles	Pago	Medianas y grandes	Cualitativo	Media
ISO/IEC 27005:2018	Español	General	Cuenta con la mayoría de los procesos principales	Cuenta con guías de apoyo en la implementación	Plan de proyecto, técnicas, cuestionarios	Activos, recursos, amenazas, vulnerabilidades y controles	Pago	Mayoría de las empresas	Cualitativo y cuantitativa	Media

Fuente: Elaboración propia

Instrumento I: Estadísticas de total de elemento

	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Correlación múltiple al cuadrado	Alfa de Cronbach si el elemento se ha suprimido
Es importante el compromiso o acuerdo de confidencialidad, por medio del cual todo personal vinculado a la Institución se comprometa a usar la información de manera reservada, no divulgarla o hacer revelación a terceros.	30,90	8,095	,351	,613	,879
Es importante contar con controles de acceso a los ambientes, equipos y sistemas de cómputo dentro de la Institución	31,10	7,117	,612	,470	,850
El personal debe recibir capacitaciones para comprender las mejores prácticas para resguardar datos confidenciales, para protegerse y proteger a la Institución contra ataques	30,96	7,360	,671	,637	,842
Toda información verbal, física o electrónica deben ser procesadas integralmente y exclusivamente por las personas autorizadas, sin modificaciones ni alteraciones, salvo que así lo determinen las personas responsables de dicha información.	30,96	7,445	,638	,568	,846
Es importante contar con permisos y autenticación del usuario, la seguridad de la red, copias de seguridad, encriptación y continuidad del negocio y un personal capacitado para administrar los permisos.	31,04	7,190	,781	,644	,830
Es importante resguardar la información en medios seguros, proteger de cualquier perdida y modificación no autorizada.	30,90	7,500	,668	,513	,843

Es importante que la información esté disponible en el momento oportuno para el cumplimiento de mis labores dentro de la Institución.	30,77	7,755	,574	,701	,853
Realizar mantenimiento a los equipos, mantener el software actualizado, así como crear respaldos, garantizan la disponibilidad de la red y los datos a los usuarios autorizados.	30,85	7,446	,687	,744	,841

Fuente: Software SPSSv26

Instrumento II: Estadísticas de total de elemento

	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Correlación múltiple al cuadrado	Alfa de Cronbach si el elemento se ha suprimido
Existe algún sistema de control de inventario de los activos (Software, hardware, documentación, datos del personal, etc.) de la Institución	41,15	58,425	,293	,492	,820
La alta dirección capacita al personal sobre la clasificación de los activos de información (Información contenida en cada activo) más críticos en la Institución.	41,33	53,504	,669	,634	,797
Puedo identificar las amenazas internas y externas a las que están expuestas los activos de información a mi cargo.	41,15	55,489	,522	,630	,806
Utilizo algún formato o instrumento para identificar y registrar las amenazas de manipulación de información.	41,21	56,509	,464	,538	,810
Puedo identificar las amenazas o peligros a las que están expuestos los equipos, sistemas de información y los datos de alto valor que tengo a mi cargo.	41,12	53,048	,615	,728	,799
Considero que mi información está vulnerable a los hackers o la alteración por personas no autorizadas.	40,79	56,424	,416	,739	,813
Realizan monitoreos a los equipos informáticos y de redes para identificar las posibles vulnerabilidades y debilidades.	41,31	59,453	,289	,644	,819
Realizan capacitaciones sobre información confidencial (privada) y su alto valor para la Institución	41,04	56,211	,411	,623	,813
Realizan capacitaciones sobre el valor económico y su relevancia de los activos de información que están a mi cargo	40,96	51,828	,582	,778	,800
Cuando se identifica una amenaza es detectada a tiempo	40,94	52,783	,623	,757	,798
La existencia de cada amenaza aumenta la probabilidad de riesgo	40,62	54,750	,593	,768	,802

El riesgo se puede determinar de acuerdo al impacto que tendrá sobre los objetivos de la organización (como el presupuesto, el cronograma y la tecnología)	40,42	55,652	,593	,538	,803
Existen controles ante un problema fuga o perdida de información actualmente en la Institución.	41,42	60,504	,190	,461	,825
Existe un proceso disciplinario para incidentes de violación de la privacidad, piratería informática, fraude por parte de los trabajadores	41,54	63,488	-,040	,506	,836
La institución cuenta o contrata a expertos en temas de seguridad para identificar y elaborar controles para el tratamiento del riesgo identificado.	41,62	59,856	,191	,475	,826
La institución cuenta o contrata a expertos en temas de seguridad para implementar los controles y reducir los riesgos de la información.	41,81	57,475	,369	,543	,815

Fuente: Software SPSSv26

INSTRUMENTO DE RECOLECCIÓN DE DATOS.

ENCUESTA I

I. INTRODUCCIÓN: A continuación, se presentan un conjunto de preguntas orientados a medir la variable política de seguridad en la Facultad de Ciencias de la UNASAM

II. INSTRUCCIONES: La encuesta está estructurada en dos (2) partes. En la primera, debe colocar el cargo que ocupa en la Facultad de Ciencias, edad en años, sexo y Tiempo que labora en la Facultad. En la segunda, debe indicar su respuesta ante cada planteamiento, haciendo uso de una escala del 1 al 5, donde 1 representa "Totalmente en desacuerdo" y 5 representa "Totalmente de acuerdo".

