ESCUELA DE POSGRADO Y ESTUDIOS CONTINUOS

EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA GESTIÓN DE RIESGOS EN EL ÁREA INFORMÁTICA DE UNA UNIVERSIDAD PÚBLICA, REGIÓN CAJAMARCA 2020.

Tesis para optar el grado de **MAESTRO** en:

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN GERENCIA DE SISTEMAS DE INFORMACIÓN

Autora:

Sarita Morelia Narro Mestanza

Asesor:

Doctor. Pedro Segundo Castañeda Vargas

Cajamarca – Perú

2021

Resumen

La presente investigación estuvo conformada por los 10 colaboradores, teniendo como objetivo establecer cómo el Sistema de Gestión de Seguridad de la Información se relaciona con la Gestión de Riesgos en el área de Informática de una Universidad Pública en la Región Cajamarca, la técnica que se utilizó para la recolección de datos fue la encuesta, la misma que contó con el instrumento denominado ficha de encuesta para cada una de las variables, la cual estuvo diseñada a través de la escala de Likert con 3 niveles de respuesta (Siempre, A veces y Nunca). Para la variable Sistema de Gestión de Seguridad de la Información estuvo conformada por 65 preguntas y en el caso de la variable Gestión de Riesgos por 18 preguntas.

La investigación se apoyó en el enfoque cuantitativo, de diseño no experimental, transeccional, correlacional. El análisis de confiabilidad arrojó como resultado el Alpha de Cronbach de 96.1% para la variable Sistema de Gestión de Seguridad de la Información y 78.7% para la variable Gestión de Riesgos. Se utilizó el software SPSS y la herramienta Excel, a través de la prueba de hipótesis presentando como resultado un nivel de significancia de 0.76 donde el valor indicado es mayor a 5%.

Se concluyó que el Sistema de Gestión de Seguridad de la Información no se relaciona de manera inversa con la Gestión de Riesgos en el área informática de una Universidad Pública, Región Cajamarca 2020.

Palabras clave**:** Sistema de Gestión de Seguridad de la Información, SGSI, Gestión de Riesgos, Riesgo.

Abstract

This research aims to establish how the Information Security Management System is related to Risk Management in the computing area of a Public University, Cajamarca 2020 Region.

The population and sample of the research was made up of the 10 collaborators to establish how the Information Security Management System is related to Risk Management in the Computing area of a Public University in the Cajamarca Region, the technique that used for data collection was the survey, the same that had the instrument called the survey card for each of the variables, which was designed using the Likert scale with 3 levels of response (Always, Sometimes and Never). For the variable Information Security Management System it was made up of 65 questions and in the case of the Risk Management variable, 18 questions.

The research was supported by the quantitative, non-experimental, transectional, correlational approach. The reliability analysis resulted in Cronbach's Alpha of 96.1% for the variable Information Security Management System and 78.7% for the Risk Management variable. The SPSS software and the Excel tool were used, through the hypothesis test, presenting as a result a significance level of 0.76 where the indicated value is greater than 5%.

It was concluded that the Information Security Management System is not inversely related to Risk Management in the computing area of a Public University, Cajamarca 2020 Region.

Key words: Information Security Management System, ISMS, Risk Management, Risk.

.

Dedicatoria

A Dios por haberme brindado la vida, la fuerza, la salud y la sabiduría para poder cumplir mis objetivos y sueños.

A mis padres Elvia y Ruvén que son mi motor, por apoyarme en cada paso, por sus consejos y la educación que me han brindado.

A mi mamita Melchora que, aunque no se encuentre presente físicamente siempre vivirá en mi corazón y recuerdos.

Agradecimiento

A mis asesores Dr. Pedro Segundo Castañeda Vargas y MBA Juan Carlos Llaque Quiroz por su orientación en la realización de mi Tesis. Al Ing. Walter Pérez Estrada; Director de la Oficina de Sistemas Informáticos y Plataformas Virtuales por brindarme las facilidades para el acceso a la información.

Tabla de contenidos

Índice de figuras

Índice de tablas

I. INTRODUCCIÓN

I.1 Realidad Problemática

En la llamada era de la información o era digital, el mundo está globalmente conectado, donde los países ricos generan riqueza a través de la información; es por ello que, hoy en día, cualquier organización tiene que gestionar sus datos, almacenarlos y sobre todo protegerlos. En mención a lo anterior, las organizaciones están constantemente analizando y gestionando información, debido a los grandes avances tecnológicos éste gran valor ya no se almacena solamente en archivadores de papel, sino que también en dispositivos tales como: pendrive, discos duros o la propia “nube”.

Las diversas organizaciones gestionan una gran cantidad de información, ya sean datos sobre sus cuentas, sobre sus trabajadores, proveedores, clientes, entre otros; estos datos, están continuamente sometidos a amenazas, por lo tanto, es de vital importancia que se garantice su seguridad y correcta gestión. Por lo que, para hacer frente a estas amenazas se deben establecer una serie de protocolos o políticas de seguridad, que son distintas dependiendo de las necesidades de la organización. (Shaw, 2018/2019)

A nivel nacional, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) ha pasado de ser utilizado no sólo en gran porcentaje en entidades privadas; sino también en las públicas, esta última ha impulsado una serie de normativas y directrices, basadas principalmente en la norma estándar internacional ISO/IEC 27001, la misma que está claramente enfocada en la gestión de riesgos que se puedan presentar en una organización. Tras la obligatoriedad en el cumplimiento de la implementación de un SGSI, se encuentra principalmente la necesidad de contar con organizaciones más robustas en cuanto a temas de manejo de información, tanto física como digital; esperando establecer procesos adecuados, controles de seguridad y personal capacitado para enfrentar los riesgos que puedan presentarse. (Arana, 2016)

La falta de un ente que regule, controle y capacite en temas relacionados a la Implementación de un Sistema de Seguridad de la Información, ha generado muchas falencias en la correcta gestión de riesgos en las diversas áreas de las entidades públicas; tal como lo muestra la Encuesta Global de Seguridad de la Información realizada por EY Latinoamérica donde demuestra que en el Perú el 90% de las organizaciones encuestadas indican que el manejo relacionado a la seguridad de la información no satisface completamente los requerimientos de su organización. (Cama, 2017)

En la Región Cajamarca diversas organizaciones han implementado diversas tecnologías que han servido de apoyo a los diversos procesos y a la obtención de información; sin embargo, se dejó de lado todo los que involucraba la seguridad de los datos, así como al capital humano que maneja la misma, estando todo el tiempo expuestos a amenazas o

vulnerabilidades que generan principalmente la pérdida de información. López (2015), indicó que al momento de que una organización sufre un fallo de seguridad, la información dañada no siempre es recuperable; ocasionando así daños en la economía, en el funcionamiento regular de la organización en incluso un gran daño en la imagen de la misma.

En la actualidad existen 5 universidades en la Región Cajamarca de las cuales tres son públicas y dos privadas, cuyas diferencias en cuanto al manejo de información son abismales, tal es así que, solamente una de ellas; la Universidad Privada Antonio Guillermo Urrelo ha realizado una investigación sobre ciertos riesgos que podrían surgir y afectar la confidencialidad, disponibilidad e integridad de la información existente dentro de su Departamento de Admisión y registro Académico (DARA) (Vásquez Atalaya, 2016) dando esto una clara visión de la precaria importancia que las demás universidades le dan a estos temas.

El área informática de la Universidad Pública en estudio, es la encargada de dar soporte con Tecnología de la Información a los procesos vitales de las Dependencias de la Universidad, para contribuir de manera eficiente y efectiva al proceso Académico y Administrativo; garantizando el correcto manejo de la información, sin embargo debido a diversos factores como la ausencia de un plan de capacitación institucional donde contemple la capacitación especializada del personal de informática, resistencia de los usuarios al cambio tecnológico, transiciones de mandatos, entre otros; ha sido difícil poder gestionar de manera adecuada los riegos presentes en el desarrollo de las actividades.

Por otro lado, si bien el área cuenta con normas y procedimientos en Tecnologías de Información basadas en las buenas prácticas, que han permitido contribuir al desarrollo de una cultura informática y un buen desempeño de actividades y gestión de la organización, no ha sido suficiente para poder afrontar los riesgos que pueden atacar a sus activos en la actualidad; ya que tras realizar un diagnóstico inicial en la implementación del SGSI se observó que a pesar de contar con un respaldo del 95% de información crítica, la materialización de alguna amenaza sobre los activos generaría la pérdida del 70 % de información crítica y por ende, el no funcionamiento de los procesos y actividades vitales.

Finalmente, en mención a lo anterior, la presente investigación está enfocada en el estudio de dos variables: por un lado, el Sistema de Seguridad de la Información (SGSI) y por otro lado la Gestión de Riesgos, que permiten la disponibilidad, confidencialidad e integridad del activo más importante como lo es la información que se maneja, logrando así salvaguardarla y estar preparados frente a cualquier riesgo que se presente en el futuro.

I.2 Pregunta de Investigación

¿Cómo el Sistema de Gestión de Seguridad de la Información se relaciona con la Gestión de Riesgos en el área informática de una Universidad Pública, Región Cajamarca 2020?

I.2.1 Problemas Específicos

- ¿Qué dimensión del Sistema de Gestión de Seguridad de la Información tiene mayor relevancia en el área informática de una Universidad Pública, Región Cajamarca 2020?
- ¿Qué dimensión de la Gestión de Riesgos tiene mayor relevancia en el área informática de una Universidad Pública, Región Cajamarca 2020?
- ¿Cómo el Sistema de Gestión de Seguridad de la Información se relaciona con cada una de las dimensiones de la Gestión de Riesgos en el área informática de una Universidad Pública, Región Cajamarca 2020?

I.3 Objetivos de la Investigación

I.3.1 Objetivo General

Determinar la relación existente entre el Sistema de Gestión de Seguridad de la Información y la Gestión de Riesgos en el área informática de una Universidad Pública, Región Cajamarca 2020.

I.3.2. Objetivos Específicos

- Identificar la dimensión del Sistema de Gestión de Seguridad de la Información que tiene mayor relevancia en el área informática de una Universidad Pública, Región Cajamarca 2020.
- Identificar la dimensión de la Gestión de Riesgos que tiene mayor relevancia en el área informática de una Universidad Pública, Región Cajamarca 2020.
- Identificar la relación entre el Sistema de Gestión de Seguridad de la Información y cada una de las dimensiones de la Gestión de Riesgos en el área informática de una Universidad Pública, Región Cajamarca 2020.

I.4 Justificación de la Investigación

Diariamente el área de informática de una Universidad Pública, recibe y gestiona información, tanto física como digital, ante la falta de directrices y normas relacionadas a la seguridad de la información, el desconocimiento de temas relacionados con la seguridad de la información y la poca capacitación hacia los colaboradores; es de suma importancia contar con un Sistema de Gestión de la Información robusto y de fácil manejo; que cualquier entidad, ya sea pública o privada puede utilizar para así evitar la pérdida o robo de información importante para el funcionamiento de la misma. La implementación y periódica evaluación de dicha metodología puede actuar como un factor importante para lograr la gestión eficaz y adecuada de la información.

En la actualidad, al hablar de información, no sólo se hace referencia a ciertos datos o a documentos físicos, sino también digitales; los mismos que en conjunto son el eslabón principal en el funcionamiento de cualquier organización, independientemente de la actividad que realicen o rubro al que pertenezcan; es así que, cuando la información ingresa

y sale de cualquier organización, representa la oportunidad de generar ventaja frente a otras si es bien gestionada, apoyando a la toma de decisiones para el logro de objetivos. Por otro lado, esta información se ve muchas veces amenazada por la existencia de riesgos y amenazas que comprometen la seguridad de los datos manejados por la empresa, adicionado a eso se suma que la digitalización e implementación de herramientas de Tecnología de la Información abrió la puerta a ataques cibernéticos; lo que ha obligado a que las organizaciones evolucionen y se adapten constantemente, creando e implementando métodos que contribuyan a la seguridad de la información, por ende a la protección de datos sensibles. (F. M. Arévalo, 2017)

Respecto a la justificación teórica, contribuirá a fundar la relación existente entre la Gestión de Riesgos según la NTP-ISO 31000:2018 y el Sistema de Gestión de Seguridad de la Información según la norma ISO27001; permitiendo así poder tener un mayor conocimiento en el aseguramiento de la información y su relación con los riesgos, disminuyendo así las consecuencias para la entidad, implementación y monitorización de controles.

Respecto a la justificación práctica, si bien es cierto existen estudios referentes a la relación existente en ambas variables de esta investigación, estas han sido en su mayoría realizadas en entidades privadas y públicas, sin embargo, en su minoría son universidades, por lo que, la presente investigación servirá como antecedente para otras universidades con realidades similares, logrando así reducir el riesgo de que se produzca pérdidas de información en el área informática de alguna Universidad Pública en la Región Cajamarca; estableciéndose una metodología gracias a la cual se puede gestionar la seguridad de la información de manera periódica y dinámica; fomentando de este modo el cumplimiento las metas y objetivos establecidos, así como la mejora de procesos y mejora de la imagen institucional de la entidad frente a otras Universidades Públicas a nivel nacional.

I.5 Alcance de la Investigación

El alcance de la presente investigación es descriptivo correlacional. Descriptivo porque se pretende recoger información de manera individualizada de cada una de las variables estudiadas, y correlacional porque se pretende conocer la relación entre el Sistema de Gestión de Seguridad de la Información y la Gestión de Riesgos en el área informática de una Universidad Pública, Región Cajamarca 2020.

Los resultados podrán ser utilizados como referencia a las áreas informáticas de Universidades Públicas a nivel nacional.

II. MARCO TEÓRICO

II.1 Antecedentes

(Acosta Ubaque & León Patiño, 2017) en su trabajo de investigación internacional titulado *"Diseño del Sistema de Gestión de Seguridad de la Información (S.G.S.I.) para el Centro De Datos De La Personería de Bogotá D.C. bajo las normas NTC ISO-IEC 27001:2013 y NTC-ISO-IEC 27002:2013"* plantearon que con el SGSI se pretende realizar un manejo adecuado de la seguridad de la entidad, donde además se toma en cuenta la gestión de riesgos; realizándose un análisis de los existentes en los servicios, infraestructura y aplicativos que representan y almacenan toda la información, que es esencial para el funcionamiento de la entidad, si bien el objetivo principal de la presente investigación es contar con un Sistema de Gestión de Seguridad de la Información periódicamente evaluado y actualizado, que contribuya a reducir los riesgos existentes en la personería de Bogotá, sino que también se busca establecer una relación entre la implementación del SGSI y la identificación de riesgos, amenazas y vulnerabilidades a los que están expuestos los activos, para su oportuno tratamiento y oportuna respuesta frente algún incidente de seguridad; concluyendo que tras el reconocimiento de las amenazas y definición de responsables, entre otros; se establece la existencia de una relación entre las normas y directrices sobre el tratamiento de los riesgos y el SGSI, siendo el primero una de las piedras angulares para la construcción del SGSI institucional.

(Perafán Ruiz & Caicedo Cuchimba, 2016) en su trabajo de investigación internacional titulado "Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca" plantearon que es importante que dentro de sus procesos existan buenas prácticas que permitan la protección de datos, por lo que es necesario llevar a cabo una evaluación de los riesgos en la seguridad de la información en cada uno de los activos de información, donde además se tiene en cuenta que la gestión de los riesgos presentan una relación estrecha de colaboración con el SGSI, ya que facilita el continuo monitoreo a través de auditorías y de la mejora continua. Finalmente, la presente investigación demuestra que en la existencia de un Sistema de Gestión de Riesgos, existen controles y políticas de seguridad de la información, y estos pueden ser tomados como soporte para la implementación futura de un SGSI más robusto.

(Ñañez Campos, 2019) en su trabajo de investigación nacional titulado "*Modelo de Gestión de Riesgos De TI Basados En La Norma ISO/IEC 27005 Y Metodología Magerit para mejorar la Gestión de Seguridad de la Información en la Universidad Nacional Toribio Rodríguez de Mendoza - Chachapoyas Perú*" planteó que al momento de la implementación de un SGSI se consideran actividades y tareas que abarcan según la ISO/IEC 27001 desde la planeación de su alcance hasta los planes de mejora continua, sin embargo el factor crítico a tomar en cuenta es la gestión de riesgos y su relación existente con el SGSI en sí, debido a esto la presente investigación se centró en el desarrollo de la gestión de riesgos de TI

para mejorar la gestión de seguridad de la información. Por lo que, la presente investigación concluye que la aplicabilidad de la gestión de riesgos de TI debe estar en relación con el sistema de seguridad de la información con la finalidad de asegurar la continuidad de los procesos académicos y administrativos críticos de la universidad; además recomienda mantener una periódica revisión de las políticas del SGSI para poder evaluar el cumplimiento de las mismas por parte del personal encargado de la seguridad y a la vez la efectividad de los riesgos de TI relacionados con el SGSI.

(Huayllani Muñoz, 2019) en su trabajo de investigación nacional titulado *"Sistema de gestión de seguridad de la información y la gestión del riesgo en el Ministerio de Salud, 2019"* planteó que el Ministerio de Salud cuenta con una reciente implementación de un Sistema de Gestión de Seguridad de la Información, así como con un Sistema de Gestión de Riesgos; sin embargo no existía una idea clara de los alcances que dichas implementaciones poseen, esto debido a que no se había realizado una evaluación de como el funcionamiento de uno estaba relacionado o no al funcionamiento del otro. Así mismo, la autora menciona que otro de los puntos a determinar es la relación que pueda existir entre estos dos sistemas, con la finalidad de contar con una base teórica más amplia del comportamiento en conjunto o por separado y así poder manejar de manera más eficiente y eficaz el activo más importante de cualquier entidad pública o privada: la información. Tras la evaluación y análisis se concluyó que existe una relación significativa y positiva entre las dos variables de estudio, y a la vez se recomienda evaluaciones periódicas de ambos sistemas con la flexibilidad necesaria para que cada sistema cumpla sus objetivos.

