UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: CASO DE ESTUDIO UNIVERSIDAD NACIONAL INTERCULTURAL FABIOLA SALAZAR LEGUÍA

PARA OPTAR TÍTULO PROFESIONAL DE

INGENIERO DE SISTEMAS

Autora:

Bach. Segura Huaman Mavila

ORCID: https://orcid.org/0000-0001-6098-648X

Asesor:

Mg. Bravo Ruiz Jaime Arturo

ORCID: https://orcid.org/0000-0003-1929-3969

Línea de Investigación:

Infraestructura, tecnología y medio ambiente

Pimentel – Perú 2022

APROBACIÓN DEL JURADO

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: CASO DE ESTUDIO UNIVERSIDAD NACIONAL INTERCULTURAL FABIOLA SALAZAR LEGUÍA

_____

Bach, Segura Huaman Mavila

Autor

_____

Mg, Bravo Ruiz Jaime Arturo

Asesor

_____

Mg, Tuesta Monteza Victor Alexci

Presidente de Jurado

_____

Mg, Bances Saavedra David Enrique

Secretario de Jurado

_____

Mg, Fuentes Adrianzen Denny John

Vocal de Jurado

Dedicatoria

A la memoria de mis padres Amado Segura Delgado y Nélida Huaman Castro, por su amor infinito, por ellos que siempre me inculcaron valores y me enseñaron a luchar por lograr nuestros sueños.

A mis hijos Diego André y Erman Leonardo, quienes son mi motor y motivo y me dan la fuerza para seguir adelante en esta etapa de mi vida profesional.

Mavila Segura Huaman

Agradecimiento

Quiero agradecer en primer lugar a Dios por darme la oportunidad y permitir que ahora pueda realizarme profesionalmente.

A la universidad Señor de Sipán y su plana docente por los conocimientos y experiencias transmitidas durante estos años de estudio.

Al ingeniero Tuesta Monteza Victor Alexci por su apoyo y capacidad de poder guiarme en mis avances y desarrollar este proyecto de tesis de manera exitosa.

A mi asesor el ingeniero Bravo Ruiz Jaime Arturo por su asesoramiento y apoyo durante el desarrollo del proyecto de tesis.

A mis padres: Amado Segura Delgado y Nélida Huaman Castro con mucho cariño, por su dedicación, su amor y enseñanzas de vida que me sirvieron de mucho, gracias a ellos es todo lo que soy.

A mi esposo Erman Ramírez Bernal, por ser un soporte importante, por comprenderme y apoyarme para seguir adelante en mi carrera profesional.

A mis hermanas Marcela, Avila Karin y Sonia por su apoyo constante, brindándome fortaleza para seguir adelante en esta nueva etapa de mi vida profesional.

Mavila Segura Huaman

Resumen

La presente investigación se realiza en la Universidad Nacional Intercultural Fabiola Salazar Leguía, ubicada en la ciudad de Bagua departamento de Amazonas, la cual cuenta con dos sedes: sede académica ubicada en Jr. Ancash N° 520 y la sede administrativa en Jr. Comercio N°128. Actualmente ofrece el servicio educativo superior universitario ofertando las carreras de pregrado: Ingeniería Civil, Negocios Globales y Biotecnología.

El objetivo es: Diseñar un Sistema de Gestión de Seguridad de la información, para garantizar la seguridad de los activos de información de los procesos organizacionales mediante un modelo estructurado de carácter preventivo (SGSI) que se encuentra basado en la norma ISO/IEC 27000:2013, Cobit5, PMBOK, ITIL y las metodologías: Magerit, Octave, de la norma ISO/IEC 27005 y la norma ISO/IEC 31000, relacionados al análisis de riesgos.

Tipo de investigación: cualitativa no experimental, para ello se contó con una población de 7 procesos y una muestra de 3 procesos de la Universidad caso de estudio, mediante información recolectada referente a los activos de información, el cual radica en la representación en cada uno de los diferentes procesos en cada área de la institución, cada uno con sus respectivos controles de entrada, proceso y salida.

Se presentan los resultados aplicando la fase donde se analiza y evalúan los riesgos mediante el uso de herramientas (BPM Bizagi Modeler, Microsoft Excel) y técnicas como la entrevista al personal de trabajo y mediante observación directa a través de programación de visitas en la universidad UNIFSL Bagua.

Posterior a ello se efectúa un análisis de controles en el cual se fundamenta en la declaración de aplicabilidad en relación con los requerimientos de la institución y desde allí proponer políticas de seguridad teniendo en cuenta los límites de cumplimiento institucional, donde su objetivo es dar un apoyo adecuado la seguridad de la información.

Palabras clave

Sistema, Sistema de seguridad de la información, seguridad de la información, diseño, gestión

Abstract

This research is carried out at the Fabiola Salazar Leguía National Intercultural University, located in the city of Bagua, department of Amazonas, which has two locations: academic headquarters located at Jr. Ancash No. 520 and the administrative headquarters at Jr. Comercio No. °128. It currently offers the university higher education service offering undergraduate careers: Civil Engineering, Global Business and Biotechnology.

The objective is: To design an Information Security Management System, to guarantee the security of the information assets of the organizational processes through a structured model of a preventive nature (ISMS) that is based on the ISO/IEC 27000 standard: 2013, Cobit5, PMBOK, ITIL and the methodologies: Magerit, Octave, of the ISO/IEC 27005 standard and the ISO/IEC 31000 standard, related to risk analysis.

Type of research: non-experimental qualitative, for this there was a population of 7 processes and a sample of 3 processes of the University case study, through information collected regarding information assets, which lies in the representation in each one of the different processes in each area of the institution, each with their respective input, process and output controls.

The results are presented applying the phase where the risks are analyzed and evaluated through the use of tools (BPM Bizagi Modeler, Microsoft Excel) and techniques such as the interview with the work staff and through direct observation through the programming of visits to the UNIFSL University Bagua.

After that, an analysis of controls is carried out, which is based on the statement of applicability in relation to the requirements of the institution and from there, propose security policies taking into account the limits of institutional compliance, where its objective is to provide support adequate information security.

Keywords

System, Information security system, information security, design, management

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

I. INTRODUCCIÓN

Toda organización o empresa maneja información la cual representa un activo muy valioso por tanto se deberá asumir con mucho cuidado cuando se realicen controles para salvaguardar la seguridad de la misma cuando exista la posibilidad de intromisiones fruto de la existencia de las vulnerabilidades en los sistemas de seguridad de la información, el cual garantiza de esta manera la integridad, confidencialidad y disponibilidad de la información.

La presente investigación denominada propone un diseño de un Sistema de Gestión de Seguridad de la información, consta de tres capítulos que se basa en el estándar ISO 27000, donde existe un aumento en los campos de aplicabilidad de salvaguardias como también contribuir en el establecimiento de políticas de seguridad, y gestión de los riesgos asociados.

En el Capítulo I, se refiere al planteamiento del problema, antecedentes de estudio, abordaje teórico, formulación del problema, justificación e importancia del estudio, objetivos y limitaciones de la investigación.

En el Capítulo II, denominado Material y método, aborda el tipo de estudio y diseño de la investigación, escenario de estudios, caracterización de sujetos, técnica e instrumentos y procedimiento para la recolección de datos, procedimiento para el análisis de datos, criterios éticos y de rigor científico.

En el Capítulo III, se sustenta los resultados, donde aborda el análisis y discusión de los resultados y las consideraciones finales de la investigación de recolección de datos y el procedimiento para recolectar datos.

También se sustenta las referencias y los anexos.

Con lo anteriormente dicho, en esta investigación se tiene como objetivo tomar conciencia acerca del valor que tiene la seguridad para los activos de información en la institución y el compromiso para su ejecución en toda organización.

1.1. Planteamiento del problema

La información son valiosos activos de los que toda organización depende para su buena actividad y funcionamiento, por ello es indispensable conservar su integridad, confidencialidad y disponibilidad para conseguir los objetivos del negocio, ya que toda organización presenta un universo de problemas con respecto a la seguridad de información para los diferentes procesos de negocio, es por ello que es preciso conocer cualquier tipo de amenaza y/o riesgos para una debida salvaguardia de los activos de la Universidad Nacional "Fabiola Salazar Leguía" – Bagua consiguiendo así la seguridad de estos ante cualquier tipo de situación que pueda verse afectada la institución.

Se propone en el presente proyecto efectuar un diseño de sistemas de seguridad de la información (SGSI) basados estándares, modelos y metodologías de evaluación de riesgos, con la finalidad de que exista una reducción de amenazas o mitigar riesgos mediante políticas de seguridad de la información incluso considerar de una manera que sea asequible para la institución.

El presente modelo es una propuesta para la Universidad Nacional Intercultural "Fabiola Salazar Leguía" de Bagua mediante el cual aportará en la mejora la competitividad en el mercado, diferenciándolo de otras instituciones y así mejora su imagen y confianza con sus usuarios, proveedores y trabajadores.
Los procesos del alcance serán:

. Proceso Matrícula
. Proceso Admisión
. Proceso Notas
. Proceso Biblioteca
. Proceso Planilla
. Proceso Trámite Documentario
. Proceso Carga Horaria

1.2. Antecedentes de estudio

1.2.1. A nivel Internacional

De acuerdo con Aguirre Cardona, J. y Aristizabal Betancourt, C. (2013), en su investigación denominada: “Diseño del Sistema de Gestión de Seguridad de la Información para el grupo empresarial la ofrenda”. La metodología que empleó fue: Análisis de varios tipos de riesgos y amenazas, con la finalidad de fundamentar y realizar argumentación de la investigación, el desarrollo y posteriormente la implementación de un sistema de seguridad de la información, Aguirre Cardona, J. y Aristizabal Betancourt, C. (2013) “Diseño de encuestas y entrevistas al personal con manejo de procesos y sub procesos de vital importancia para la organización. Diseño del sistema de gestión de la seguridad de la información. Pruebas y la validación del SGSI”. Donde concluye: “De esta investigación se logra determinar que el Sistema de Gestión de la Seguridad de la Información (SGSI) beneficia de gran manera a la institución en mención, el cual es un aporte para constituir políticas y procedimientos referentes a los objetivos de negocio, manteniendo el nivel de exposición debajo del nivel del riesgo que la misma institución ha visto conveniente obtener”.

La aportación de esta investigación es de gran significancia en términos de seguridad de la información, es por ello su importancia tomando referencia en estos sistemas a este proyecto de investigación.

Velasco Melo, H (2011), en su investigación realizada la ciudad de Barranquilla, el cual denomina: “El Derecho Informático y la Gestión de la Seguridad de la Información una perspectiva establecida en la normativa ISO 27001”, utiliza la normativa ISO 27001 como sistemática, donde los resultados conseguidos son: “Protección de datos de las personas; la contratación de recursos referentes a la informática y telemática; derecho laboral y prestaciones de servicios, relacionado a la disposición referente a lo tecnológico; servicios de E- commerce; la propiedad intelectual, y el tratamiento de las eventualidades informáticas”. Velasco Melo, H. (2011)

La importancia de esta investigación es: Que a través de las TIC requieren del Derecho objeciones con innovación y global en relación a las contradicciones el cual estas son específicos; de esta manera, a los operadores normativos les corresponde tener suficientemente preparación con el fin de brindar apoyo a la sociedad y solucionar problemáticas en términos de la Informática-Derecho.

Voutssas, J. (2011), en su proyecto de investigación realizada en la ciudad de México, al cual denomina: “Preservación documental digital y seguridad informática, en donde se utilizó como metodología las normativas ISO/17799 o las normas ISO/IEC 27001 y 27002” el cual señala en su resultado: “Diseño para cualquier tipo de organización en el ámbito de seguridad informática que precisamente no requiere que desboquen en la conservación de registros digitales en periodos extensos”.

Es de gran importancia que hoy en día toda organización cuente con protocolos de seguridad que brinden la protección de los activos de mucho valor que es la información, Políticas de seguridad, el cual estén documentadas y puestas en marcha y que genere buenas prácticas por todos los involucrados dentro de la organización, el cual también deben ser actualizados y revisados por control interno y capacitado.

En Santiago de Cuba, Días Ricardo, Y. et al. (2014), realizaron una investigación que denominaron: “Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín, se utilizó la metodología UML”, consiguiendo el siguiente resultado: “Es un trabajo muy eficaz de la indagación de seguridad informática, con una perspectiva no experimental cuantitativo”. “En este estudio elaborado se detectó insuficiencias durante el transcurso de gestión de información de seguridad informática, por cuanto se realizó un plan a fin de determinar e implantar el sistema el cual se ha desarrollado”, Días, R. y otros (2014).

Barcos, S. (2010), en su investigación realizada en la ciudad La Plata el cual denomina: “Reflexiones relacionados con los sistemas de información universitarios frente a los retos y modificaciones provocados a través de los procesos de estimación y acreditación”, en este trabajo se empleó como metodología el análisis documental con un diseño no experimental. Como resultado obtenemos: Barcos, S. (2010) “La Investigación representa y/o expone el escenario a partir la severidad en su metodología, donde manifiesta regularidades en el cual sostiene la elaboración de teorías que genera impacto en el entorno únicamente si se consigue agregar de nuevo al proceso puesto que es soporte del proceso de aprendizaje y enseñanza”.

Los sistemas de información tienen que seguir un nuevo patrón de integración que a través de las funciones de docencia, extensión e investigación reflejará las variaciones en el modelo y su modalidad de gestión.

1.2.2 A Nivel Nacional

Chuna, G. (2018), en sus investigaciones para su propuesta de un SGSI que se basa en controles que se ha seleccionado de la Norma Técnica Peruana ISO/IEC 27001:2014, que se encuentra en vigencia para la Dirección Regional de Trabajo y Promoción de Empleo – Filial Piura. En el cual se evidenció el diagnóstico de los activos de información en la institución, donde se pudo identificar vulnerabilidades y riesgos el cual se evaluaron mediante la metodología Magerit, además, se seleccionó los controles adecuados para mitigar los riesgos basada en la norma mencionada, mediante la declaración de aplicabilidad.

Para ello se realizó el planteamiento de controles y políticas de seguridad acorde a los controles que se ha seleccionado. En esta investigación de propuesta se realiza con la finalidad de proponer la utilización admisible hacia los activos, implantar los mecanismos que van a permitir un adecuado manejo de posibles incidentes inesperados mediante el uso del plan de tratamiento de riesgos, identificación de roles y responsabilidades,

todo ello para dar pronta respuesta ante incidencias y poder salvaguardar los activos de la institución

Aguirre Mollehuanca, D. (2014), en la ciudad de Lima, en su proyecto de investigación denominada: “Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A.” donde utiliza a modo de herramienta a la norma técnica peruana NTP-ISO/IEC 27001:2008 y de la NTP ISO/IEC 17799:2007, el cual hace uso de la metodología Magerit; las cuales brindan los controles y recomendaciones necesarios para el tratamiento de los riesgos en una organización.

1.2.3 A Nivel Local

Alcántara Flores, J. (2015), en su proyecto de indagación realizado en la ciudad de Chiclayo: “Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, trabajo realizado con el fin de dar apoyo en la seguridad en los Sistemas Informáticos de la Comisaria del Norte P.N.P en la ciudad de Chiclayo”. La herramienta que se utilizó fue la normativa ISO /IEC 27001 y como metodología se utilizó Magerit. Como resultado se obtuvo: “Como producto acreditable un protocolo estándar para la observación de registros y documentaciones, y en cuanto a la seguridad de la información, como metodología concerniente a la evaluación y tratamiento de riesgo, entre otros”.

La importancia del presente aporte se haya orientado en la obtención de una Guía de implementación de la seguridad el cual se encuentra basado en la normativa ISO/IEC 27001, donde suministra soporte a la seguridad de los sistemas de información en el establecimiento Policial Comisaria del Norte – Chiclayo.

1.3. Abordaje teórico

1.3.1. Términos y definiciones

Activo

Según Parra Alvernia, H. et al. (2015), activo es todo tipo de información o sistema en relación con los procedimientos del mismo y en el cual posee una valoración para la institución.

Según la (ISO 27000, s. f.) citado por Cuevas Riaño, E. (2015) señala que es primordial la capacitación del personal de la institución, en relacionado con las políticas de seguridad esto con la finalidad de reducir riesgos y amenazas del cual puedan verse afectados los activos de información, ya que estos se presentan de manera documentada, informativa, tecnológica, medios físicos, digitales y humana.

Activo de información

Es considerado un recurso valioso para toda organización, ya que pueden contener información relevante como por ejemplo Bases de Datos con diversos tipos de registros y que se debe velar por su protección, (27001 ACADEMY), citado por Zacarías Villafranca, J. (2017)

Según Díaz Fonseca, D. Y Ramírez Rodríguez, M. (2015), los activos de información son base de datos el cual se encuentran contenidos en los equipos computacionales, documentos del sistema, procesos y procedimientos de operaciones, información archivada en medios físicos y digitales, y por ende es de vital importancia que estos sean protegidos teniendo en cuenta su confidencialidad, integridad y disponibilidad.

Información

Según Avenía Delgado, C. (2017), son los conocimientos que pueden ser expresados en documentos, así como también pueden existir diversas maneras: impresiones, papel escrito, almacenamiento electrónico, transmisión por medios electrónicos, presentación de imágenes,

conversaciones expuestas, todo aquel conjunto de datos el cual están debidamente organizados, todo a cargo de una entidad el cual posean valor para la misma.

Según Parra Alvernia, H. et al. (2015), información es toda comunicación o representación de conocimientos como los datos, en cualquiera de las formas (textual, numérica, gráfica, cartográfica, narrativa o audiovisual, y en cualquier medio, (magnético, impreso en papel, en pantallas de computadoras, audiovisual u otro).

Además, Parra Alvernia, H. et al. (2015), hace referencia que la información es toda comunicación o representación de conocimiento el cual, los datos se pueden representar de forma textual, numérica, gráfica, cartográfica, narrativa o audiovisual, y a través de cualquier medio: magnéticos, papel impreso, pantalla computarizada, etc.

Seguridad de Información (SI)

Suarez Gonzales, R. (2018), sostiene que la SI radica en la conservación de su confidencialidad, integridad y disponibilidad, mediante un conjunto de metodologías, de igual manera también los sistemas comprometidos en su tratamiento, que es de vital importancia en una institución.

La seguridad de la información engloba cada uno de los mecanismos de protección del ser humano, de las instituciones, así como también de los sistemas tecnológicos el cual permite proteger y resguardar los activos de información ante amenazas de la disponibilidad de la misma. (Cruz-Zapata; Fernández-Alemán; Toval, 2015); citado por Cárdenas Solano, L. et al. (2016)

Para Parra Alvernia, H. et al. (2015), la seguridad de la información es la conservación de la misma a través del tiempo, aplicado a su confidencialidad, integridad, disponibilidad, autenticidad, auditabilidad, la protección a la duplicación y al no repudio, con el objetivo de salvaguardar los activos de información.

Para Solarte Solarte, F. et al. (2015), la seguridad de la información está estrechamente relacionada con las medidas de prevención que se aplican con la finalidad de realizar la salvaguardia y protección de la información mediante la confidencialidad, disponibilidad e integridad. Tal es así que toda organización debe tomar medidas y adaptarse a metodologías para afirmar la protección de los activos, debido a que existen en diversos formatos.

La SI comprende en el resguardo de la confidencialidad, integridad y disponibilidad de los activos de información, así también de los sistemas comprometidos en su tratamiento en una institución. Por lo tanto, esta trilogía conforma la base en la cual se establece toda edificación de la seguridad de la información:

•**Confidencialidad:** Para la OCDE (Organización para la Cooperación Económica y el Desarrollo), citado por Avenía Delgado, C. (2017), el cual precisa en sus lineamientos de la Seguridad de los Sistemas de Información, que la confidencialidad de los datos y la información deben tener disponibilidad solo a personas, organizaciones o mecanismos autorizados, evitando así todo tipo de divulgación.

• **Integridad:** Para Carolina Nieves, A. (2017)**,** la información y sus técnicas de proceso deben tener y mantener sustento de precisión y completitud de la información.

• **Disponibilidad:** Teniendo en cuenta el programa MAGERIT, citado por Avenía Delgado, C. (2017), sostiene que la accesibilidad de la información debe estar presente en cualquier momento, esto quiere decir que debe estar disponible públicamente (personas, entidades, procesos autorizados) para que puedan acceder en el momento que lo requieran.

Gestión de Seguridad de la Información (GSI)

Gómez, A. & Suarez, C. (2005), afirma que para tener que implementar el SGSI en una institución es necesaria una estructura organizativa, el cual

abarca la política, los procesos y los recursos en el que comprende el sistema general de gestión de toda institución.

Sistema de Gestión de Seguridad de la Información (SGSI)

De acuerdo con Merino Bada, C. & Cañizares Sales, R. (2014), un SGSI, es la estructura funcional de las organizaciones mediante el cual se encuentra integrado: la misión, visión, valores, objetivos, políticas, procedimientos, registros e indicadores, unidos componentes formado el sistema para que sea eficaz y eficiente en sus procesos.

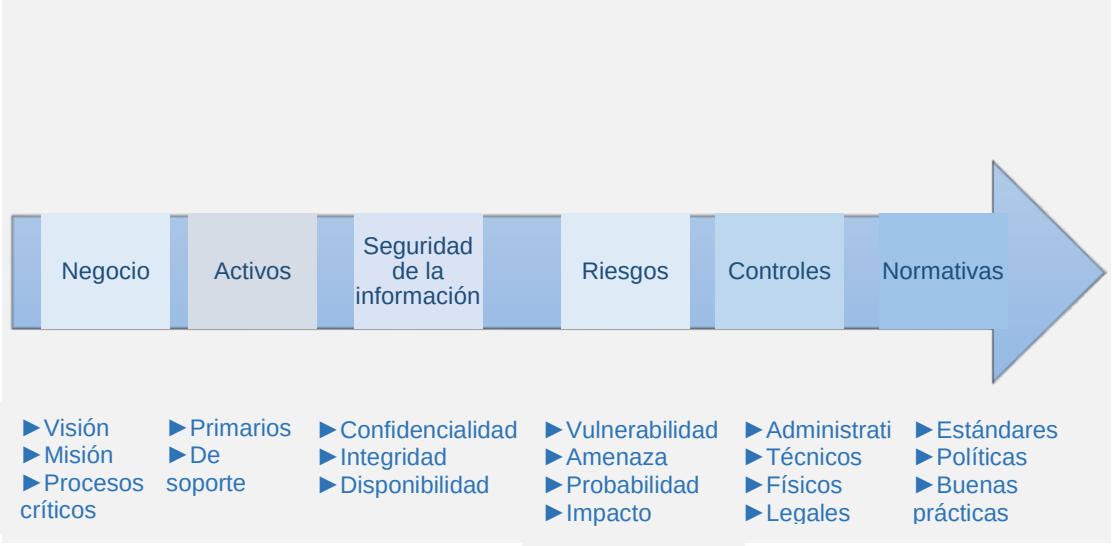


Figura 1: Ejes y elemento de la gestión de la seguridad de la información

Amenaza.

Según Ledezma Espin, D. (2015), amenaza es la oportunidad de ataque al sistema por diversos factores que pueden ser personas, dispositivos e incidencias no deseadas, el cual aprovechando su vulnerabilidad ocasionarían graves daños. Existen diversos tipos de amenaza tanto físicas, del sistema, dispositivos de entrada, por error intencionado de usuarios y/o manipulación, modificación y extracción de los activos de información, y que de los cuales se debe tener en cuenta para su debida protección.

Para Cuevas Riaño, E. (2015), una amenaza es cualquier evento o suceso con un potencial que acecha perjudicando de forma negativa a las organizaciones ocasionando graves daños en las operaciones organizacionales el cual incluyen: misión, funciones organizacionales, imagen institucional, activos de la organización, personas, diferentes organizaciones o el Estado mediante un sistema de información con accesos no autorizados, pérdida de información, difusión o de información modificada y carencia de servicio.

Vulnerabilidad

De acuerdo con Avenía Delgado, C. (2017), es la debilidad de un activo el cual consigue ser explotado por una o más amenazas afectando así el sistema de información, operaciones de seguridad del sistema, control interno o implementación el cual podría ser explotada por una fuente de amenaza.

Riesgo

Según Avenía Delgado, C. (2017), es la posibilidad de que una amenaza sea provocada, es decir que es probable que el ataque sea producido por parte de la vulnerabilidad que se encuentra por la amenaza. Es por ello que el riesgo permite la toma de decisiones y el aseguramiento de la protección del sistema.

Como lo define Aguirre Cardona, J. y Aristizabal Betancourt, C. (2013), el riesgo es cualquier amenaza que pueda causar impedimento a la organización evitando que esta logre sus objetivos.

Tal es así que lo que cause daños a una organización es lo que está relacionado mediante la capacidad donde las amenazas hagan explotar diferentes vulnerabilidades del activo o grupo de activos de información.

1.3.2. Normas ISO 27000

La serie ISO 27000 comprende cada una de las normativas con respecto a la seguridad de la información. Las más relevantes de esta familia son las normativas ISO 27001 e ISO 27002.

La normativa ISO 27001, es aquella por el cual las organizaciones deben optar para la certificación, el cual es la que comprende los requisitos donde establece los lineamientos que se debe dar cumplimiento en una organización, para estar coherente a las buenas prácticas registradas en las otras normas de la familia (principalmente la 27002). Publicada en octubre 2005, actualmente la norma ISO 27002 es la certificación en seguridad con más popularidad y su aplicación es en empresas de todo tipo a nivel mundial.

Además de estas dos normas, podemos adicionar las siguientes que forman parte de la familia 27000:

Tabla 1.