III. ENCUESTA

3.1. Datos del cliente

Cargo: 1. Administrativo ( ), 2. Docente ( )

Edad:____Años

Sexo: 1. Masculino ( ), 2. Femenino ( )

Tiempo que labora en la Facultad: ____Años

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

3.2. Formulaciones

N°	Ítems	Escala				
		1	2	3	4	5
1	Es importante el compromiso o acuerdo de confidencialidad, por medio del cual todo personal vinculado a la Institución se comprometa a usar la información de manera reservada, no divulgarla o hacer revelación a terceros.	1	2	3	4	5
2	Es importante contar con controles de acceso a los ambientes, equipos y sistemas de cómputo dentro de la Institución	1	2	3	4	5
3	El personal debe recibir capacitaciones para comprender las mejores prácticas para resguardar datos confidenciales, para protegerse y proteger a la Institución contra ataques	1	2	3	4	5
4	Toda información verbal, física o electrónica deben ser procesadas integralmente y exclusivamente por las personas autorizadas, sin modificaciones ni alteraciones, salvo que así lo determinen las personas responsables de dicha información.	1	2	3	4	5
5	Es importante contar con permisos y autenticación del usuario, la seguridad de la red, copias de seguridad, encriptación y continuidad del negocio y un personal capacitado para administrar los permisos.	1	2	3	4	5
6	Es importante resguardar la información en medios seguros, proteger de cualquier perdida y modificación no autorizada.	1	2	3	4	5
7	Es importante que la información esté disponible en el momento oportuno para el cumplimiento de mis labores dentro de la Institución.	1	2	3	4	5
8	Realizar mantenimiento a los equipos, mantener el software actualizado, así como crear respaldos, garantizan la disponibilidad de la red y los datos a los usuarios autorizados	1	2	3	4	5

ENCUESTA II

I. INTRODUCCIÓN: A continuación, se presentan un conjunto de preguntas orientados a medir la variable riesgos de la información en la Facultad de Ciencias de la UNASAM

Los activos de la Facultad son muy valiosos, ya que son los recurso que utilizan para el manejo y almacenamiento de la información y gestionar los riesgos de pérdida de dicha información es muy importante para que las instituciones funciones y evitar pérdidas económicas.

I. INSTRUCCIONES: Debe indicar su respuesta ante cada planteamiento, haciendo uso de una escala del 1 al 5, donde 1 representa "Nunca" y 5 representa "Siempre".

II. ENCUESTA

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

2.1. Formulaciones

N°	Ítems	Escala				
		1	2	3	4	5
1	Existe algún sistema de control de inventario de los activos (Software, hardware, documentación, datos del personal, etc.) de la Institución	1	2	3	4	5
2	La alta dirección capacita al personal sobre la clasificación de los activos de información (Información contenida en cada activo) más críticos en la Institución	1	2	3	4	5
3	Puedo identificar las amenazas internas y externas a las que están expuestas los activos de información a mi cargo	1	2	3	4	5
4	Utilizo algún formato o instrumento para identificar y registrar las amenazas de manipulación de información	1	2	3	4	5
5	Puedo identificar las amenazas o peligros a las que están expuestos los equipos, sistemas de información y los datos de alto valor que tengo a mi cargo	1	2	3	4	5
6	Considero que mi información está vulnerable a los hackers o la alteración por personas no autorizadas	1	2	3	4	5
7	Realizan monitoreos a los equipos informáticos y de redes para identificar las posibles vulnerabilidades y debilidades.	1	2	3	4	5
8	Realizan capacitaciones sobre información confidencial (privada) y su alto valor para la Institución	1	2	3	4	5
9	Realizan capacitaciones sobre el valor económico y su relevancia de los activos de información que están a mi cargo	1	2	3	4	5
10	Cuando se identifica una amenaza es detectada a tiempo	1	2	3	4	5
11	La existencia de cada amenaza aumenta la probabilidad de riesgo	1	2	3	4	5
12	El riesgo se puede determinar de acuerdo al impacto que tendrá sobre los objetivos de la organización (como el presupuesto, el cronograma y la tecnología)	1	2	3	4	5
13	Existen controles ante un problema fuga o perdida de información actualmente en la Institución.	1	2	3	4	5
14	Existe un proceso disciplinario para incidentes de violación de la privacidad, piratería informática, fraude por parte de los trabajadores	1	2	3	4	5
15	La institución cuenta o contrata a expertos en temas de seguridad para identificar y elaborar controles para el tratamiento del riesgo identificado.	1	2	3	4	5
16	La institución cuenta o contrata a expertos en temas de seguridad para implementar los controles y reducir los riesgos de la información.	1	2	3	4	5

LINK DE LOS INSTRUMENTOS VIRTUALIZADOS

https://forms.gle/qCvi1uMxtw9VmHFEA