(Jara Mendoza, 2018) en su trabajo de investigación nacional titulado *"Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018",* realizado en la Municipalidad Distrital de Carabayllo, se planteó que es necesario contar con información de calidad para la toma de decisiones, así como asegurar la disponibilidad, confidencialidad e integridad de la misma, por lo que el objetivo de la investigación es establecer la correlación existente entre el SGSI y el proceso de gestión de riesgo, como la funcionalidad de ambas permitan salvaguardar los activos de información, por lo que se concluye tras evidencias estadísticas la existencia de una correlación significativa entre ambas variables lo que permite que la gerencia de la Municipalidad defina de manera oportuna los controles para el tratamiento de riesgos según su criticidad.

(Vásquez Atalaya, 2016) en su trabajo de investigación local titulado "Propuesta de un Sistema de Seguridad de la Información para la Oficina de Admisión y Registro Académico de la Universidad Privada Antonio Guillermo Urrelo, 2016", tuvo como objetivo la identificación de los riesgos de seguridad que puedan existir dentro del departamento de Admisión y registro Académico, y luego de la evaluación, determinar la relación de estos y con la existencia de un SGSI que permita que los principios básicos de la información estén seguros, además concluye que la existencia de riesgos es un peligro la latente para la

información al no ser gestionados; es así que la relación que establezca con el SGSI propone mitigar o eliminar estos riesgos y así permitir la continuidad de las operaciones de la universidad.

II.2 Bases Teóricas

II.2.1 Sistema de Gestión de Seguridad de la Información

Sistema de Información

(Salinas Rodríguez & Valencia Moncada, 2017) define al Sistema de Información como diversas piezas o eslabones que en conjunto se relacionan para lograr ser un soporte a los procesos diarios y decisiones de una organización, sin importar el tamaño o rubro. Por mucho tiempo se ha considerado que un sistema de información solo representa hardware, software o medios electrónicos, sin embargo, se debe comprender que el sistema información va más allá; incluye todo tipo de información que gestione una organización; ya sea de naturaleza física o digital.

Componentes de los Sistemas de Información

(Trujillo & Rozo, 2015) mencionan que los Sistemas de Información brindan a la organización una visión completa sobre los lugares, personas y evento importantes para toda gestión, es así que un Sistema de Información se encuentra formado por los siguientes componentes: hardware, software, procedimientos, datos y recurso humano; tal como se muestra en la figura a continuación:

Figura 1. Componentes del Sistema de Información. Trujillo y Rozo (2015)

Los datos son la entrada a todo Sistema de Información, pero por si solos no pueden ser entendidos por la organización para ser utilizados de manera efectiva. Por otro lado, el hardware y el software en conjunto son necesarios para la funcionalidad del Sistema de Información, para el almacenamiento, proceso de tareas que permiten la continuidad del negocio.

El recurso humano en cambio son los encargados de alimentar el Sistema de Información con información importante y actualizada para gestionarla para obtener informes y resultados.

Los procedimientos usan los datos para brindar resultados que satisfagan las necesidades existentes y soluciones basadas en tecnologías de la Información.

Seguridad de la Información

La seguridad de la información es de gran importancia para garantizar el buen funcionamiento de cualquier organización, para (Hassan, Ismail, & Maarop, 2015) “es conocida como la actividad para proteger la información de una amplia gama de amenazas, minimizar el daño y maximizar las oportunidades de la organización”.

La Seguridad de la Información deber ser preservada y considerar que es crítica, valiosa y sensible. Para el presente estudio la criticidad de la información es muy importante para garantizar la continuidad de los procesos académicos y administrativos; a la vez es valiosa porque la información es un activo que tiene un único y propio valor; y es sensitiva porque toda la información académica y administrativa debe ser conocida y gestionada solamente por personas autorizadas a su acceso. (Acosta Ubaque & León Patiño, 2017)

Dimensiones de la Seguridad de la Información

Las dimensiones sirven de pilares para la seguridad de la información, son como ejes donde se aplican todas las medidas de protección, y son tres: Integridad, Disponibilidad y Confidencialidad.

Figura 2. Dimensiones de la Seguridad de la Información. INCIBE (2017)

Integridad, evita que la información que maneja y transita por toda la organización sufra modificaciones o errores, para la presente investigación con la integridad se busca evitar la alteración intencionada o errores involuntarios, y así evitar la toma de decisiones basadas en información equivoca que puede generar pérdidas económicas, vulneración de información privada (datos de estudiantes y trabajadores), entre otros; colocando en riesgo la continuidad del propósito de la organización.

Confidencialidad, busca que la información sea accesible únicamente al personal autorizado en los diferentes niveles que existan en la organización (personas, entidades o sistemas); para el caso con la confidencialidad se busca evitar el robo total o parcial de información crítica ya sea por parte de la propia persona o de algún ataque a través de internet y sobre todo evitar la divulgación o uso inadecuado de esta información.

Disponibilidad, permite el acceso a la información cuando se necesite en cualquier momento del día, mes o año; para la presente investigación es necesario por ejemplo tener acceso al correo institucional en todo momento, ya que a través de él funciona el trámite documentario interno y externo, así como la gestión educativa para el acceso al sistema académico, la falta de disponibilidad en la actualidad de este servicio generaría únicamente la paralización parcial de actividades. (Ciberseguridad, 2017)

Sistema de Gestión de Seguridad de la Información

Según (ISOTOOLS, 2016) “el Sistema de Gestión de Seguridad de la Información es el conjunto de elementos interactuantes (estructura organizativa, políticas, responsabilidades, procesos y recursos) que permiten establecer políticas y objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua”

Por otro lado (Calder, 2017) lo considera como “un enfoque de gestión estructurado y coherente para la seguridad de la información, que está diseñado para asegurar la interacción eficaz de los componentes clave de la implementación de una política de seguridad de la información: Proceso o Procedimiento, Tecnología y Comportamiento del usuario.

El contar con un Sistema de Gestión de Seguridad de la Información es especialmente interesante y realmente necesario en sectores como el de salud, público y financiero; la principal razón de su implementación en el sector público se origina por la gran cantidad de información que se maneja diariamente, mucha de esa información siendo de carácter personal y de un alto nivel de criticidad; por lo que es primordial contar con sistemas y protocolos que aseguren la confidencialidad, seguridad e integridad de los mismos. (ISOTOOLS, 2016)

Para la organización de ISO 27000 España, “la información gestionada por la organización está expuesta ante amenazas de ataque (extorsión), error (intencionado o por negligencia), ambientales (inundación o incendio), fallo en los sistemas (de almacenamiento de datos, informáticos, redes) y también a vulnerabilidades que representan puntos débiles inherentes en su ciclo de vida”. (ISO27000.es, 2015)

Por lo que (Ladino A., Villa S., & López E., 2017) mencionan que “las organizaciones deben generar un plan de acción frente a éstas conocido como Sistema de Gestión de Seguridad de la Información (SGSI) que contiene los lineamientos que deben cumplirse, los responsables y la documentación necesaria para garantizar que el SGSI sea aplicado y genere una retroalimentación”

SGSI basado en la Norma ISO 27001

“ISO/IEC 27001 es un reconocido marco internacional de mejores prácticas para un sistema de gestión de seguridad de la información. Le ayuda a identificar las amenazas para la información importante y pone en su lugar los controles apropiados para ayudarle a prevenir.”

Los beneficios de contar con un SGSI basado en la Norma ISO/IEC 27001 se basa principalmente en “la flexibilidad para adaptar controles a todas las áreas o áreas seleccionadas de la organización y la identificación de vulnerabilidades y amenazas para la colocación de controles y así gestionarlos o eliminarlos” (Group, 2015)

Esta norma nos presenta un sistema de gestión basado en el ciclo de Deming:

> "Plan, Do, Check, Act, conocido como PDCA y que traducido al castellano sería Planificar, Hacer, Comprobar y Mejorar, que supone la implantación de un sistema de mejora continua que requiere una constante evolución para adaptarse a los cambios producidos en su ámbito y para tratar de conseguir la máxima eficacia operativa mediante las cuatro fases que lo componen. Cada una de estas fases marca los objetivos que describe la norma ISO 27001." (Muñoz Martín, 2015)

Figura 3. Ciclo PDCA. ISOTools Excellence (2016)

Procesos del Ciclo PDCA

La Norma ISO/IEC 27001 establece un mapeo de las etapas del ciclo de Deming y los productos o entregables exigidos por la norma. (María Eugenia Corti, Gustavo Betarte y Reynaldo de la Fuente, 2005, (Pallas Mega , 2015) "especifican los principales procesos que indica la referida norma, mapeados con las etapas del ciclo PHVA".

Tabla 1. Ciclo de Deming (PHVA) aplicado a la norma ISO/IEC 27001. Pallas (2015)

Ciclo PHVA	**Procesos**
P**lanificar (*Plan*)**	Establecer el contexto. Alcance y Limites Definir Política del SGSI Definir Enfoque de Evaluación de Riesgos Identificación de riesgos Análisis y Evaluación de riesgos

	Evaluar alternativas para el Plan de tratamiento de riesgos Aceptación de riesgos Declaración de Aplicabilidad
H**acer (*D*o)**	Implementar plan de tratamiento de riesgos Implementar los controles seleccionados Definir las métricas Implementar programas de formación y sensibilización Gestionar la operación del SGSI Gestionar recursos Implementar procedimientos y controles para la gestión de incidentes de seguridad
V**erificar (*C*heck)**	Ejecutar procedimientos de seguimiento y revisión de controles. Realizar revisiones regulares de cumplimiento y eficacia de los controles y del SGSI. Medir la eficacia de los controles y verificación de satisfacción de los requerimientos de seguridad. Revisión de la evaluación de riesgos periódicamente. Realizar auditorías internas Revisión de alcance y líneas de mejoras del SGSI por la Dirección. Actualizar los planes de seguridad Registrar acciones que podrían impactar la eficacia y/o eficiencia del SGSI
A**ctuar (*A*ct)**	Implementar las mejoras identificadas para el SGSI Implementar las acciones correctivas y preventivas pertinentes. Comunicar acciones y mejoras a todas las partes involucradas. Asegurarse que las mejoras logren los objetivos previstos.

Implantación del SGSI

Para la implantación inicial de un SGSI y su posterior mantenimiento es necesario que se considere como un proyecto que emprende la organización, esto mediante la identificación de actividades críticas asociadas a la una planificación donde se tengan en cuenta los principales responsables, los recursos necesarios y los posibles riesgos que puedan surgir a lo largo del proyecto. Esta implantación según la ISO/IEC 27001 debe seguir las siguientes fases:

1. Alcance del SGSI

La ISO 27001:2013 indica que el alcance sirve para “aclarar los límites del SGSI en función del contexto, importancia y de los activos críticos de información de la organización y los riesgos propios o externos asociados, así como los flujos de información que cruza los límites del alcance.” (ISO 27001, 2015) Si bien la norma brinda una guía para definir el alcance, cada organización evalúa desde su interior el alcance que tendrá, por consiguiente el alcance en las organizaciones puede parecerse pero no ser iguales.

2. Política del SGSI

"Establece y confirma el compromiso de la alta dirección con los objetivos de seguridad de la información de la organización y la mejora continua del SGSI, entre otros posibles aspectos relevantes." (ISO27000.es, 2015)

"Para asegurar la exactitud y protección de la información utilizada, se mantiene la certificación de los sistemas, con el fin de proteger los activos de información contra amenazas potenciales, así como para cumplir con la legislación y normas más relevantes relacionados con la seguridad de la información." (Lizarazo Lozano, 2016) Para cualquier implementación o mejora dentro de una organización, el factor humano es clave para una implementación exitosa, si se encuentran barreras desde la alta dirección será muy difícil que el resto de la organización se comprometa con los objetivos y la mejora continua.

3. Evaluación de riesgos

"Se realiza un procedimiento documentado de evaluación de riesgos que explique cómo se identifican, analizan y priorizan los riesgos relacionados con los activos de información más relevantes del alcance." (ISO27000.es, 2015) Tal como se muestra en el siguiente gráfico la existencia de amenazas y vulnerabilidades aumentan la probabilidad de que un riesgo impacte en el valor de los activos, por eso la norma busca evaluar los riesgos e implementar controles y requerimientos de seguridad que protejan la información como el activo más importante de cualquier organización en estos tiempos.

Figura 4. Evaluación de Riesgos. ISO27000.ES (2015)

4. Declaración de aplicabilidad

SOA (Statement of Applicability) en sus siglas en inglés, "establece los riesgos de información y los controles de seguridad que son relevantes y aplicables al

SGSI de la organización, como resultado de la determinación de sus evaluaciones periódicas del riesgo" (ISO27000.es, 2015)

La aplicación primordial de la declaración de aplicabilidad o el documento SOA radica en mostrar que cada control recomendado por la ISO/IEC 27001 es aplicado según el alcance que ha fijado la organización y para el rubro de la misma, muchas veces una organización intenta copiar los controles que otra implementa, resultando un total fracaso debido a que los requerimientos de seguridad son totalmente distintos.

5. Tratamiento de riesgos

Uno de los más importantes principios de la ISO/IEC 27001 consiste en poder percibir o encontrar los incidentes a los que la organización está expuesta y así poder encontrar la forma más efectiva de evitarlos. Es por eso que se considera que en esta fase de la implementación, "se debe pasar de la teoría a la práctica, hasta este momento el trabajo de tratamiento de riesgos del sistema de seguridad de la información ha sido teórico, pero en este momento en donde se deben mostrar los resultados." (PMG SSI, 2017)

6. Objetivos y planes

Cada organización debe conservar la información documentada sobre los objetivos de la seguridad de la información que pretende implementar, según (PMG SSI, 2017) la organización de determinar lo siguientes: "lo que se va a hacer, los recursos que se requieren, quién será la persona responsable, cuando se finalizará y como se realizará la evaluación de resultados" (PMG SSI, 2017)

Todo lo antes mencionado permitirá que la organización pueda evaluar el nivel de cumplimiento de las políticas de seguridad y el nivel de eficacia; con el fin de poder realizar mejoras para obtener mejores resultados, además que en cada organización los objetivos pueden ser de alto nivel u otros de nivel inferior, siempre apoyándose unos con otros para cumplir mejor su función.

7. Competencias

ISO/IEC 27001 concluye que es importante "retener información documentada como evidencia de la competencia y además considerar funciones y responsabilidades específicas para las personas asignadas a los roles relacionados con el SGSI" (ISO27000.es, 2015)

Pero no solamente centrarse en las personas relacionadas al SGSI, sino que también a personas relacionadas con los riesgos de información que pueden existir en la seguridad física, privacidad, continuidad del negocio o normas legales; por otro lado en el año 2015, la Guideline for Roles & Responsibilities Information Asset Management hace mención a las responsabilidades de gestión de activos de información que son: "Alta Dirección, dueña legal de los activos de información; el CEO, que es quien aprueba la gestión de seguridad de la

información; Director de Gestión de la Información, quien brinda apoyo y liderazgo para administrar recursos de la información, el CIO, quien establece políticas de seguridad para garantizar la calidad e integridad de los recursos de información y el Oficial de Seguridad, que se encarga de implementar políticas de seguridad para proteger la información" (Security, 2015)

8. Planificación y control operacional y métricas

En esta fase de la implementación toda organización debe tener en cuenta que es importante contar con toda la información debidamente documentada para así tener la certeza y confianza que los procesos se llevaron a cabo según lo planificado.

Por otro lado (PMG SSI, 2017) explica que además "la organización debe controlar los cambios planificados y revisar todas las consecuencias de los cambio son previstos, tomando acciones para mitigar todos los efectos adversos, cuando sea necesario" (PMG SSI, 2017). La ISO/IEC 27001 menciona que, "aunque los detalles varían según la organización, debería ser claramente evidente a partir de la documentación de que el SGSI está en funcionamiento con el nivel de eficacia requerido" (ISO27000.es, 2015)

9. Auditorías internas y revisión por la dirección

"Los informes de auditoría interna del SGSI son la evidencia más directa que documenta los principales hallazgos, conclusiones y recomendaciones de la auditoría con la posibilidad de comunicar no conformidades y acciones correctivas, mejoras." (ISO27000.es, 2015)

Es de vital importancia que la auditoria que se realice sea imparcial y hecha por profesionales competentes designados para auditar los requisitos del SGSI. En el documento ISMS Auditing Guideline, 2017; explica acerca de los principios de auditoria en general según la ISO 19001, sección 4, "en todos los asuntos relacionados con la auditoría, el auditor debe ser independiente tanto en actitud como en apariencia. La función o equipo de auditoría debe ser independiente del área o actividad que se está revisando para permitir la finalización objetiva de la tarea de auditoría." (Toolkit, 2017)

10. No conformidades y acciones correctivas

Las no conformidades son requisitos del SGSI parcial o totalmente insatisfechos, que generan una o varias acciones correctivas para subsanarlas, tal como lo indica la ISO/IEC 27001, las no conformidades, "también surgen de las necesidades aplicadas por la propia organización (estrategias, políticas, procedimientos) o por partes externas a ella (leyes, regulaciones y contratos) en relación a las actividades del alcance del SGSI." (ISO27000.es, 2015)

Las no conformidades también deben ser documentadas ya sea como problemas, incidentes o hallazgos de auditoria, los auditores cumplen un rol muy

importante ya que deben identificarlas, investigar las causas de su origen, informarlas y resolverlas.