Familia de la ISO/IEC 27000

Norma	Descripción
ISO/IEC 27000	Engloba el vocabulario estándar para el SGSI y equivale a cada una de las normativas.
ISO/IEC 27001	Describe los requerimientos para el establecimiento del SGSI. Esta normativa se publicó como estándar internacional en octubre de 2005. Admite una perspectiva de gestión de riesgos donde favorece el mejoramiento continuo en los procesos.
ISO/IEC 27002	Es una relación de código de buenas prácticas para administrar la seguridad de la información. Se publicó en julio de 2005 como ISO 17799:2005 y luego oficialmente se llamó ISO/IEC 27002:2005 el 1 de julio de 2007. Anteriormente BS 7799 Parte 1 y la normativa ISO/IEC 17799.
ISO/IEC 27003	La norma ISO 27003 proporciona directrices para implementar un SGSI. Es la columna de la normativa

	ISO/IEC 27001. Su publicación fue el 1 de febrero del 2010.
ISO/IEC 27004	La norma ISO 27004 facilita las métricas para administrar la seguridad de la información, mediante el cual suministra y recomienda, cómo, cuándo y quién realiza medidas de seguridad de la información. Su publicación fue el 7 de diciembre de 2009.
ISO/IEC 27005	La norma ISO 27005 dedicada únicamente gestionar los riesgos en el marco de seguridad de la información. Proporcionando recomendaciones y lineamientos de técnicas y metodologías para evaluar los riesgos de Seguridad en la Información, basados en los procesos de administrar los riesgos de la normativa ISO/IEC 27001.
ISO/IEC 27006	La norma ISO 27006 suministra los requerimientos para la acreditación de las organizaciones mediante el cual facilitan la certificación de los SGSI Esta normativa señala los requerimientos para certificar un SGSI y es utilizada juntamente con la normativa 17021-1, la normativa de acreditación genérica.
ISO/IEC 27007	Guía para auditoría del SGSI.
ISO/IEC 27799:2008	Guía para implementar ISO/IEC 27002 en industrias de la salud.

Nota: Tomado de Ministerio de educación, cultura y deporte. Gobierno de España (2012)

Como implementar la ISO 27000

Según Wang Chi, H. (2010), afirma que la normativa ISO 27000 es un estándar de calidad general orientado a la seguridad de la información y está desarrollada bajo la ISO (en español, Organización Internacional de Estándares) orientado a la seguridad de la información.

Wang Chi, H. (2010), sostiene: "generalmente, contiene todo tipo o forma de información de SI dentro de una organización como son: Datos, comunicaciones, correos electrónicos, faxes, conversaciones, grabaciones,

documentos, fotografías". Donde afirma que conseguir una certificación para el sistema administrativo relacionado con la seguridad de la información (SGSI) en toda institución, el cual es usado concretamente para la implementación del ISO 27001.

El SGSI especifica el estándar para la institución, proporcionando objetivos claros por un propósito observable mediante el cual se puede conseguir y desarrollar referente a ello conforme al estándar de la administración. (Wang Chi, H., 2010).

Instrucciones:

Establecer objetivos.

Wang Chi, H. (2010), señala que cualquier sistema administrativo concerniente a la seguridad de la información le correspondería adquirir vinculado un SGSI en torno adonde se labora". También afirma que los objetivos correctos penderán de la organización y el medio regularizador industrial en donde se está trabajando, por ejemplo, testifica que:

En una entidad bancaria donde se labora con interesados con un elevado patrimonio neto requerirá constituir propósitos mucho más drásticos en relación con la seguridad de la información que una organización ganadera. Wang Chi, H. (2010)

Define el alcance y los límites de los objetivos de tu ISMS.

Wang Chi, H. (2010), sostiene que por cada propósito, se determina un costo que te apoye en la medición del alcance del éxito en una organización. Por ejemplo, garantiza que, si se desea minimizar el dolo en el marco de la SI, se puede crear un propósito que comprenda una disminución de la estafa anual de un 5 al 10 por ciento. También afirma que "si se desea implantar objetivos en distintas áreas dentro de una institución". Como por ejemplo, "El personal del área de ventas, consigue obtener una tasa más elevada de estafas que cualquier función como el área administrativa o de apoyo. Precisar el alcance e implantar los términos optimizará una implementación exitosa". Wang Chi, H. (2010)

Identifica la mejor manera de abordar la evaluación de riesgos.

Según Wang Chi, H. (2010), asevera que los riesgos son acontecimientos que consiguen dificultar la seguridad de los activos de información dentro de una institución. El cual explica en un ejemplo, donde dice que si una organización consigue efectuar una auditoría o contabilización dentro de una organización para la evaluación de riesgos habitualmente junto con sus labores normales. Estos grupos suelen trabajar con objetividad dentro de la organización y constantemente aportan ayuda para establecer y monitorear controles dentro de la organización.

Identificación de los riesgos de mayor relevancia de seguridad en una organización.

Wang Chi, H. (2010), señala que posterior a la evaluación de los riesgos, se obtendrá un inventario de los diferentes eventos de seguridad de la información. Donde se efectúa la priorización de los riesgos para el equipo de ejecución.

Evaluación del entorno de seguridad de la información actual y medición de la amenaza de cada riesgo.

Wang Chi, H. (2010), sostiene que, para medir el desempeño en un periodo largo del tiempo, cada uno de aquellos riesgos de seguridad de la información asimismo se comprometen estar conectados en un objetivo específico.

Creación del plan para tratamiento y mejoramiento sobre estos riesgos.

Según Wang Chi, H. (2010), para que el equipo haga el seguimiento para evaluar de riesgos, el cual cada uno de los riesgos deben tener un inventario de acciones y elecciones con la finalidad de realizar un seguimiento a través del equipo encargado de la evaluación de riesgos.

Wang Chi, H. (2010), resalta que las actividades corresponden proporcionar con mayor claridad para conseguir los objetivos, de la misma manera

controles específicos con la finalidad de lograr realizar el monitoreo de los riesgos. “Cuando existe una institución grande, se realiza la separación del plan en distintos elementos. Podemos decir con un ejemplo, que si se quiere comenzar con un plan piloto, en seguida se realiza el despliegue del plan dentro de la institución”.

Obtener la aprobación de gerencia.

Antes de implementar el plan debe ser ratificado formalmente por la gerencia. Donde se debe realizar un informe general del plan para presentarlo a la organización.

“Asimismo proporciona un orden cronológico para que se apruebe la implementación y se realice la diseminación en todos los niveles de la institución” Wang Chi, H. (2010).

Inicio de la implementación.

Wang Chi, H. (2010), afirma que renueva de forma adecuada los objetivos y los planes de seguridad. Efectúa auditorías internas regularmente reportando a gerencia los resultados con la misma regularidad.

NORMA ISO/IEC 27001

Esta Norma Internacional describe claramente los requisitos en el entorno de una institución para la consecución del establecimiento, asimismo con la ejecución, mantenimiento y mejoramiento continuo un SGSI.

Asimismo, esta Normativa Internacional contiene los requisitos para evaluar los riesgos como también el tratamiento de los mismos, tales que estas se adecuen a la necesidad de la institución. Los requerimientos señalados en esta Normativa Internacional son genéricos el cual tratan de quedar ajustables en toda organización, independiente de su tipo, capacidad o medio que le rodee.

Para el presente proyecto, se utilizará algunos hitos de la normativa para diseñar el SGSI en la Universidad Nacional Intercultural “Fabiola Salazar Leguía” Bagua.

Como lo menciona Solarte Solarte, F. et al. (2015), el software para la administración de Sistemas de Gestión y Modelos de Excelencia, señala que la Normativa ISO 27001 es un procedimiento para el mejoramiento continuo por el cual se puede desarrollar un SGSI, referente a ello se apruebe la evaluación de cualquier clase de riesgos o amenazas capaces de exponer al riesgo los activos de información en una institución bien sea la existencia de daños propia e igualmente datos de terceros.

Asimismo, sustenta que admite la implantación de controles y estrategias más apropiadas con la finalidad de disminuir o reducir tales riesgos.

Así pues, como sucede con la familia de las normativas ISO, la 27001 es un sistema establecido en una perspectiva el cual se basa en el ciclo de Deming o ciclo del mejoramiento continuo. Este ciclo también se le conoce como ciclo PDCA (Plan-Do-Check-Act) que tiene su significado en castellano: Planificar-Hacer-Verificar-Actuar.

La Normativa ISO 27001 plantea el ciclo PDCA que es llevado a las necesidades de un SGSI, el cual se dividiría en cuatro pasos esenciales, el cual cada uno de ellos se encuentra unido a una continuación de actividades:

Tabla 2.

La norma ISO 27001: Aspectos claves de su diseño e implantación

FASES	Aspectos claves
PLANIFICAR	Descripción de las políticas de seguridad Establecimiento del alcance del SGSI Efectuar el análisis de los riesgos Selección de controles. Definición de competencias. Establecimiento del diagrama de procedimientos. Definición de autoridades y responsabilidades
HACER	Establecer el procedimiento de administración de los riesgos, Implantar el SGSI Establecer controles
VERIFICAR	Realizar una Revisión interna del SGSI Ejecutar auditorías internas del SGSI Colocar en curso los indicadores y métricas Realizar revisiones encargado por Gerencia.
ACTUAR	Implantar acciones correctivas Implantar acciones de mejora

Nota: Aspectos claves de su diseño e implantación, tomado de Solarte Solarte, F. et al. (2015)

NORMA ISO/IEC 27002

Según Solarte Solarte, F. et al. (2015), esta normativa contiene una guía de buenas prácticas correspondiente a la seguridad de la información y en donde detalla los objetivos de control y controles recomendables. Comprende 39 objetivos de control y 133 controles, donde se agrupan en 11 dominios. Tal como lo menciona en el capítulo proporcionado, la normativa ISO27001 comprende un adjunto en donde abarca un resumen de los controles de ISO 27002:2005. No es certificable.

NORMA ISO/IEC 27003

Según López Armendaris, D. (2017), está norma está basado en una guía para la implementación de un SGSI además de la información donde define sobre cómo utilizar el modelo de Deming, así como también los requisitos de sus cuatro etapas. Esta normativa tiene sus inicios en el anexo B de la normativa BS7799-2 así como también en la sucesión de documentaciones publicadas por BSI con el pasar del tiempo el cual comprende recomendaciones y guías de implementación.

NORMA ISO/IEC 27004

Según Ledezma Espin, D. (2015), esta norma Puntualizará las métricas y los métodos de medida ajustables para comprobar que un SGSI y los controles correspondientes sean eficaces. Fundamentalmente se utilizan para realizar la medición de los elementos de la fase “Do” (Hacer) del ciclo PDCA.

(27) La estructura de esta norma Internacional se encuentra de la siguiente manera:

- La descripción general del Programa de medición y el Modelo de medición de seguridad de la información, en donde se encuentra especificados en: (Cláusula 5);

- Los compromisos de gestión de las medidas de seguridad de la información por cual se encuentra especificados en: (Cláusula 6); y

- Los constructos de medición y los procesos (planificación y desarrollo, implementación y operación, y mejora de mediciones: Se debe informar los resultados de medición) que se implementarán mediante la presentación de medición de seguridad de la información, el cual están especificados en: (Cláusulas 7-10).

NORMA ISO/IEC 27005

Según Valencia Duque, F. Y Orozco Alzate, M. (2017), la normativa ISO/IEC 27005 en su publicación del 4 de junio de 2008, comprende las

normas para gestionar los riesgos relacionado con la seguridad de la información y es adaptable a toda clase de organizaciones (comerciales, gubernamentales, organizaciones no lucrativas) el cual persiguen un propósito de administrar aquellos riesgos el cual consigan obstaculizar la seguridad de la información en la organización.

Afirma los conocimientos de manera general que están referidos en la norma ISO/IEC 27001 el cual se encuentra planteada de manera que estas sirvan de ayuda en la utilización apacible de la seguridad de la información fundamentada en una perspectiva de gestión de riesgos.

Asimismo, señala que para lograr una mejor comprensión de la normativa ISO/IEC 27005:2008 se deberá obtener conocimientos acerca de conceptos, procesos, modelos y cláusulas explicados en la normativa ISO/IEC 27001 e ISO/IEC 27002 es muy significativo con la finalidad de abordar y entender mejor la normativa ISO/IEC 27005:2008.

NORMA ISO 31000

Según Ramírez Castro, A. & Ortiz Bayona, Z. (2011), esta norma es un estándar adaptable a toda clase de institución, más allá de su entorno, actividades, escenarios comerciales o clase de producto, entre otros elementos. Esta normativa explora a las instituciones para que decidan por implementar un sistema de gestión de riesgos, todo ello mediante un orden de criterios y principios, con el objetivo de reducir los impedimentos que obstaculizan el logro de sus objetivos, existiendo compatibilidad con cada sector.

1.3.3. PMBOK (Project Management Body of Knowledge)

Fernández Parra, K. et al. (2015), el PMI (Project Management Institute) es un instituto estadounidense sin fines de lucro creado en 1969 para avanzar en el estado del arte relacionado con la gestión de proyectos.

El órgano del conocimiento de Gestión de Proyectos (PMBOK) ha sido aprobado en los EE.UU por el organismo estadounidense de normalización

ANSI (Instituto Nacional Estadounidense de Normas). PMI se compromete a mejorarlo y desarrollarlo.

Asimismo, Fernández Parra, K. et al. (2015), señala que el PMBOK define la gestión de proyectos como la implementación de conocimientos, habilidades, herramientas y métodos en una amplia gama de actividades requeridas para la realización de cualquier proyecto.

La originalidad del PMBOK es describir la misión del gerente del proyecto de acuerdo con un enfoque orientado a procesos y áreas de conocimiento.

Los campos de conocimiento son nueve e incluyen todos los procesos en los que se basa la gestión del proyecto.

Es la integración del proyecto, su contenido, plazos, costos, calidad, recursos humanos, comunicación, riesgos y suministro.

Los grupos de procesos definen una estructura básica para comprender la gestión de proyectos: inicio, planificación, ejecución, masterización y cierre.

Las métricas se definen como parte del Informe de progreso procesado en el área Conocimiento de comunicación del proyecto. Las mediciones se basan en tres tipos de análisis:

- Análisis de brechas que expresa la relación entre lo esperado y lo realizado;
- Análisis de tendencias que anticipa un posible deterioro futuro;
- Análisis del valor adquirido basado en indicadores específicos definidos en el sistema de referencia.

1.3.4. Ciclo de Deming.

Jimeno Bernal, J. (2013), indica que, para implementar el ciclo de Deming, que es la sistemática más utilizada. “A continuación explica cuál es su significado y su función relacionadas con otras normativas ISO, específicamente con la normativa ISO 9001” (Jimeno, 2013). “Requerimientos de los Sistemas de gestión de la calidad”, en el que

muestra indicando a manera de un principio elemental para el mejoramiento continuo de la calidad".

¿Qué es el Ciclo de Deming, PDCA (o Ciclo PHVA)?

Jimeno Bernal, J. (2013), indica que el ciclo de Deming se debe a Edwards Deming por ser el autor, es nombrado así porque proviene de las siglas PDCA en inglés (Plan, Do, Check, Act) y, que tiene su significado en español: Planificar, Hacer, Verificar y Actuar, (Ciclo PHVA)

"La sistemática detalla los cuatro pasos fundamentales en el que se debe realizar de una manera metodológica, todo ello encaminado al mejoramiento continuo en una organización". "Comprendiendo así la mejora continua de la calidad (disminuir fallos, aumentar la eficacia y eficiencia, solucionar complicaciones, previsión y eliminación de potenciales riesgos)."

Además, Jimeno Bernal, J. (2013), explica que el ciclo de Deming está conformado por 4 fases cíclicas, de tal manera que cuando se termina la cuarta fase, el ciclo deberá retornar a la etapa primera y repetirse nuevamente el ciclo, de esta manera cada actividad será reevaluada de manera periódica con la finalidad de reincorporar nuevas mejoras"

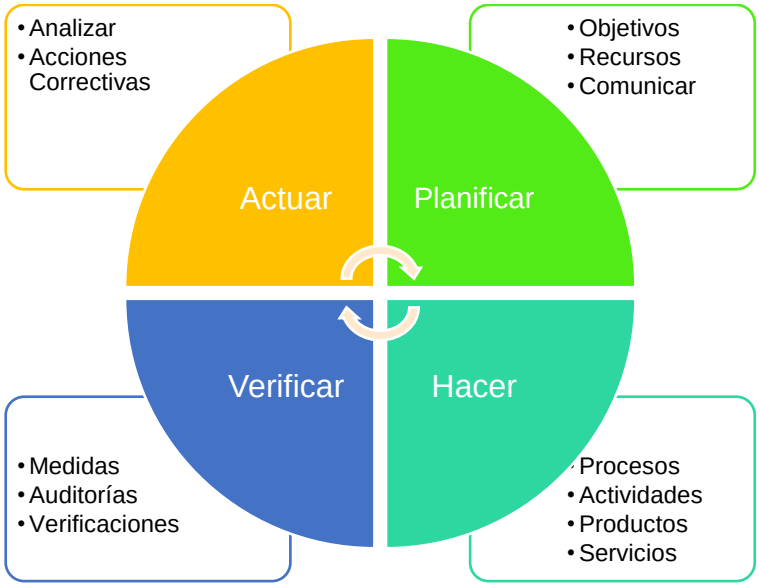


Figura 2: Ciclo PHVA: Planificar, Hacer, Verificar, Actuar

Fuente: Jimeno Bernal, J. (2013)

¿Cómo implementar el Ciclo PDCA en una organización?

El ciclo de Deming está conformado por cuatro etapas que se explican a continuación:

Planificar (Plan)

Jimeno Bernal, J. (2013), afirma que la búsqueda de posibles mejoramientos en una organización se consigue efectuando equipos de trabajo, escuchando las opiniones del personal de trabajo, buscando tecnologías nuevas, etc. En esta etapa se establecen los objetivos que se desea alcanzar, para ello se realiza una búsqueda de las actividades susceptibles de mejoramiento”

Hacer (Do)

“En esta etapa se ejecutan cambios para la implantación de la propuesta de mejoramiento. Para experimentar el funcionamiento primeramente es conveniente realizar una prueba piloto previo a la ejecución de cambios a gran escala” (Jimeno Bernal, J. 2013).

Controlar o Verificar (Check)

Jimeno Bernal, J. (2013), “Luego de ser ejecutado el mejoramiento, es recomendable dejar un tiempo de prueba para su verificación y funcionamiento adecuado”. “Habrá que modificar el mejoramiento para ajustarlo a los objetivos deseados si es que esta no cumple las expectativas iniciales”

Actuar (Act)

Jimeno Bernal, J. (2013), afirma que una vez culminado el tiempo de prueba y previamente implantar el mejoramiento se realizará un estudio del producto y será comparados con la funcionalidad de las actividades”. “La mejora se implantará de manera concluyente, siempre y cuando los resultados sean satisfactorios en caso contrario se decidirá qué cambios se debe realizar para ajustar los resultados y sino desecharla”
Jimeno Bernal, J. (2013), “Finalizada la cuarta fase, se debe regresar a la primera fase de forma periódica para estudiar nuevas mejoras a ejecutar”

Además, Jimeno Bernal, J. (2013), señala que “Existen muchas maneras con respecto a la aplicación de los principios del PDCA (Planificar, Hacer, Controlar y Actuar) indica la manera de realizar la implantación de un Programa de Acciones (Correctivas, de prevención y de Mejoramiento), del mismo modo se realiza la consulta en la sección de Herramientas de mejora”

Ejemplo de implantación del Ciclo PDCA

Jimeno Bernal, J. (2013), mediante este ejemplo explica acerca de una industria que fabrica productos elaborando piezas a base de aluminio” “Admite que la organización se fundamenta en el ciclo de mejora continua (PDCA) simultáneamente con diferente clase de herramientas (Lean Manufacturing, Seis Sigma, 5S o Kaizen)” empleando el mejoramiento continuo mediante el cual sucedería lo siguiente:

1º) “Se detectan problemas, porque el personal de trabajo ha presentado maneras diferentes para ejecutar cualquier actividad, puesto que en el mercado resulta que salieron maquinaria más eficiente el cual permite acceder al ahorro costos, etc. A todo ello, se analiza la posibilidad de mejoras en la fábrica, Jimeno Bernal, J. (2013).

2º) “Se estudian y se eligen las mejoras favorables de igual forma su impacto, lo de mayor importancia el cual van a poner en marcha el buen funcionamiento de la empresa en donde se realiza la decisión de ejecutarlas mediante una prueba piloto a pequeña escala” Jimeno Bernal, J. (2013).

3º) “Se comprueba el funcionamiento correcto de los cambios y proporciona el resultado esperado una vez ejecutada la prueba piloto, se ejecutan los cambios siempre y cuando los cambios que se hayan realizado no satisfagan las perspectivas para que estos funcionen acordes a lo deseado” Jimeno Bernal, J. (2013)

4º) “Finalmente, se realiza la implantación de considerable magnitud en el límite de productividad de la fábrica siempre y cuando los resultados sean satisfactorios” Jimeno Bernal, J. (2013), “Las funciones en la fábrica de piezas de aluminio realizan su funcionamiento con eficiencia una vez que se haya finalizado e implantado las mejoras,” “Sin embargo, habrá que realizar de forma periódica una búsqueda de posibles nuevas mejoras y regresar nuevamente a emplear el ciclo de Deming” Jimeno Bernal, J. (2013).

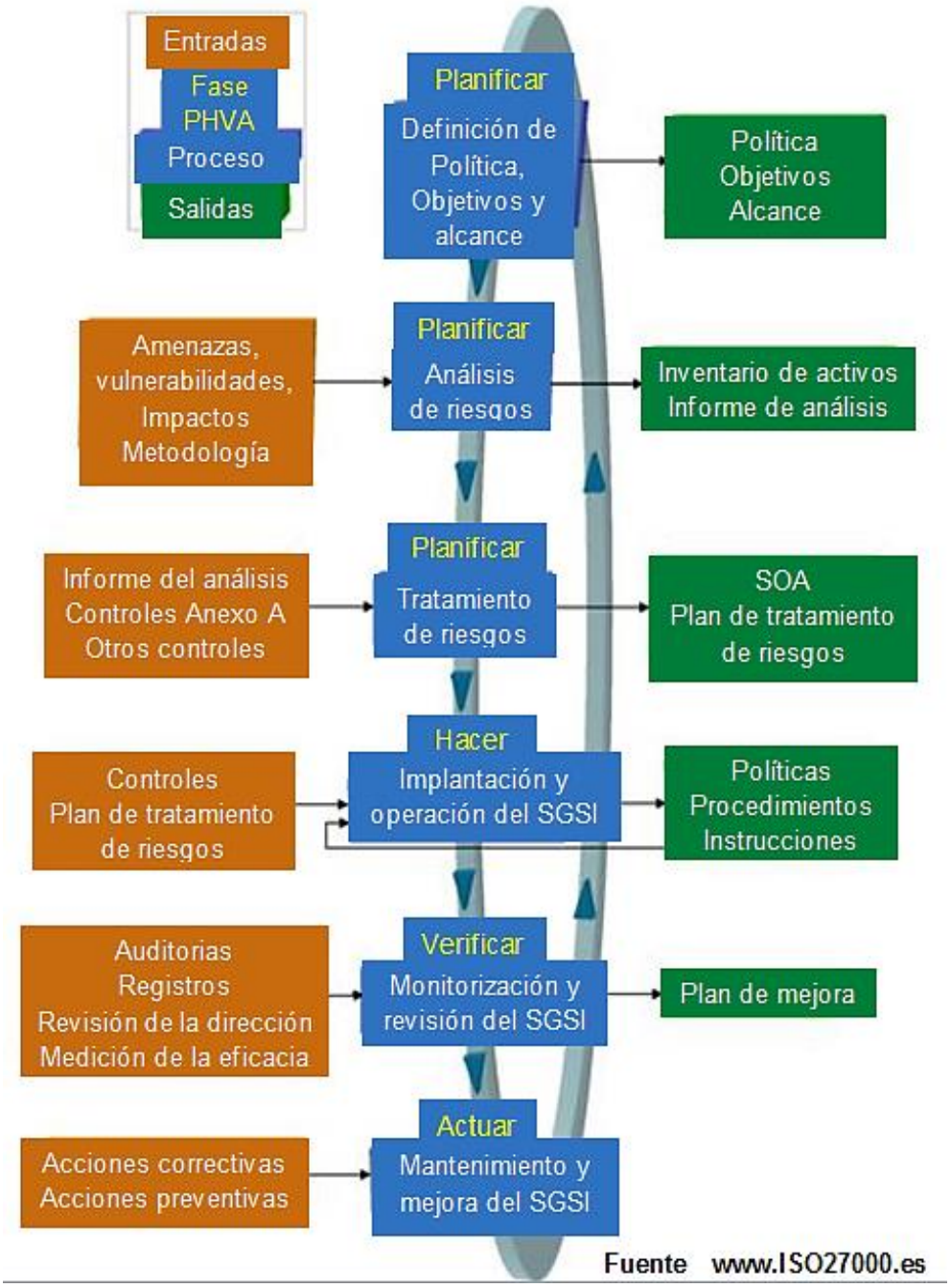


Figura 3: Ciclo de Deming

1.3.5. COBIT 5

Aguirre Cardona, J. y Aristizabal Betancourt, C. (2013), COBIT es una asociación internacional desarrollado por ISACA para guiar su trabajo en este contexto con relación a las TI, COBIT se desarrolló inicialmente como un marco para la ejecución de asignaciones de auditoría de TI, construido

en torno a un íntegro grupo de objetivos de control para los procesos de TI el cual provee de ayuda a las organizaciones para lograr objetivos que favorecen a la administración y el gobierno de las TI empresariales.