La norma ISO 27002 Código de buenas prácticas para los controles de Seguridad de la Información

Es considerada como, “un inventario de buenas prácticas para la seguridad de la Información desarrollado con la experiencia de la implantación de controles para la seguridad de la información aceptadas por las empresas y organizaciones más importantes del mundo” (ISO 27001, 2016)

Su objetivo es evaluar la implementación actual de cada control de la norma ISO /IEC 27001 con el fin de determinar el grado de cumplimiento de éstos y, como resultado del análisis, presentar los hallazgos en temas relacionados con Seguridad de la Información junto con las respectivas recomendaciones.

Además busca “asegurar que las deficiencias y mejoras al SGSI de identifiquen claramente y cuando sea necesario, de acuerdo con las acciones correctivas requeridas, se realice periódicas auditorías internas para identificar el cumplimiento de controles” (Cuervo Alvarez, 2016)

La norma contiene 114 controles agrupados en 14 capítulos cada uno subdividido en áreas de seguridad. Por otro lado se consideran categorías u objetivos de control dentro de los cuales se sitúan los controles asociados a estos objetivos: (Wawak, 2015)

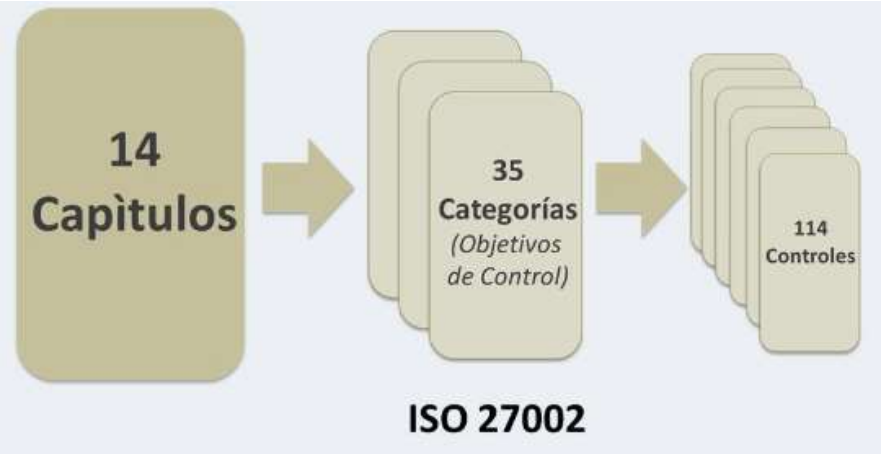

Figura 5. Estructura ISO 27001. Norma ISO 27001.es (2016)

Capítulo 5: Política de Seguridad de la Información

En este capítulo se establecen los objetivos y formas de control de la seguridad de la información, incluyendo el compromiso de la dirección y otros factores, además que

se muestra la importancia de contar con una "adecuada política de seguridad, aprobada por la dirección, comunicada a todo el personal, revisada de forma periódica y actualizada con los cambios que se producen en el interior y en el exterior". (SSI, 2016)

Capítulo 6: Organización de la Seguridad de la Información

"Los controles indicados en este capítulo buscan estructurar un marco de seguridad eficiente tanto mediante los roles, tareas, seguridad, etc. como en los dispositivos móviles." (SSI, 2016)

En la actualidad el teletrabajo está ocupando un lugar importante dentro de cualquier organización, es por eso que es importante tener en cuenta todas las amenazas que puedes surgir y así evitar que de alguna manera la seguridad de la información se vea afectada.

Capítulo 7: Seguridad relativa a los recursos humanos

En este capítulo se busca, "mitigar el riesgo de robo, fraude o mal uso de los recursos, a fin de que el trabajador esté laborando en la empresa, debe ser consciente de las amenazas relativas a la seguridad de la información, así como de sus responsabilidades y obligaciones." (ABNT - Associação Brasileira de Normas Técnicas, 2015)

Además para el correcto cumplimiento de los controles que presenta este capítulo es importante concienciar y formar al personal en la importancia que tiene la información en el desarrollo de sus actividades diarias, por lo que el principal objetivo que deben perseguir es promover, mantener y mejorar el nivel de seguridad de dicha información.

Capítulo 8: Gestión de Activos

Según la norma, un activo es "cualquier cosa que tenga valor para la organización y que necesita ser protegido. Pero para ello los activos deben ser identificados y clasificados, de modo que un inventario pueda ser estructurado y posteriormente mantenido, definiéndose qué tipo de uso se permite hacer con dichos activos." (ABNT - Associação Brasileira de Normas Técnicas, 2015)

Otro factor importante que se controla en este capítulo son las acciones que deben cumplir los trabajadores; antes, durante y después de su contratación, con la finalidad de no

Capítulo 9: Control de Accesos

En este capítulo se habla precisamente del acceso a la información, la existencia de "roles que necesitan un mayor acceso y otros con un acceso mucho más limitado. Para poder marcar las diferencias, se deben establecer todos los controles como registro de los usuarios, gestión de los privilegios de acceso, etc." (SSI, 2016), todo lo anterior con la finalidad de evitar algún tipo de daño a la información física o digital o robo de la misma y así poder continuar con el objetivo principal de la norma, mantener la seguridad de la información.

Capítulo 10: Criptografía

Este capítulo se enfoca en la información sensible o crítica, y mediante diversas técnicas criptográficas se busca proteger y garantizar su autenticidad, confidencialidad e integridad. "La criptografía brinda todas las oportunidades de proteger la data de todo tipo de amenazas virtuales, para la conservación de la integridad de la data manejada y compartida." (Guedez, 2018)

Capítulo 11: Seguridad física y del entorno

En este capítulo se hace hincapié en la seguridad que se debe tener en los equipos e instalaciones donde se realiza el procesamiento de información crítica para la organización, incluyendo protección contra amenazas físicas o incidentes ambientales.

Es importante considerar que "la seguridad no debe ser solo a nivel tecnológico sino también físico, como por ejemplo no dejar las pantallas e impresoras en zonas que sean fácilmente accesibles por parte del personal externo" (SSI, 2016) estas buenas prácticas permitirán crear hábitos que aporten eficiencia en la gestión de la organización.

Capítulo 12: Seguridad de las operaciones

Precisa la seguridad en "el componente técnico entrado en todos los aspectos disponibles como la protección del software malicioso, copias de seguridad, control de software en explotación, gestión de vulnerabilidad, etc." (SSI, 2016), además no se debe dejar de lado la seguridad de los servicios tercerizados y así minimizar el riesgo de fallas.

Capítulo 13: Seguridad de las comunicaciones

En la era tecnológica que actualmente vivimos, todo se transmite mediante correos electrónicos, redes sociales, entre otros; es por eso que es necesario asegurar la información que se transmite o difunde. "La creación de procedimientos para la generación de copias de seguridad y su recuperación, así como la administración

segura de las redes de comunicaciones es otra forma de cuidar la seguridad en la comunicaciones" (ABNT - Associação Brasileira de Normas Técnicas, 2015)

Capítulo 14: Adquisiciones, desarrollo y mantenimiento de los sistemas de información

En este capítulo lo primordial es la seguridad en los sistemas de información, los requisitos para dichos sistemas deben ser especificados y acordados antes de su desarrollo e implementación para que así puedan ser protegidos, otro factor primordial es que estos sistemas "mantengan su confidencialidad, autenticidad o integridad por medios criptográficos." (ABNT - Associação Brasileira de Normas Técnicas, 2015)

Capítulo 15: Relación con los proveedores

Así como existe un capítulo de la seguridad en el recurso humano, no se puede dejar de lado las relaciones con externos o terceras partes, por lo que es necesario "establecer medidas de seguridad pudiendo ser muy recomendable e incluso necesario en determinados casos." (SSI, 2016)

Capítulo 16: Gestión de incidentes de seguridad de la información

Es importante tener en cuenta que al tratar los controles de seguridad en un SGSI, no se debe dejar de lado los incidentes de seguridad, para que así la organización esté preparada para cuando sucedan y pueda responder de manera rápida y eficiente. Otro factor clave para estar preparados ante los incidentes de seguridad es por eso que "los empleados, proveedores y terceros deben ser conscientes de los procedimientos para notificar los eventos de seguridad de la información para asegurar que se comuniquen lo más rápido posible y sean corregidos en tiempo hábil" (ABNT - Associação Brasileira de Normas Técnicas, 2015)

Capítulo 17: Aspectos de seguridad de la información para la gestión de la continuidad del negocio

La importancia de mantener la seguridad de la información en una organización, se basa primordialmente en que la pérdida de esta puede generar grandes pérdidas económicas y de reputación, generar interrupciones de las actividades, por eso "los planes de continuidad del negocio deben ser desarrollados e implementados, con el fin de asegurar que las operaciones esenciales sean rápidamente recuperadas." (ABNT - Associação Brasileira de Normas Técnicas, 2015)

Capítulo 18: Cumplimiento

"No podemos hablar de seguridad de la información, sin hablar de legislación, normas y políticas aplicables que se encuentre relacionadas con este campo y con las que conviven en las organizaciones." (SSI, 2016)

Es de vital importancia estar actualizados en los últimos cambios que presentan la legislación, normas o políticas, y garantizar que se cumplan en todos los niveles a fin de evitar problemas más adelante.

Tabla 2. Áreas de control y controles según ISO/IEC 27001. Munich Personal RePEc Archive (2015)

ÁREA DE CONTROL	CONTROLES
POLÍTICA DE SEGURIDAD	• Políticas de Seguridad de la Información
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	• Organización interna • Dispositivos móviles y teletrabajo
SEGURIDAD DE LOS RECURSOS HUMANOS	• Previo al empleo • Durante el empleo • Finalización o cambio de empleo
GESTIÓN DE ACTIVOS	• Responsabilidad de los activos • Clasificación de la información • Manejo de medios
CONTROL DE ACCESOS	• Requerimientos de negocio para el control de acceso • Gestión de accesos de usuarios • Responsabilidades de usuario • Control de acceso a la información y las aplicaciones
CRIPTOGRAFÍA	• Controles criptográficos
SEGURIDAD FÍSICA Y AMBIENTAL	• Áreas seguras • Equipamiento
SEGURIDAD DE LAS OPERACIONES	• Responsabilidad y procedimientos operacionales • Protección contra código malicioso • Copias de respaldo • Registro y monitoreo • Control de software operacional

	• Gestión de vulnerabilidades técnicas • Consideraciones de auditoria de sistemas de información
SEGURIDAD DE LAS COMUNICACIONES	• Controles en la red • Transferencia de información
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	• Requerimientos de seguridad de los sistemas de información • Seguridad en el desarrollo y soporte de procesos • Datos de prueba
RELACIONES CON PROVEEDORES	• Seguridad de información en relaciones con el proveedor • Gestión de servicios por terceras partes
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	• Informes de los eventos de seguridad de la información y vulnerabilidades
ASPECTOS DE SEGURIDAD DE INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO	• Gestión de los aspectos de seguridad de la continuidad del negocio • Redundancias
CUMPLIMIENTO	• Cumplimiento de los requerimientos legales • Revisiones a la seguridad de la información

II.2.2 Gestión de Riesgos

Concepto de Riesgo

(Trujillo & Rozo, 2015) Plantean el riesgo como el grado de exposición a la ocurrencia de una pérdida, esto debido a que la amenaza a la que se esté expuesto se materialice y use las vulnerabilidades existentes en un activo, y se generen pérdidas o daños.

Por otro lado la ISO materializa la anterior definición indicando que el riesgo es “la probabilidad de que una amenaza determinada se materialice explotando las vulnerabilidades de un activo o grupo de activos y por lo tanto causar daño o pérdidas a la organización” (Arévalo, Cedillo, & Moscoso, 2017), además los riesgos se dividen

de acuerdo al impacto que causan en la organización en tres grupos: daños a las operaciones, daños legales y daños a la reputación.

Así mismo (Salah Llanes, 2017) considera que el riesgo "está caracterizado por la referencia a los eventos potenciales y las consecuencias o una combinación de ellos."; ya que recurrentemente el riesgo se ve reflejado tal como indica en la combinación de los efectos, ya sean positivos o negativos de un evento y en la probabilidad de que suceda, estos pueden verse reflejados en niveles diferentes dentro de la organización: estratégico, producto o procesos.

Elementos del riesgo

1. Activos de Información

Los activos hacen referencia a todo aquel elemento que contenga algún tipo de información, que deben estar clasificados de acuerdo a su criticidad, funcionalidad o la sensibilidad con la que debe ser tratada, con el fin de proteger dicha información. (ISO, 2017)

Según INCIBE, 2015 "cualquier recurso de la empresa necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste y cuya protección es el fin último de la gestión de riesgos." (Ciberseguridad, 2015)

2. Amenazas

Son los elementos que causan daño o alteración en la información de la organización, que generalmente se originan a partir de una vulnerabilidad encontrada, además existen varios tipos de amenazas: de origen natural, del entorno, por defecto de aplicaciones, causadas por personas de forma accidental o de forma deliberada. (Molina, 2015)

También es considerada por (Ciberseguridad, 2015) como "circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor."

3. Vulnerabilidades

Según la metodología MAGERIT, las vulnerabilidades son la probabilidad de que una amenaza se materialice y cause un daño a los activos. (ens-Esquema Nacional de Seguridad). Además las vulnerabilidades deben ser expresadas en forma cuantitativa para poder medir el nivel de su impacto.

4. Impacto

Es considerado como la medida del daño causado cuando una amenaza se materializa sobre un activo, es así que "el impacto se suele estimar en porcentaje de degradación que afecta al valor del activo, el 100% sería la pérdida total del activo." (Molina, 2015)

Figura 6. Diagrama de relación de los elementos del riesgo. INCIBE (2015)

Gestión del Riesgo

(Osorio Corredor, 2016) Considera que la gestión de riesgos consiste en pronosticar e identificar las acciones o circunstancias que pueden afectar los aspectos estratégicos, financieros, sociales y legales de cualquier organización, por otro lado para realizar una correcta gestión de riesgos es importante que cada integrante de la organización sea consciente de los riesgos con los que conviven a diario para de esa manera poder tener más protegidos los activos.

“La Gestión de Riesgos se define como una disciplina que existe para hacer frente a los riesgos no especulativos, que son aquellos riesgos de los cuales sólo puede ocurrir una pérdida para la organización” (Arévalo, Cedillo, & Moscoso, 2017)

Es importante que todos los involucrados en el tratamiento de la información comprendan que una correcta administración de los riesgos permitirá tener un mayor control y protección de la información, ayudando a un mejor funcionamiento de la organización, reduciendo en gran manera el costo que implicaría estar sometidos a un riesgo sin estar preparados. (Lugani & Peña, 2017)

La Gestión de Riesgos según ISO 31000 es principalmente el grupo de actividades que permitirán dirigir y controlar una organización con respecto al riesgo, a través de una serie de principios que contribuyen con el logro de objetivos, mejoras en el desempeño, establecimiento de prioridades y el reconocimiento de factores culturales y humanos

que influyen en la toma de decisiones cuando nuevos riesgos aparecen, ciertos riesgos cambian o cuando los riesgos desaparecen. (ISOTools, 2018)

ISO 31000:2018

Las Normas ISO, ofrecen una visión ordenada y metodológica para implantar un programa de seguridad de la información, de forma tal de tener una guía que contemple todos los aspectos sobre el tema y que es producto de los representantes internacionales con mayores fortalezas en la disciplina. (Ramírez Castro, 2016)

La ISO 31000:2018 tiene como objetivo brindar principios y directrices para la gestión de riesgos, a través de la planificación y toma de decisiones, estableciendo dentro de la organización una referencia sobre los riesgos para poder dar lugar al desarrollo de otros sistemas de gestión, además de que fija la gestión de riesgos al cumplimiento objetivos y no de eventos como la anterior versión. Por otro lado la ISO 31000: 2018 reconoce que en la actualidad toda organización opera en un medio incierto donde el riesgo es el efecto de la incertidumbre sobre los objetivos.

El liderazgo en uno de los factores claves para la gestión de riesgos según la ISO 31000:2018, ya que sin eso y sin el compromiso de integrarlo en la estrategia y la cultura organizacional, no tendría los mismos resultados; así como comprender que la gestión de riesgos presenta una naturaleza cíclica donde no todo puede salir bien la primera vez sino que se debe mejorar cada vez que se complete el ciclo. (González, 2019)

Metodología de la Gestión de Riesgos

Para que la gestión de riesgos sea eficaz, la norma ISO 31000 recomienda “que las organizaciones desarrollen, implementen y mejoren de manera continuada un marco de trabajo cuyo objetivo sea integrar el proceso de gestión del riesgo en los procesos de gobierno, de estrategia y de planificación, de gestión y de elaboración de informes, así como en las políticas, los valores y en la cultura de toda la organización” (Alemán Novoa & Rodríguez Barrera, 2015) esto con la finalidad de que sea útil para cualquier entidad, ya sea pública o privada, asociaciones, grupos o individuos; lo que permite la identificación oportuna de los puntos más débiles de las estructuras de TI que permiten el funcionamiento óptimo de cualquier organización. Estos principios básicos facilitan además la toma de decisiones, se basan en la información disponible y segura que integra además al factor humano y cultural como actores activos en la gestión de riesgos, facilitando la mejora continua constante.