COBIT 5 indica que las TI permite ser administradas y agenciadas de una forma holística para toda la organización, esto significa que abarca a todo el negocio de inicio a fin como también las áreas de TI con función que demandan responsabilidad, tomando en cuenta los beneficios concernientes con TI de Stakeholders internos y externos. Además, COBIT 5 es muy útil y genérico para toda organización y de cualquier rubro, tamaño, tanto comerciales, como sin fines de lucro o ya sea estatal o privado.

Figura 4: Principios de COBIT 5

Principios de COBIT 5

López Armendaris, D. (2017), lo que muestra la figura 4 son los 5 elementos claves de COBIT para la administración y el gobierno de las TI empresariales:

1. Satisfacción de las Necesidades de los Stakeholders.
2. Satisfacer a la Empresa Extremo a Extremo
3. Aplicación del Marco Referencial Único Integral
4. Realizar un contexto Holístico
5. Separación del Gobierno de la Gestión

Los Habilitadores de COBIT 5

1. Principios, políticas y marcos de trabajo.
2. Procedimientos.
3. Estructuras organizacionales.
4. Ética, cultura y comportamiento.
5. Información
6. Servicios, infraestructura y aplicaciones.
7. Personas, habilidades y competencias.

Metas relacionadas con las TI (COBIT 5):

Tabla 3.

Metas relacionadas con las TI

Figura 6—Metas relacionadas con las TI		
Dimensión del CMI TI	Meta de Información y Tecnología Relacionada	
Financiera	01	Alineamiento de TI y estrategia de negocio
	02	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
	03	Compromiso de la dirección ejecutiva para la toma de decisiones en relación con las TI
	04	Riesgo en organizaciones concernientes con las TI formalizados
	05	Obtención de beneficios del portafolio de Inversión y Servicios en relación con las TI

Cliente	06	Transparencia de los costes, beneficios y el riesgo de las TI
	07	Entrega de servicios de TI teniendo en cuenta los requerimientos del negocio
	08	Uso correcto de aplicaciones, información y soluciones tecnológicas
Interna	09	Agilidad de las TI
	10	Seguridad de la información, infraestructura de procesos y aplicaciones
	11	Optimización de activos, recursos y capacidades de las TI
	12	Capacitación y soporte de procesos de negocio con la integración de aplicaciones y tecnología en términos de negocio
	13	Entrega de Programas que aporten beneficios, dentro del presupuesto y cumpliendo con los requisitos y normas de calidad.
	14	Información disponible y confiable para la toma de decisiones
	15	Cumplimiento de las políticas internas por parte de las TI
Aprendizaje y Crecimiento	16	Personal del negocio y de las TI competitivo y motivado
	17	Conocimiento, experiencia e iniciativas de innovación.

Nota: Tomado de Monfort Casañ, R. (2016)

1.3.6. ITIL (Biblioteca de Infraestructura de Tecnología de la Información)

De acuerdo con López Armendaris, D. (2017), ITIL es el marco de gestión internacional de facto que describe las "buenas prácticas" para gestionar los servicios de TI. El marco ITIL evolucionó durante la década de 1980 a partir de que el gobierno del Reino Unido tuvo esfuerzos para documentar cómo las organizaciones exitosas abordaron la gestión de servicios. A principios de la década de 1990, habían producido una gran colección de libros para la gestión de servicios de TI que documentaban las "buenas prácticas". Esta biblioteca finalmente se denominó Biblioteca de infraestructura de TI. La Oficina de Comercio del Gobierno en el Reino Unido continúa operando como el propietario de la marca registrada de ITIL.

ITIL ha pasado por varias evoluciones y recientemente se actualizó con el lanzamiento de la versión 3 en 2007. A través de estas evoluciones, el alcance de las prácticas documentadas ha aumentado para mantenerse al día con la madurez continua de la industria de TI y sobre todo la satisfacción, necesidades y exigencias de la comuna profesional de ITSM.

ITIL es solo una de las muchas fuentes de mejores prácticas, incluidas las documentadas por:

• Marcos públicos (ITIL, COBIT, CMMI, etc.)
• Normas (ISO 20 000, BS 15 000)
• Conocimiento de propiedad de organizaciones e individuos.

Generalmente, las mejores prácticas son aquellas formalizadas como resultado de tener éxito en el uso de la industria.

5 volúmenes componen la Biblioteca de Infraestructura de TI (Vs. 3).

• Estrategia de servicio
• Diseño de servicio
• Transición de servicio
• Operación de servicio
• Servicio de Mejora continua

Ciclo de vida del servicio ITIL V3

Para Pérez Villamizar, M. (2017)**,** el concepto de ciclo vital de los servicios TI donde indica la gestión de los servicios TI. Este punto de vista lleva como propósito brindar un enfoque global sobre la existencia de un servicio a partir de su diseño hasta abandonarlo eventualmente sin dejar de lado las especificaciones de cada uno de las funciones y procesos implicados eficientemente sobre prestación del mismo. Señala que la composición del ciclo vital del servicio es de 5 fases y además existe una retroalimentación a través de cada una de las fases de forma constante (González, A. 2013), citado por Pérez Villamizar, M. (2017)**,** así como se muestra en la figura 5.

Figura 5: Ciclo de vida del servicio ITIL V3

Fuente: Pérez Villamizar, M. (2017)

Se describe las 5 fases del Ciclo vital del servicio ITIL V3 el cual contiene sus definiciones conforme a los conocimientos de investigación realizada por Lozano, F. y Rodríguez, K. (2011) (citado por Pérez Villamizar, M., 2017)

Comparativo COBIT, ITIL, ISO 27000

Tabla 4.

Comparativo COBIT, ITIL, ISO 27000

ÁREA	CobiT	ITIL	ISO 27000
Funciones	Mapeo de los procesos IT	Mapeo de la Gestión de Niveles de Servicio de IT	Marco de referencia de SI
Áreas	4 Procesos y 34 Dominios	9 Procesos	10 Dominios ISO International.
Creador	ISACA	OGC	
¿Para qué se implementa?	Auditorías de Sistemas de Información	Gestión de Niveles de Servicio	Cumplimiento del Estándar de Seguridad de la Información
¿Quiénes lo evalúan?	Compañías de contabilidad Compañías de consultoría en IT	Compañías de consultoría en TI	Compañías de consultoría en IT. Empresas de seguridad consultores de seguridad en redes.

Nota: Recuperado de la Revista Pensamiento Americano: (Orrego, 2011)Comparativo COBIT, ITIL, ISO 27000 - Fuente: Seguridad de la Información en Colombia.

1.3.7. Metodologías para el análisis de riesgos

El análisis de riesgos es fundamental porque permite tener una perspectiva general de las posibles amenazas que podrían afectar e impactar la organización generando graves daños o perjudicando a los activos sino reciben una adecuada protección. Entre las metodologías que se ha tomado en cuenta son:

MAGERIT:

De acuerdo con el Ministerio de Hacienda y Administraciones Públicas (2012), en el vocabulario de la normativa ISO 31000, Magerit con referencia a la Gestión de Riesgos, donde realiza su manifestación y menciona “Proceso de Gestión de Riesgos”, sección 4.4 (“Ejecución de la

Gestión de los Riesgos"). Dicho de otra manera, MAGERIT dentro de un entorno de trabajo ejecuta el Procesamiento de Gestión de los Riesgos donde los órganos de gobierno llevan a cabo la toma de decisiones teniendo en cuenta aquellos riesgos procedentes del uso de las TI.

MAGERIT propone las siguientes 4 etapas para el análisis de riesgos:

Etapa 1:

Planificación del análisis y gestión de riesgos, implanta los cuidados necesarios para dar inicio al proyecto de análisis y gestión de riesgos.

Etapa 2:

Análisis de riesgos, mediante el cual proporciona la identificación y evalúa los organismos que interceden en los riesgos.

Etapa 3:

Gestión de riesgos, donde proporciona la identificación de sus funciones o servicios de salvaguardia que ejecuta la reducción de los riesgos que se han averiguado.

Etapa 4:

La elección de salvaguardas que consiste en la selección de los mecanismos de salvaguardia que a través de ello es muy importante en la implementación del análisis de riesgos.

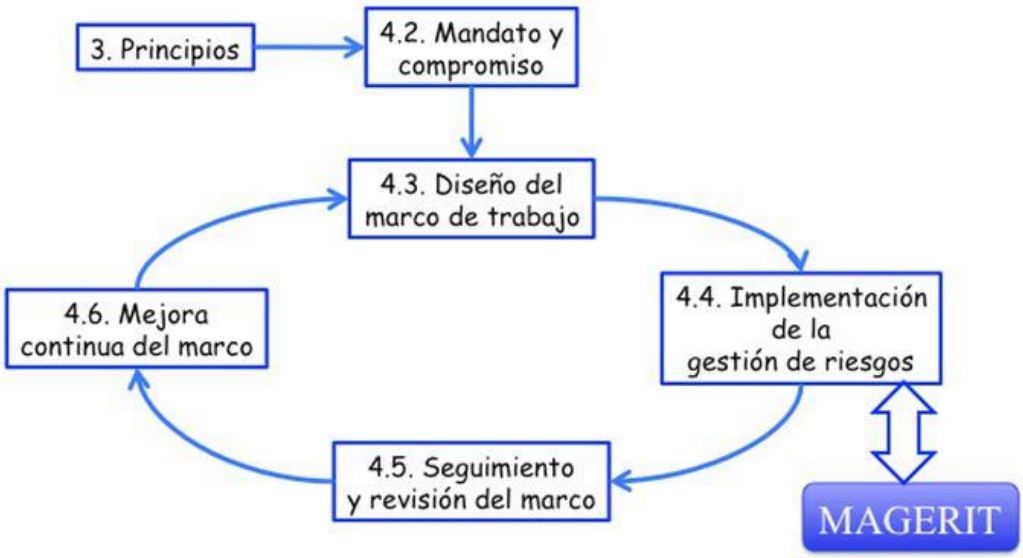


Figura 6: ISO 31000 – Marco de trabajo para la gestión de riesgos.

Fuente: el Ministerio de Hacienda y Administraciones Públicas (2012)

ISO/IEC 27005

Según Ramírez Castro, A. & Ortiz Bayona, Z. (2011), esta norma proporciona las directrices tomando en consideración e indicando ‘los requerimientos para la gestión de riesgos incluyendo recomendaciones y buenas prácticas en donde además asegura y controla los niveles físicos, lógico y el factor humano relacionado con los procesos del desarrollo tecnológico.

De acuerdo con Espinoza T., D., Martínez P., & Amador D., S. (2014), esta norma suministra las directrices para la gestión de riesgos en el marco de la seguridad de la información asimismo proporciona como base los conocimientos generales donde se encuentran descritos en la normativa ISO/IEC 27001 también está proyectada para proporcionar y ejecutar satisfactoriamente la seguridad de la información teniendo como soporte la perspectiva de gestión del riesgo.

Esta norma se adapta a toda clase de organizaciones que pretendan tramitar aquellos riesgos el cual pudieran dificultar la seguridad de la información en las instituciones (instituciones comerciales, gubernamentales, organizaciones no lucrativas).

Evaluación de los riesgos de seguridad de la información:

8.1 Descripción global para evaluar riesgos de seguridad de la información

8.2 Análisis de riesgo

8.2.1 Identificar los riesgos

8.2.2 Estimar los riesgos

8.3 Evaluación de riesgos.

OCTAVE

Como señalan Espinoza T., D. Martínez P., & Amador D., S. (2014), el método OCTAVE se realiza en tres fases siguientes:

Fase 1, Primeramente, se lleva a cabo la fase donde identifican los activos relevantes concernientes a los activos de información y las estrategias de salvaguarda actual hacia esos activos, esta identificación lo realiza el equipo de análisis, luego se determina qué activos se encuentran en estado más crítico para el triunfo de la institución, se evidencia sus requerimientos de seguridad e identifica amenazas el cual consiguen obstaculizar con el cumplimiento de los requerimientos.

Fase 2, En esta fase el personal encargado del análisis de riesgo efectúa los mecanismos para evaluar la infraestructura de información como complementación del análisis de amenazas elaborado en la etapa anterior, luego se informa las disposiciones de mitigación en la fase 3. Y, por último,

Fase 3, En esta fase el equipo de análisis de riesgo efectúa actividades para la identificación de riesgos como también el progreso de la programación de la disminución de los riesgos para los activos críticos.

OCTAVE-S

Según Espinoza T., D. et al. (2014), el desarrollo de OCTAVE-S estuvo amparado por el programa de Inclusión, Demostración y Evaluación de Tecnología (TIDE) el 4 de setiembre, con la finalidad de dirigir una perspectiva fundamentado en OCTAVE a las instituciones pequeñas de fabricación.

La versión 1.0 de la perspectiva de OCTAVE-S es la más actualizada, se encuentra particularmente proyectada para aquellas organizaciones de aproximadamente 100 personas.

Conforme a los criterios OCTAVE, el enfoque OCTAVE-S se compone de 3 fases semejantes.

No obstante, OCTAVE-S es elaborado por un equipo encargado del análisis de riesgos con grandes conocimientos de la organización.

Por lo tanto, OCTAVE-S no se basa en escuelas juiciosos de obtención de conocimientos para recopilar información porque se supone que el equipo de análisis de riesgo (en general está compuesto de tres a cinco personas) posee juicio práctico de los activos más relevantes en relación con la información, los requerimientos, amenazas y prácticas de seguridad de la institución.

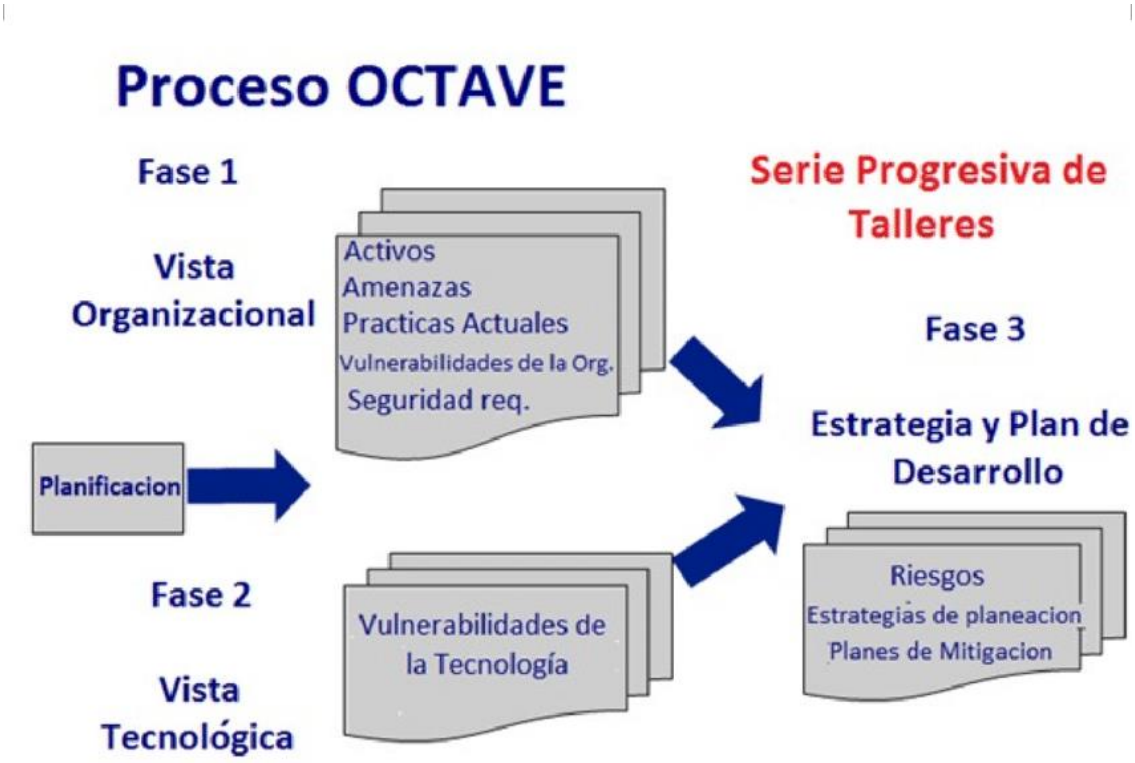


Figura 7: Fases del Método OCTAVE

1.4. Formulación del problema

¿De qué manera un Sistema de Gestión de Seguridad de la información mejorará la seguridad de la información de los procesos de la Universidad Nacional Intercultural “Fabiola Salazar Leguía”?

1.5. Justificación e importancia del estudio

Justificación teórica

La justificación es teórica, toda vez que la investigación se realiza con el objetivo de diseñar un sistema de gestión de seguridad de la información, mediante el cual se presenta la propuesta de las políticas de seguridad de la información para ser incorporado adecuadamente en la Universidad.

Justificación práctica

Mediante la reciente indagación se podrá proponer un sistema de gestión de seguridad de la información (SGSI) como marco normativo con el propósito de poder realizar internamente todo tipo de actividad concerniente a la seguridad de la información en la institución.

Justificación Metodológica

En la presente investigación se utiliza como análisis metodológico el ciclo de Deming o PDCA basada en modelos de gestión concerniente a la seguridad de la información, para proponer un Sistema de Gestión de Seguridad de la Información para la Universidad Nacional Intercultural “Fabiola Salazar Leguía” de Bagua, y de esta forma asegurar su confidencialidad, integridad y disponibilidad de sus procesos.

Importancia de la investigación:

La importancia de realizar la propuesta de un sistema de gestión de seguridad de la información surge de la necesidad de la mejora continua para la Universidad Nacional Intercultural “Fabiola Salazar Leguía” de Bagua, de igual forma conseguir un funcionamiento mejor y un manejo

eficiente de los activos de la información de la institución, por tal motivo es que es fundamental implantar una estrategia de seguridad, que minimice las vulnerabilidades y amenazas de estos tomando en consideración cada uno de aquellos factores que se encuentran involucrados en la administración del activo más importante en la institución que es la información (Sistemáticos, Tecnológicos, Culturales, Económicos, entre otros).

1.6. Objetivos

1.6.1. Objetivo General

Diseñar una propuesta de un Sistema de Gestión de Seguridad de la información para la Universidad Nacional Intercultural “Fabiola Salazar Leguía”

1.6.2. Objetivos Específicos

a) Seleccionar modelos de gestión de seguridad de la información.
b) Proponer el sistema de gestión de seguridad de la información.
c) Validar el modelo con la simulación de procesos de una universidad.
d) Evaluar resultados.

1.7. Limitaciones

Como limitaciones del proyecto de investigación se puede considerar:

El proyecto presenta de una propuesta de un Sistema de Gestión de Seguridad de la Información para la la Universidad Nacional Intercultural “Fabiola Salazar Leguía” Bagua, basadas en políticas de seguridad de la información, este modelo se realizó tomando como referencias modelos de gestión de seguridad de la información.

II. MATERIAL Y MÉTODO

2.1. Tipo de estudio y diseño de la investigación

Tipo de investigación

El tipo de esta investigación es Tecnológica Aplicada cualitativa, “El cual es una actividad orientada a la elaboración de un nuevo conocimiento técnico que alcanza a ser incluido claramente en la obtención y abastecimiento de bienes y servicios” Lara M. (2013), en este proyecto se diseña un Sistema de Gestión de Seguridad de la información para el mejoramiento de la seguridad de la información de los procesos de la Universidad Nacional Intercultural “Fabiola Salazar Leguía” Bagua.

Diseño de la investigación

El presente proyecto de indagación concierne a un diseño no experimental, Propositiva ya que se constituye en las necesidades internas de la universidad, se usará el método deductivo. Mediante el cual se elaborará una propuesta de un sistema de gestión de seguridad de la información para la Universidad Nacional Intercultural “Fabiola Salazar Leguía”

2.2. Escenario de Estudio

El contexto es la Universidad Nacional Intercultural “Fabiola Salazar Leguía”, situada en la ciudad de Bagua departamento de Amazonas, cuenta con dos sedes: La sede académica situada en Jr. Ancash N°520 y la sede administrativa en Jr. Comercio N°128.

El 13 de agosto de 2018 la Superintendencia Nacional de Educación Superior Universitaria (SUNEDU) concedió el licenciamiento institucional a la Universidad Nacional Intercultural Fabiola Salazar Leguía de Bagua (UNIBAGUA), inmediatamente después de confirmar que logra cumplir con las CBS (Condiciones Básicas de Calidad) para proporcionar el soporte a la educación superior universitario. Ofertando las carreras universitarias de:, Biotecnología, Ingeniería Civil y Negocios Globales.

Marco Estratégico Institucional

Universidad Nacional Intercultural “Fabiola Salazar Leguía” Bagua

Ubicación: La Universidad Nacional Intercultural “Fabiola Salazar Leguía”, actualmente se encuentra situada en la ciudad de Bagua departamento de Amazonas, cuenta con dos sedes: La sede académica sito en Jr. Ancash N° 520 y la sede administrativa en Jr. Comercio N°128.

a. b.

Figura 8: Sedes de la UNIFSL, a. Sede Administrativa, b. Sede académica

Misión

La formación profesional de forma integral, con calidad científico tecnológico, intercultural, compromiso social y liderazgo, entregados al progreso y sostenibilidad de las comunas propias de la región y el país.

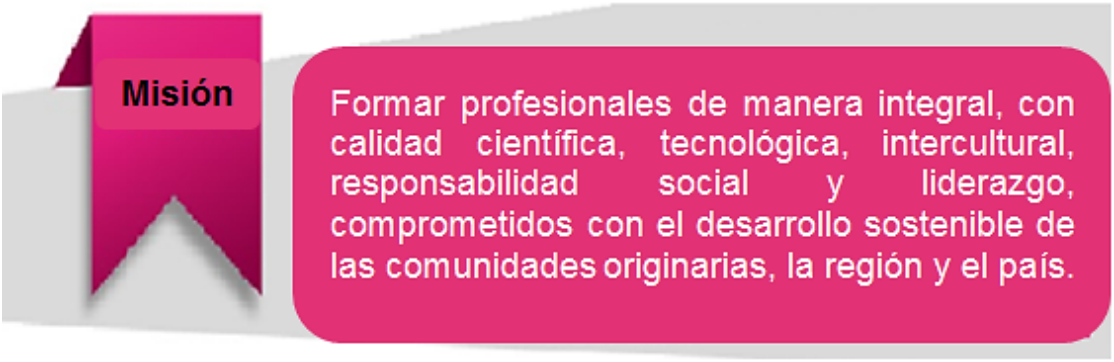


Figura 9: Misión UNIFSL-Bagua. Fuente https://www.unibagua.edu.pe/

Visión

"convertirse en el 2021, una institución plenamente integrada, cumpliendo con las Condiciones Básicas de Calidad en la formando profesionales, con calidad académico y científico; identificado y teniendo en consideración el valor cultural y sus derechos, contribuyendo al desarrollo local, regional y nacional".

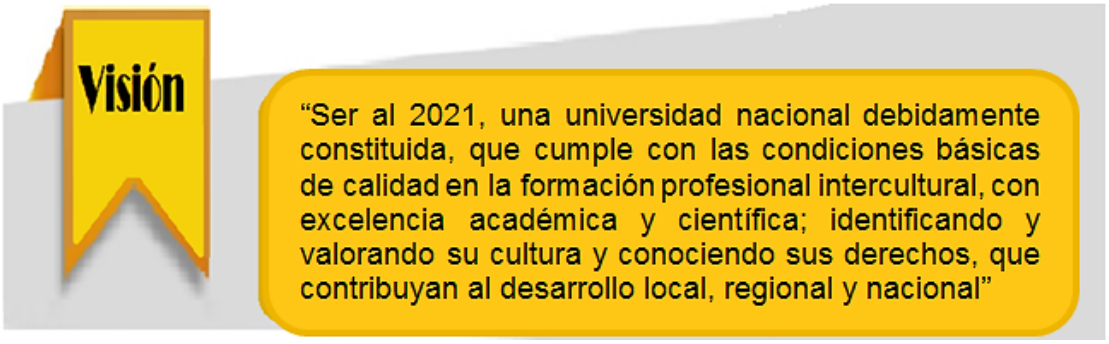


Figura 10: Visión UNIFSL-Bagua. Fuente: https://www.unibagua.edu.pe/

Valores

Los valores que regirán los comportamientos de las personas en la Universidad Nacional Intercultural "Fabiola Salazar Leguía" de Bagua (UNIFSL-Bagua) son:

-Transparencia. - Promover resultados con pleno conocimiento de la institución y otros actores de la sociedad civil.

-Compromiso. - Para desarrollar la práctica personal e institucional basado en la comunicación, en la integración y el trabajo colaborativo, se deben desempeñar con objetivos, las normas internas, las políticas, y valores de la institución, así como al desarrollo personal y laboral.

-Respeto. - Reconocimiento y revaloración de las personas, teniendo en cuenta la diversidad de culturas en la población indígena de la Amazonía y la interacción con ellos en un plano de igualdad.

-**Justicia. -** Conjunto de normas y reglas que constituyen un marco apropiado el cual contenga relaciones equitativas entre organización y personas, delegando, obstaculizando y cediendo acciones determinadas en la interacción de éstos.

-Honestidad. - Cumplimiento transparente de las actividades propias de la administración universitaria a todo nivel, actuando con honradez y sinceridad.

-Identidad. - Sentido de pertenencia a la UNIFSL-B, comprensión, respeto y protección a la unidad académica en todo momento.