Según ISO 31000 el proceso para la Gestión de Riesgos tiene los siguientes componentes:

1. **Comunicación y consulta:** este ítem del proceso es el primer acercamiento entre la organización y la gestión de riesgos, a través de esto se brinda una asesoría pertinente para que las partes involucradas comprendan el riesgo.
2. **Alcance, contexto y criterios:** el principal propósito de este ítem es adaptar el proceso de la gestión del riesgo, definiendo el alcance del mismo y comprendiendo los contextos tanto internos como externos, para poder así realizar una eficaz evaluación y tratamiento del riesgo.
3. **Evaluación del riesgo:** en este ítem de agrupa lo relacionado a la identificación, análisis y valoración del riesgo; donde se encuentra, reconoce y describe el riesgo para luego comprender su naturaleza y características para el apoyo en la toma de decisiones.
4. **Tratamiento del riesgo:** El propósito de es ítem es la selección e implementación de las opciones necesarias para abordar el riesgo, de tal manera de implementar acciones adicionales si se requiere.
5. **Registro e informe:** Como todo proceso se debe realizar la documentación respectiva de las actividades realizadas, para luego ser socializadas con toda la organización a través de los mecanismos apropiados. (Delgado, 2018)

NTP ISO/IEC 31000:2018

La Norma Técnica Peruana pretende ser utilizada para el trabajo en equipo de los procesos de gestión de riesgos establecidos en las normas existentes internacionales y nacionales, a la vez busca ser un apoyo a las normas que tratan cualquier tipo de riesgo, cualquier sea su naturaleza o si sus consecuencias son negativas o positivas; la NTP no pretende sustituir a otro tipo de normas, sino que buscando el bien común de cualquier tipo de organización. (INACAL, 2018)

Principios de la NTP ISO/IEC 31000:2018

- **La gestión del riesgo crea y protege al valor:** logra contribuir de manera tangible al logro de los objetivos y al desempeño de la organización
- **La gestión de riesgo es una parte integral de todos los procesos de la organización:** es parte de un todo no es una actividad que se pueda desarrollar de manera independiente sin tener en cuenta las actividades y procesos principales de la organización.
- **La gestión de riesgos es parte de la toma de decisiones:** permite definir y dar prioridad a las acciones más relevantes para la organización y a distinguir entre planes de acción diferentes.
- **La gestión de riesgos habla sobre la incertidumbre:** se toma muy en cuenta la naturaleza de las incertidumbres y la manera en que pueden ser tratados.

- **La gestión de riesgos es sistemática, estructurada y oportuna:** este enfoque de la gestión de riesgos contribuye a la eficacia y a resultados coherentes, comparables y fiables.
- **La gestión del riesgo se adapta:** se alinea con el contexto externo e interno de la organización y con el perfil del riesgo. (INACAL, 2018)

Dominios para la Gestión de Riesgos

La NTP ISO/IEC 31000:2018 describe tres dominios que son: evaluación, orientación y supervisión del riesgo, los cuales determinan puntos de control y de acción correctiva que deben ser implementados con el fin de garantizar que se cuente con el tratamiento adecuado según el tipo de riesgo que se pueda presentar en una organización. (Huayllani Muñoz, 2019)

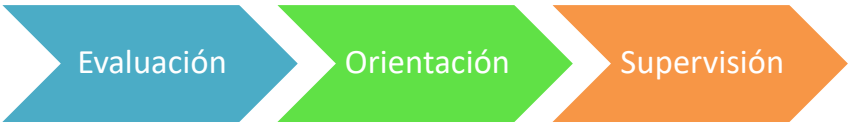

Figura 7: Dominios de la Gestión de Riesgos según NTP ISO/IEC 31000:2018.INACAL (2018)

1. **Evaluación:** Permite asegurar la alineación de los objetivos de TI con las metas de la Entidad, como se están usando las tecnologías determinado la capacidad actual y el nivel de madurez de los Sistemas de Información en los procesos de la organización.
2. **Orientación:** Permite dirigir la preparación y ejecución de los planes y políticas, asignando las responsabilidades, impulsar una cultura de buen gobierno de TI en la organización, dirigiendo las inversiones en materia de TI de acuerdo a las prioridades de la organización.
3. **Supervisar:** Permite monitorear los indicadores necesarios para medir el rendimiento de TI en la organización, asegurándose que las TI cumple con los requisitos externos como de los internos; supervisando la prioridad de los recursos asignados de acuerdo a los objetivos de la organización. (Salah Llanes, 2017)

III. HIPÓTESIS

III.1 Declaración de Hipótesis

El Sistema de Gestión de Seguridad de la Información se relaciona inversamente con la Gestión de Riesgos en el área informática de una Universidad Pública, Región Cajamarca 2020.

III.2 Operacionalización de variables

Variable	Tipo de Variable	Operacionalización		Dimensiones (Sub-variables)	Definición conceptual	Indicador	Ítems	Nivel de Medición	Nivel de Medición
	Según su naturaleza	Definición Conceptual	Definición Operacional						
Sistema de Gestión de Seguridad de la Información	Variable Cualitativa	Conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales.(ISO 27000.es)	Según ISO/IEC 27001, es la búsqueda de protección de los activos de información mediante: seguridad de los recursos humanos, gestión de activos, control de acceso, seguridad física y ambiental, seguridad de las operaciones, gestión de incidentes de seguridad de la información. Su evaluación y cumplimientos pueden actuar como un factor clave en evitar la pérdida, robo o corrupción de información con la posibilidad de continuar la actividad después de un incidente grave.	Seguridad en los Recursos Humanos	El principal objetivo es mitigar el riesgo de robo, fraude o mal uso de los recursos, a fin de que el trabajador que esté laborando en la empresa, debe ser consciente de las amenazas relativas a la seguridad de la información, así como de sus responsabilidades y obligaciones	Nivel de influencia en la selección de los colaboradores	• ¿Se investigan los antecedentes de los candidatos? (Formación, Experiencia, Verificar Titulación y Referencias)(1) • ¿Se incluyen cláusulas relativas a la Seguridad de la Información en los contratos de trabajo?(21)	Ordinal	Se toma en 3 niveles: Siempre, Algunas Veces, Nunca
						Nivel de cumplimiento de políticas durante la realización del trabajo	• ¿El cumplimiento de las responsabilidades sobre la Seguridad de la Información es exigida de forma activa a empleados y contratistas?(2) • ¿Existen procesos de información, formación y sensibilización sobre las responsabilidades de Seguridad de la Información?(22) • ¿Existe un plan disciplinario donde se comunica a los colaboradores y contratistas las consecuencias de los incumplimientos sobre las políticas de la Seguridad de la Información?(37) • ¿Se consideran requisitos especiales para la Seguridad de la Información en la utilización de dispositivos móviles?(46) • ¿Se aplican los criterios de seguridad para los accesos de teletrabajo?(54)		
						Nivel de cumplimiento de política al finalizar el contrato	• ¿Existe un procedimiento para garantizar la Seguridad de la Información en los cambios de empleo, puesto de trabajo o al finalizar un contrato?(3) • ¿Se definen responsabilidades sobre la Seguridad de la Información que se extiendan más allá de la finalización de un contrato como por ejemplo cuestiones relativas a la confidencialidad de la Información?(23)		

Gestión de Activos	El principal objetivo son los activos, que deben ser identificados y clasificados, de modo que un inventario pueda ser estructurado y posteriormente mantenido, definiéndose qué tipo de uso se permite hacer con dichos activos.	Nivel de responsabilidad sobre los Activos	• ¿Se ha realizado un inventario de activos que den soporte a la organización ?(4) • ¿Se ha identificado al responsable de cada activo en cuanto a su seguridad?(24) • ¿Se han establecido normas para el uso de activos en relación a su seguridad?(38) • ¿Existe un procedimiento para la devolución de activos cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato?(47)	Ordinal	Se toma en 3 niveles: Siempre, Algunas Veces, Nunca
		Nivel de influencia en la clasificación de la información	• ¿Se clasifica la información según su confidencialidad o su importancia en orden a establecer medidas de seguridad especificas?(5) • ¿Los activos de información son fácilmente identificables en cuanto a su grado de confidencialidad o su nivel de clasificación?(25) • ¿Existen procedimientos para el manipulado de la información de acuerdo a su clasificación?(39)		
		Nivel de influencia en la manipulación de soportes	• ¿Existen controles establecidos para aplicar a soportes extraíbles? (Uso, Cifrado, Borrado, Etc.)(6) • ¿Se revisan todos los medios, para asegurarse que ningún tipo de dato sensible o software licenciado haya sido eliminado o sobrescrito con seguridad antes del desecho o reutilización del medio?(26) • ¿Los medios que contienen información, están protegidos en contra del acceso no autorizado, el mal uso o su alteración durante el transporte más allá de los límites físicos de la organización?(65)		
Control de Acceso	En este capítulo se habla precisamente del acceso a la información, la existencia de roles que necesitan un mayor acceso y otros con un acceso mucho más limitado. Para poder marcar las diferencias, se deben establecer todos los controles como registro de	Nivel de cumplimiento de los requisitos generales para el control de accesos	• ¿Existe una política para definir los controles de acceso a la información que tengan en cuenta el acceso selectivo a la información según las necesidades de cada actividad o puesto de trabajo?(7) • ¿Se establecen accesos limitados a los recursos y necesidades de red según perfiles determinados?(27)	Ordinal	Se toma en 3 niveles: Siempre, Algunas Veces, Nunca

					los usuarios, gestión de los privilegios de acceso, etc.	Nivel de influencia de la gestión de accesos de usuarios	• ¿Existen procesos formales de registros de usuarios?(8) • ¿Existen procesos formales para asignación de perfiles de acceso?(28) • ¿Se define un proceso específico para la asignación y autorización de permisos especiales de administración de accesos?(40) • ¿Se ha establecido una política específica para el manejo de información clasificada como secreta? en cuanto a: Autenticación o Compromisos.(48) • ¿Se establecen periodos concretos para renovación de permisos de acceso?(55) • ¿Existen un proceso definido para la revocación de permisos cuando se finalice una actividad, puesto de trabajo o cese de contratos?(59)		
						Nivel de responsabilidades de los usuarios	• ¿Se establecen normas para la creación y salvaguarda de contraseñas de acceso?(9)		
						Nivel de influencia en los control de acceso a la información y las aplicaciones	• ¿Se establecen niveles y perfiles específicos de acceso para los sistemas de Información de forma que se restringa la información a la actividad específica a desarrollar? (10) • ¿Se han implementado procesos de acceso seguro para el inicio de sesión considerando limitaciones de intentos de acceso, controlando la información en pantalla etc.?(29) • ¿Los sistemas de gestión de contraseñas son interactivos y aseguran igualmente la calidad de las contraseñas?(41) • ¿El uso de programas de usuario capaces de modificar el sistema y los controles de las aplicaciones, está restringido y fuertemente controlado?(49) • ¿Se restringe el acceso a códigos fuente de programas y se controla cualquier tipo de cambio a realizar?(56)		

			Seguridad Física y Ambiental	En este capítulo se hace hincapié en la seguridad que se debe tener en los equipos e instalaciones donde se realiza el procesamiento de información crítica para la organización, incluyendo protección contra amenazas físicas o incidentes ambientales.	Nivel de implementación de áreas seguras	• ¿Se establecen perímetros de seguridad física donde sea necesario con barreras de acceso?(11) • ¿Existen controles de acceso a personas autorizadas en áreas restringidas?(30) • ¿Se establecen medidas de seguridad para zonas de oficinas para proteger la información de pantallas etc. en áreas de accesibles a personal externo?(42) • ¿Se controla o supervisa la actividad de personal que accede a áreas seguras?(50)	Ordinal	Se toma en 3 niveles: Siempre, Algunas Veces, Nunca
					Nivel de seguridad en el equipamiento	• ¿Se protegen los equipos tanto del medioambiente como de accesos no autorizados?(12) • ¿Se protegen los equipos contra fallos de suministro de energía?(31) • ¿Existen protecciones para los cableados de energía y de datos?(43) • ¿Se planifican y realizan tareas de mantenimiento sobre los equipos?(51) • ¿Se consideran medidas de protección específicas para equipos que se utilicen fuera de las instalaciones de la propia oficina?(57) • ¿Se establecen protocolos para proteger o eliminar información de equipos que causan baja o van a ser reutilizados?(60) • ¿Se establecen normas para proteger la información de equipos cuando los usuarios abandonan el puesto de trabajo?(62) • ¿Se ha adoptado una política de "escritorio despejado" para los papeles, medios de almacenamiento removibles y una política de "pantalla limpia" en la infraestructura para el procesamiento de información?(64)		
			Seguridad en las Operaciones	Precisa la seguridad en el componente técnico entrado en todos los aspectos disponibles como la protección del software malicioso, copias de seguridad, control de software en explotación, gestión de vulnerabilidad,	Nivel de cumplimiento de los procedimientos y responsabilidades	• ¿Se documentan los procedimientos y se establecen responsabilidades?(13) • ¿Se controla que la información sobre procedimientos se mantenga actualizada?(32) • ¿Se controla el uso de los recursos en cuanto al rendimiento y capacidad de los sistemas?(44) • ¿Los entornos de desarrollo de software y pruebas están convenientemente separados de los entornos de producción?(52)	Ordinal	Se toma en 3 niveles: Siempre, Algunas Veces, Nunca

					etc, además no se debe dejar de lado la seguridad de los servicios tercerizados y así minimizar el riesgo de fallas.	Nivel de protección contra software malicioso	• ¿Existen sistemas de detección para Software malicioso o malware?(14)		
						Nivel de cumplimiento en la implementación de copias de respaldo	• ¿Se ha establecido un sistema de copias de seguridad acordes con las necesidades de la información y de los sistemas?(15)		
						Nivel de cumplimientos de los registros y supervisión	• ¿Se realiza un registro de eventos? (Intentos de acceso fallidos/exitosos, Desconexiones del sistema, Alertas de fallos, etc.(16) • ¿Se protege convenientemente y de forma específica los accesos o los de los administradores?(33)		
						Nivel de control de software	• ¿Las instalaciones de nuevas aplicaciones software o modificaciones son verificadas en entornos de prueba y existen protocolos de seguridad para su instalación?(17)		
						Nivel de influencia de la vulnerabilidad técnica	• ¿Se establecen métodos de control para vulnerabilidades técnicas "hacking ético" etc.?(18) • ¿Se establecen medidas restrictivas para la instalación de software en cuanto a personal autorizado evitando las instalaciones por parte de usuarios finales?(34)		
						Nivel de cumplimiento de las auditorías de Sistemas de Información	• ¿Existen mecanismos de auditorías de seguridad de los sistemas?(19) • ¿Se establecen protocolos específicos para desarrollo de auditorías software considerando su impacto en los sistemas?(35)		

				Gestión de Incidentes de Seguridad de la Información	Permite que la organización esté preparada para cuando sucedan y pueda responder de manera rápida y eficiente. Otro factor clave para estar preparados ante los incidentes de seguridad es por eso que los colaboradores, proveedores y terceros deben ser conscientes de los procedimientos para notificar los eventos de seguridad de la información para asegurar que se comuniquen lo más rápido posible y sean corregidos en tiempo hábil	Nivel de implementación de los informes de los eventos de seguridad de la información y vulnerabilidades	• ¿Se definen responsabilidades y procedimientos para responder a los incidentes de la Seguridad de la Información?(20)• ¿Se han implementado canales adecuados para la comunicación de incidentes en la seguridad de la Información?(36)• ¿Se promueve y se han establecidos canales para comunicar o identificar puntos débiles en la Seguridad de la Información?(45)• ¿Se ha establecido un proceso para gestionar los incidentes en la Seguridad de la Información?(53)• ¿Existen mecanismos para dar respuesta a los eventos de la Seguridad de la Información?(58)• ¿La información proporcionada por los eventos en la Seguridad de la información son tratados para tomar medidas preventivas?(61)• ¿Existe un proceso para recopilar evidencias sobre los incidentes en la seguridad de la Información?(63)	Ordinal	Se toma en 3 niveles: Siempre, Algunas Veces, Nunca
Gestión del Riesgo	Variable Cualitativa	La gestión del riesgo se define como el proceso de identificar, analizar y cuantificar las probabilidades de pérdidas y efectos secundarios que se desprenden de los desastres,	Según lo establecido por la NTP - ISO 31000:2018, la Gestión de Riesgos considera que la Gestión de Riesgos es el conjunto de acciones que permiten identificar, analizar y cuantificar un desastre, mediante el	Evaluación	Permite asegurar la alineación de los objetivos de TI con las metas de la Entidad, como se están usando las tecnologías determinado la capacidad actual y el nivel de madurez de los Sistemas de Información en los procesos de la organización	Nivel de riesgos relacionados a las TI	• ¿Determina el área de informática el nivel de riesgos relacionados con TI que está dispuesta a asumir para cumplir con sus objetivos?(1)	Ordinal	Se toma en 3 niveles: Siempre, Algunas Veces, Nunca
						Nivel de tolerancia	• ¿Frente a los niveles de riesgo y oportunidades aceptables, el área de informática evalúa y aprueba propuestas de tolerancia al riesgo de TI?(2)		
						Nivel de influencia de los riesgos en la organización	• ¿Determina el área de informática el grado de alineación de la estrategia de riesgos de TI con la estrategia de riesgos organizacionales?(3)		

		así como de las acciones preventivas, correctivas y reductivas correspondientes que deben emprenderse, además ha de estar plenamente integrada en los procesos de la organización y requiere un compromiso fuerte y sostenido de la dirección así como del establecimiento de una rigurosa planificación estratégica. (Arévalo, Cedillo, & Moscoso, 2017)	uso de acciones de **evaluación, orientación y supervisión**. Estas acciones permiten transferir el riesgo a otra parte, evitándolo o reduciendo el impacto negativo.			Nivel de influencia de las decisiones estratégicas	• ¿Se evalúa con frecuencia los factores de riesgo de TI con anterioridad a las decisiones estratégicas de la organización pendientes?(4) • ¿Se asegura que las decisiones de la organización se toman conscientes de los riegos?(15)		
						Nivel de valoración según políticas	• ¿Se determina si el uso de TI se realiza según estándares nacionales e internacionales?(5) • ¿El uso de TI está sujeto a una valoración y evaluación de riesgos adecuada?(16)		
						Nivel de recuperación y tolerancia ante pérdidas de TI	• ¿La entidad evalúa las actividades de gestión de riesgos para garantizar su alineamiento con las capacidades de la organización para pérdidas relacionadas con TI?(6) • ¿La entidad evalúa las actividades de gestión de riesgos para garantizar su alineamiento con la tolerancia de los encargados frente a pérdidas relacionadas con TI?(17)		
				Orientación	Permite dirigir la preparación y ejecución de los planes y políticas, asignando las responsabilidades, impulsar una cultura de buen gobierno de TI en la organización, dirigiendo las inversiones en materia de TI de acuerdo a las prioridades de la organización.	Nivel de oportunidades e impactos potenciales	• ¿Se promueve una cultura consciente de los riesgos de TI que impulse a la identificación proactiva de riesgos, oportunidades e impactos potenciales en la entidad?(7)	Ordinal	Se toma en 3 niveles: Siempre, Algunas Veces, Nunca
						Nivel de influencia de las decisiones y operaciones estratégicas	• ¿Se orienta la integración de las operaciones y la estrategia de riesgos de TI con las decisiones y operaciones estratégicas de la entidad?(8)		
						Nivel de influencia de la elaboración de planes	• ¿Se comunican los planes de acción frente a un riesgo?(9)• ¿Los empleados cuentan con la formación, recursos y habilidades necesarias para asumir responsabilidades frente a un riesgo?(18)		
						Nivel de capacidad de respuesta	• ¿Se realiza capacitación para la implementación de mecanismos apropiados para responder rápidamente a los riesgos cambiantes y se notifica a los niveles adecuados de gestión?(10)		

				Supervisión	Permite monitorear los indicadores necesarios para medir el rendimiento de TI en la organización, asegurándose que las TI cumple con los requisitos externos como de los internos; supervisando la prioridad de los recursos asignados de acuerdo a los objetivos de la organización.	Nivele de apetito de riesgo	• ¿Se supervisa con regularidad, hasta qué punto se gestiona el perfil de riesgo dentro del apetito del riesgo?(11)	Ordinal	Se toma en 3 niveles: Siempre, Algunas Veces, Nunca
						Nivel de influencia de las metas y métricas claves	• ¿Se supervisa con regularidad las metas y métricas clave de gestión de los procesos de gobierno y gestión del riesgo respecto a los objetivos?(12)		
						Nivel de influencia de los objetivos identificados	• ¿Se facilita la revisión por las partes interesadas del progreso de la entidad hacia el control de los riesgos identificados?(13)		
						Nivel de influencia del comité de dirección	• ¿Se informa cualquier problema de gestión de riesgos al responsable del área?(14)		

III.3 Propuesta de solución

A. TÍTULO:

"POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN"

La siguiente política está dada para implementar de manera progresiva las charlas y talleres que ayuden a gestionar la seguridad de la información y la gestión de riesgos.

1. **Propósito**

   Proporcionar entrenamiento a todos los colaboradores en temas de seguridad de la información para que de esa manera puedan identificar los activos de acuerdo a su grado de confidencialidad, para que así estos no se encuentren expuestos y en caso de estar expuestos a algún riesgo interno o externo, se comunique al responsable y se lo gestione de manera adecuada.

2. **Objetivo**

   Educar adecuadamente a todos los colaboradores en temas de seguridad de la información para conocer el manejo de los activos y la gestión de riesgos evitando pérdidas de información en el área informática de una Universidad Pública, Región Cajamarca 2020.

3. **Alcance**

   Área Informática de una Universidad Pública, Región Cajamarca 2020.

4. **Situación Actual**

   Luego del análisis, investigación y observación a los colaboradores que formaron parte de la presente investigación desde el mes de abril de 2020 hasta julio de 2020, se logró identificar que la clasificación de activos de acuerdo a su grado de confidencialidad no se realiza de manera adecuada lo que se evidencia en la falta de comunicación con el responsable del área sobre problemas de gestión de riesgos. Debido a que a mayor cumplimiento de las políticas y procedimientos del sistema de gestión de seguridad de la información mayor es la gestión de riesgos, se implementa esta política con la finalidad de brindarles la capacitación necesaria para mejorar la clasificación de activos y poder enfrentar los riesgos que puedan ocurrir sin sufrir pérdidas o daños.

5. **Bases**

   a. **Activos**:

      Los colaboradores del área informática de una Universidad Pública, Región Cajamarca deben interiorizar que un activo es todo aquel recurso que se emplea para realizar el procesamiento, almacenamiento y en general todo el mantenimiento de la información, desde su creación hasta su destrucción, además de que la identificación de los activos, se realizará empezando por identificar toda la información que se maneja al interior de la organización, tanto de forma digital como física, analizando el grado de confidencialidad de cada activo para así poder gestionar los riesgos que puedan presentarse.

Tabla 3. Nivel de Confidencialidad de un activo

	MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
Confidencialidad	El activo tiene un mínimo grado de sensibilidad para la organización por lo que afecta casi de forma imperceptible la operación, la economía o aspectos de cumplimiento.	El activo tiene un bajo grado de sensibilidad para la organización por lo que afecta de cierta forma la operación, la economía o aspectos de cumplimiento.	El activo tiene un mediano grado de sensibilidad para la organización por lo que afecta la operación, la economía o aspectos de cumplimiento.	El activo tiene un alto grado de sensibilidad para la organización por lo que afecta considerablemente la operación, la economía o aspectos de cumplimiento.	El activo tiene muy alto grado de sensibilidad para la organización por lo que afecta totalmente la operación, la economía o aspectos de cumplimiento.

- *Información:* la pérdida de confidencialidad se debe entender como el conocimiento no autorizado o la divulgación intencional o no intencional de la información de forma inoportuna que se encuentre contenida en los documentos, bases de datos, códigos fuentes, archivos de datos, estrategias, políticas, comunicados o de cualquier activo de este tipo.
- *Software:* la pérdida de confidencialidad del software se debe entender como el acceso a las aplicaciones de la organización o a programas de forma no autorizada.
- *Físicos:* la pérdida de confidencialidad de los activos físicos se debe entender como el acceso de personas no autorizadas al activo y a partir de esto se obtenga acceso a la información.
- *Servicios:* la pérdida de confidencialidad de los servicios se debe entender como el acceso no autorizado al servicio o sistema de información.
- *Personas:* la pérdida de confidencialidad de las personas ocurre cuando de forma intencional o no, divulgan información de sus funciones laborales o de la información que manejan en sus actividades.

6. Actividades

a. Capacitaciones teóricas a los colaboradores del área de informática de una Universidad Pública, para reforzar los conceptos de clasificación de activos, seguridad de la información y gestión de riesgos.

b. Talleres prácticos:

- **Caso Práctico "El falso proveedor", para poder detectar "email spoofing".**

  Alberto, un empresario que hace tres años fundó una pequeña empresa de marketing y diseño. Actualmente tiene cinco empleados en plantilla y todo marcha mejor de lo previsto. Cada vez tienen más clientes y gracias a su buen hacer son muy conocidos en su sector. Debido al volumen actual de facturación, Alberto ha tenido que adquirir una aplicación contable que les facilite las tareas de administración. A esta

aplicación únicamente tienen acceso Ángel, el responsable de contabilidad y el propio Alberto, mediante un usuario y contraseña que ambos comparten. Esta contraseña cumple con las recomendaciones de seguridad ya que tiene más de ocho caracteres incluyendo mayúsculas, minúsculas, números y caracteres especiales, y lo más importante, no contiene información que pueda identificar a la empresa o a Ángel o Alberto, como usuarios.

Una mañana de viernes, Ángel recibió un email del supuesto jefe de soporte técnico de la empresa de mantenimiento de la aplicación de contabilidad. En este correo le explicaba que se había registrado una anomalía en el sistema y que para solventarla necesitaba acceder a la aplicación utilizando el usuario y contraseña de la empresa. Por el tono del mensaje, Ángel pensó que se trataba de una incidencia grave así que decidió actuar con rapidez facilitando los datos de acceso del sistema de contabilidad a la falsa empresa de mantenimiento. Cuanto antes estuviera solucionado el error informático, antes podría reanudar su trabajo. Ese mismo día Alberto se disponía a consultar unos datos contables a través de la aplicación cuando descubrió unos movimientos que no reconocía haber realizado. Alarmado, contactó con Ángel para ver si se trataba de algún error por su parte, pero Ángel tampoco reconocía dichas transacciones. ¿Qué podía haber pasado? Inmediatamente Alberto llamó al banco para informarles de lo ocurrido y así evitar más movimientos fraudulentos.

- **Caso Práctico "El soporte técnico", para poder conocer cómo funciona la "ingeniería social".**

  Luis es el dueño de una pequeña tienda online que gestiona desde su oficina junto su gran equipo de media docena de empleados. Desde que acudió a varias charlas, Luis está muy concienciado con la ciberseguridad en su empresa. Por eso, es meticuloso e intenta implementar las medidas de seguridad adecuadas a su negocio que le ayuden a permanecer a salvo de los peligros de la red.

  Cierto día, recibió una llamada telefónica de una persona que decía ser de Microsoft en Londres. El interlocutor, en un inglés con incorrecciones y con un tono bastante amenazante, le explicó que habían recibido numerosos informes de los equipos de la empresa con errores y advertencias de seguridad, indicándole que esos equipos estaban en peligro y se podrían bloquear, por lo que podría afectar a su trabajo.

Esta situación hizo sospechar a Luis, pues en las charlas sobre ciberseguridad que había acudido recientemente, había oído hablar sobre casos parecidos de ciberdelincuentes que llamaban a las empresas para hacerse pasar por bancos, compañías energéticas, etc. para engañar a sus víctimas pidiéndoles datos personales o bancarios. Así que le pidió al operador que identificase los equipos afectados y también como había vinculado la IP de sus equipos con su número de teléfono. A lo que el operador le contestó con evasivas y subiendo el tono amenazante. Tras amenazarle con el bloqueo de sus equipos y de la actividad de su empresa, finalmente colgó.

- **Presentación de videos sobre "Qué es el pishing", "Cómo prevenir la fuga de información en tu organización" y "Escritorio limpio".**
- **Monitoreo constante del responsable encargado del área de informática.**

7. Metas

- Realizar las capacitaciones teóricas una vez al mes.
- Realizar talleres prácticos trimestralmente.
- Monitorear el progreso en los colaboradores.
- Desarrollar el 80% de las actividades propuestas hasta el mes de diciembre de 2021.

8. Cronograma

Tabla 4. Cronograma propuesto

Actividad	Ago. 28/08	Sep. 25/09	Oct. 30/10	Nov. 27/11	Dic. 18/12	Responsable
Capacitaciones Teóricas						Especialista en Seguridad de la Información
Talleres Prácticos						Especialista en Seguridad de la Información
Monitoreo						Director del Área de Informática

9. Presupuesto

Tabla 5. Presupuesto para la implementación

Actividad	Descripción	Tiempo	Costo
Especialista	Realizar capacitaciones y talleres	Mensual	S/ 2 000.00
Capacitaciones y Talleres	Laptop	Mensual	S/ 3 500.00
	Proyector		S/ 2 000.00

Materiales	S/ 200.00
Total	**S/ 7 700.00**

Debido a que el área de informática cuenta con laptops y un proyector para la ejecución de las capacitaciones y talleres; se evita el gasto de la adquisición de dichas herramientas; por otro lado, el Director del área de informática será el responsable del monitoreo constante de los colaboradores; por lo que, la inversión total sería S/ 2 200.00 mensuales, con un total de S/ 11 000.00 en toda la implementación de las **"POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN".**

IV. DESCRIPCIÓN DE MÉTODOS Y ANÁLISIS

IV.1 Diseño de la Investigación

No experimental, transeccional, correlacional. No experimental porque se realizará sin manipular deliberadamente ninguna de las variables "sistema de gestión de seguridad de la información" y el "gestión de riesgos" y se observará tal como se encuentran en la realidad propia del área informática de una Universidad Pública en la Región Cajamarca 2020. Transeccional porque se recolectarán los datos en un solo momento, en un tiempo único, para describir las variables, y analizar su incidencia e interrelación en un momento dado, teniendo en cuenta a toda la población de estudio. Correlacional porque se relacionará los resultados obtenidos de las observaciones de ambas variables, teniendo en cuenta los valores o datos de los indicadores del conjunto de variables.

IV.2 Unidad de análisis

La unidad de análisis son los colaboradores que laboran en el área de informática de una Universidad Pública en la Región Cajamarca 2020.

IV.3 Población

La población está constituida por 10 colaboradores del área de informática de una Universidad Pública en la Región Cajamarca 2020.

IV.4 Tamaño de Muestra

No existe muestra debido a que en la presente investigación se trabajará con toda la población.

IV.5 Técnica e Instrumento

La técnica que se utilizará es la encuesta, que utiliza un conjunto de procedimientos estandarizados de investigación mediante los cuales se recoge y analiza una serie de datos de información independientemente tanto del "sistema de gestión de seguridad de la información" y el "gestión de riesgos", así como indicios de la relación entre las variables.

El instrumento que se utilizará es la ficha de encuestas, en primer lugar se sometió a validación por tres expertos (profesionales familiarizados con las variables) obteniendo un resultado promedio de 86.4%; así mismo, habiendo cumplido el requisito anterior, la encuesta fue sometida a una prueba piloto para verificar su confiabilidad en base a 7 colaboradores, debido a que la población de estudio es 10; es así que utilizando el Alfa de Cronbach, coeficiente que nos permite calcular la "consistencia interna"; se obtuvo como resultado para las dimensiones de la variable *Sistema de Gestión de Seguridad de la Información* del 0,96 como se puede observar en la Tabla 6, y para las dimensiones de la variable *Gestión de Riesgos* del 0,79 como se puede observar en la Tabla 7. Finalmente, después de haber obtenido la **validación** y **confiabilidad** se aplicó la encuesta a los 10 colaborares que conforman la población de estudio.

Tabla 6. Análisis de Fiabilidad para la variable Sistema de Gestión de Seguridad de la Información

Estadísticas de fiabilidad	
Alfa de Cronbach	N de elementos
0,961	**65**

Nota: En la tabla se observa que el coeficiente alfa de Cronbach es 0.961 y nos indica que el instrumento es **excelente** y debe aplicarse a la muestra real.

Tabla 7. Análisis de Fiabilidad para la variable Gestión de Riesgos

Estadísticas de fiabilidad	
Alfa de Cronbach	N de elementos
0,787	**18**

Nota: En la tabla se observa que el coeficiente alfa de Cronbach es 0.787 y nos indica que el instrumento es **bueno** y debe aplicarse a la muestra real.

IV.6 Método

Deductivo porque teniendo en cuenta el cuerpo teórico científico y tecnológico del marco teórico del "sistema de gestión de seguridad de la información" y la "gestión de riesgos" se deducirá la relación de ambas variables en la realidad del área informática de una Universidad Pública en la Región Cajamarca 2020.

Inductivo, porque desde las observaciones realizadas a través del conjunto de sus variables e indicadores, obtenidos desde la realidad del área informática de una Universidad Pública en la Región Cajamarca 2020 se identificará la relación del "sistema de gestión de seguridad de la información" y el "gestión de riesgos".

.

V. RESULTADOS

Del objetivo específico 1: Identificar la dimensión del Sistema de Gestión de Seguridad de la Información que tiene mayor relevancia en el área informática de una Universidad Pública, Región Cajamarca 2020.

Tabla 8. Dimensiones de la variable Sistema de Gestión de Seguridad de la Información

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Siempre	A veces	Nunca
DIMENSIONES	Seguridad en los Recursos Humanos	0.0	100.0	0.0
	Gestión de Activos	0.0	90.0	10.0
	Control de Accesos	0.0	90.0	10.0
	Seguridad Física y Ambiental	0.0	80.0	20.0
	Seguridad en las Operaciones	0.0	90.0	10.0
	Gestión de Incidentes de Seguridad de la Información	0.0	90.0	10.0

Nota: Se puede observar las 6 dimensiones de la variable Sistema de Gestión de Seguridad de la Información, donde se observa que en la Dimensión Seguridad en los Recursos Humanos es la que tiene mayor relevancia en cuanto al cumplimiento de las políticas y procedimientos necesarios para la protección de activos en el área de informática de una

Universidad Pública, Región Cajamarca 2020. Esto debido a que, en dicha dimensión, se tiene como principal agente el recurso humano, desde su contratación, durante y hasta la culminación del contrato en el cual se especifican y consideran los ítems que permiten contar con un recurso humano que tenga en cuenta la importancia de la seguridad de los activos con los que se relaciona para que el Sistema de Gestión de Seguridad de la Información funcione de manera adecuada en el área. Por otro lado, se observa que, aunque en menor medida, las otras cinco dimensiones también cumplen de manera parcial las políticas y procedimientos en el Sistema de Gestión de Seguridad de la Información; sin embargo, en general se puede observar que en ninguna de las dimensiones se cumplen de manera constante y frecuente las políticas y procedimientos.

Del objetivo específico 2: Identificar la dimensión de la Gestión de Riesgos que tiene mayor relevancia en el área informática de una Universidad Pública, Región Cajamarca 2020.