-Tolerancia. - Comprensión de las diferencias en el comportamiento y resultados del accionar de otras unidades académicas y actores relacionados, otorgándoles la oportunidad de manifestarse según sus percepciones necesidades y expectativas.

-Solidaridad. - Identificar la importancia de las instancias de las áreas académicas proporcionando el cumplimiento de sus objetivos. Ayudando a solucionar los problemas de aquéllos en condiciones vulnerables.

2.3. Caracterización de sujetos

Población:

Conformada por 7 procesos de la Universidad Nacional Intercultural “Fabiola Salazar Leguía” Bagua.

Muestra:

Está formada por 3 procesos de la Universidad Nacional Intercultural “Fabiola Salazar Leguía”, a continuación, se describe los siguientes:

Matriz de distribución de los procesos de información:

Tabla 5.

Matriz de los procesos de información

Procesos	Cantidad	Selección por conveniencia
Matricula	1	X
Admisión	1	X
Notas	1	X
Biblioteca	1	
Planilla	1	
Trámite Documentario	1	
Carga horaria	1	
Total	7	3

Procesos seleccionados:

Proceso Admisión: Proceso para establecer y uniformizar el proceso de selección y matrícula de la institución.

Proceso Matricula: Proceso que se realizan para Registro e inscripción de los alumnos de la institución.

Proceso Notas: Proceso de grado de una escala establecida, mediante una puntuación, que se asigna a los estudiantes para valorar los conocimientos o formación mostrados en un examen.

¿Qué juicio se ha realizado para tomar en consideración como muestra a los procesos?

Para considerar como muestra a los procesos el criterio que se ha utilizado es por conveniencia, ya que es un método de muestreo no probabilístico y no aleatorio empleada hacia la creación de muestras conforme al fácil acceso, la disposición de los procesos donde para pertenecer al muestreo es en un periodo de tiempo proporcionado a cualquiera sea las especificaciones técnicas de un componente específico.

¿Cuáles son las características observables que poseen en común?

Las características perceptibles que tienen en común entre los procesos son los activos de seguridad de la información de la Universidad Nacional Intercultural “Fabiola Salazar Leguía”

¿Qué información se recabará de ellos para contribuir a la indagación?

Se recabará la información necesaria y relevante referente a los activos de la información de los procesos seleccionados que realiza la Universidad Nacional Intercultural “Fabiola Salazar Leguía” Bagua.

2.4. Técnicas e instrumentos de recolección de datos

TÉCNICAS

Según Bernal Torres (2010), las técnicas son las estrategias que se utilizan para recabar la información que se requiere con el objetivo de construir el conocimiento de lo que se está investigando, donde estas técnicas son un conjunto de normas, instrucciones u operaciones específicas para la conducción de instrumentos, donde se ubican a la altura de los sucesos o de los periodos prácticos que aprueba aplicar la técnica.

La técnica a utilizar en la presente investigación será:

Observación

Según Hernández Sampieri, R. et al. (2010), este es un método que se basa en registrar sistemáticamente, autorizado y confidencial de procedimientos y escenarios perceptibles, mediante un conjunto de categorías y subcategorías.

Para obtener una buena observación Inicialmente se traza todo lo que es de nuestro interés, para poder aplicar la técnica de observación,

Entrevista

Hernández Sampieri, R. et al. (2010), sostiene que es una técnica mediante el cual se emplea una lista de preguntas, con la finalidad de conseguir información de la población con características objetivas y subjetivas.

El presente proyecto de investigación empleará como técnica la entrevista, mediante el cual se aplicará a los dirigentes de la Universidad caso de estudio.

INSTRUMENTOS

“Son aquellos objetos específicos que proveen la atención exacta de la técnica y sin embargo tienen particularidades propias por el cual corresponden adecuarse al objeto de estudio” (Hernández Sampieri, R. et al., 2014).

Hernández Sampieri, R. et al. (2014), afirma que los instrumentos son recursos que maneja el investigador y en donde registra datos o la información hacia las variables que posee en su intelecto.

Cuadro Comparativo de Metodologías

Tabla 6.

Criterios de los modelos de mejora continua

Criterios	**Modelo**					
	EFQM	Deming	Kaisen	Los 7 pasos	Seis-Sigma	Philip Crosby
Clientes	X	x	x	x	x	x
Liderazgo	X	x	x	x	x	x
Planeación	X	x	x	x	x	x
Información/ Conocimiento				x	x	x
Personal	X	x	x	x		x
Procesos	X	x	x	x	x	x
Mejora Continuo	X	x	x	x	x	x
Impacto social	X		x			
Resultados	X	x	x	x	x	x

Nota: Criterios de los modelos de mejora continua. Recuperado de "Análisis de los Diferentes Métodos de Mejora Continua" de Herrera, J. et al. (2012)

Tabla 7.

Elementos de retroalimentación

Modelos					
EFQM	**Deming**	**Kaisen**	**Los 7 pasos**	**Seis-Sigma**	**Philip Crosby**
Planeamiento Método Implementación Revisión y comprobación	Planificación Ejecución Verificación Revisión	Organizar Ordenar Limpiar Control visual Disciplina y hábito	Selección Cuantificación Análisis Definición Solución	Definición Medición Análisis Mejora Control La definición	Estructura La estandarización del cumplimiento Medición

Nota: Elementos de retroalimentación. Recuperado de "Análisis de los Diferentes Métodos de Mejora Continua" de (Herrera , D'Armas , & Arzola, 2012)

Metodología

Para el presente proyecto se utilizó el modelo ciclo de Deming, el cual narra 4 pasos fundamentales que se debe realizar de manera sistematizada para alcanzar la mejora continua, también es conocido con las siglas PHVA: que significa: Planificar, Hacer, Verificar, Actuar.

Esta sistemática describe estas 4 fases el cual se tomarán en consideración para conseguir la mejora continua de la organización.

2.5. Procedimiento para la recolección de datos

La información accesible para el diseño de un SGSI de la Universidad Nacional Intercultural “Fabiola Salazar Leguía” Bagua, se realiza la clasificación y el análisis cuidadosamente para comprobar amenazas, vulnerabilidades, riesgos y políticas de seguridad de la información mediante la propuesta del SGSI.

En la presente investigación se realizó la entrevista como técnica mediante el cual se hizo la recolección los datos para recabar información pertinente de usuarios que manejan y tienen acceso a los activos de información de la UNIBAGUA.

También se usó el método de observación y la revisión documental directa el cual también ayudará en la recolección de información objeto de estudio.

Observación

Se observará los procesos que forman parte de las diferentes áreas que conforma la Universidad Nacional Intercultural “Fabiola Salazar Leguía” de Bagua, como son: admisión, matrícula, notas, biblioteca, planilla, trámite documentario, carga horaria y la revisión documental el cual permite confirmar la información que es objeto de estudio.

Entrevista

Se realizará una entrevista abierta o no estructurada a los operadores inmersos en la investigación que vienen a ser el personal de trabajo directivos de la Universidad Nacional Intercultural “Fabiola Salazar Leguía” de Bagua.

2.6. Procedimiento de análisis de datos

Se realizó una entrevista a la alta dirección y a los trabajadores de la institución para obtener un diagnóstico sobre la seguridad de los activos de información y a partir de ello determinar las medidas de control de seguridad necesarias.

La presente investigación se realiza basándose en el Ciclo PHVA, Planificar, Hacer, Verificar y Actuar, el cual servirá de guía para el presente modelo como propuesta del SGSI, el cual funciona bajo la filosofía del mejoramiento continuo.

Se utilizó BPM Bizagi Modeler para diseñar el modelo de gestión de seguridad de la información, donde se realizan cada uno de procesos que se basan en la sistemática Planificar, Hacer, Verificar, Actuar.

Seguidamente a la realización de los procesos, se lleva a cabo la documentación pertinente de las actividades específicas de los procedimientos conjuntamente a ello también se utilizarán las herramientas correspondientes para cada una de ellas.

Análisis de la entrevista realizada en la Universidad Nacional Intercultural “Fabiola Salazar Leguía” Bagua.

Se analiza la información obtenida de la entrevista a diferentes autoridades que trabajan en la Universidad en mención, se realizó mediante 10 preguntas, el cual se encuentran enfocadas en la evaluación de los aspectos siguientes: Gestión de riesgos, roles y responsabilidades definidos, medidas y políticas de seguridad de la información y

mejoramiento continuo adoptados actualmente por la universidad, a todo ello se puede alcanzar las conclusiones siguientes:

- El manejo de contraseñas no es el adecuado al momento del ingreso del nuevo personal a la universidad toda vez que no se actualizan a tiempo las contraseñas de las diferentes áreas de la institución.
- Los usuarios manifiestan inconvenientes al utilizar los ordenadores como falta de antivirus, lentitud en la carga de archivos, mensajes erróneos, inconveniencias mientras se accede a la red, asimismo declaran tener conocimiento sobre políticas de seguridad específicas que debe tenerse en cuenta para la salvaguardia de los activos de información en la universidad.
- En cuanto a la seguridad de la información no se efectúa el análisis y gestión de los riesgos como también concientización y apoyo a la protección de los activos y tampoco se emplean políticas que puedan brindar y gestionar la información de una manera adecuada.
- No se posee de un control respecto al inventariado de los activos actuales tipo y clasificación de activos en la institución.
- En lo que respecta al acceso de personal a distintas áreas no hay un control apropiado, que debe ser solo para personal autorizado donde están instalados: el equipo y el mecanismo que se maneja en la universidad.
- De las conclusiones anteriores se plantea la siguiente propuesta: Diseñar un Sistema de Gestión de Seguridad de la Información que permita salvaguardar los activos de la UNIFSL-Bagua, conocer los activos más relevantes, efectuar el análisis de los riesgos, especificar salvaguardias, especificar responsabilidades referente a la administración de la información y proteger políticas y controles de seguridad para salvaguardar los procesos siguientes: proceso matrícula, procesos admisión y procesos notas de la universidad caso de estudio.

2.7. Criterios éticos

Transparencia

La información recabada y plasmada en esta investigación se muestra tal y como se han recolectado sin que se haya modificado en el resultado, y de una manera sencilla y ordenada, para su fácil comprensión y entendimiento.

Privacidad

Se respetará la política de confidencialidad de los datos que se estableció y se obtuvo en la entrevista inicial con el jefe de TI y Presidencia, manteniendo la información para la institución y los miembros que le competen.

Originalidad

El presente trabajo de investigación, es propiedad de la tesista, así como también el presente modelo propuesto de gestión de seguridad de la información planteada, por lo tanto, indica que es producto de la misma investigación.

Veracidad

La información presente en esta investigación es fidedigna, el cual es representación real de la institución en objeto de estudio.

2.8. Criterios de rigor científico

Credibilidad

La presente investigación mantiene un seguimiento continuo, lo que representa la validez necesaria que enmarca el campo de estudio y cuyos resultados son verdaderos.

Flexibilidad

También tiene la flexibilidad por ser ágil, de fácil comprensión y aplicabilidad en la institución objeto de estudio.

III. REPORTE DE RESULTADOS

3.1. Análisis y discusión de los resultados

El resultado del diagnóstico realizado, enfatiza la problemática identificada y muestra la necesidad de diseñar una propuesta de un Sistema de Gestión de Seguridad de la información para la Universidad Nacional Intercultural “Fabiola Salazar Leguía”, que tenga en cuenta los procesos de acuerdo al modelo del SGSI, para lograr la mejora continua en la institución:

1. Se realizó la etapa planificar de acuerdo al modelo de SGSI descrito en la presente investigación, se validó la propuesta de Gestión de seguridad de la información, donde se entregaron 24 documentos tomando en consideración sus procesos, el cual será de conocimiento de toda la organización:

Tabla 8:

Documentos del SGSI

N	Documentos	Descripción
1	Reunión inicial de proyecto	Comprende los objetivos, el alcance del SGSI, las políticas, los roles y responsabilidades, y además mantener comunicación con todos los involucrados.
2	Documento de aprobación del proyecto	La aprobación del proyecto de la Alta Dirección, el cual consigue los objetivos de un SGSI.
3	Entrevista con los Stakeholders	La entrevista se realizó con la finalidad de llegar a conocer las necesidades relacionadas a la seguridad de la información de la institución caso de estudio.
4	Matriz Stakeholder	Se identifican los involucrados y definen los niveles de interés e influencia en el proyecto.
5	Alcance del proyecto	Describe que el presente proyecto: propuesta de Gestión de Seguridad de Información el cual abarcará como muestra tres procesos:

		Admisión, matrícula y notas.
6	EDT del proyecto	Donde se subdivide el trabajo en porciones más pequeñas para la fácil comprensión y manejo del proyecto.
7	Identificación de activos	Donde se detallan las clases de activos esenciales de un sistema de información de la universidad caso de estudio.
8	Inventario de activos	Comprende la relación de activos de la universidad caso de estudio el cual se lista de acuerdo a la identificación de activos.
9	Valoración de activos	Se detalla el inventario con su respectiva valoración, el cual se han definido dimensiones, los cuales se van a tomar 3 concernientes a la seguridad de la información (confidencialidad, integridad, disponibilidad), procediendo a realizar su valoración en una escala del 1 al 3, (1 bajo, 2 medio y 3 alto), y como resultado son los activos de mayor relevancia.
10	Identificación de amenazas	Donde se detalla los tipos de amenazas y el origen de estas (Deliberado D, Accidental A y Ambiental E)
11	Identificación de vulnerabilidades	Donde se detalla un inventario de vulnerabilidad de los activos con su respectivo código y tipo de vulnerabilidad.
12	Identificación de riesgos	Donde se detalla una lista de riesgos con su respectivo código, tipo y descripción del riesgo.
13	Análisis preliminar de riesgos	Comprende el objetivo del plan de gestión de los riesgos del proyecto, así como también roles y responsabilidades y el control de los riesgos.
14	Análisis de riesgos	Comprende la valoración del riesgo como resultado de la probabilidad y el impacto de

		este que podría verse afectado los activos de información.
15	Políticas de seguridad de la información	Donde se establecerán en un contexto normativo para la institución.
16	Tratamiento de riesgos	Comprende el tratamiento de los riesgos de activos críticos de la universidad caso de estudio.
17	Declaración de aplicabilidad	Comprende los controles, aplicabilidad y su ejecución referente a la SI.
18	Plan de auditoría	Especifica el procedimiento de auditoría para tener acceso a la información de la universidad caso de estudio.
19	Seguimiento	Detalla la indagación de la adaptación de políticas de seguridad de la información.
20	Matriz RACI	Detalla las responsabilidades de los responsables mediante la matriz RACI con sus respectivas actividades.
21	Informe final de auditoría	Donde se muestra como resultado de los documentos revisados, indicando las no conformidades.
22	Diagrama de causa efecto	Detalla las relaciones de causa – efecto que existe, el cual muestra como consecuencia la ausencia de seguridad de la información.
23	Tratamiento de No Conformidades	Donde se muestran la identificación de No conformidades y la descripción de las mismas.
24	Plan de mejora continua	Describe el objetivo, alcance, responsabilidades, descripción de actividades del plan de mejora.

2. En la etapa ejecutar se efectuó la ejecución de las acciones planteadas descritas en la etapa planificar primeramente se llevó a cabo una reunión inicial del proyecto, para mantener comunicación con todos los involucrados desde el inicio hasta finalizar el proyecto, luego de la aprobación del proyecto se realizó una entrevista con los stakeholders, para ello se formuló 10 preguntas al jefe de tecnologías de la información, el cual indica ausencia de resguardo en la dirección de los activos concernientes a la información como también ausencia de conocimiento y concientización por parte del personal de la universidad.

   Se realizó una relación de todos los activos en la cual como resultado se obtuvo 11 ámbitos el cual se han definido 3 dimensiones de seguridad de la información para la valoración de activos (confidencialidad, integridad, disponibilidad), procediendo a valorar en una escala del 1 al 3, (1 bajo, 2 medio y 3 alto), todo ello para tomar las medidas de resguardo de seguridad de los activos con mayor relevancia dentro de la universidad caso de estudio.

   Se realizó un listado donde se describen: amenazas, vulnerabilidades y riesgos debido a lo cual se puede estar exponiendo los activos de información, el análisis de riesgos se realizó mediante la valoración del riesgo como resultado de la probabilidad y el impacto de este que podría verse afectado los activos de información y posterior a ello tomar las consideraciones necesarias de probables amenazas y los perjuicios que consigan ocasionar negativamente los activos de información de la universidad caso de estudio, realizado lo anterior estudiamos el impacto ocasionado por la ejecución del mismo, evaluado en cada uno de los 11 ámbitos examinados, en esta actividad se desarrollan los planes de mitigación de riesgos de los activos críticos de la universidad con la finalidad de dar el respectivo tratamiento de éstos, para ello se realizó políticas de seguridad de información para salvaguardar activos que luego de ser aprobados por la Alta Dirección deberá ejecutarse con capacitación al personal de la universidad el cual creará concientización para adaptarse a las buenas prácticas.

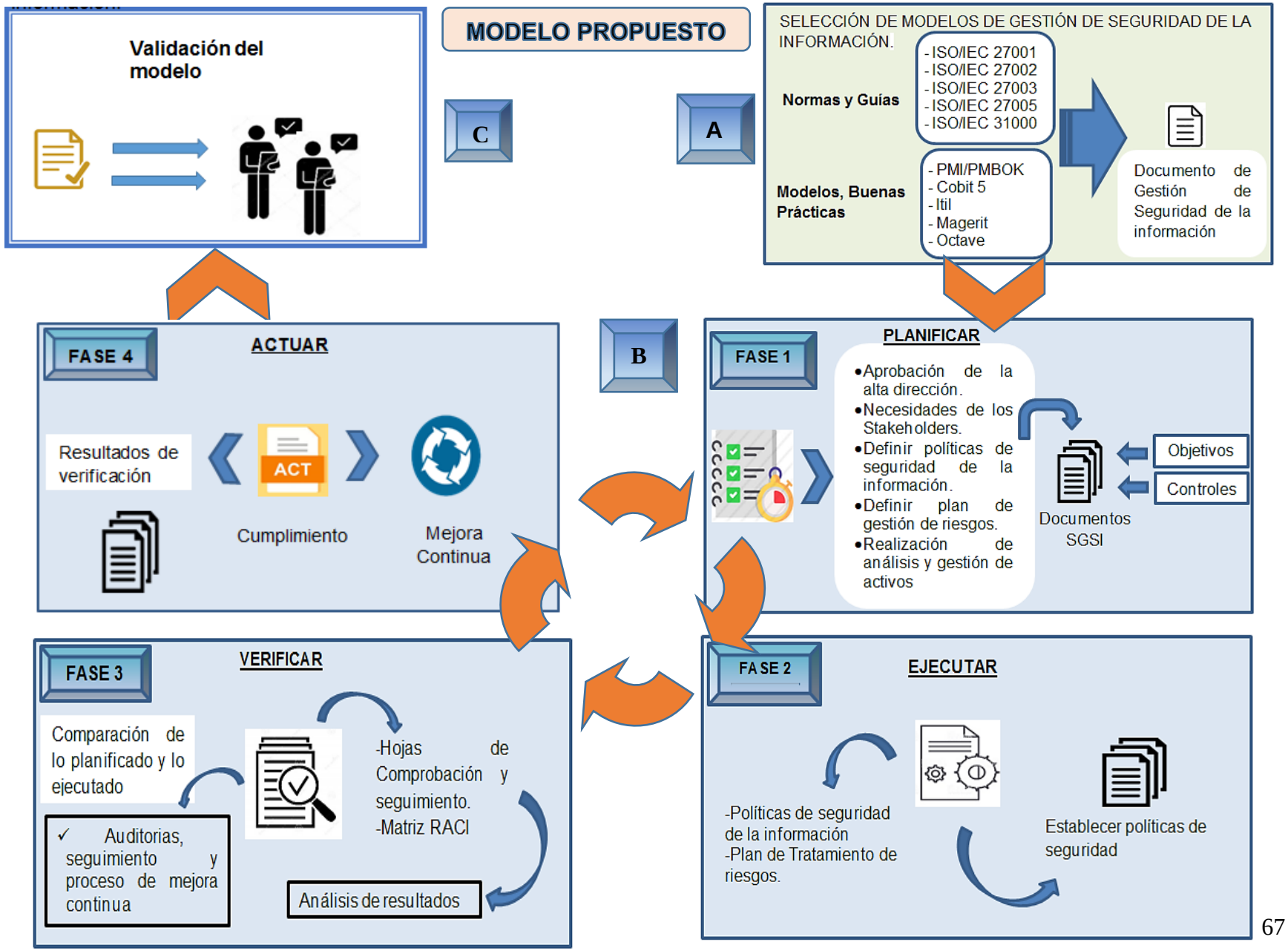
3. En la etapa de verificación se realizó el plan de auditoría con un equipo técnico, encargado de realizar todas las actividades de auditoría a la institución materia de investigación, lo cual se necesita la confidencialidad, privacidad y disponibilidad de los activos de información y tomar las medidas de seguridad que sean necesarios. Luego es elevado al Auditor encargado a fin de preparar o generar el Informe Final de auditoría, el mismo que debe contener toda la información debidamente detallada, indicando fecha y lugar donde se desarrolló la auditoría, los objetivos, los hallazgos, y las conclusiones necesarias. Para la asignación de roles y responsabilidades se utilizó la Matriz RACI. Al culminar las actividades de auditoría y luego ser debidamente aprobado por la Alta Dirección mediante un informe, se puede dar por finalizada la auditoría.

   En último lugar se realizó una auditoría interna basado en políticas de seguridad de la información que presenta este modelo, el cual muestra en efecto una lista detallada de las no conformidades el cual deben ser solucionadas en términos determinados.

4. En la etapa actuar se realizó las acciones correspondientes correctivas de las no conformidades necesarias de las actividades de la fase anterior que fueron detectadas en la auditoría, esto incluye la revisión constante lo cual conlleva a la actualización continua del SGSI. Desde este instante empieza el ciclo segundo PDCA (Planificar-Ejecutar-Verificar-Actuar) del SGSI.

3.1.1. Modelo de Gestión de Seguridad de la Información

El presente capítulo describe el modelo de gestión de seguridad de la información basado en el ciclo de Deming o ciclo PDCA: Planear, ejecutar, Verificar, Actuar.


Validación del modelo
MODELO PROPUESTO
C
A
B
SELECCIÓN DE MODELOS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.
Normas y Guías
- ISO/IEC 27001
- ISO/IEC 27002
- ISO/IEC 27003
- ISO/IEC 27005
- ISO/IEC 31000
Modelos, Buenas Prácticas
- PMI/PMBOK
- Cobit 5
- Itil
- Magerit
- Octave
Documento de Gestión de Seguridad de la información
FASE 4
ACTUAR
Resultados de verificación
ACT
Cumplimiento
Mejora Continua
FASE 1
PLANIFICAR
•Aprobación de la alta dirección.
•Necesidades de los Stakeholders.
•Definir políticas de seguridad de la información.
•Definir plan de gestión de riesgos.
•Realización de análisis y gestión de activos
Documentos SGSI
Objetivos
Controles
FASE 3
VERIFICAR
Comparación de lo planificado y lo ejecutado
-Hojas de Comprobación y seguimiento.
-Matriz RACI
✓ Auditorias, seguimiento y proceso de mejora continua
Análisis de resultados
FASE 2
EJECUTAR
-Políticas de seguridad de la información
-Plan de Tratamiento de riesgos.
Establecer políticas de seguridad

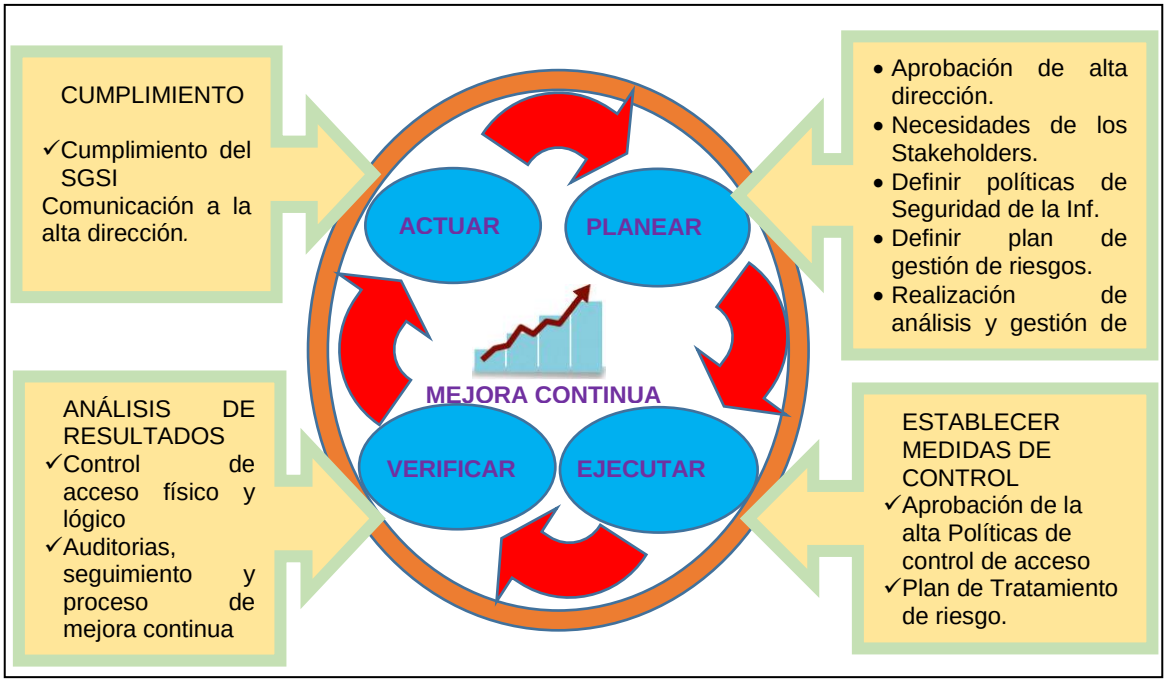


Figura 11: Ciclo PDCA, Tomado de [a] (27000 I. , 2005-2013). [b] (ISACA, 2012). [c] (Ministerio de Hacienda , 2012)

A) Selección de normas y guías de buenas prácticas.