Tabla 9. Dimensiones de la variable Gestión de Riesgos

	GESTIÓN DEL RIESGO		
DIMENSIONES	Siempre	A veces	Nunca
Evaluación	20.0	80.0	0.0
Orientación	0.0	90.0	10.0
Supervisión	0.0	90.0	10.0

Nota: Se puede observar las tres dimensiones de la variable Gestión del Riesgo, donde en la Dimensión Evaluación se cumple de manera constante con las acciones necesarias para evitar o reducir el impacto negativo de un riesgo en la organización, esto a través de la alineación de los objetivos de TI con las metas de la organización, determinando la capacidad actual y nivel de madurez de los Sistemas de Información, por otro lado se observa que las dimensiones Orientación y Supervisión cumplen de manera parcial acciones necesarias para evitar o reducir el impacto negativo de un riesgo, notándose que si bien es importante contar inicialmente con lineamientos para la gestión del riesgo, también deben ir acompañados constantemente con planes que impulsen constantemente una cultura de buen gobierno de TI, así como monitorear los indicadores necesarios para medir el rendimiento de estos lineamientos.

Del objetivo específico 3: Identificar la relación entre el Sistema de Gestión de Seguridad de la Información y cada una de las dimensiones de la gestión de riesgos en el área informática de una Universidad Pública, Región Cajamarca 2020.

Tabla 10. Correlación de las variables Sistema de Gestión de la Seguridad de la Información y Gestión de Riesgos

Correlaciones

		Seguridad en los Recursos Humanos	Gestión de Activos	Control de Accesos	Seguridad Física y Ambiental	Seguridad en las Operaciones	Gestión de Incidentes de Seguridad de la Información	Evaluación	Orientación	Supervisión
Seguridad en los Recursos Humanos	Correlación de Pearson	.[a]	.[a]	.[a]	.[a]	.[a]	.[a]	.[a]	.[a]	.[a]
	Sig. (bilateral)		.	.	.	.	.	.	.	.
Gestión de Activos	Correlación de Pearson	.[a]	1	1,000**	,667*	1,000**	1,000**	,167	,111	,167
	Sig. (bilateral)	.		,000	,035	,000	,000	,645	,760	,645
Control de Accesos	Correlación de Pearson	.[a]	1,000**	1	,667*	1,000**	1,000**	,167	,111	,167
	Sig. (bilateral)	.	,000		,035	,000	,000	,645	,760	,645
Seguridad Física y Ambiental	Correlación de Pearson	.[a]	,667*	,667*	1	,667*	,667*	,250	,167	,250
	Sig. (bilateral)	.	,035	,035		,035	,035	,486	,645	,486
Seguridad en las Operaciones	Correlación de Pearson	.[a]	1,000**	1,000**	,667*	1	1,000**	,167	,111	,167
	Sig. (bilateral)	.	,000	,000	,035		,000	,645	,760	,645
Gestión de Incidentes de Seguridad de la Información	Correlación de Pearson	.[a]	1,000**	1,000**	,667*	1,000**	1	,167	,111	,167
	Sig. (bilateral)	.	,000	,000	,035	,000		,645	,760	,645
Evaluación	Correlación de Pearson	.[a]	,167	,167	,250	,167	,167	1	-,167	-,250
	Sig. (bilateral)	.	,645	,645	,486	,645	,645		,645	,486
Orientación	Correlación de Pearson	.[a]	,111	,111	,167	,111	,111	-,167	1	,667*
	Sig. (bilateral)	.	,760	,760	,645	,760	,760	,645		,035
Supervisión	Correlación de Pearson	.[a]	,167	,167	,250	,167	,167	-,250	,667*	1
	Sig. (bilateral)	.	,645	,645	,486	,645	,645	,486	,035	

**. La correlación es significativa en el nivel 0,01 (2 colas).

Nota: Se puede observar que las seis Dimensiones de la variable Sistema de Gestión de Seguridad de la Información están correlacionados con las tres Dimensiones de la variable Gestión del Riesgo, donde la mayoría de dimensiones tienen como significancia un valor mayor a 0.05, concluyendo así que mientras más se cumplan las políticas y procedimientos del Sistema de Gestión de Seguridad de la Información mayor será la Gestión de Riesgos en el área informática de una Universidad Pública, Región Cajamarca 2020.

PRUEBA DE HIPÓTESIS

En la Tabla 6. Se muestra la prueba de Shapiro Wilk, en la cual se observa que la significancia de la variable Sistema de Gestión de Seguridad de la Información es 0.723 > 0.05 y de la variable Gestión de Riesgos es 0.310 > 0.05 por lo que ambas variables corresponden a una distribución normal, lo que significa que la relación entre el Sistema de Gestión de Seguridad de la Información y la Gestión de Riesgos se utilizó la prueba paramétrica Pearson.

Tabla 11. Prueba de Normalidad de las variables Sistema de Gestión de Seguridad de la Información y Gestión de Riesgos

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Sistema de Gestión de Seguridad de la Información	,139	10	,200*	,955	10	,723
Gestión de Riesgos	,180	10	,200*	,914	10	,310

a. Corrección de significación de Lilliefors

Se enuncian las hipótesis:

H_0: El Sistema de Gestión de Seguridad de la Información no se relaciona inversamente con la gestión de riesgos en el área informática de una Universidad Pública, Región Cajamarca 2020.

H_1: El Sistema de Gestión de Seguridad de la Información se relaciona inversamente con la gestión de riesgos en el área informática de una Universidad Pública, Región Cajamarca 2020.

Tabla 12. Correlación Pearson de las variables Sistema de Gestión de Seguridad de la Información y la Gestión de Riesgos en el área informática de una Universidad Pública, Región Cajamarca 2020

Correlaciones

		Sistema de Gestión de Seguridad de la Información	Gestión de Riesgos
Sistema de Gestión de Seguridad de la Información	Correlación de Pearson	1	,111
	Sig. (bilateral)		,760
	N	10	10
Gestión de Riesgos	Correlación de Pearson	,111	1
	Sig. (bilateral)	,760	
	N	10	10

Nota. Se muestra que la significancia es 0.760 > 0.05, por lo que se aprueba la H_0; comprobando así que los valores de la variable Sistema de Gestión de Seguridad de la Información no se relacionan con los valores de la variable Gestión de Riesgos; es decir, que mientras más incremente el cumplimiento de las políticas y procedimientos del Sistema de Gestión de Seguridad de la Información mayor será la Gestión de Riesgos.

V.I. Propuesta de Mejora:

Tras la evaluación de las diversas metodologías de Gestión de Riesgos, entre ellas NISTP SP 800-30, MAGERIT Y CRAMM, se identificó que MAGERIT, además de utilizar la terminología de la normativa ISO 31000, trabaja con organizaciones como la que se evaluó; que gestiona información digital y servicios de tipo informático.

Debido a lo antes mencionado es la ideal para trabajar en conjunto con la ISO 31000:2018, y tratar los riesgos oportunamente, preparando además a la organización para futuras auditorias, certificaciones o acreditaciones que sean necesarias.

1. **Comunicación y consulta:**

   Se busca con las partes interesadas internas y externas la comunicación para promover la toma de conciencia y la comprensión del riesgo, mientras que con la consulta se pretende obtener retroalimentación e información para apoyar la toma de decisiones.

2. **Alcance, contexto y criterios:**

   En esta etapa se adapta el proceso de la gestión del riesgo, para permitir una evaluación del riesgo eficaz y un tratamiento apropiado del riesgo.

3. **Identificación de los riesgos:**

   Se busca encontrar la relación con los posibles puntos de peligro, para luego ser tratados. Es importante identificar todos los posibles riesgos existentes y tener en cuenta que, a pesar de una identificación inicial, pueden surgir en el transcurso de los procesos o actividades diarias ciertos riesgos. Algunas de las herramientas que sería ideal usar para esta etapa son:

   - ✓ Revisar las lecciones aprendidas de otros proyectos: Mediante esto se busca indagar en proyectos desarrollados principalmente en organizaciones similares a las nuestras, pueden haber tenido éxito o no, pero lo mismo nos permitirá conocer que errores no cometer y que aspectos tener en cuenta para lograr el éxito.
   - ✓ Lluvia de ideas (Brainstorming): La interacción con todos los involucrados es fundamental para evitar que todo lo implementado no cumpla con su fin principal; gestionar los riesgos; es por eso que mediante reuniones entre los

responsables de áreas, alta dirección y todos los usuarios finales, con la finalidad de que entre todos se compartan abiertamente ideas por medio de discusiones y conversatorios donde se realice intercambio de conocimientos en todos los niveles.

4. Análisis de los riesgos:

Se califican los riesgos, cuantitativa y cualitativamente, para así centrarse en los más importantes. Una de las herramientas que sería ideal usar para esta etapa es:

- ✓ Lista de Verificación de riesgos: Estas listas permitirán considerar puntos clave a considerarse luego de identificar a los riesgos, además de permitir categorizar los riesgos y garantizar una clasificación integral de cada uno de los riesgos, logrando así ver de una manera más clara y ordenada todos los riesgos presentes en cada eje, que pueden afectar a la organización.

5. Evaluación de los riesgos:

En este paso se traducen los efectos del riesgo con una visión de negocio, cuáles se pueden aceptar y cuáles no; ayudando a entender el impacto que puede sufrir la organización si un riesgo llega a materializarse. Una de las herramientas que sería ideal usar para esta etapa es:

- ✓ Cuadrícula de probabilidad e impacto: Mediante esta tabla se evalúa de manera subjetiva los riesgos y el impacto que podrían ocasionar los mismos, asignándoles una clasificación numérica, que al final al ser multiplicadas ambas; nos generan la gravedad del riesgo.

(Probabilidad) x (Impacto) = Gravedad del Riesgo

6. Tratamiento de los riesgos:

Se realizan una serie de actividades que permitan modificar la situación de los riesgos. Pueden ser acciones preventivas o reactivas a la materialización de los riesgos, o en algunos casos cuando el impacto o probabilidad del riesgo son muy bajos se lo acepta. Una de las herramientas que sería ideal usar para esta etapa frente a riesgos potenciales es:

- ✓ Despunte basado en riesgo: Son experimentos que implican una investigación o realizar un prototipo de respuestas para atender mejor los riesgos potenciales, este tipo de acciones serían más reactivas que preventivas, permitirán tener un Plan B o hasta Plan C para dar respuesta a un riesgo si es que el Plan A no funcionará, logrando así que el riesgo potencial no afecte a la organización y que al no ser mitigado por el Plan A o B, ya el responsable del área o usuario estén alerta para poder tomar las acciones necesarias e informar al responsable de la organización.

7. **Seguimiento y Revisión:**
   Mantener siempre la evaluación del funcionamiento de los sistemas de información y los controles de seguridad, para mejorar la funcionalidad y la experiencia del usuario.
8. **Registro e Informe:**

Se comunica las actividades y resultados de la gestión de riesgos, brindar información para la toma de decisiones, interactuar con los responsables de la organización.

VI. DISCUSIÓN, CONCLUSIONES Y RECOMENDACIONES

VI.1 Discusión

La (ISOTOOLS, 2016), menciona que el Sistema de Gestión de Seguridad de la Información es el conjunto de elementos interactuantes (estructura organizativa, políticas, responsabilidades, procesos y recursos) que permiten establecer políticas y objetivos de seguridad de la información y alcanzar dichos objetivos, teniendo como resultado una mejora en el manejo de la gestión de riesgos y mejora continua; así mismo, se menciona que los beneficios de contar con un SGSI basado en la Norma ISO/IEC 27001 se basa principalmente en la flexibilidad para adaptar controles a todas las áreas seleccionadas de la organización y la identificación de vulnerabilidades y amenazas que pueden explotar riesgos, para la colocación de controles y así gestionarlos o eliminarlos; por lo que, en esta investigación, se permitió contrastar los resultados obtenidos, los cuales demuestran que mientras más se cumplan las políticas y procedimientos del Sistema de Gestión de Seguridad de la Información, mayor será la Gestión de Riesgos en el área informática de una Universidad Pública, Región Cajamarca 2020.

Perafán Ruiz & Caicedo Cuchimba en su trabajo de investigación internacional titulado “Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca” concluye que los controles y políticas de seguridad de la información que existen en el SGSI pueden ser tomados como soporte para la implementación de un Sistema de Gestión de Riesgos más robusto, lo que apoya a los resultados de la presente investigación, donde se demuestra que el Sistema de Gestión de Seguridad de la Información correctamente gestionado, habiéndose corroborado su relación directa, permitirá una correcta Gestión de Riesgos. Por otro lado Lugani & Peña mencionan que es importante que todos los involucrados en el tratamiento de la información comprendan que una correcta administración de los riesgos permitirá tener un mayor control y protección de la información, tal como se muestra en los resultados de la ficha de encuesta donde la Seguridad en los Recursos Humanos es la que tiene mayor relevancia con un 100% en cuanto al cumplimiento de las políticas y procedimientos necesarios para la protección de activos en el área de informática.

Ñañez Campos en su trabajo de investigación "*Modelo de Gestión de Riesgos De TI Basados En La Norma ISO/IEC 27005 y Metodología Magerit para mejorar la Gestión de Seguridad de la Información en la Universidad Nacional Toribio Rodríguez de Mendoza - Chachapoyas Perú*", concluye que la aplicabilidad de la gestión de riesgos de TI debe estar en relación con el sistema de seguridad de la información y recomienda mantener una periódica revisión de las políticas del SGSI para evaluar el cumplimiento de las mismas por parte del personal encargado de la seguridad y a la vez la efectividad de los riesgos de TI relacionados con el SGSI, tal como se menciona líneas arriba, es importante revisar constantemente las políticas y además los procedimientos del SGSI ya que mientras se realice un mayor control en estas, será más factible poder estar preparados para la gestión de riesgos ya sea externos o internos y de esa manera evitar pérdidas económicas, materiales y de imagen.

Huayllani Muñoz en su investigación titulada *"Sistema de gestión de seguridad de la información y la gestión del riesgo en el Ministerio de Salud, 2019"* concluye que existe una relación significativa y positiva entre las dos variables de estudio mencionadas en esta investigación, y a la vez se recomienda evaluaciones periódicas de ambos sistemas con la flexibilidad necesaria para que cada sistema cumpla sus objetivos y se pueda conocer más acerca del funcionamiento en conjunto o por separado de ambas variables; en lo que respecta; el estudio realizado en la presente investigación demuestra que el funcionamiento correcto del SGSI es el que permite que se realice una correcta Gestión de Riesgos.

VI.2 Conclusiones

El Sistema de Gestión de Seguridad de la Información está relacionado de manera inversa con la Gestión de Riesgos en en el área informática de una Universidad Pública, Región Cajamarca 2020, dado que a través de la aplicación de la prueba de hipótesis con la prueba estadística Pearson se obtuvo que el nivel de significancia corresponde a un 76 %, siendo este mayor al valor límite permitido (5%); por lo tanto, se rechaza la hipótesis planteada debido a que mientras más se cumplan las políticas y procedimientos del Sistema de Gestión de Seguridad de la Información, mayor será la Gestión de Riesgos.

Se evidencia que la dimensión de la variable Sistema de Gestión de Seguridad de la Información que tiene mayor nivel de relevancia en el área informática de una Universidad Pública, Región Cajamarca 2020 es la Seguridad en los Recursos Humanos ya que cumple las políticas y procedimientos de manera regular en un 100%; lo que muestra que, al ser el recurso humano el principal agente dentro de la organización, se cumplen con los estándares de seguridad desde su contratación, durante y hasta la culminación del contrato en el cual se especifican y consideran los ítems que permiten contar con un recurso humano que tenga en cuenta la importancia de la seguridad de los activos con los que se relaciona para que el Sistema de Gestión de Seguridad de la Información funcione de manera adecuada en el área, permitiendo la correcta y oportuna gestión de riesgos.

Se evidencia que las dimensiones de la variable Gestión de Riesgos que tienen mayor nivel de relevancia en en el área informática de una Universidad Pública, Región Cajamarca 2020, es la evaluación, ya que presenta un nivel de cumplimientos constante del 20 %; lo que demuestra que se realizan las acciones necesarias para evitar o reducir el impacto negativo de un riesgo en la organización, esto a través de la alineación de los objetivos de TI con las metas de la organización, determinando la capacidad actual y nivel de madurez de los Sistemas de Información.

VI.3 Recomendaciones

Tras realizar la evaluación de diversas metodologías para reforzar la Gestión de Riesgos, se detectó que MAGERIT, es la metodología que aportaría cuatro secciones adicionales, las cuales permiten tener una mejor incidencia en encontrar la relación con los posibles puntos de peligro, para luego ser tratados con las técnicas de la metodología ágil SRUM; por tal motivo, se recomienda que la ISO 31000:2018 debe ser trabajada de manera conjunta con las metodologías antes mencionada debido a que sus procesos se complementan permitiendo tratar los riesgos oportunamente, preparando además a la organización para futuras auditorias, certificaciones o acreditaciones que sean necesarias.

VII. Lista de referencias

Muñoz Martín, M. (2015). *Guía de implantación de un SGSI basado en la norma UNE-ISO/IEC 27001.* Catalunya: Universitat Oberta de Catalunya. Recuperado el 30 de mayo de 2020

Salah Llanes, J. E. (2017). *Repositorio Fundación Universidad del Norte.* Obtenido de Repositorio Fundación Universidad del Norte: http://manglar.uninorte.edu.co/bitstream/handle/10584/8079/131482.pdf?sequence=1&isAllowed=y

27001, N. I. (agosto de 2016). *ISO 27001*. Obtenido de ISO 27001: https://normaiso27001.es/#h3

ABNT - Associação Brasileira de Normas Técnicas. (2015). *Ostec Segurança digital de resultados*. Recuperado el 31 de mayo de 2020, de Ostec Segurança digital de resultados: https://ostec.blog/padronizacao-seguranca/iso-27002-boas-praticas-gsi

Acosta Ubaque, N. E., & León Patiño, T. (2017). *Universidad Nacional Abierta y a Distancia UNAD.* Obtenido de Universidad Nacional Abierta y a Distancia UNAD: https://repository.unad.edu.co/handle/10596/11940

Acosta Ubaque, N. E., & León Patiño, T. K. (2017). *DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (S.G.S.I.) PARA EL CENTRO DE DATOS DE LA PERSONERÍA DE BOGOTÁ D.C. BAJO LAS NORMAS NTC-ISO-IEC 27001:2013 Y NTC-ISO-IEC 27002:2013.* Tesis, Bogotá. Recuperado el 28 de mayo de 2020

Alemán Novoa, H., & Rodríguez Barrera, C. (2015). *Metodologías Para el análisis de riesgos en los sgsi.* Boyacá: Fundación Universitaria Juan de Castellanos, Facultad de Ingeniería, Tunja, Boyacá, Colombia.

Arana, J. A. (2016). Factores que afectan la implementación del sistema de gestión de seguridad de la información en las Entidades Públicas Peruanas. *COMTEL 2016 VIII Congreso Internacional de Computación y Telecomunicaciones*, 141 - 142. Recuperado el 27 de abril de 2020

Arévalo, F., Cedillo, I., & Moscoso, S. (mayo - agosto de 2017). Metodología Ágil para la Gestión de Riesgos Informáticos. *Revista Killkana Técnica, 1*(2), 31-42. Recuperado el 02 de junio de 2020

Blog especializado en Sistemas de Gestión de Seguridad de la Información. (25 de mayo de 2017). *PMG SSI*. Recuperado el 30 de mayo de 2020, de PMG SSI: https://www.pmg-ssi.com/2017/05/iso-27001-plan-de-tratamiento-de-riesgos-de-seguridad-de-la-informacion/

Calder, A. (2017). ISO 27001/27002 - Una guía de bolsillo. En A. Calder, *ISO 27001/27002 - Una guía de bolsillo* (págs. 25- 26). Reino Unido: IT Governance Publishing. Obtenido de https://ebookcentral.proquest.com/lib/upnpe/reader.action?docID=5255172&query=sistema+de+gesti%C3%B3n+de+seguridad+de+la+informaci%C3%B3n#

Cama, E. (01 de marzo de 2017). *EY Building a better working world*. Obtenido de https://perspectivasperu.ey.com/2017/03/01/19na-encuesta-global-seguridad-informacion-2016-17/

Ciberseguridad, I. N. (2015). Gestión de Riesgos. España.

Ciberseguridad, I. N. (2017). PROTECCIÓN DE LA INFORMACIÓN. *Colección: Protege tu empresa*, 5. Recuperado el 28 de mayo de 2020

Cuervo Alvarez, S. (2016). Implementación ISO 27001. Recuperado el 30 de mayo de 2020, de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/64827/8/scuervoTFM0617memoria.pdf

Delgado, E. (11 de junio de 2018). *SPConsulting group*. Obtenido de https://spcgroup.com.mx/iso310002018-proceso-para-la-gestion-de-riesgos/

F. M. Arévalo, I. P. (Mayo - Agosto de 2017). Metodología Ágil para la Gestión de Riesgos Informáticos. *Revista Killkana Técnica. Vol. 1, Vol. 1*(No. 2), 31-42. Recuperado el 21 de abril de 2020

González, H. (31 de mayo de 2019). *isolución*. Obtenido de https://web.isolucion.com.co/iso-31000-2018-fundamentos-de-gestion-de-riesgos/#:~:text=La%20versi%C3%B3n%202018%20de%20la,organizaci%C3%B3n%20en%20todos%20los%20niveles.

Group, B. (2015). Gestión de Seguridad de la Información ISO/IEC 27001. Recuperado el 29 de mayo de 2020, de https://www.bsigroup.com/es-PE/seguridad-de-la-informacion-isoiec-27001-/

Guedez, A. (23 de abril de 2018). *gb advisors*. Recuperado el 30 de mayo de 2020, de gb advisors: https://www.gb-advisors.com/es/criptografia-y-seguridad-informatica/

Hassan, N., Ismail, Z., & Maarop, N. (2015). INFORMATION SECURITY CULTURE: A SYSTEMATIC LITERATURE REVIEW. *5th International Conference on Computing and Informatics, ICOCI 2015* (págs. 456-457). Istanbul, Turkey: Universiti Utara Malaysia . Recuperado el 28 de mayo de 2020

Huayllani Muñoz, O. Y. (2019). *Repositorio Digital Institucional Universidad César Vallejo.* Obtenido de Repositorio Digital Institucional Universidad César Vallejo: http://repositorio.ucv.edu.pe/handle/20.500.12692/42775

INACAL, D. d. (2018). *INACAL.* Obtenido de INACAL.

ISO 27001. (2015). *ISO27000.es*. Recuperado el 30 de mayo de 2020, de ISO27000.es: http://www.iso27000.es/sgsi.html

ISO, 2. (2017). ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls. Obtenido de https://www.iso.org/standard/54533.html

ISOTOOLS. (julio de 2016). La norma ISO 27001: Aspectos clave de su diseño e implantación. *ISOTools Excellence*, 4. Obtenido de ISO 27000.ES: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

ISOTools. (06 de junio de 2018). *ISOTools Excellence*. Obtenido de https://www.isotools.org/2018/06/06/principales-cambios-norma-iso-310002018-gestion-riesgos/

Jara Mendoza, O. Y. (2018). *Repositorio Digital Institucional Universidad César Vallejo.* Obtenido de http://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/31209/Jara_MOY.pdf?sequence=1&isAllowed=y

Ladino A., M. I., Villa S., P. A., & López E., A. M. (2017). Fundamentals of ISO 27001 and its application in enterprises. *Scientia et Technica Año XVI*, 334-335. Recuperado el 28 de mayo de 2020, de https://www.redalyc.org/pdf/849/84921327061.pdf

Lizarazo Lozano, K. O. (2016). *PLANTEAMIENTO DE UN SGSI BASADO EN LA NORMA ISO 27001:2013 PARA LA EMPRESA DE SERVICIOS DE TECNOLOGÍA SITECH DE COLOMBIA SAS EN LOS PROCESOS GESTIÓN FINANCIERA, GESTIÓN DE LOGÍSTICA Y GESTIÓN DE IT.* Bógota: Universidad Piloto de Colombia. Recuperado el 30 de mayo de 2020

López, P. A. (2010). Seguridad Informática. En P. A. López, *Seguridad Informática* (pág. 9). Madrid, España: Editorial Editex S. A.

Lugani, C. F., & Peña, R. L. (2017). Desarrollo de un esquema de Gestión de Riesgos Informáticos en la Universidad Nacional de Río Negro. *SIE, Simposio de Informática en el Estado*, (págs. 170 - 171).

Martinez, & March. (2016). CARACTERIZACIÓN DE LA VALIDEZ Y CONFIABILIDAD EN EL CONSTRUCTO METODOLÓGICO DE LA INVESTIGACIÓN SOCIAL. *Revista Electrónica de Humanidades*, 112 - 113.

Molina, M. (2015). *Propuesta de un plan de gestión de.* Madrid: Universidad Politécnica de Madrid. Recuperado el 02 de junio de 2020

Ñañez Campos, O. (2019). *Repositorio Institucional Universidad Nacional Pedro Ruiz Gallo.* Obtenido de Repositorio Institucional Universidad Nacional Pedro Ruiz Gallo: http://repositorio.unprg.edu.pe/bitstream/handle/UNPRG/6110/BC-%204020%20%c3%91A%c3%91EZ%20CAMPOS.pdf?sequence=1&isAllowed=y

Osorio Corredor, L. E. (2016). *Gestión de Riesgos de Seguridad de la Información en el Sector Público.* Universidad Piloto de Colombia .

Pallas Mega , G. (2015). *Metodología de Implantación de un SGSI.* Montevideo: Universidad de la República. Recuperado el 30 de mayo de 2020

Perafán Ruiz, J. J., & Caicedo Cuchimba, M. (2015). *Universidad Nacional Abierta y a Distancia.* Obtenido de Universidad Nacional Abierta y a Distancia: https://repository.unad.edu.co/handle/10596/2655

Públicas, M. d. (s.f.). *ens-Esquema Nacional de Seguridad.* Obtenido de ens-Esquema Nacional de Seguridad: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Ramírez Castro, A. (2016). Technology risk management based on ISO 31000. *Ingeniería*, 56-66.

Salinas Rodríguez, M. S., & Valencia Moncada, J. A. (2017). *Sistema de Gestión de Seguridad de la Información y Riesgos de Información en seis sedes de una entidad bancaria del Perú.* Trujillo: Universidad Privada del Norte.

Security, I. 2. (2015). Guideline for Roles & Responsibilities in Information Asset Management. 3.4 y 5. Recuperado el 02 de junio de 2020

Shaw, J. A. (2018/2019). *EL PAPEL DEL INFORMÁTICO COMO AUDITOR EN LA "ISO 27001:2017 TECNOLOGÍA DE LA INFORMACIÓN.* Valencia.

SSI, P. (14 de junio de 2016). *SGSI - Blog especializado en Sistemas de Gestión de Seguridad de la Información*. Obtenido de https://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la-iso-27001/

Toolkit, I. (2017). Principles os auditing. *ISMS Auditing Guideline*, 7-8. Recuperado el 30 de mayo de 2020, de https://www.iso27000.es/assets/files/ISO27k%20Guideline%20on%20ISMS%20audit%20v2.pdf

Trujillo, D., & Rozo, J. (01 de enero de 2015). Gestión del riesgo en seguridad de la información : caso de estudio en el repositorio institucional Unisalle - Rius colección tegra y propuesta metodológica a partir de la comparación de normas y estándares internacionales ISO 27005, ISO 31000 y Octave. Bogotá. Recuperado el 28 de mayo de 2020, de Universidad de La Salle: https://ciencia.lasalle.edu.co/cgi/viewcontent.cgi?article=1034&context=sistemas_informacion_documentacion

Vásquez Atalaya, O. (2016). *ROPUESTA DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA LA OFICINA DE ADMISIÓN Y REGISTRO ACADÉMICO DE LA UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO, 2016.* Cajamarca.

Wawak, S. (2015). The Importance of Information Security Management in Crisis Prevention in the Company. *6th International Symposium on Business Administration GLOBAL ECONOMIC CRISIS AND CHANGES*, (págs. 5-6). Cracovia. Recuperado el 31 de mayo de 2020

VIII. Anexos

ANEXO N° 01

MATRIZ DE CONSISTENCIA

TÍTULO: EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA GESTIÓN DE RIESGOS EN EL ÁREA INFORMÁTICA EN UNIVERSIDAD PÚBLICA, REGIÓN CAJAMARCA 2020

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	METODOLOGÍA
¿Cómo el Sistema de Gestión de Seguridad de la Información se relaciona con la Gestión de Riesgos en el área informática de una Universidad Pública, Región Cajamarca 2020?	Determinar la relación que existe entre el Sistema de Gestión de Seguridad de la Información y la Gestión de Riesgos en el área informática de una Universidad Pública, Región Cajamarca 2020.	El Sistema de Gestión de Seguridad de la Información se relaciona inversamente con la Gestión de Riesgos en el área informática de una Universidad Pública, Región Cajamarca 2020.	Sistema de Gestión de Seguridad de la Información	**1. Tipo de Investigación** Aplicada **2. Nivel de Investigación** Descriptivo Correlacional **3. Método:** Deductivo - Inductivo **4. Diseño de la Investigación:** No experimental, transeccional y correlacional **5. Población:** 10 colaboradores del área de informática de una Universidad Pública **6. Muestra** 10 colaboradores del área informática de una Universidad Pública **7. Unidad de Estudio** El colaborador del área informática de una Universidad Pública **8. Técnicas:** Encuesta **9. Instrumentos** Ficha de encuesta
2. Problemas Específicos:	**2. Objetivos Específicos**	**2. Hipótesis Específicas (opcional):**	**Variable 2**	
1.- ¿Qué dimensión del Sistema de Gestión de Seguridad de la Información tiene mayor relevancia en el área informática de una Universidad Pública, Región Cajamarca 2020?	1.- Identificar la dimensión del Sistema de Gestión de Seguridad de la Información que tiene mayor relevancia en el área informática de una Universidad Pública, Región Cajamarca 2020.	1.- La dimensión gestión de activos del Sistema de Gestión de Seguridad de la Información es el que tiene mayor relevancia en el área informática de una Universidad Pública, Región Cajamarca 2020.	Gestión de Riesgos	
2.- ¿Qué dimensión de la Gestión de Riesgos tiene mayor relevancia en el área informática de una Universidad Pública, Región Cajamarca 2020?	2.- Identificar la dimensión de la Gestión de Riesgos que tiene mayor relevancia en el área informática de una Universidad Pública, Región Cajamarca 2020.	2.- La dimensión supervisión de la Gestión de Riesgos es la que tiene mayor relevancia en el área informática de una Universidad Pública, Región Cajamarca 2020.		
3.- ¿Cómo el Sistema de Gestión de Seguridad de la Información se relaciona con cada una de las dimensiones de la Gestión de Riesgos en el área informática de una Universidad Pública, Región Cajamarca 2020?	3.- Identificar la relación entre el Sistema de Gestión de Seguridad de la Información y cada una de las dimensiones de la gestión de riesgos en el área informática de una Universidad Pública, Región Cajamarca 2020.	3.- Cada dimensión del Sistema de Gestión de Seguridad de la información se relacionan inversamente con cada dimensión de la Gestión de Riesgos en el área informática de una Universidad Pública, Región Cajamarca 2020.		

ANEXO N° 02

ENCUESTA PARA MEDIR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Estimado colaborador, la presente encuesta tiene por objetivo identificar la relación existente entre el Sistema de Gestión de Seguridad de la Información y la Gestión de Riesgos en el área informática. La encuesta **es anónima** para lo cual solicito que las preguntas sean respondidas de manera honesta.

INDICACIONES

Marque con una X la respuesta que considere correcta de acuerdo a la pregunta.

1. Siempre **2.** Algunas Veces **3.** Nunca

N°	ITEM	1	2	3
1	¿Se investigan los antecedentes de los candidatos? (Formación, Experiencia, Verificar Titulación y Referencias			
2	¿El cumplimiento de las responsabilidades sobre la Seguridad de la Información es exigida de forma activa a empleados y contratistas?			
3	¿Existe un procedimiento para garantizar la Seguridad de la Información en los cambios de empleo, puesto de trabajo o al finalizar un contrato?			
4	¿Se ha realizado un inventario de activos que den soporte a la organización?			
5	¿Se clasifica la información según su confidencialidad o su importancia en orden a establecer medidas de seguridad especificas?			
6	¿Existen controles establecidos para aplicar a soportes extraíbles? (Uso, Cifrado, Borrado, Etc.)			
7	¿Existe una política para definir los controles de acceso a la información que tengan en cuenta el acceso selectivo a la información según las necesidades de cada actividad o puesto de trabajo?			
8	¿Existen procesos formales de registros de usuarios?			
9	¿Se establecen normas para la creación y salvaguarda de contraseñas de acceso?			
10	¿Se establecen niveles y perfiles específicos de acceso para los sistemas de Información de forma que se restringa la información a la actividad específica a desarrollar?			
11	¿Se establecen perímetros de seguridad física donde sea necesario con barreras de acceso?			
12	¿Se protegen los equipos tanto del medioambiente como de accesos no autorizados?			
13	¿Se documentan los procedimientos y se establecen responsabilidades?			
14	¿Existen sistemas de detección para Software malicioso o malware?			
15	¿Se ha establecido un sistema de copias de seguridad acordes con las necesidades de la información y de los sistemas?			
16	¿Se realiza un registro de eventos? (Intentos de acceso fallidos/exitosos, Desconexiones del sistema, Alertas de fallos, etc.			
17	¿Las instalaciones de nuevas aplicaciones software o modificaciones son verificadas en entornos de prueba y existen protocolos de seguridad para su instalación?			
18	¿Se establecen métodos de control para vulnerabilidades técnicas "hacking ético" etc.?			
19	¿Existen mecanismos de auditorías de seguridad de los sistemas?			
20	¿Se definen responsabilidades y procedimientos para responder a los incidentes de la Seguridad de la Información?			
21	¿Se incluyen cláusulas relativas a la Seguridad de la Información en los contratos de trabajo?			
22	¿Existen procesos de información, formación y sensibilización sobre las responsabilidades de Seguridad de la Información?			
23	¿Se definen responsabilidades sobre la Seguridad de la Información que se extiendan más allá de la finalización de un contrato como por ejemplo cuestiones relativas a la confidencialidad de la Información?			
24	¿Se ha identificado al responsable de cada activo en cuanto a su seguridad?			
25	¿Los activos de información son fácilmente identificables en cuanto a su grado de confidencialidad o su nivel de clasificación?			
26	¿Se revisan todos los medios, para asegurarse que ningún tipo de dato sensible o software licenciado haya sido eliminado o sobrescrito con seguridad antes del desecho o reutilización del medio?			
27	¿Se establecen accesos limitados a los recursos y necesidades de red según perfiles determinados?			