Luego de seleccionar las normas, buenas prácticas y modelos se ha extraído partes de cada estructura, el cual especifica el marco de trabajo de cada una de ellas, para luego poder generar un nuevo modelo SI.

En esta etapa se analizará las normas y guías de buenas prácticas para la gestión de seguridad de la información dentro de las cuales tenemos:

- **Normas y Guías**

- ISO/IEC 27001: Requerimientos del SGSI.
- ISO/IEC 27002: Prácticas de control de SGSI.
- ISO/IEC 27005: Gestión de los riesgos de un SGSI.
- ISO/IEC 31000: Gestión de riesgos y la seguridad.

➢ **Modelos de Gestión de Seguridad de la Información**

- Modelo PMI/PMBOK
- Cobit 5
- Itil
- Magerit
- Octave

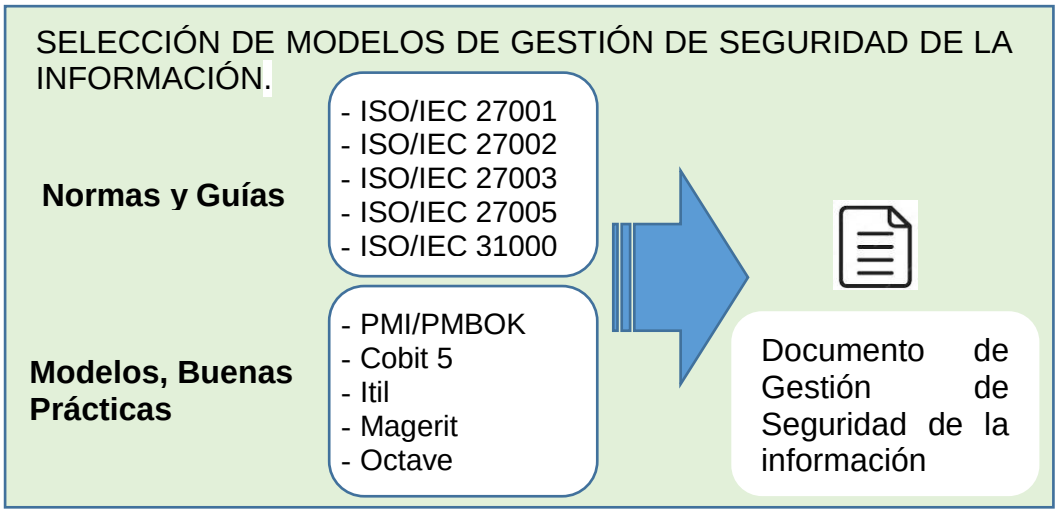


Figura 12: Selección de normas, guías de buenas prácticas y modelos

B) Propuesta del modelo de gestión de seguridad de la información.

Fase 1: Planificar

Se puntualiza las diferentes actividades en el proceso de planificación, el cual se obtendrá documentos conteniendo los objetivos y controles de cada uno de ellos:

i. Aprobación de la alta dirección para dar inicio al proyecto.
ii. Necesidades de los Stakeholders.
iii. Definir responsabilidades/formación de las personas implicadas.
iv. Definición de políticas de seguridad de la información.
v. Definición del plan de gestión de riesgos.

Figura 13: Fase planificar

Fase 2: Ejecutar

En esta fase se ejecutará los objetivos y controles especificados en la etapa de planificación.

En respuesta a las necesidades, existen algunos estándares de buenas prácticas que permiten comprender la administración y la gestión de las TI, en esta fase del proyecto se diseña una metodología usando como línea de base a COBIT 5 y a la norma ISO/IEC 27002 donde permita comprender y gestionar políticas correspondientes a la seguridad de la información para entornos de la Gobernabilidad Autónoma de la institución en mención.

i. Políticas de Seguridad de la Información.

ii. Plan de Mitigación de riesgo.

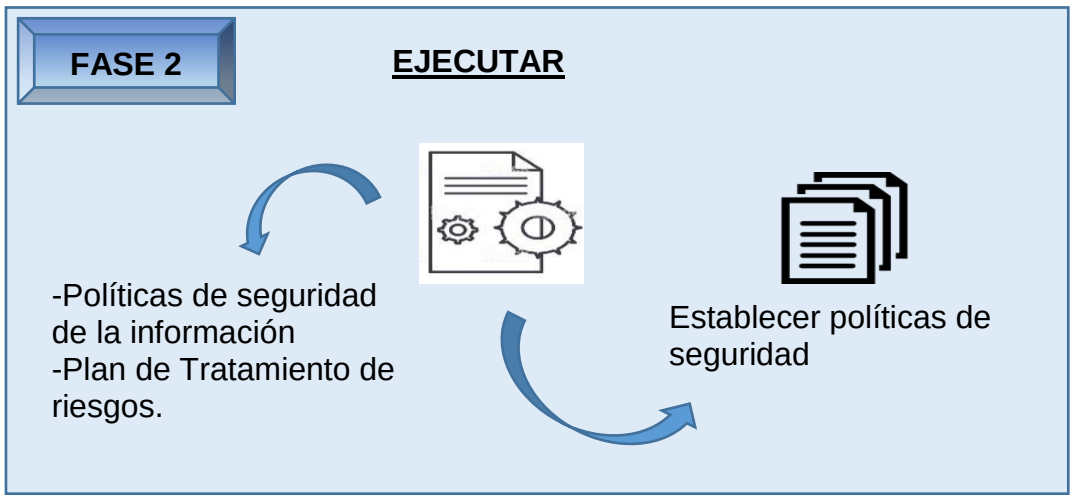


Figura 14: Fase Ejecutar

Fase 3: Verificar

En esta fase se efectuará una comparación entre la etapa de planificación y ejecución, el cual se obtendrá un análisis de los resultados.

Control de acceso físico y lógico

i. Auditoria, seguimiento y procesos de mejora continua

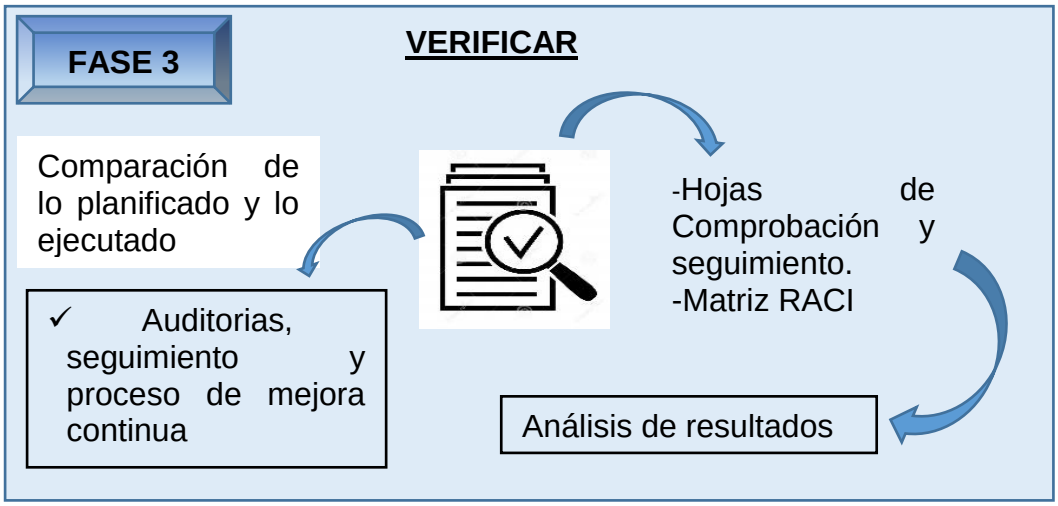


Figura 15: Fase Verificación.

Fase 4: Actuar

Realizamos las acciones necesarias para la mejora continua.

i. Cumplimiento:

No conformidad acción correctiva.

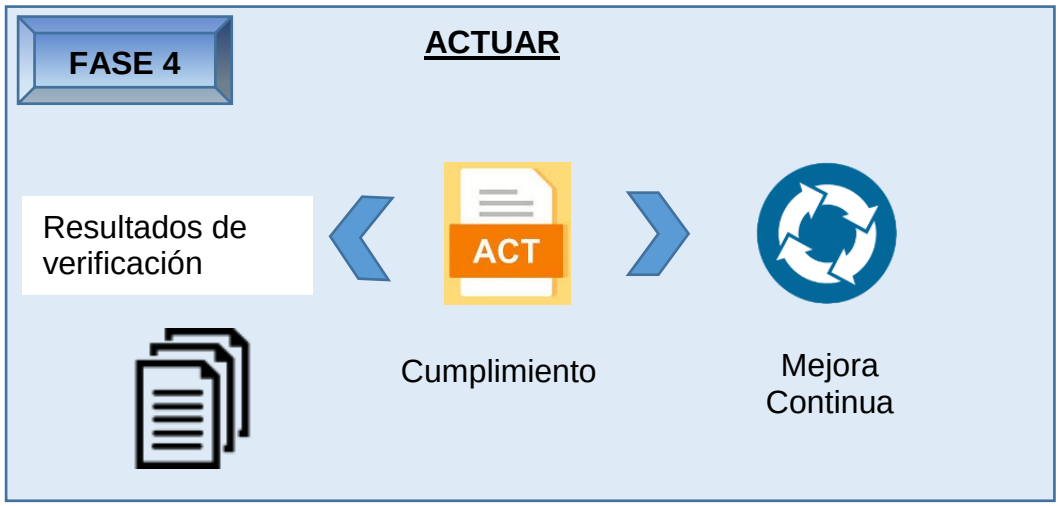


Figura 16: Fase Actuar

C) Validación del modelo.

Este proceso de validación de la presente propuesta de indagación se ejecutará por expertos en la gestión de seguridad de la información.

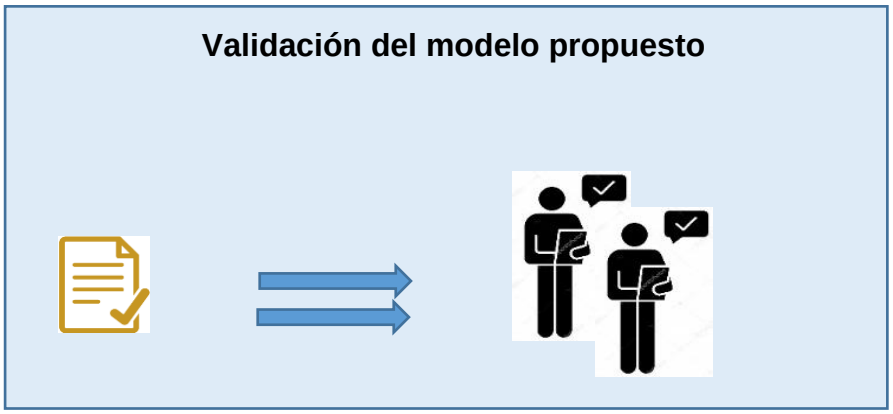


Figura 17: Fase de validación

3.1.2. Desarrollo de la propuesta del SGSI

Diagnóstico de la empresa

El diagnóstico de la empresa se efectuará para el establecimiento de la iniciación del proyecto, donde el objetivo de la indagación es proponer un sistema de gestión de seguridad de la información, para la mejora continua en la Universidad Nacional Intercultural “Fabiola Salazar Leguía” Bagua.

1. PLANIFICAR:

En esta fase se definen los procesos donde se establecerán los controles de seguridad de información propuesta en la presente investigación para la universidad caso de estudio, estos procesos nos dan un alcance en cuanto a qué gestiones se va a realizar sobre el resguardo de los activos de la institución que involucra los procesos de: Admisión, Matrícula y de Notas.

Aprobación del proyecto

El actual Proyecto es una propuesta de un Sistema de Gestión de Seguridad de la Información en la Universidad Nacional Intercultural “Fabiola Salazar Leguía”

Bagua. El proyecto se presentará a la oficina de presidencia para su evaluación y aprobación.

Posteriormente se inicia el proyecto lo cual es suma importancia que la alta dirección de dicha institución universitaria apoye y se comprometa con el resguardo de la información y especificar a partir qué objetivos se está comenzando. Véase en la figura Nº19.

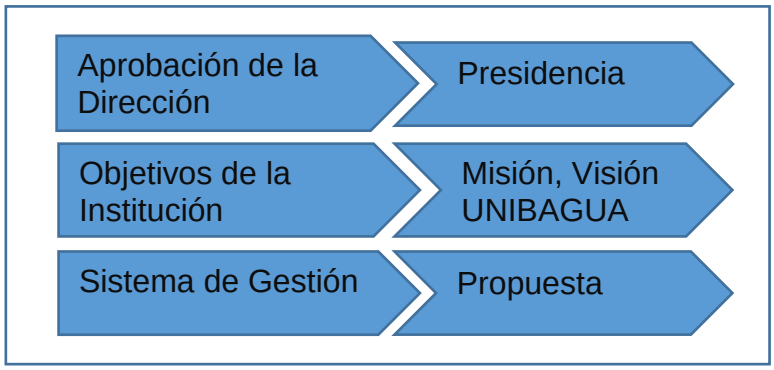


Figura 18: Inicio del proyecto

Proceso de Aprobación del Proyecto:

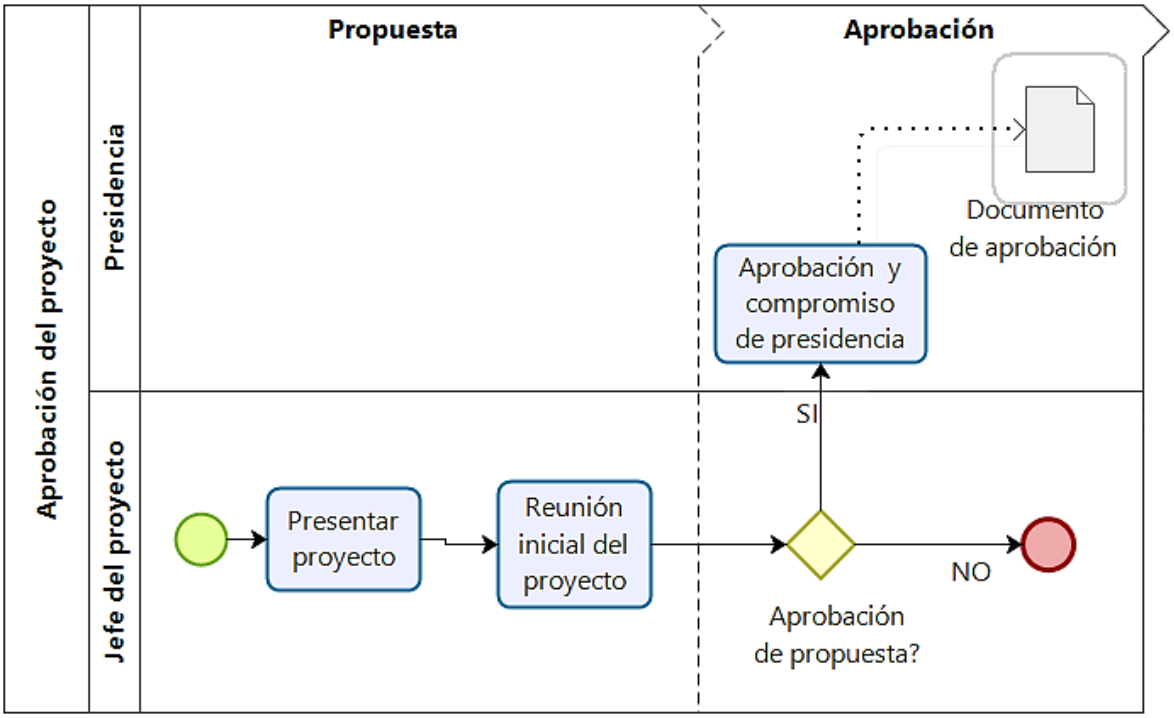


Figura 19: Proceso de la aprobación del proyecto

Reunión Inicial del Proyecto (RIP)

La reunión inicial del proyecto es muy importante ya que de ello depende encaminar bien el proyecto, aquí se comunica los objetivos, el alcance del SGSI, las políticas, controles, los roles y responsabilidades, y además mantener comunicación con todos los involucrados desde el inicio hasta finalizar el proyecto, explicar los roles y las responsabilidades de los stakeholders. **VER ANEXO N°03.**

Aprobación y compromiso de Presidencia (ACP)

La aprobación y compromiso de presidencia es la fase inicial y primordial del proyecto, definiendo un plan del proyecto que contenga primacías y objetivos como propuesta de un Sistema de Gestión de Seguridad de la Información, asimismo de la distribución de la universidad.

El jefe de proyecto presenta la propuesta del SGSI para su respectiva revisión y aprobación correspondiente, la Dirección debe estar comprometida con el proyecto que favorecería en forma positiva en lo que concierne a los activos de la información y la importancia del SGSI en una organización.

Documento de Aprobación del Proyecto (DAP)

El resultado deseado en esta fase será la conformidad precedente de alta Dirección y la responsabilidad de realizar cada actividad descrita en la propuesta presente. **VER ANEXO N°04.**

Necesidades de los Stakeholders.

Después de haber sido aprobado la propuesta del SGSI, los Stakeholders deben brindar soporte al proyecto y un compromiso más constante encargado por los directivos de la universidad.

Tomar medidas de control de seguridad siguiendo los objetivos de identificar los activos, así como también evaluando los riesgos.

Tabla 9.

Necesidades de los Stakeholders

COBIT			ISO /IEC 27001	
APO002	Gestión de seguridad	Requerimientos	Protección	Justificar
APO00201	Comprender la trayectoria de la compañía	4.2) Entendiendo las carencias y expectaciones de los Stakeholders.	A+	Según La ISO, se tiene que alcanzar las carencias de los Stakeholders teniendo acceso a una adecuada información.

Nota: Cuadro comparativo de las necesidades de los Stakeholders según COBIT y la ISO /IEC 27001

Proceso Necesidades de los Stakeholders:

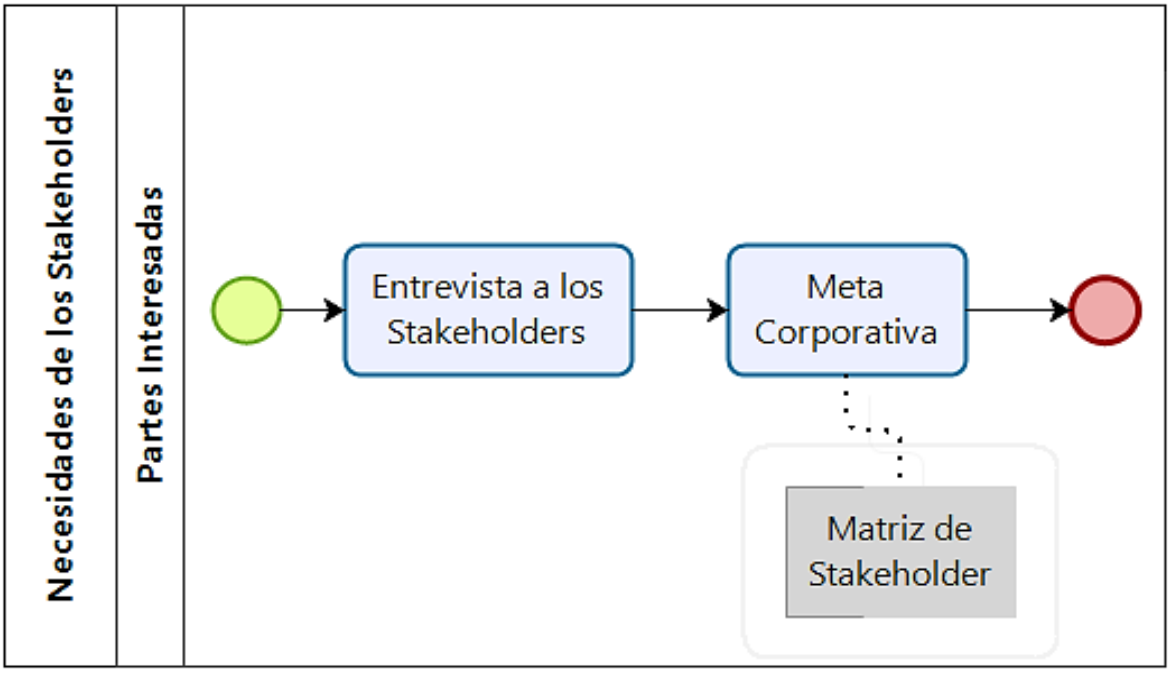


Figura 20: Proceso Necesidades de los Stakeholders

Identificación necesidades y expectativas:

Para la identificación de necesidades y expectativas se utilizó entrevistas a los stakeholders para tener un alcance las necesidades presentes en la institución y a la vez comprometidos en la presente propuesta de SI.

Entrevista con los Stakeholders (ES)

La entrevista efectuada a los Stakeholders se realizó con la finalidad de tomar conocimiento acerca de las insuficiencias en cuanto a la seguridad de la información y alcanzar los objetivos. **VER ANEXO N°05.**

Meta Corporativa (MC)

De la cascada de metas con respecto a las TI, se tomarán en cuenta la información y tecnología relacionada, interna de COBIT 5, en el marco de la seguridad de la información y cumplir con las políticas internas de seguridad de la información.

Matriz de Stakeholders (MS)

La matriz stakeholders es una herramienta de gran importancia porque es donde se identifican los involucrados y definen sus niveles de interés e influencia, lo cual es muy importante porque la información obtenida nos ayudará en todo el desarrollo del proyecto y nos conducirá al éxito del proyecto. **VER ANEXO N°06**.

Definir políticas de seguridad de la información

Luego de realizar el análisis de los procesos seleccionados: (Admisión, matrícula y de notas) la sistemática de gestión de seguridad de la información propone políticas de seguridad con la finalidad de tomar acciones que correspondan y que protejan los activos de información de la universidad.

Proceso definir políticas de seguridad

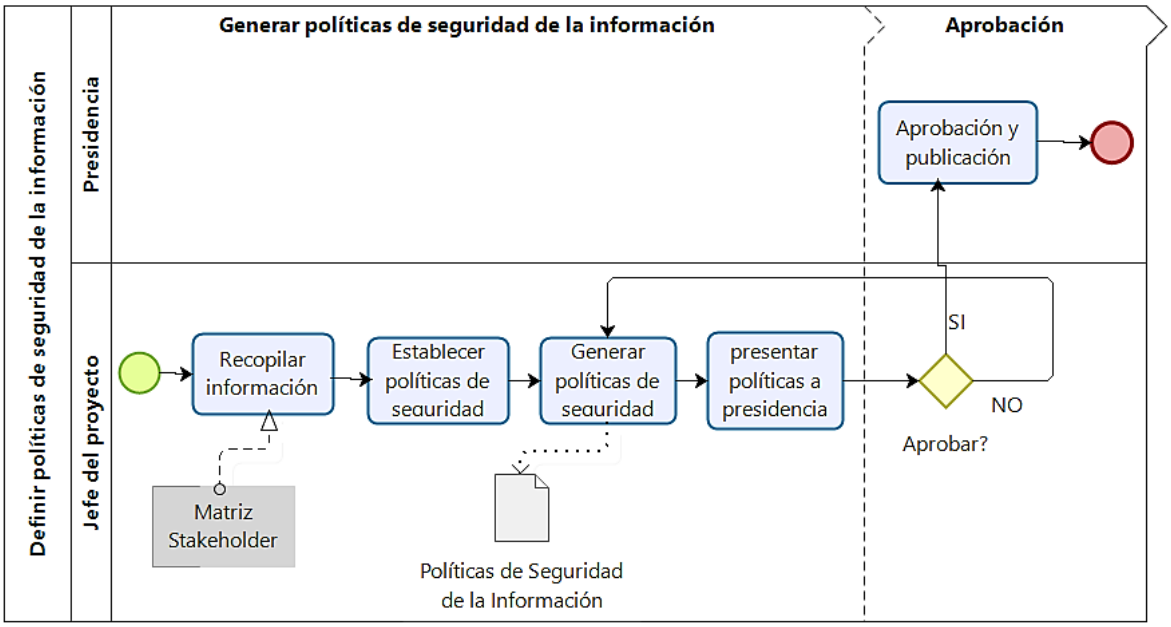


Figura 21: Proceso definir políticas de seguridad de la información

Recopilar Información (RI)

La recopilación de la información mediante los Stakeholders realizada en el proceso anterior va a ser de vital importancia ya que enmarca los objetivos de control del SGSI, considerando los requerimientos establecidos con relación a la seguridad de la información.

Establecer políticas de seguridad (EPS)

Se establecerán políticas de seguridad donde contenga el marco general, así como también los objetivos vinculados con la seguridad de la información y en donde también se encuentra organizada en el entorno esencial de gestión de los riesgos de la universidad a través del cual se creará y salvaguardará el SGSI. **VER ANEXO N°17.**

Generar políticas de seguridad (GPS)

Generar políticas relativo a la seguridad para brindar protección a los activos de información de la organización el cual presenta introducción, objetivos, alcance, cumplimiento y conformidad, marco legal, marco

referencial, objetivos de control, políticas de seguridad de la información, para luego presentarlo y esta debe ser aprobada por los altos directivos y posteriormente publicada y comunicada a los involucrados en el proyecto.

Gestión del alcance del proyecto

El presente proyecto se concibe para la Universidad Nacional Intercultural "Fabiola Salazar Leguía" Bagua, toma como referencia los estándares de buenas prácticas de MPBOK, el cual se plasma en la presente propuesta modelo de Gestión de Seguridad de Información el cual abarcará como muestra tres procesos que se tomará en cuenta para tomar medidas de seguridad apropiadas.

Los procesos de: Admisión, matrícula y notas se encuentran definido en la tabla N° 5 Matriz de distribución de los procesos de información de la caracterización de los sujetos.

El presente modelo no se implementa, pero sí propone un SGSI basado en el ciclo de Deming, mediante políticas de seguridad que permitan a la institución un mejor desempeño en la administración de la información y por lo tanto un activo de gran importancia.

Proceso Alcance del proyecto

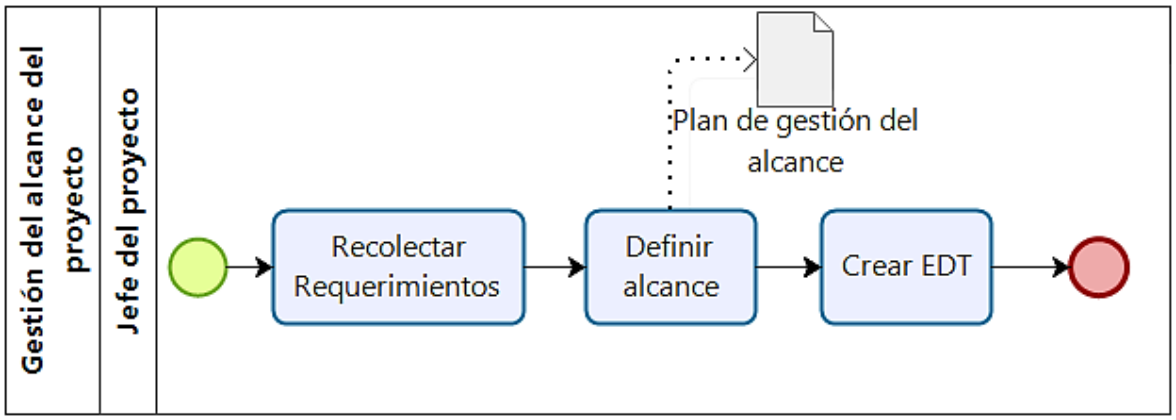


Figura 22: Alcance del proyecto

Definir Alcance del proyecto (DAP)

Se realizó en vista a las necesidades que el proyecto pretende encaminar, esto Implica un desglose en componentes más pequeños de las principales prestaciones del proyecto, todo ello con la finalidad de llevar a cabo un adecuado manejo de las estimaciones de costo, tiempo y recursos.

La definición del alcance debe incluir: la justificación del proyecto, las especificaciones y el propósito que el proyecto pretende abordar como también las restricciones del proyecto.

Plan de Gestión del Alcance (PGA)

En este proceso del PGA se establece cómo se especificará el alcance del proyecto, también cómo se establecerá y detallará la Estructura de Desglose del Trabajo (EDT). **VER ANEXO N°07.**

Crear EDT

La creación de un EDT para la fácil comprensión y manejo del proyecto donde se subdivide el trabajo en porciones más pequeñas. Esto con la finalidad de organizar y definir el alcance total del proyecto. **VER ANEXO N°08**

Tabla 10.

Proceso EDT

Entrada		Salida
Definir alcance	⇨	EDT

La figura Nº24 contempla los procesos que pertenecen al alcance del SGSI:

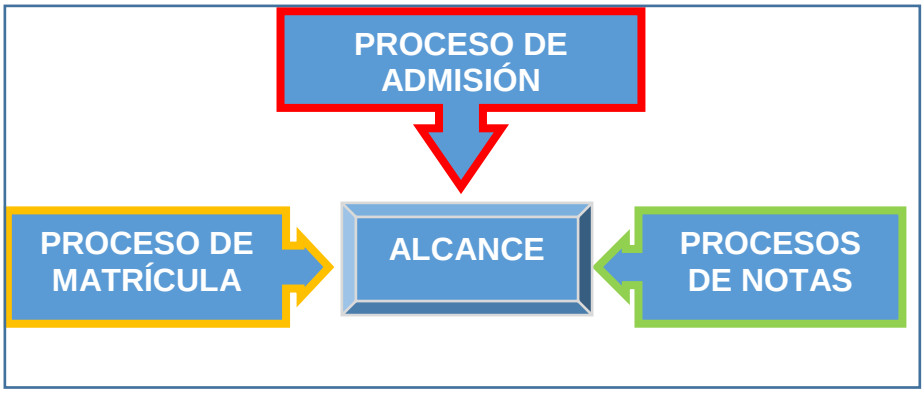


Figura 23: Alcance del proyecto. Fuente: Elaboración propia

Definir plan de gestión de riesgos

Toda entidad se halla en exposición a los riesgos constantemente, ante este tipo de situaciones se deberá estar preparado ante cualquiera amenaza que podría perjudicar negativamente los activos de información, es por ello debemos tomar medidas de seguridad para su adecuada protección.

Se utilizó diferentes modelos de metodologías para analizar y gestionar los riesgos, en la presente investigación: ISO/IEC 27005, Magerit y Octave, que muestran las gestiones a continuar para su adecuada realización.

Proceso Análisis Y gestión de riesgos

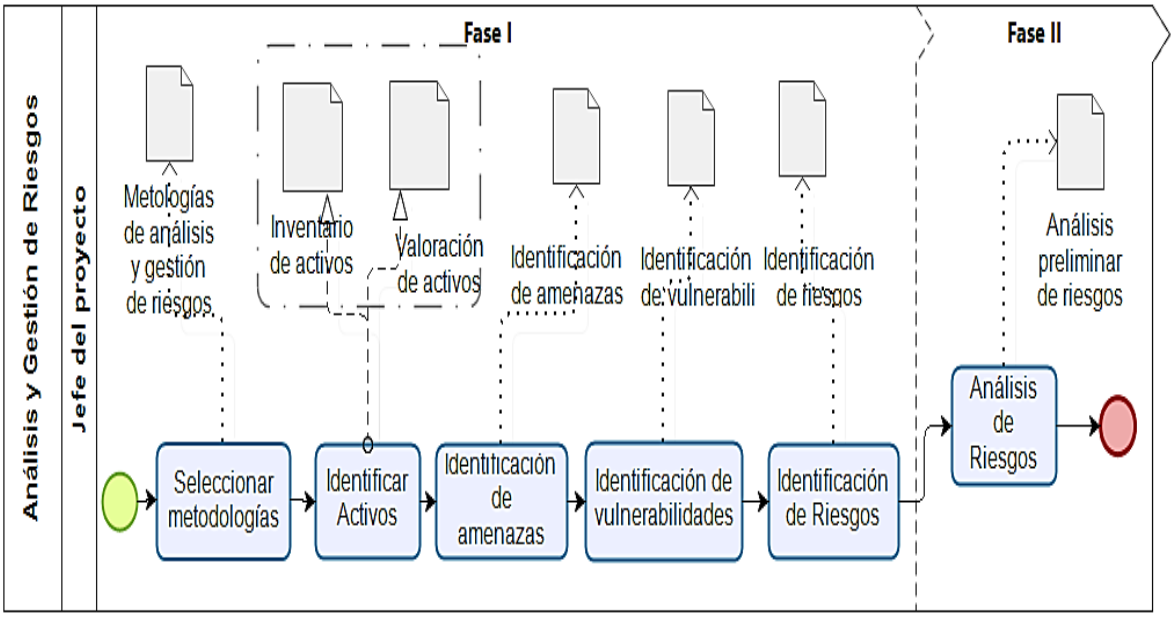


Figura 24: Análisis y gestión de riesgos

Selección de metodologías (SM)

Se seleccionó metodologías para la ejecución de análisis y gestión de los riesgos en donde se puede especificar que de los modelos que se ha tomado en cuenta, la normativa consagrada únicamente a gestionar riesgos relacionado con la seguridad de la información, ISO/IEC 27005, el cual suministra las recomendaciones y los lineamientos de metodologías y sistemáticas sobre valoración de los riesgos concernientes a la Seguridad de la Información, con base a la normativa ISO/IEC 27001 del proceso de gestión de riesgos. Todo ello de suma importancia para poner en marcha para analizar y gestionar de riesgos, a través del cual es una etapa principal del SGSI.

Tabla 11:

Cuadro comparativo de metodologías

ISO/IEC 27005	MAGERIT	OCTAVE
Establecimiento del contexto.	Modelo de valor.	Construcción de perfiles de amenaza basada en los activos.
Valoración de riesgos:	Mapa de riesgos.	Identificar vulnerabilidades de infraestructura.
Identificación del riesgo	Declaración de aplicabilidad.	
Estimación del riesgo	Evaluación de Salvaguardas.	
Evaluación de riesgos		

Nota: La tabla muestra el cuadro comparativo de las metodologías: ISO/IEC 27005, Magerit y Octave

Identificación de Activos (IA)

Los componentes esenciales de un sistema de información son los activos y a la vez estos son susceptibles a cualquier tipo de amenazas dentro de una organización.

Para la identificación de los activos se tomarán en base al catálogo de elementos del libro II Magerit v3. **VER ANEXO N°09.**

Inventario de Activos (IAc)

El IAc de la UNIBAGUA accede especificar los activos y proteger todos aquellos activos de gran relevancia para la universidad, como también debe tener asignado un propietario se responsabilizará en el mantenimiento de los controles adecuados. **VER ANEXO N°10.**

Valoración de los Activos (VA)

Los activos adquieren valor para toda organización es por ello que necesita de su protección, para lo cual vamos a tomar en cuenta los criterios de valoración de Magerit (MAGERIT V3 libro 2 Catalogo de elementos), en este sentido proviene efectuar una estimación cualitativa de cada activo tomando en cuenta sus dimensiones de seguridad como confiabilidad, disponibilidad, integridad y autenticidad.

1. La valoración de activos en de suma importancia para la evaluación de riesgos, por tal motivo es que vamos a estimar el impacto que causa a la universidad su interrupción, el cual se ha determinado 3 dimensiones de seguridad de la información (confidencialidad, integridad, disponibilidad), procediendo a valorar en una escala del 1 al 3, (1 bajo, 2 medio y 3 alto), todo ello para tomar las medidas correspondientes de salvaguardia de seguridad de los activos de mayor relevancia para la institución. **VER ANEXO N°11.**

Identificación de Amenazas (IAm)

Para identificar las amenazas debemos tener en claro que estas pueden desencadenar un incidente ocasionando daños graves sobre los activos de información, en este sentido esta normativa (ISO/IEC 27005) tiene una lista de amenazas el cual se utilizará para establecer la matriz de riesgos. **VER ANEXO N°12**

Identificación de Vulnerabilidades (IV)

Las vulnerabilidades son aquellas debilidades que adquieren los activos y es ahí donde consiguen aprovecharse las amenazas, es por ello que es muy importante conocerlos para efectuar medidas de seguridad adecuadas con la finalidad de reducir los riesgos evitando así las amenazas.

Para la identificación de las debilidades se hallan fundamentados en la normativa ISO/IEC 27005 donde pueden proporcionar ayuda para determinar escenarios de incidentes relevantes. **VER ANEXO N°13.**

Identificación de Riesgos (IR)

Los riesgos se definen como eventos que dañan de manera negativa la obtención de los objetivos de la institución.

Se elabora la identificación de los riesgos por medio de una matriz de riesgos con la finalidad de estar preparados ante cualquier situación de peligro que afectan negativamente la obtención de los objetivos de la institución.

La identificación de riesgo está basada en la normativa ISO/IEC 31000 en el cual se consideran factores y su relación entre ellos. **VER ANEXO N°14.**

Análisis Preliminar de Riesgos (APR)

Después de analizar los riesgos, se generará un análisis preliminar de riesgos, el cual es un mecanismo de mucha utilidad en la detección y localización de riesgos para su posterior mitigación. **VER ANEXO N°15.**

Análisis de Riesgos (AR)

El AR basado en la metodología Magerit es una alternativa en lo concerniente a la gestión de riesgos en una institución, saber y tener en cuenta los riesgos que se hallan afectando los activos y de esta manera controlarlos.

Para el análisis y valoración de los riesgos se debería llevar a cabo basándose en el juicio y perspectiva de los Stakeholders. **VER ANEXO N°16.**

2. EJECUTAR

Esta fase comprende la implementación de las actividades precisas para la consecución las mejoras proyectadas en esta fase planificar, en el cual implica salvaguardar de las amenazas que atenten contra los activos, protegiéndolo con una apropiada gestión de riesgos, así como también el cumplimiento de los controles utilizando las buenas prácticas dentro y fuera de la universidad.

1. Políticas de Seguridad de la Información (PSI)

Las políticas de la seguridad de la información para la Universidad caso de estudio se establecerán un marco normativo con todos los involucrados en el proyecto.

Proceso Políticas de Seguridad de la Información

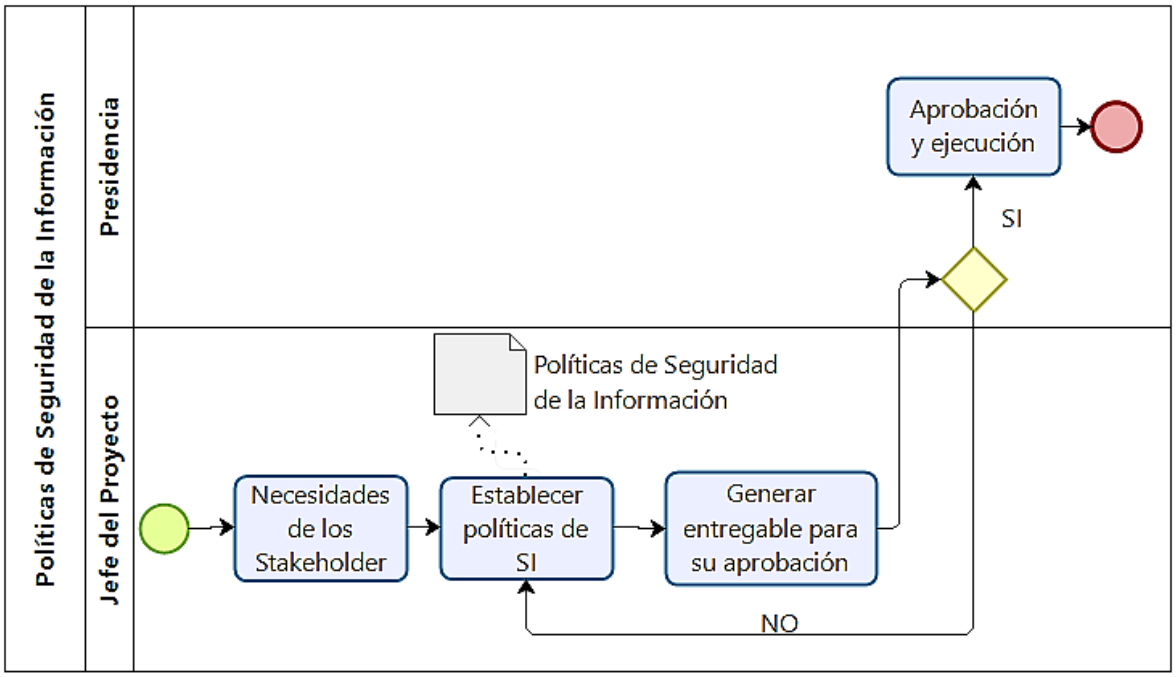


Figura 25: Políticas de Seguridad de la Información

Necesidades de los stakeholders (NS)

Habiendo hecho un estudio previo en la Universidad caso de estudio, se detectó la ausencia de documentos de gestión de seguridad de la información de acuerdo a las insuficiencias de los stakeholders, por lo que implica la obtención de políticas de seguridad de información, que sirve en la ejecución de tareas del área administrativa y académica, eso significa el compromiso de todos los involucrados el cual tiene por finalidad de obtener los objetivos de la organización.

Establecer políticas de seguridad de la información (EPSI)

Establecer políticas de seguridad con la finalidad de reunir las instrucciones que tiene como responsabilidad el seguimiento de la seguridad de la información tras ver los requerimientos de los stakeholders, además se deberá implantar las modelos de acción en caso de incidencias y también determinar las responsabilidades.

Las políticas de seguridad de la información se encuentran basados en la normativa ISO/IEC 27002, el cual ofrece controles indispensables para poner en marcha el SGSI. **VER ANEXO N°17.**

Aprobación y ejecución (AE)

En esta actividad se efectuó la presentación sobre las Políticas de Seguridad de la Información, equivalente a las que se han elaborado de tal forma que se acopla a los requerimientos de la institución, siendo muy necesarias a fin de tomar medidas de control pertinentes, para establecer un mejor resguardo de los activos de información teniendo en consideración por ser una institución universitaria lo amerita.

2. Plan de tratamiento contra riesgos (PTR)

En el plan de mitigación contra los riesgos se realizó la elaboración basada en la metodología Octave, la cual está enfocado a la estrategia y a la práctica que van a ayudar en el plan de trabajo a fin de obtener los objetivos de la institución.

Proceso Plan de tratamiento contra riesgos

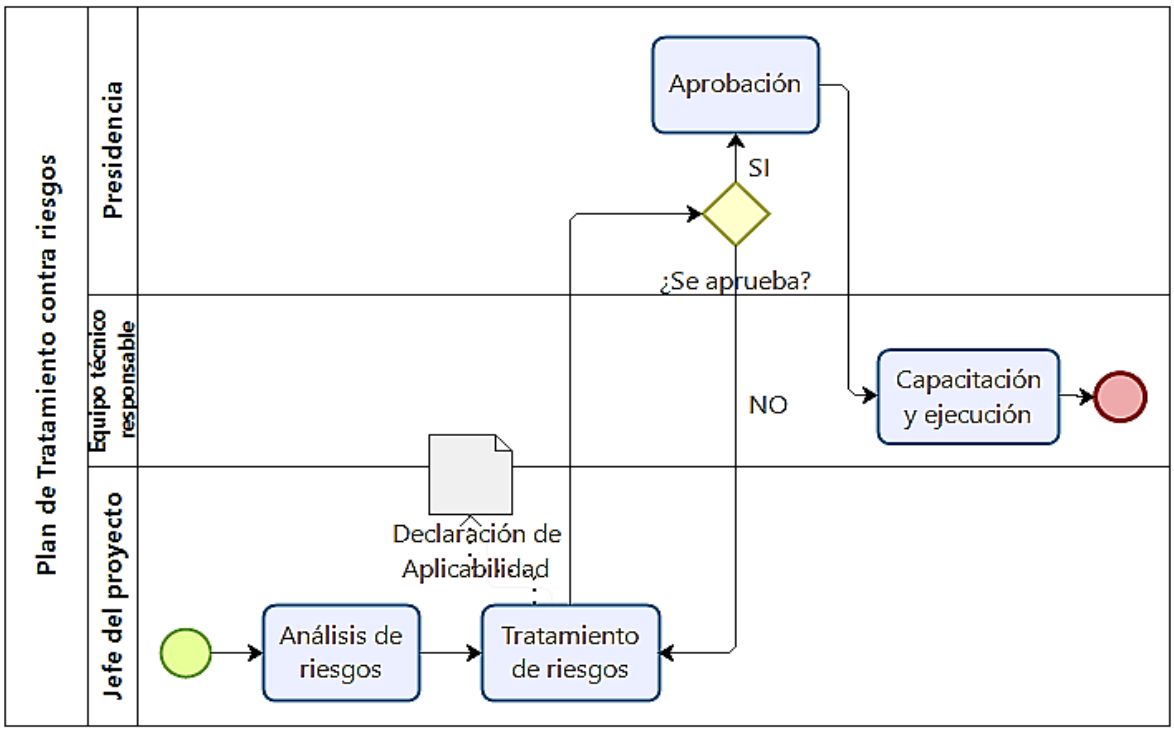


Figura 26: Plan de Tratamiento contra riesgos

Análisis de riesgos (AR)

El paso siguiente después de la identificación de riesgos es analizarlos, todo aquello es realización sobre aquellas posibilidades de amenazas y los daños que consigan perjudicar de forma negativa los activos de información de la organización. Para ello se ha tomado en cuenta el análisis de la metodología Magerit.

Tratamiento de riesgos (TR)

Esta actividad es donde se desarrolla el plan de tratamiento de riesgos de los activos críticos de la universidad donde se basa en el análisis de los riesgos que se han formulado en el proceso anterior, estos están basados en la metodología Octave, lo cual toma como objetivo el riesgo organizacional el cual está enfocado a la estrategia y a la práctica. **VER ANEXO N°18.**

Declaración de Aplicabilidad (DA)

Este documento, contiene los controles para el SGSI de la universidad, donde se informan los resultados sobre la evaluación y tratamiento de riesgos, referente a la seguridad de la información. **VER ANEXO N°19.**

Aprobación de la alta Dirección (AAD)

Después de haber presentado La Declaración de Aplicabilidad a la alta dirección se realizó una evaluación exhaustiva por los miembros encargados y después de un amplio debate fue aprobado.

Capacitación y ejecución (CE)

La capacitación al personal de la institución es muy importante ya que creará concientización para adaptarse a las buenas prácticas dentro y fuera de la institución y ello deberá estar a cargo de un equipo técnico especializado.

3. VERIFICAR:

En la fase de verificación se efectuará una comparación con los objetivos iniciales entre la etapa de planificación y ejecución, la observación de los controles de seguridad propuestos en la etapa planificar.

Proceso de Auditorias, seguimiento y proceso de mejora continua

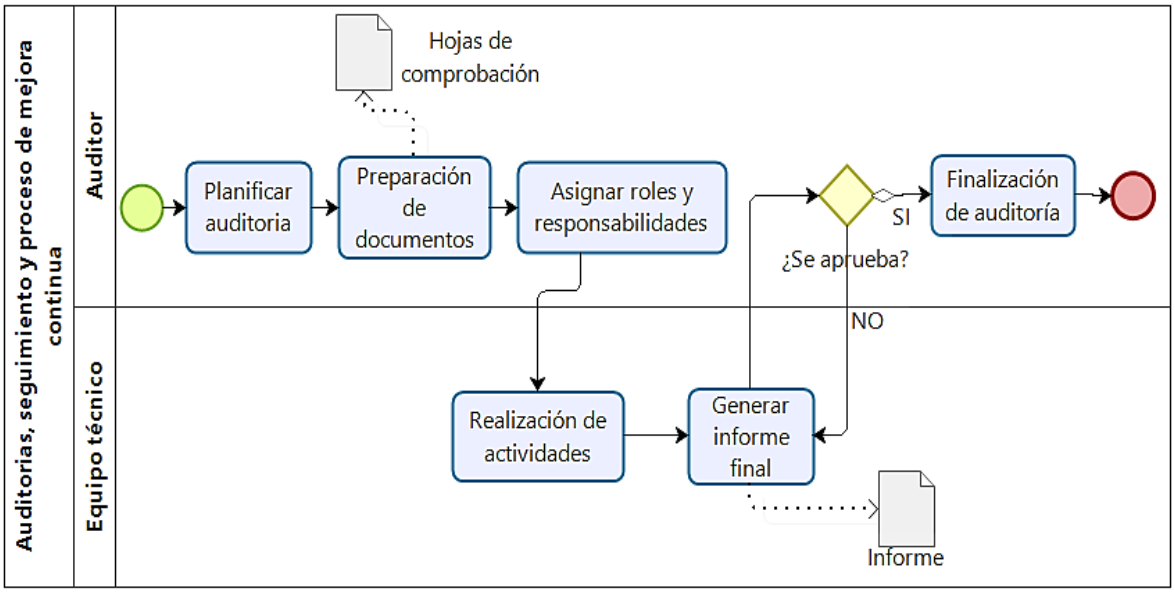


Figura 27: Auditorias, seguimiento y proceso de mejora continua

Auditorias, seguimiento y proceso de mejora continua

Plan de Auditoría (PA)

Tomar medidas y disponer del plan de auditoría para acceder a la información que se requiere, la misma que servirá de utilidad a ambas partes, tanto para el auditor como para la institución. **VER ANEXO N°20.**

Preparación de Documentos de Trabajo (PDT)

La disposición de documentos de trabajo estará a cargo del auditor, todo ello como parte del inicio de las actividades para llevar a cabo la auditoría.

Hoja de Comprobación y Seguimiento (HCS)

Llegado a esta actividad se realiza el seguimiento sobre el acatamiento de políticas con respecto a la seguridad de la información, el cual es aplicable a toda la institución. **VER ANEXO N°21.**

Asignar Roles y Responsabilidades (ARR)

La distribución de roles y responsabilidades se producirá a cabo con el propósito de delegar funciones pertinentes al equipo técnico encargado, quienes deberán realizarlo de manera óptima lo encomendado. Para la asignación de roles y responsabilidades se empleará la Matriz RACI. **VER ANEXO N°22.**

Realización de Actividades (RA)

Se designa un equipo técnico especialista, encargado de realizar todas las actividades de auditoría a la institución materia de investigación, lo cual se necesita la confidencialidad, privacidad y disponibilidad de los activos y tomar las medidas de seguridad que sean necesarios.

Generar Informe Final (GIF)

Después de haber recabado la información solicitada por el equipo técnico de auditoría, es elevado al Auditor encargado a fin de preparar o generar el Informe Final de auditoría, el mismo que debe contener toda la información debidamente detallada, indicando fecha y lugar donde se desarrolló la auditoría, los objetivos, los hallazgos, y las conclusiones necesarias, así mismo identificando a la institución auditada, el auditor y equipo técnico de auditoría.