28	¿Existen procesos formales para asignación de perfiles de acceso?			
29	¿Se han implementado procesos de acceso seguro para el inicio de sesión considerando limitaciones de intentos de acceso, controlando la información en pantalla etc.?			
30	¿Existen controles de acceso a personas autorizadas en áreas restringidas?			
31	¿Se protegen los equipos contra fallos de suministro de energía?			
32	¿Se controla que la información sobre procedimientos se mantenga actualizada?			
33	¿Se protege convenientemente y de forma específica los accesos o los de los administradores?			
34	¿Se establecen medidas restrictivas para la instalación de software en cuanto a personal autorizado evitando las instalaciones por parte de usuarios finales?			
35	¿Se establecen protocolos específicos para desarrollo de auditorías software considerando su impacto en los sistemas?			
36	¿Se han implementado canales adecuados para la comunicación de incidentes en la seguridad de la Información?			
37	¿Existe un plan disciplinario donde se comunica a los colaboradores y contratistas las consecuencias de los incumplimientos sobre las políticas de la Seguridad de la Información?			
38	¿Se han establecido normas para el uso de activos en relación a su seguridad?			
39	¿Existen procedimientos para el manipulado de la información de acuerdo a su clasificación?			
40	¿Se define un proceso específico para la asignación y autorización de permisos especiales de administración de accesos?			
41	¿Los sistemas de gestión de contraseñas son interactivos y aseguran igualmente la calidad de las contraseñas?			
42	¿Se establecen medidas de seguridad para zonas de oficinas para proteger la información de pantallas etc. en áreas de accesibles a personal externo?			
43	¿Existen protecciones para los cableados de energía y de datos?			
44	¿Se controla el uso de los recursos en cuanto al rendimiento y capacidad de los sistemas?			
45	¿Se promueve y se han establecidos canales para comunicar o identificar puntos débiles en la Seguridad de la Información?			
46	¿Se consideran requisitos especiales para la Seguridad de la Información en la utilización de dispositivos móviles?			
47	¿Existe un procedimiento para la devolución de activos cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato?			
48	¿Se ha establecido una política específica para el manejo de información clasificada como secreta? en cuanto a: Autenticación o Compromisos.			
49	¿El uso de programas de usuario capaces de modificar el sistema y los controles de las aplicaciones, está restringido y fuertemente controlado?			
50	¿Se controla o supervisa la actividad de personal que accede a áreas seguras?			
51	¿Se planifican y realizan tareas de mantenimiento sobre los equipos?			
52	¿Los entornos de desarrollo de software y pruebas están convenientemente separados de los entornos de producción?			
53	¿Se ha establecido un proceso para gestionar los incidentes en la Seguridad de la Información?			
54	¿Se aplican los criterios de seguridad para los accesos de teletrabajo?			
55	¿Se establecen periodos concretos para renovación de permisos de acceso?			
56	¿Se restringe el acceso a códigos fuente de programas y se controla cualquier tipo de cambio a realizar?			
57	¿Se consideran medidas de protección específicas para equipos que se utilicen fuera de las instalaciones de la propia oficina?			
58	¿Existen mecanismos para dar respuesta a los eventos de la Seguridad de la Información?			
59	¿Existen un proceso definido para la revocación de permisos cuando se finalice una actividad, puesto de trabajo o cese de contratos?			
60	¿Se establecen protocolos para proteger o eliminar información de equipos que causan baja o van a ser reutilizados?			
61	¿La información proporcionada por los eventos en la Seguridad de la información es tratados para tomar medidas preventivas?			
62	¿Se establecen normas para proteger la información de equipos cuando los usuarios abandonan el puesto de trabajo?			
63	¿Existe un proceso para recopilar evidencias sobre los incidentes en la seguridad de la Información?			
64	¿Se ha adoptado una política de "escritorio despejado" para los papeles, medios de almacenamiento removibles y una política de "pantalla limpia" en la infraestructura para el procesamiento de información?			

65	¿Los medios que contienen información, están protegidos en contra del acceso no autorizado, el mal uso o su alteración durante el transporte más allá de los límites físicos de la organización?			

MUCHAS GRACIAS POR SU COLABORACIÓN

ANEXO N° 03

ENCUESTA PARA MEDIR LA GESTIÓN DE RIESGOS

Estimado colaborador, la presente encuesta tiene por objetivo identificar la relación existente entre el Sistema de Gestión de Seguridad de la Información y la Gestión de Riesgos en el área informática. La encuesta **es anónima** para lo cual solicito que las preguntas sean respondidas de manera honesta.

INDICACIONES

Marque con una X la respuesta que considere correcta de acuerdo a la pregunta.

1. Siempre **2.** Algunas Veces **3.** Nunca

N°	ITEM	1	2	3
1	¿Determina el área de informática el nivel de riesgos relacionados con TI que está dispuesta a asumir para cumplir con sus objetivos?			
2	¿Frente a los niveles de riesgo y oportunidades aceptables, el área de informática evalúa y aprueba propuestas de tolerancia al riesgo de TI?			
3	¿Determina el área de informática el grado de alineación de la estrategia de riesgos de TI con la estrategia de riesgos organizacionales?			
4	¿Se evalúa con frecuencia los factores de riesgo de TI con anterioridad a las decisiones estratégicas de la organización pendientes?			
5	¿Se determina si el uso de TI se realiza según estándares nacionales e internacionales?			
6	¿La entidad evalúa las actividades de gestión de riesgos para garantizar su alineamiento con las capacidades de la organización para pérdidas relacionadas con TI?			
7	¿Se promueve una cultura consciente de los riesgos de TI que impulse a la identificación proactiva de riesgos, oportunidades e impactos potenciales en la entidad?			
8	¿Se orienta la integración de las operaciones y la estrategia de riesgos de TI con las decisiones y operaciones estratégicas de la entidad?			
9	¿Se comunican los planes de acción frente a un riesgo?			
10	¿Se realiza capacitación para la implementación de mecanismos apropiados para responder rápidamente a los riesgos cambiantes y se notifica a los niveles adecuados de gestión?			
11	¿Se supervisa con regularidad, hasta qué punto se gestiona el perfil de riesgo dentro del apetito del riesgo?			
12	¿Se supervisa con regularidad las metas y métricas clave de gestión de los procesos de gobierno y gestión del riesgo respecto a los objetivos?			
13	¿Se facilita la revisión por las partes interesadas del progreso de la entidad hacia el control de los riesgos identificados?			
14	¿Se informa cualquier problema de gestión de riesgos al responsable del área?			
15	¿Se asegura que las decisiones de la organización se toman conscientes de los riegos?			
16	¿El uso de TI está sujeto a una valoración y evaluación de riesgos adecuada?			
17	¿La entidad evalúa las actividades de gestión de riesgos para garantizar su alineamiento con la tolerancia de los encargados frente a pérdidas relacionadas con TI?			
18	¿Los empleados cuentan con la formación, recursos y habilidades necesarias para asumir responsabilidades frente a un riesgo?			

ANEXO N° 04
Alfa de Cronbach
Sistema de Gestión de Seguridad de la Información

UE	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29
1	1	2	2	2	3	3	2	2	3	3	3	3	2	2	3	3	3	3	3	3	3	3	3	3	3	3	3	2	3
2	1	1	2	1	1	2	1	1	2	2	1	2	1	1	2	3	3	3	2	3	3	2	3	2	3	2	2	1	2
3	2	2	2	2	1	2	1	1	2	2	2	2	1	1	1	2	2	3	2	2	2	1	3	2	3	3	1	1	2
4	1	1	3	2	1	3	1	1	1	1	1	2	3	2	2	1	1	3	3	1	2	2	3	2	3	3	2	2	2
5	1	1	2	1	2	2	3	2	1	1	1	3	1	3	3	2	2	2	2	2	2	3	3	3	2	2	2	2	2
6	2	3	3	3	3	3	3	3	3	3	3	3	1	1	1	2	2	2	2	2	2	2	2	2	2	1	1	1	1
7	1	1	2	1	1	3	2	1	1	1	1	2	1	2	2	1	1	2	2	1	3	2	2	1	2	1	1	2	2
Var	**0.24**	**0.62**	**0.24**	**0.57**	**0.91**	**0.29**	**0.81**	**0.62**	**0.81**	**0.81**	**0.91**	**0.29**	**0.62**	**0.57**	**0.67**	**0.67**	**0.67**	**0.29**	**0.29**	**0.67**	**0.29**	**0.48**	**0.24**	**0.48**	**0.29**	**0.81**	**0.57**	**0.29**	**0.33**

P30	P31	P32	P33	P34	P35	P36	P37	P38	P39	P40	P41	P42	P43	P44	P45	P46	P47	P48	P49	P50	P51	P52	P53	P54
3	2	2	3	3	3	3	2	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
3	1	2	2	3	2	3	1	2	2	1	2	2	1	2	2	3	2	1	2	2	1	1	2	1
2	2	2	2	2	2	3	1	1	1	1	2	2	2	2	2	2	2	2	2	2	1	1	2	1
3	1	2	2	2	2	2	1	1	2	2	2	2	2	2	2	2	2	2	2	3	1	2	2	1
2	3	3	2	2	2	2	3	3	2	3	2	3	3	2	2	3	3	3	2	2	2	3	3	2
1	1	1	2	3	2	3	3	2	3	3	2	1	1	3	2	2	3	3	3	3	2	3	2	2
2	1	2	1	2	1	2	1	2	2	1	2	2	1	2	2	2	1	2	2	1	2	1	2	1
0.57	**0.62**	**0.33**	**0.33**	**0.29**	**0.33**	**0.29**	**0.91**	**0.48**	**0.48**	**1**	**0.14**	**0.48**	**0.81**	**0.29**	**0.14**	**0.29**	**0.57**	**0.57**	**0.29**	**0.57**	**0.57**	**1**	**0.29**	**0.62**

P57	P58	P59	P60	P61	P62	P63	P64	P65	SUMA	
3	3	3	3	2	2	2	2	3	**177**	
2	2	1	2	2	2	3	2	2	**123**	
2	1	1	2	1	1	2	2	2	**114**	
2	2	2	2	2	2	2	2	2	**123**	
3	3	2	3	3	3	2	2	2	**148**	
2	2	2	2	3	2	2	2	1	**140**	
3	1	3	2	1	2	2	2	2	**106**	
0.29	**0.67**	**0.67**	**0.24**	**0.67**	**0.33**	**0.14**	**0**	**0.33**	**31.571**	**Suma de las varianzas de los ítems**
									583.33	**Varianza de los totales**

PARAMETROS

Numero de Ítems (K)	65
Suma de las varianzas de los ítems	31.57
Varianza de los totales	583.3
ALFA DE CROMBACH	0.961

Confiable

La fórmula para calcular el mismo es:

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\sum_{i=1}^{k} S_i^2}{S_x^2}\right]$$

donde:

K = cantidad de preguntas del instrumento evaluativo.

Sx^2 = varianza de las calificaciones del instrumento evaluativo.

S_i^2 = varianza de la i-esima pregunta del instrumento evaluativo.

ANEXO N° 05
Alfa de Cronbach
Gestión de Riesgos

UE	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	SUMA	
1	2	2	2	2	2	2	2	2	3	1	2	2	2	1	2	2	2	2	35	
2	3	2	2	2	2	2	2	3	1	1	2	2	2	1	2	3	3	3	38	
3	1	2	1	1	1	2	2	2	1	2	2	2	1	1	1	2	2	2	28	
4	1	3	2	2	1	2	2	2	1	1	2	1	1	1	1	2	1	2	28	
5	2	2	1	1	2	2	2	2	2	2	2	1	1	2	1	2	2	2	31	
6	1	1	1	1	1	2	2	1	1	2	1	1	2	2	2	2	2	2	27	
7	1	1	1	2	1	2	1	1	1	2	1	1	2	1	2	2	2	1	25	
Var	0.62	0.48	0.29	0.29	0.29	0	0.14	0.48	0.62	0.29	0.24	0.29	0.29	0.24	0.29	0.14	0.33	0.33	5.619	Suma de las varianzas de los ítems
																			21.905	Varianza de los totales

PARAMETROS

Numero de Ítems (K)	18
Suma de las varianzas de los ítems	5.619
Varianza de los totales	21.9
ALFA DE CROMBACH	0.787
	Confiable

La fórmula para calcular el mismo es:

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\sum_{i=1}^{k} S_i^2}{S_x^2}\right]$$

donde:

K = cantidad de preguntas del instrumento evaluativo.

Sx^2 = varianza de las calificaciones del instrumento evaluativo.

S_i^2 = varianza de la i-esima pregunta del instrumento evaluativo.

ANEXO N° 06

UNIVERSIDAD PRIVADA DEL NORTE

FICHA PARA VALIDACION DEL INSTRUMENTO

I. **REFERENCIA**

1.1. Experto: Luis Miguel Cotrina Malca
1.2. Especialidad: Gerencia de Proyectos, Tecnologías de Información y Liderazgo
1.3. Cargo actual: Gerente y Project Manager en Daccos.
1.4. Grado académico: Maestro en Gerencia de Proyectos y Liderazgo.
1.5. Institución: University of Maryland, Estados Unidos
1.6. Tipo de instrumento: Encuesta
1.7. Lugar y fecha: Cajamarca, 09 de julio de 2020

II. **TABLA DE VALORACION POR EVIDENCIAS**

N°	EVIDENCIAS	VALORACION					
		5	4	3	2	1	0
1	Pertinencia de indicadores		X				
2	Formulado con lenguaje apropiado	X					
3	Adecuado para los sujetos en estudio		X				
4	Facilita la prueba de hipótesis	X					
5	Suficiencia para medir la variable		X				
6	Facilita la interpretación del instrumento		X				
7	Acorde al avance de la ciencia y tecnología		X				
8	Expresado en hechos perceptibles		X				
9	Tiene secuencia lógica	X					
10	Basado en aspectos teóricos		X				
	Total	15	28				

Coeficiente de valoración porcentual: c = 86%

III. **OBSERVACIONES Y/O RECOMENDACIONES**

Instrumento de la variable gestión de riesgos, validado a la bachiller Sarita Narro Mestanza.

.....
Firma y sello del Experto

FICHA PARA VALIDACION DEL INSTRUMENTO

IV. REFERENCIA

- 4.1. Experto: Luis Miguel Cotrina Malca
- 4.2. Especialidad: Gerencia de Proyectos, Tecnologías de Información y Liderazgo
- 4.3. Cargo actual: Gerente y Project Manager en Daccos.
- 4.4. Grado académico: Maestro en Gerencia de Proyectos y Liderazgo.
- 4.5. Institución: University of Maryland, Estados Unidos
- 4.6. Tipo de instrumento: Encuesta
- 4.7. Lugar y fecha: Cajamarca, 09 de julio de 2020

V. TABLA DE VALORACION POR EVIDENCIAS

N°	EVIDENCIAS	VALORACION					
		5	4	3	2	1	0
1	Pertinencia de indicadores		X				
2	Formulado con lenguaje apropiado	X					
3	Adecuado para los sujetos en estudio		X				
4	Facilita la prueba de hipótesis		X				
5	Suficiencia para medir la variable		X				
6	Facilita la interpretación del instrumento		X				
7	Acorde al avance de la ciencia y tecnología		X				
8	Expresado en hechos perceptibles		X				
9	Tiene secuencia lógica	X					
10	Basado en aspectos teóricos		X				
	Total	10	32				

Coeficiente de valoración porcentual: c = 84%

VI. OBSERVACIONES Y/O RECOMENDACIONES

Instrumento de la variable sistema de gestión de seguridad de la información, validado a la bachiller Sarita Narro Mestanza.

.....

Firma y sello del Experto

FICHA PARA VALIDACION DEL INSTRUMENTO

I. REFERENCIA

1.1. Experto: Juan Carlos Llaque Quiroz
1.2. Especialidad: Administración y Negocios
1.3. Cargo actual: Docente Escuela de Postgrado UPN
1.4. Grado académico:
- Licenciado en Administración de Empresas
- MBA (Magister en Administración de Negocios)
- Maestro en Dirección y Gestión del Talento Humano

1.5. Institución: Universidad Privada del Norte
1.6. Tipo de instrumento: Cuestionario
1.7. Lugar y fecha: Cajamarca, 30 de junio de 2020

II. TABLA DE VALORACION POR EVIDENCIAS

N°	EVIDENCIAS	VALORACION					
		5	4	3	2	1	0
1	Pertinencia de indicadores		X				
2	Formulado con lenguaje apropiado		X				
3	Adecuado para los sujetos en estudio		X				
4	Facilita la prueba de hipótesis		X				
5	Suficiencia para medir la variable		X				
6	Facilita la interpretación del instrumento		X				
7	Acorde al avance de la ciencia y tecnologia		X				
8	Expresado en hechos perceptibles		X				
9	Tiene secuencia lógica	X					
10	Basado en aspectos teóricos		X				
	Total	05	36				

Coeficiente de valoración porcentual: c = 82%

III. OBSERVACIONES Y/O RECOMENDACIONES

Instrumento de la variable gestión de riesgos, validado a la bachiller Sarita Narro Mestanza.

Firma y sello del Experto

FICHA PARA VALIDACION DEL INSTRUMENTO

IV. REFERENCIA

4.1. Experto: Juan Carlos Llaque Quiroz
4.2. Especialidad: Administración y Negocios
4.3. Cargo actual: Docente Escuela de Postgrado UPN
4.4. Grado académico:
- Licenciado en Administración de Empresas
- MBA (Magister en Administración de Negocios)
- Maestro en Dirección y Gestión del Talento Humano

4.5. Institución: Universidad Privada del Norte
4.6. Tipo de instrumento: Cuestionario
4.7. Lugar y fecha: Cajamarca, 30 de junio de 2020

V. TABLA DE VALORACION POR EVIDENCIAS

Nº	EVIDENCIAS	VALORACION					
		5	4	3	2	1	0
1	Pertinencia de indicadores		X				
2	Formulado con lenguaje apropiado		X				
3	Adecuado para los sujetos en estudio		X				
4	Facilita la prueba de hipótesis		X				
5	Suficiencia para medir la variable		X				
6	Facilita la interpretación del instrumento		X				
7	Acorde al avance de la ciencia y tecnologia		X				
8	Expresado en hechos perceptibles		X				
9	Tiene secuencia lógica	X					
10	Basado en aspectos teóricos		X				
	Total	05	36				

Coeficiente de valoración porcentual: c = 82%

VI. OBSERVACIONES Y/O RECOMENDACIONES

Instrumento de la variable sistema de gestión de seguridad de la información, validado a la bachiller Sarita Narro Mestanza.

Firma y sello del Experto