El informe aprobado debe emitirse a las partes involucradas a la brevedad posible.

Finalización de Auditoría (FA)

Al culminar las actividades de auditoría y luego ser debidamente revisado aprobado y por la alta dirección mediante un informe, se puede dar por finalizada la auditoría. **VER ANEXO N°23.**

4. ACTUAR:

Esta fase es para mantener y mejorar el sistema de gestión de seguridad de la información, de ser necesario se hacen las gestiones correspondientes correctoras y preventivas necesarias de las actividades de la fase anterior que fueron detectadas en la auditoría, esto incluye la revisión constante lo cual conlleva a la actualización continua del SGSI.

a) No Conformidad, Acción Correctiva

Proceso de No Conformidades-Acción Correctiva

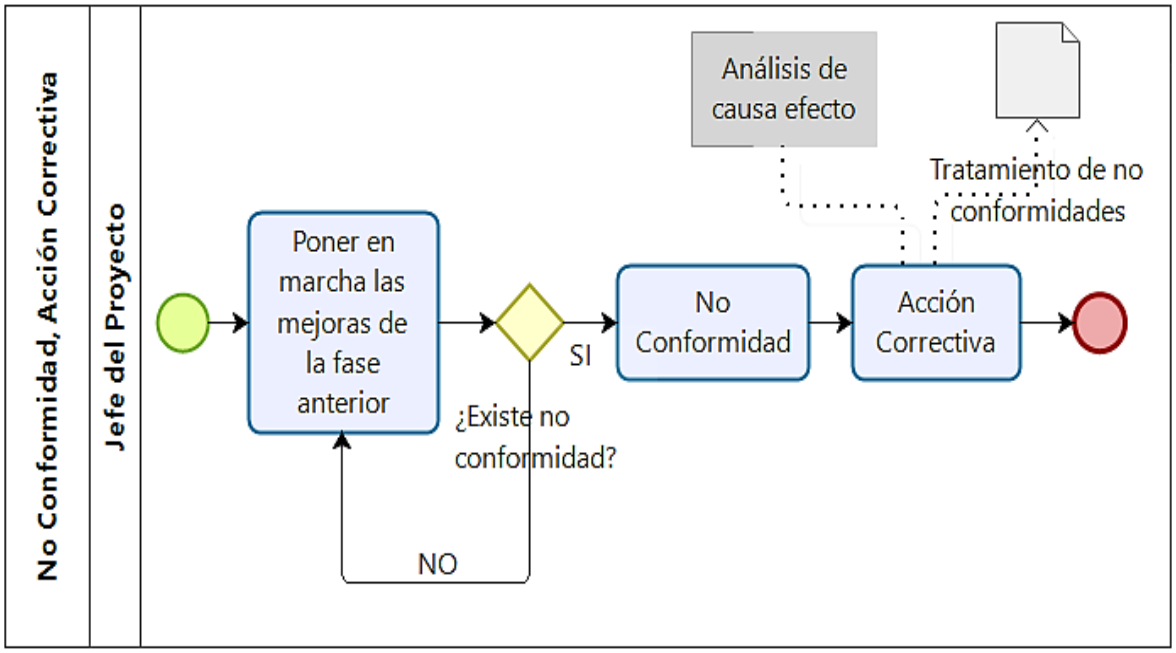


Figura 28: No Conformidades, Acciones Correctivas

Puesta en Marcha (PM)

La puesta en marcha es el siguiente paso de la fase de verificación en donde se toman en cuenta las acciones correctivas y la no conformidad del SGSI y estas sean apropiadas para evitar los resultados de las no conformidades localizadas.

No Conformidad (NC)

La No Conformidad viene a ser el no cumplimiento de políticas o controles establecidos de seguridad de la información que están

establecidos en el SGSI.

Acción Correctiva (AC)

Tomar acciones correctivas es de vital importancia ya que representan las medidas tomadas frente a diversas causas el cual perjudican el progreso y desarrollo de la institución, estas se derivan de la supervisión y evaluación de los resultados del sistema.

Análisis de Causa Efecto (ACE)

En el presente trabajo se utilizó el análisis de causa efecto que es una herramienta para graficar las relaciones causa – efecto que existe en el SGSI, lo cual es suma importancia ya que garantiza los niveles de seguridad requeridos. **VER ANEXO N°24**

Tratamiento de No Conformidades (TNC)

En este proceso del tratamiento de las no conformidades concerniente a la seguridad de la información nos brinda apoyo sobre las acciones correctivas utilizadas sean las adecuadas para la mejora continua del SGSI. **VER ANEXO N°25.**

1. Mejora Continua (MC)

La Mejora Continua es la fase en donde se integran los procesos de mejora del SGSI de forma sistemática, el compromiso y la participación de todos los involucrados también suma y es muy importante mantener la comunicación y prácticas de cultura el cual se base en el ciclo de Deming.

Proceso Mejora Continua

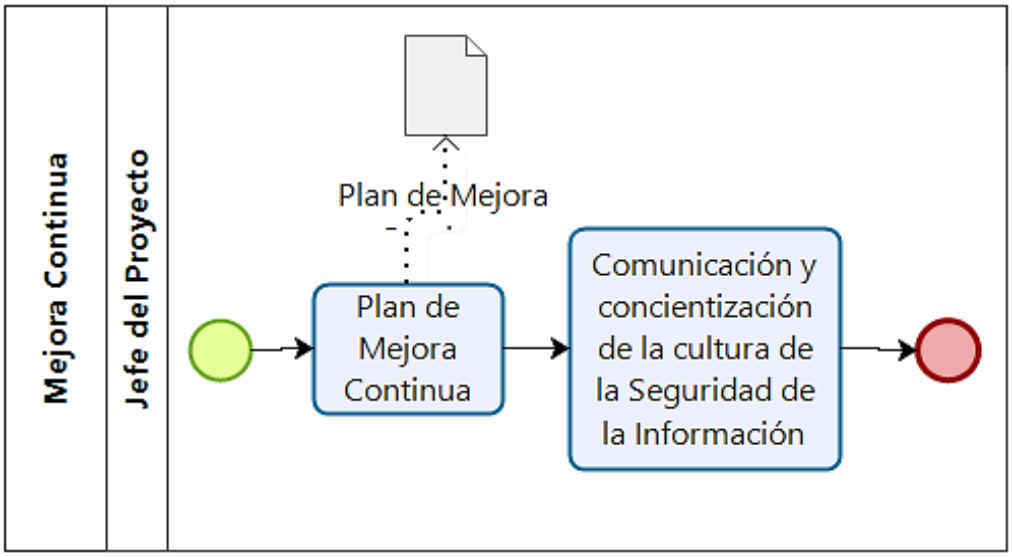


Figura 29: Mejora Continua

Plan de mejora continua (PMC)

El PMC describe el objetivo, alcance, responsabilidades, descripción de actividades del plan de mejora **VER ANEXO N°26.**

Comunicación y concientización de la cultura (CC)

En este proceso es en donde se integran el compromiso y la participación de todos los involucrados también suma y es muy importante mantener la comunicación y buenas prácticas, esto no significa que el ciclo termine, es aquí donde inicia otro ciclo PDCA.

3.1.3. Propuesta de un modelo de SGSI

Propuesta de Sistema de Gestión de Seguridad de la Información Caso de Estudio: Universidad Nacional Intercultural “Fabiola Salazar Leguía” Bagua.

Reunión Inicial del proyecto

REUNIÓN INICIAL DEL PROYECTO	< Logo >

REUNIÓN INICIAL DEL PROYECTO	REVISIÓN N° 1	CÓDIGO RI-001
	FECHA Y HORA DE REUNIÓN 8/07/2019 9:00 am	PÁGINA 1/2

Asistencia a reunión inicial del proyecto

Área asistente a	Nombre	Abrev.	Correo
Presidencia	Presidente	Pdte.	jaliaga@lamolina.edu.pe
Área Académica	Vicepresidente académico	Vpdte.	jchepiu@gmail.com
Área de Investigación	Vicepresidente de investigación	Vpdte,	huayky@hotmail.com
Tecnologías de la Información	Jefe de Tecnologías de la información	Jefe de TI	hebsanz@hotmail.com
Dirección General de Administración	Director General de Administración	Admr.	eldevasa@yahoo.com
Gestión del Talento Humano	Jefe de Gestión del Talento Humano	Jefe de RRHH	angie154@hotmail.com
Secretaría General	Secretario General	SC	carlotupayachi05@hotmail.com
Imagen Institucional	Jefe de Imagen Institucional	Jefe de II	hvwiliar@hotmail.com
Área de Interculturalidad	Jefe de Interculturalidad	Jefe Intercult.	bikut4@hotmail.com

Justificación de inasistencia

Área asistente a reunión	Nombre	Correo
–		
–		

Agenda de trabajo

Tema	Beneficiario	Hora inicio	Descripción
Propuesta de Gestión de seguridad de la información	UNIFSL-Bagua	9:10 a.m	Propuesta basada en políticas de información para salvaguarda de los activos de la universidad caso de estudio.

Presidencia

Jefe del Proyecto

Documento de Aprobación del proyecto

DOCUMENTO DE APROBACIÓN DEL PROYECTO

LOGOTIPO DE LA ORGANIZACIÓN	**PROYECTO**: SGSI-2019-001
	NOMBRE DEL DOCUMENTO: Diseño de un Sistema de Gestión de Seguridad de la Información
	FECHA DE CREACIÓN: 8/07/2019
	AUTOR: Mavila Segura Huaman
	REVISIÓN: Presidencia

DESCRIPCIÓN DEL PROYECTO: El presente proyecto se desarrolla en al marco normativo ISO/IEC 27000:2013, el marco de Cobit, pmbok, Itil; y para la administración de los riesgos la metodología de Magerit, Octave, y la Norma 27005. Todo ello basado en el modelo del ciclo de Deming.
DESCRIPCIÓN DEL PRODUCTO: El alcance del proyecto del SGSI permitirá salvaguardar los activos de información y así conseguir los objetivos de la institución y al mismo tiempo la reducción de los riesgos de seguridad de la información mediante políticas de seguridad.
OBJETIVOS: 1. Alcance: El proyecto se presenta como propuesta de un SGSI para la UNIBAGUA. 2. Tiempo: El proyecto debe terminar en el plazo indicado 3. Costo: El presupuesto del proyecto es de s/.50.000
CRITERIOS DE ÉXITO: Alcance: Aprobación de todos los entregables por la institución Tiempo: El proyecto debe culminar en un lapso de 6 meses Costo: No exceder el límite del presupuesto indicado en el proyectado.
REQUISITOS DE APROBACIÓN DEL PROYECTO: - Propuesta de Gestión de Seguridad de la Información, donde se adjuntan Políticas de seguridad de la información y planes de mejora continua.

FINALIDAD DEL PROYECTO: Beneficio: Un SGSI ayuda a la institución en la administración y protección de los activos de información, así como también con la continuación del negocio basada en la adopción de un mejoramiento continuo de la universidad.
ENTREGABLES PRINCIPALES: - Políticas de seguridad de la información. - Documento de aplicabilidad tratamiento de los riesgos.
JUSTIFICACIÓN DEL PROYECTO: La ausencia de seguridad en administrar los activos de la información de la institución como también conocimiento y concientización relacionado a la seguridad de la información
PRINCIPALES INTERESADOS: Presidencia: Presidente Vicepresidencia Académica: Vicepresidente Académico Vicepresidencia de Investigación: Vicepresidente de Investigación Área de Tecnologías de la Información: Jefe de TI Área de Gestión del Talento Humano: Jefe de Gestión del Talento Humano Área de Interculturalidad: Jefe de Interculturalidad
RIESGOS INICIALES: **Amenazas:** Daños físicos, eventos naturales, fallo de servicios esenciales, acciones no autorizadas. **Vulnerabilidades:** Carencia de finalización de sesión por parte del usuario, susceptibilidad al polvo y humedad.
DURACIÓN*:* 8 meses
PRESUPUESTO: s/10,000
SPONSOR*;* Comisión Organizadora UNIFSL-Bagua
DIRECTOR DEL PROYECTO*:* Jefe del proyecto

Entrevista con los Stakeholders

FORMATO DE PREGUNTAS REALIZADAS EN LA ENTREVISTA AL JEFE DE TECNOLOGÍAS DE LA INFORMACIÓN.
1. ¿Sabe usted si la institución cuenta con un departamento de seguridad de la información con personal especializado? **Rpta:** Por el momento la universidad no cuenta con esta área, ya que recién estamos iniciando como institución al servicio de la educación universitaria. **2. ¿En la actualidad se adoptan políticas de seguridad para administrar la información?** **Si ( ) Enunciar** **No (x)** **Rpta:** Con relación a la seguridad de la información todavía, pero si realizan protocolos de seguridad para laboratorio de cómputo, laboratorio de ciencias, talleres y biblioteca. **3. ¿Conoce usted sobre las políticas concernientes a la seguridad de la información de su trabajo?** ( ) Sí, las conozco completamente ( ) No, pero sé que existen. (x) No existen ( ) No sé Si su respuesta es sí, indique si estas políticas son lo suficientemente robustas para solventar las dificultades de la seguridad de la información en la universidad: ……..…… **4. ¿Las funciones y responsabilidades se encuentran adecuadamente establecidos y designados al personal debidamente capacitados?** **Rpta:** La universidad ahora cuenta con capacitaciones al personal de acorde a las

áreas que así lo requiera, en cuanto a los roles y responsabilidades falta reforzar para una mayor asistencia del personal.

5. ¿Existe el conocimiento y respaldo apropiados sobre la arquitectura de riesgo y seguridad de la información

Rpta:

La universidad está trabajando con muchos proyectos entre ellos está la gestión del riesgo y en la protección de activos ya que estamos en una zona lluviosa y muchas veces se ha visto afectadas algunas áreas por el ingreso de agua producto de las fuertes lluvias.

6. ¿Existe un control acerca del acceso sin autorización de personal, con el objeto de protección del equipo y sistemas que se gestionan en la universidad?

Rpta:

Se necesita reforzar ese tema puesto que todavía existen acciones que se deben corregir por el bien de la institución.

7. ¿Se efectúa de manera periódica el mantenimiento de los equipos computacionales de la universidad?

Rpta:

Sí, periódicamente hacemos un mantenimiento de los equipos informáticos previa programación y sobretodo fines de semana.

8. ¿Se ha realizado simulacros relacionado con los fallos de sistema de información y comunicaciones?

Rpta:

Si se ha logrado realizar con el apoyo de dirección y el personal de trabajo encargado del área administrativa.

9. ¿Se efectúan funciones para monitorear los sistemas de información manejados en la universidad?

Rpta:

Si, la universidad cuenta con un sistema de monitoreo el cual nos da un alcance en cuanto a la seguridad de la información.

10. Seleccione una opción de acuerdo a la siguiente pregunta. ¿Con que frecuencia ha sido víctima la institución de amenazas que perjudiquen y violenten la seguridad de la información?

Cada día ( )
Cada semana ( )
Cada mes (x)
Cada 2 meses ( )
Cada 4 meses ( )
Anual
Nunca

Matriz de Stakeholders

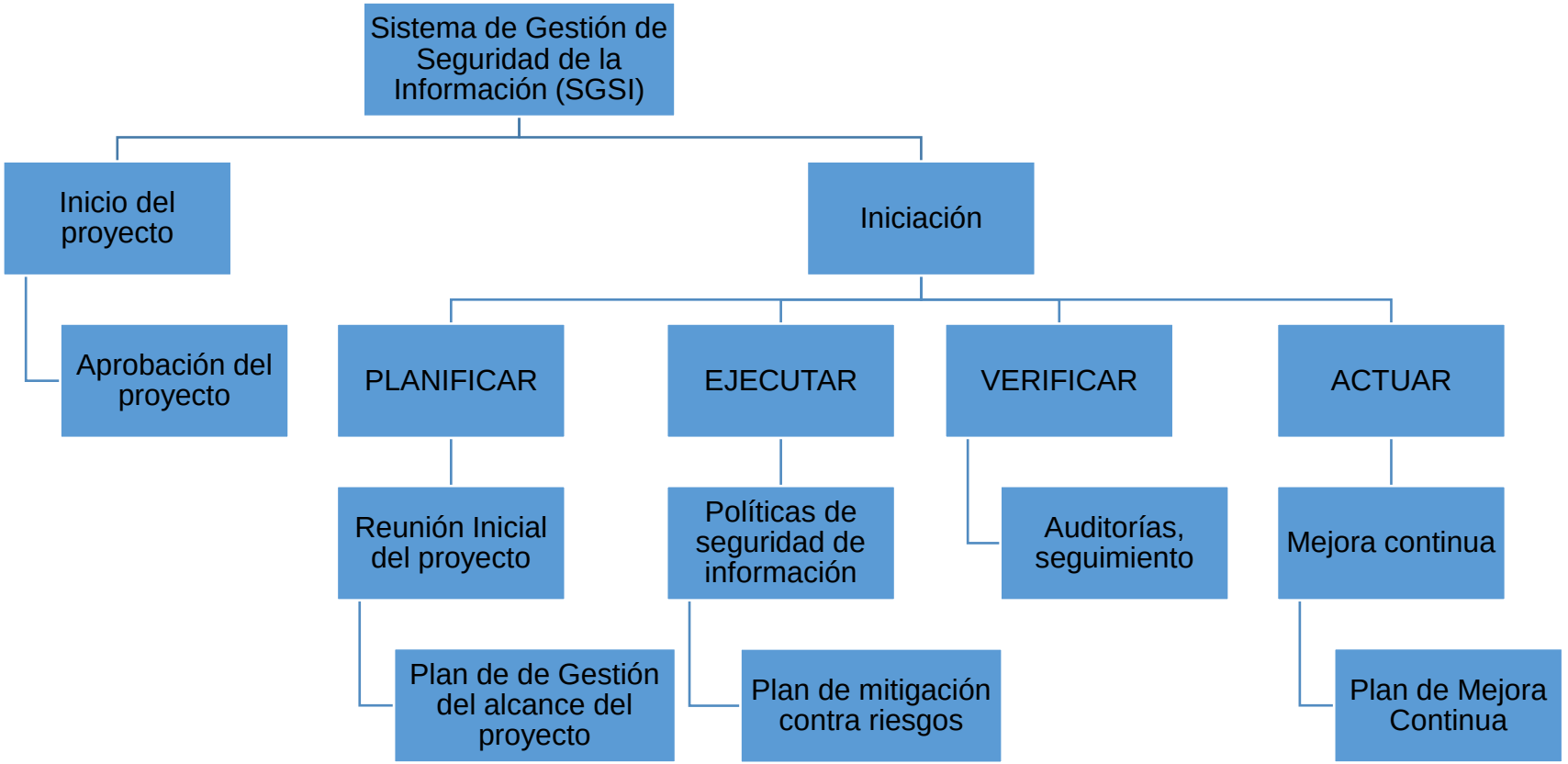
Matriz de Stakeholder					
Proyecto:	Propuesta de un Sistema de Gestión de Seguridad de la Información				
Código:	001-2019				
Fecha de Inicio:	8/07/2019				
Stakeholder:	UNIBAGUA				
Tipo:	Interno				
Objetivo o Resultados	**Nivel de Interés**	**Nivel de Influencia**	**Acciones Posibles**		**Estrategias**
			De impacto positivo	**De impacto negativo**	
Proponer un Sistema de Gestión de Seguridad de la Información.	Alto	Alto	Salvaguardar los activos de información de la universidad	Desconocimiento de la importancia de seguridad de la información una institución.	Mantener información constante con la alta Dirección. Charlas de cultura y concientización, exponiendo los beneficios que conlleva un SGSI dentro de una institución.
Conclusiones:	Es importante llevar a cabo la concientización de los involucrados mediante una cultura y buenas prácticas el cual permita una mejora continua dentro de universidad.				

Plan del Alcance del proyecto

DOCUMENTO DEL ALCANCE DEL PROYECTO					
	Estado	Versión **0.0**			
TITULO PROPUESTO DEL PROYECTO: SGSI01		**CLASIFICACION DE CONFIDENCIALIDAD**			
PATROCINANTE DEL PROYECTO:		Uso General		Uso interno Solamente	**X** Documento Confidencial
NUMERO DEL PROYECTO: 01					
ESPECIFICACIONES/PROPOSITO DEL PROYECTO: Proponer un Sistema de Gestión de Seguridad de la Información para salvaguardar los activos de la información de la Universidad Nacional Intercultural “Fabiola Salazar Leguía” Bagua.					
RESTRICCIONES DEL PROYECTO: El costo del proyecto se va a reflejar al término del proyecto, ya que la estimación del costo aumenta a lo largo del proyecto, conforme avanza de fase en fase.					
FACTORES CRITICOS DE EXITO: - Políticas de seguridad para administrar los activos de información de la universidad. - Apoyo y compromiso del personal involucrado en el proyecto. - Cultura organizacional y buenas prácticas dentro y fuera de la universidad.					
SUPOSICIONES: Asumimos que los futuros usuarios del SGSI mantendrán el compromiso de buenas prácticas dentro de la universidad tomando en cuenta las medidas de seguridad establecidas que corresponde a la gestión de seguridad de la información.					
DEPENDENCIAS: Cumplimientos legales y contractuales del Proyecto.					
PREPARADO POR:	Mavila Segura Huaman	FECHA	REVISIÓN	INICIALES	
		15/07/2019	05/08/2019	SGSI001	

EDT del Proyecto

PROYECTO	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO DE PROYECTO	SGSI01
ELABORADO POR	Mavila Segura Huaman	FECHA DE ELABORACIÓN	08/08/2019



Identificación de activos

TIPO DE ACTIVO	
ESENCIAL	**[ESSENTIAL]**
DATOS/INFORMACIÓN	**[D]**
SERVICIOS	**[S]**
APLICACIONES INFORMÁTICAS (SOFTWARE)	**[SW]**
EQUIPO INFORMÁTICO (HARDWARE)	**[HW]**
REDES DE COMUNICACIONES	**[COM]**
SOPORTES DE INFORMACIÓN	**[SI]**
EQUIPAMIENTO AUXILIAR	**[AUX]**
INSTALACIONES	**[I]**
PERSONAL	**[P]**

Inventario de activos

INVENTARIO DE ACTIVOS	CÓDIGO
[ESSENTIAL] ESENCIAL	
Resoluciones Comisión Organizadora	E01
Resoluciones Presidenciales	E02
Reglamentos	E03
Directivas	E04
Planes y Políticas	E05
Convenios	E06

Protocolos	E07
[D] DATOS/INFORMACIÓN	
Documentos de Trámite Documentario	D01
Información del área de Gestión del Talento Humano	D02
Información de DGA	D03
Módulo Contable	D04
Información de Logística	D05
Información de Interculturalidad	D06
Información de Secretaría General	D07
Inventario de Hardware	D08
Bandeja de Correos Electrónicos	D09
[K] CLAVES CRIPTOGRÁFICAS	
Contraseñas SIGA	C01
Contraseña SIAF	C02
Contraseña página Web	C03
Contraseñas de correos electrónicos Institucional	C04
Contraseñas de sistemas de aplicaciones informáticas	C05
[S] SERVICIOS	
Servicios Académicos	S01
Servicios Institucionales	S02
Servicios de Internet	S03
[SW] APLICACIONES INFORMÁTICAS (SOFTWARE)	
SISTEMA AKADEMICO	AS01

SISTEMA DE PLANILLA	AS02
SISTEMA DE ADMISIÓN	AS03
SISTEMA DE BIBLIOTECA	AS04
SIAF	AS05
SIGA	AS06
[HW] EQUIPAMIENTO INFORMÁTICO (HARDWARE)	
Servidor Data Center	EH01
Servidores de base de datos	EH02
Servidores HP Prolian 360	EH03
Servidores HP Prolian 390	EH04
Servidor DELL	EH05
PCs de ecritorio	EH06
PCs Portátiles	EH07
Dispositivos móviles	EH08
[COM] REDES DE COMUNICACIONES	
Cableado de red	RC01
Router	RC02
Switch	RC03
Hub	RC04
[SI] SOPORTES DE INFORMACIÓN	
Discos duros externos	SI01
DVD´s	SI02
[AUX] EQUIPAMIENTO AUXILIAR	

Impresoras	EA01
Proyectores	EA02
Cámaras de seguridad	EA03
Reloj Biométrico	EA04
[I] INSTALACIONES	
Local Administrativo UNIBAGUA	I01
Local Académico UNIBAGUA	I02
[P] PERSONAL	
Presidente	P01
Vicepresidente Académico	P02
Vicepresidente de Investigación	P03
Coordinador Académico	P04
Jefe Planeamiento y Presupuesto	P05
Jefe de Infraestructura	P06
Secretaria ODTH	P07
Secretaria de Logística	P08
Director General de Administración	P09
Agente de Seguridad	P10
Jefe de Imagen Institucional	P11
Ingeniero II de la U.F.	P12
Jefe de Logística	P13
Secretaria de Secretaría General	P14
Especialista SIAF	P15

Asistente Vicepresidencia Académica	P16
Agente de Seguridad	P17
Ingeniero II de la U.F.	P18
Coordinador de Investigación	P19
Asistente de Presidencia	P20
Asistente de Vicepresidencia de Investigación	P21
Planificador II	P22
Jefe de Contabilidad	P23
Secretario General	P24
Técnico Administrativo Planeamiento y Presupuesto	P25
Asistente de DGA	P26
Jefe de la Unidad Formuladora	P27
Jefe Oficina Interculturalidad	P28
Técnico Trámite Documentario	P29
Jefe Tecnologías de la Información	P30
Asistente de Imagen Institucional	P31
Personal de Mantenimiento	P32
Jefe Oficina Central de Certificación, Calidad y Acreditación	P33
Personal de Limpieza	P34
Personal SIGA	P35
Auxiliar de Logística	P36

Valoración de Activos

Valoración de activos teniendo en cuenta las dimensiones de seguridad

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

UNIFSL-BAGUA
Fecha elaboración:
Fecha aprobación:

Inventario de activos								Valoración de activos			Valoración Final	Gestión	
N°	Nombre del activo	Descripción del activo	Tipo de activo	Ubicación	Unidad responsable	Responsable	Custodio	Disponibilidad	Integridad	Confidencialidad		Fecha de ingreso:	Fecha de salida:
1	Resoluciones Comisión	Información Pública	Esenciales	Área Adm.	Secretaría General	Secretaría General	Secretario general	2	3	1	6	08/07/2019	12/07/2019

	Organizadora												
2	Resoluciones Presidenciales	Información Pública	Esenciales	Área Adm.	Secretaría General	Secretaría General	Secretario general	3	3	1	7	08/07/2019	12/07/2019
3	Reglamentos	Información Pública	Esenciales	Área Adm.	Secretaría General	Secretaría General	Secretario general	2	3	1	6	08/07/2019	12/07/2019
4	Directivas	Información Pública	Esenciales	Área Adm.	Secretaría General	Secretaría General	Secretario general	3	3	1	7	08/07/2019	12/07/2019
5	Planes y Políticas	Información Pública	Esenciales	Área Adm.	Secretaría General	Secretaría General	Secretario general	2	3	1	6	08/07/2019	12/07/2019
6	Convenios	Información Pública	Esenciales	Área Adm.	Secretaría General	Secretaría General	Secretario general	2	3	1	6	08/07/2019	12/07/2019
7	Protocolos	Información Pública	Esenciales	Área Adm.	Secretaría General	Secretaría General	Secretario general	2	3	1	6	08/07/2019	12/07/2019
8	Documentos de Trámite Documentario	Información Pública	Datos/Información	Área Adm.	Trámite documentario	Asistente de trámite Doc.	Técnico de tramite doc.	3	2	3	8	08/07/2019	12/07/2019
9	Información de Recursos Humanos	Información Privada	Datos/Información	Área Adm.	Área de RR HH	Jefe de RRHH	Jefe de RRHH	3	2	3	8	08/07/2019	12/07/2019

10	Información de DGA	Información Privada	Datos/Información	Área Adm.	Administración	Administrador	Administrador	2	3	3	8	08/07/2019	12/07/2019
11	Módulo Contable	Información Privada	Datos/Información	Área Adm.	Area de contabilidad	Area de contabilidad	Jefe de contabilidad	3	3	2	8	08/07/2019	12/07/2019
12	Información de Logística	Información Privada	Datos/Información	Área Adm.	Logística	Área de logística	Jefe de logística	3	3	2	8	08/07/2019	12/07/2019
13	Información de Interculturalidad	Información Privada	Datos/Información	Área Adm.	Interculturalidad	Área de interculturalidad	Jefe de interculturalidad	2	3	1	6	08/07/2019	12/07/2019
14	Información de Secretaría General	Información Privada	Datos/Información	Área Adm.	Secretaría General	Secretaría General	Secretario general	3	3	1	7	08/07/2019	12/07/2019
15	Inventario de Hardware	Información Privada	Datos/Información	TI	TI	Jefe de TI	Jefe de TI	2	1	3	6	08/07/2019	12/07/2019
16	Bandeja de Correos Electrónicos	Información Privada	Datos/Información	TI	TI	Jefe de TI	Jefe de TI	2	3	3	8	08/07/2019	12/07/2019
17	Contraseñas SIGA	Información confidencial	Claves criptográficas	TI	TI	Jefe de TI	Jefe de TI	3	3	3	9	08/07/2019	12/07/2019
18	Contraseña SIAF	Información confidencial	Claves criptográficas	TI	TI	Jefe de TI	Jefe de TI	3	3	3	9	08/07/2019	12/07/2019

19	Contraseña página Web	Información confidencial	Claves criptográficas	TI	TI	Jefe de TI	Jefe de TI	3	3	3	9	08/07/2019	12/07/2019
20	Contraseñas de correos electrónicos Institucional	Información confidencial	Claves criptográficas	TI	TI	Jefe de TI	Jefe de TI	3	3	3	9	08/07/2019	12/07/2019
21	Contraseñas de aplicaciones informáticas	Información confidencial	Claves criptográficas	TI	TI	Jefe de TI	Jefe de TI	3	3	3	9	08/07/2019	12/07/2019
22	Servicios Académicos	Información Privada	Servicios	Área Adm.	Área Acad.	Vpdte	Vpdte Acad.	3	3	1	7	08/07/2019	12/07/2019
23	Servicios Institucionales	Información Privada	Servicios	Área Adm.	Área Acad.	Vpdte Acad.	Vpdte Acad.	3	3	1	7	08/07/2019	12/07/2019
24	Servicios de Internet	Información Privada	Servicios	Área Adm./ Área Acad.	TI	TI	Jefe de TI	2	2	2	6	08/07/2019	12/07/2019
25	Sistema Akademico	Aplicaciones informátic	Software	Área Adm.	TI	TI	Jefe de TI	3	3	3	9	08/07/2019	12/07/2019

		as											
26	Sistema de planillas	Aplicaciones informáticas	Software	Área Adm.	TI	TI	Jefe de TI	3	3	3	9	08/07/2019	12/07/2019
27	Sistema de Admisión	Aplicaciones informáticas	Software	Área Adm.	TI	TI	Jefe de TI	3	3	3	9	08/07/2019	12/07/2019
28	Sistema de Biblioteca	Aplicaciones informáticas	Software	Área Adm.	TI	TI	Jefe de TI	3	3	3	9	08/07/2019	12/07/2019
29	Software para control de asistencias	Aplicaciones informáticas	Software	Área Adm./ Área Acad.	TI	TI	Jefe de TI	3	3	3	9	08/07/2019	12/07/2019
30	Software de videovigilancia	Aplicaciones informáticas	Software	Área Adm./ Área Acad.	TI	TI	Jefe de TI	3	3	3	9	08/07/2019	12/07/2019
31	SIAF	Aplicaciones informáticas	Software	Área Adm./ Área Acad.	TI	TI	Jefe de TI	3	3	3	9	08/07/2019	12/07/2019
32	SIGA	Aplicaciones informáticas	Software	Área Adm./ Área Acad.	TI	TI	Jefe de TI	3	3	3	9	08/07/2019	12/07/2019

33	Servidor Data Center	Equipamiento informático	Hardware	Área Acad.	TI	TI	Jefe de TI	3	3	3	9	08/07/2019	12/07/2019
34	Servidores de base de datos	Equipamiento informático	Hardware	Área Acad.	TI	TI	Jefe de TI	3	3	3	9	08/07/2019	12/07/2019
35	Servidores HP Prolian 360	Equipamiento informático	Hardware	Área Acad.	TI	TI	Jefe de TI	3	3	3	9	08/07/2019	12/07/2019
36	Servidores HP Prolian 390	Equipamiento informático	Hardware	Área Acad.	TI	TI	Jefe de TI	3	3	3	9	08/07/2019	12/07/2019
37	Servidor DELL	Equipamiento informático	Hardware	Área Acad.	TI	TI	Jefe de TI	3	3	3	9	08/07/2019	12/07/2019
38	PCs de escritorio	Equipamiento informático	Hardware	TI	TI	TI	Jefe de TI	1	1	2	4	08/07/2019	12/07/2019
39	PCs Portátiles	Equipamiento informático	Hardware	TI	TI	TI	Jefe de TI	1	3	3	7	08/07/2019	12/07/2019
40	Proyectores	Equipamiento informátic	Hardware	TI	TI	TI	Jefe de TI	1	1	2	4	08/07/2019	12/07/2019

		o											
41	Cableado de red	Redes y comunicaciones	Hardware	TI	TI	TI	Jefe de TI	2	3	2	7	08/07/2019	12/07/2019
42	Router	Redes y comunicaciones	Hardware	TI	TI	TI	Jefe de TI	2	3	2	7	08/07/2019	12/07/2019
43	Switch	Redes y comunicaciones	Hardware	TI	TI	TI	Jefe de TI	2	3	2	7	08/07/2019	12/07/2019
44	Hub	Redes y comunicaciones	Hardware	TI	TI	TI	Jefe de TI	2	3	2	7	08/07/2019	12/07/2019
45	Discos duros externos	Soporte de información	Hardware	TI	TI	TI	Jefe de TI	1	3	3	7	08/07/2019	12/07/2019
46	Dvd´s	Soporte de información	Hardware	TI	TI	TI	Jefe de TI	1	1	2	4	08/07/2019	12/07/2019
47	Impresoras	Equipamiento auxiliar	Hardware	TI	TI	TI	Jefe de TI	2	1	2	5	08/07/2019	12/07/2019
48	Cámaras de seguridad	Equipamiento auxiliar	Hardware	TI	TI	TI	Jefe de TI	3	3	3	9	08/07/2019	12/07/2019
49	Reloj Biométrico	Equipamiento auxiliar	Hardware	TI	TI	TI	Jefe de TI	2	3	3	8	08/07/2019	12/07/2019

50	Local Adm. UNIBAGUA	Infraestructura	Instalaciones	Área Adm.	Área Admin.	Área Admin.	Área Admin.	3	3	2	8	08/07/2019	12/07/2019
51	Local Acad. UNIBAGUA	Infraestructura	Instalaciones	Área Acad.	Área Acad.	Área Acad	Área Acad	2	2	1	5	08/07/2019	12/07/2019
52	Presidente	Personas	Personal	Área Adm.	Presidencia	RRHH	Jefe de RRHH	3	3	1	7	08/07/2019	12/07/2019
53	Vicepresidente Académico	Personas	Personal	Área Acad.	Vicepresidencia acad	RRHH	Jefe de RRHH	3	3	1	7	08/07/2019	12/07/2019
54	Vpdte de Investigación	Personas	Personal	Área Adm.	Vicepresidencia de investigación	RRHH	Jefe de RRHH	3	3	1	7	08/07/2019	12/07/2019
55	Personal	Personas	Personal	Área Adm./ Acad.	RRHH	RRHH	Jefe de RRHH	2	2	1	5	08/07/2019	12/07/2019

Elaborado por: Mavila Segura Huaman

Firma:

_____

Cargo:

_____

Aprobado por:

Firma:

_____

Cargo:

_____

Identificación de Amenazas

Origen de las amenazas		
Deliberado	**D**	Acciones Voluntarias
Accidental	**A**	Acciones humanas
Ambiental	**E**	Acciones no humanas

Tipo	Amenaza	Origen
Daño Físico	Daño causado por fuego	A,D,E
	Daño causado por Agua	A,D,E
	Daño causado por agente contaminante	A,D,E
	Daño causado por accidentes	A,D,E
	Destrucción de Equipos	A,D,E
	Deterioro, polvo, Corrosidad	A,D,E
Eventos Naturales	Fenómenos Naturales	E
	Sismos	E
	Inundaciones	E
	Falla en el aire acondicionado	E
Fallo de Servicios esenciales	Falla energética	A,D
	Fallas en el equipamiento de telecomunicaciones	A,D,E
	Radiación electromagnética	A,D
Radiación	Radiación térmica	A,D,E
	Pulsaciones electromagnéticas	A,D,E
	Intersección de señales	A,D,E
Compromiso de la información	Interceptación, infiltración	D
	Monitorización ilícita	D
	Documentación robada	D
	Equipo robado	D
	Información divulgada	D
	Datos de fuentes no confiables	A,D
	Alteración de Hardware	A,D
	Alteración de Software	D
	Fallo de los equipos	A,D
Fallas técnicas	Malfuncionamiento de los equipos	A
	Congestión de los sistemas de información	A
	Mala funcionalidad del software	A,D
	Carencia de mantenimiento del software	A
	Uso desautorizado de equipos	A,D
Acciones no autorizadas	Duplicado y fraude de software	D
	Pirateo de software	D
	Data dañada y/o viciada	A,D
	Procedimiento irregular de data	D
	Fallo en el manejo	D

Compromiso de funciones	Abuso de admisión	A
	Falsificación de derecho	A,D
	Accesos denegados	D
	Indisponibilidad del personal	D

Identificación de Vulnerabilidades

LISTA DE VULNERABILIDADES

TIPO	Cod	VULNERABILIDAD
HARDWARE	H1	Deficiente mantenimiento/ Fallas de instalación de equipos de almacenaje.
	H2	Carencia de sustitución periódica
	H3	Exposición a la humedad y polvo
	H4	Susceptibilidad en los cambios de voltaje / Susceptibilidad a los cambios de temperaturas
	H5	Almacenaje sin protección
	H6	Ausencia de la custodia para disponer del hardware
	H7	Deficiencias del software
	H8	Carencia de culminación de sesión nivel usuaria
	H9	Utilización correcta de los medios de almacenaje sin una limpieza y formateo adecuados
SOFTWARE	S1	Carencia de prueba de auditorías
	S2	Fallo en el repartimiento de accesibilidad
	S3	Uso de aplicaciones a datos erróneos en época de culminación
	S4	Complejidad de interfaz de usuario
	S5	Ausencia de documentos
	S6	Data incorrecta
	S7	Carencia de herramientas de autenticación
	S8	Tablas de contraseña desprotegidas
	S9	Gestión deficiente de contraseñas
	S10	Servicios habilitados no necesarios

	S11	Software reciente o nuevo
	S12	Uso y descargas incontroladas de Software
	S13	Respaldos carentes
	S14	Fallo en los documentos administrativos
	S15	Ausencia de pruebas de emisión o recepción de mensajería
	S16	Línea de comunicación desprotegidas
	S17	Sensibilidad desprotegida del tráfico
	S18	Cableado deficiente
	S19	Falta de autentificación del emisor y receptor
	S20	Inseguridad de la arquitectura de red
	S21	Remisión de contraseñas sin autorización
RED	R1	Gestión no adecuada de red
	R2	Desautorización de la conexión pública de red.
	R3	Incumplimiento del personal
	R4	Contrataciones no adecuadas de procedimiento
	R5	Seguridad mostrada deficiente
	R6	Inadecuado uso de Software y Hardware
	R7	Deficiente seguridad cultural
	R8	Carencia de mecanismos de monitorización
	R9	Actividades no controladas del personal externo
PERSONAL	P1	Ausencia de políticas de uso de las líneas de comunicación
	P2	Acceso físico a las instalaciones no inadecuadas
	P3	Áreas con susceptibilidad a desastres
	P4	Redes con inestabilidad energética
	P5	Carencia de seguridad física de las estructuras de las edificaciones
	P6	Ausencia de procesos formales para registrar y eliminar usuarios.
	P7	Ausencia de procesos formales de la evaluación del acceso nivel usuario

	P8	Disposición insuficiente en la contratación usuaria
LUGAR	L1	Ausencia de monitorización sobre los recursos de procesos de información.
	L2	Ausencia periódica de auditorías
	L3	Ausencia de procesos para identificar y evaluar riesgos.
	L4	Ausencia del informe de error y fallos en los logs de administración y operadores.
ORGANIZACIÓN	O1	Intervención no adecuada de mantenimiento
	O2	Ausencia de acuerdos de servicios
	O3	Ausencia de procesos de controles de cambio
	O4	Ausencia de procesos estructurales para la verificación de los documentos del SGSI.
	O5	Ausencia de procesos estructurales para información pública autorizada
	O6	Ausencia de roles y responsabilidades en SGSI
	O7	Ausencia del plan continuo de negocio
	O8	Ausencia de políticas acerca del empleo de E-mail
	O9	Ausencia de procesos estructurales para el empleo de Software nuevo
	O10	Ausencia de logs en el gestor y administradores
	O11	Ausencia de procesos para manejar información calificada
	O12	Ausencia de documentación sobre responsabilidades sobre la seguridad y la descripción de los cargos
	O13	Ausencia de procesos acerca de disciplinas en el caso de incidencia de seguridad
	O14	Ausencia de políticas acerca del empleo de equipos portátiles (Laptops)
	O15	Ausencia de control de activos fuera de la institución
	O16	Ausencia de políticas de escritorio y pantalla limpios
	O17	Procedimientos de la información sin autorización

	O18	Mecanismos de monitorización ausentes
	O19	Evaluación de parte de la gerencia ausentes
	O20	Procesos para el informe de vulnerabilidad en la seguridad ausentes

Identificación de Riesgos

LISTA DE RIESGOS

Lista de Riesgos potenciales	
Hardware	Información extraviada, daño en los equipos, tiempo perdido en procedimientos recurrentes.
Software	Mala funcionalidad del sistema, destrucción del Sistema Operativo, aplicativos e información destruidos o modificados.
	Información extraviada o modificada, hurto de claves de usuario, datos modificados, inseguridad de bases de datos por autorización y confidencialidad no establecidos
	Equipos de usuarios modificados sin autorización, información borrada y/o robada, ataques de DoS, obtención de privilegios.
Seguridad Física	Información extraviada, destruida, modificada o borrada, o equipos desarticulados.
Seguridad Lógica	Destrucción, alteración o sustracción de datos, suplantación de identidades de usuarios, claves de usuarios robadas
Redes de Comunicaciones	Alteración de la funcionalidad del código, programas y sitios, desautorización de la información.
Personal	Sustracción de información personal, pérdida de archivos, destrucción del S.O.

TIPO DE RIESGOS	CÓDIGO	DESCRIPCIÓN
Hardware	R1	Pérdida de información.
	R2	Daños y falla de los equipos
	R3	Tiempo perdido en redundancia de los procesos
Software	R4	Mala funcionalidad del sistema, destrucción del Sistema Operativo,
	R5	Aplicativos e información destruida o modificada
	R6	Información extraviada o modificada
	R7	Claves de usuario robadas
	R8	Inseguridad en las bases de datos por permisos y privilegios indefinidos
	R9	Intromisión en los equipos de usuarios para modificar sin autorización, información borrada y/o extraviada
	R10	Ataques de DOS, obtención de privilegios
Seguridad Física	R11	Destrucción, modificación, robo o borrado de información.
	R12	Desarticulación física o destrucción de equipos
Seguridad Lógica	R13	Robo de la data
	R14	Datos alterados o destruidos
	R15	Suplantaciones de identidad de los usuarios
	R16	Sustracción de claves de usuario
Redes de Comunicaciones	R17	Cambios en la funcionalidad del código, programas y sitios web
	R18	Información no autorizada
Personal	R19	Archivos borrados o eliminados
	R20	Alteración y/o destrucción del S.O
	R21	Sustracción de información personal

Análisis preliminar de riesgos

NOMBRE DEL PROYECTO:	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
CÓDIGO DEL PROYECTO:	SGSI01
DIRECTOR DEL PROYECTO:	
FECHA DE ELABORACIÓN:	

HISTORIAL DE VERSIONES			
FECHA Y HORA	**N° DE VERSIÓN**	**DESCRIPCIÓN**	**ELABORADO POR**
08/07/2019	01	Sistema de gestión de seguridad de la información.	Mavila Segura Huaman

PROPÓSITO DEL PLAN DE GESTIÓN DE RIESGOS DEL PROYECTO

Propósito: Identificar los posibles riesgos, desarrollar estrategias para abordarlos, mejorarán las probabilidades de éxito del proyecto.

ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDADES
Equipo del proyecto	Definir y actualizar políticas y plan de seguridad de información
Jefe de TI	Ejecución de protocolos y controles de seguridad establecidos en plan
Todo el personal de la universidad	Socialización y divulgación de medidas de seguridad y responsabilidades
Jefe de TI	Evaluación de controles de seguridad y proceso de gestión de la seguridad de información
Jefe de TI	Verificación de la gestión de la seguridad
Todo el personal de la universidad	Actualización y mejora continua de políticas y plan de seguridad de información

SEGUIMIENTO Y AUDITORÍA

Seguimiento acerca del acceso y utilización de los sistemas para la detección de actividades sin autorización.

Seguimiento acerca de la seguridad de los recursos humanos de la universidad.

CONTROL DE LOS RIESGOS

Control de los riesgos mediante políticas de seguridad de la información.

APROBACIÓN

Nombre	Cargo	Firma	Fecha
	Iniciador/Patrocinador del Proyecto		20/08/2019
	Director del Proyecto		

Análisis de riesgos

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO

PROBABILIDAD	VALOR NUMÉRICO	IMPACTO	VALOR NUMÉRICO
Muy Improbable	1	Muy Bajo	1
Relativamente Probable	2	Bajo	2
Probable	3	Moderado	3
Muy Probable	4	Alto	4
Casi Certeza	5	Muy Alto	5

TIPO DE RIESGO	PROBABILIDAD X IMPACTO
Muy Alto	Mayor a 19
Alto	15 a 19
Moderado	10 a 15
Bajo	5 a 10
Muy Bajo	0 a 5

CÓDIGO DEL RIESGO	DESCRIPCIÓN DEL RIESGO	CAUSA RAIZ	TRIGGER	ESTIMACIÓN DE PROBABILIDAD	ESTIMACIÓN DE IMPACTO	PROB. X IMPACTO	TIPO DE RIESGO
R1	Pérdida de información	Descuido por parte del encargado de esa área.	Información extraviada o dañada.	**4**	**4**	**16**	**ALTO**
R2	Daños y falla en los equipos	Falta de aire acondicionado adecuados.	Sobrecalentamiento de los equipos	**4**	**4**	**16**	**ALTO**
R3	Pérdida de tiempo en procesos repetidos	Término de contrato, despido o renuncia de personal	Falta de planificación de actividades	**5**	**2**	**10**	**MODERADO**

R4	Mala funcionalidad del sistema, destrucción de SO,	Malas instalaciones de sistemas informáticos	Falta de capacitación en instalaciones de SW	**4**	**4**	**16**	**ALTO**
R5	Destrucción o modificación de aplicativos e información.	Acciones malintencionadas de personas ajenas a la universidad.	Bloqueos de sistemas de aplicaciones	**2**	**5**	**10**	**MODERADO**
R6	Pérdida o modificación de información.	Visitas a las instalaciones	Conversaciones o consultas informales	**4**	**4**	**16**	**ALTO**
R7	Robo de claves de usuario	Abuso de privilegios de acceso	Información personal vulnerable	**3**	**4**	**12**	**MODERADO**
R8	Inseguridad en las bases de datos por permisos y privilegios indefinidos	Abuso de privilegios de acceso	Falta responsabilidad del Personal Encargado de cada equipo.	**4**	**5**	**20**	**MUY ALTO**
R9	Intromisión en los equipos de usuarios para modificar sin autorización, información borrada y/o	Uso de dispositivos extraíbles (pen drives)	Ausencia de monitoreo del estado de antivirus	**3**	**5**	**15**	**MODERADO**

	extraviada						
R10	Ataques de DoS, obtención de privilegios	Abuso de privilegios en los accesos	Falla de equipos tecnológicos	**3**	**5**	**15**	**MODERADO**
R11	Robo, destrucción, modificación o borrado de información	Accesos no autorizados de personal externo	Información adulterada	**4**	**5**	**20**	**MUY ALTO**
R12	Destrucción o desarticulación física de equipos.	Acciones malintencionadas de personas ajenas a la universidad.	Equipos desfasados	**3**	**5**	**15**	**ALTO**
R13	Robo de datos.	Abuso de privilegios de acceso	Conversaciones o consultas informales	**2**	**3**	**6**	**BAJO**
R14	Alteración o destrucción de datos	Accesos no permitidos a los ambientes de trabajo	Falla técnica	**2**	**5**	**10**	**MODERADO**
R15	Suplantación de identidad de usuarios	Ausencia de mecanismos de seguridad	Mala reputación del personal interno	**1**	**5**	**5**	**MUY BAJO**
R16	Robo de claves de usuarios	Accesos no permitidos de personal interno	Información personal vulnerable	**2**	**4**	**8**	**BAJO**
R17	Cambios en la	Accesos no	Bloqueos de	**2**	**5**	**10**	**MODERADO**

	funcionalidad del código, programas y sitios web	permitidos de personal interno	sistemas de aplicaciones				
R18	Información sin autorización.	Abuso de privilegios de acceso	Mala reputación del personal	**3**	**3**	**9**	**BAJO**
R19	Borrado o eliminación de archivos.	Acceso de personas malintensionadas a la universidad	Bloqueos de sistemas de aplicaciones	**2**	**5**	**10**	**BAJO**
R20	Destrucción del S.O	Acceso de personas ajenas a la universidad	Ausencia de instructivos de soporte	**3**	**5**	**15**	**ALTO**
R21	Robo de información personal	Abuso de privilegios de acceso	Posesión ilícita de información personal	**3**	**5**	**15**	**ALTO**

Políticas de seguridad de la información

LOGO	POLÍTICA	
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
	No: 01	**Páginas: 1**6

1. INTRODUCCIÓN

Las Políticas de Seguridad constituyen los objetivos para realizar salvaguardas apropiadas de los activos de información para garantizar la continuidad de la universidad, es por ello la necesidad de la seguridad de la información ya que cada vez las instituciones se ven afectadas con riesgos y amenazas.

2. OBJETIVOS

Proponer un sistema de gestión de seguridad de la información de la Universidad Nacional Intercultural “Fabiola Salazar Leguía” Bagua.

3. ALCANCE

La aplicabilidad de estas políticas rige para la Universidad Nacional Intercultural “Fabiola Salazar Leguía” de Bagua en su totalidad.

La seguridad de la información es aplicable y está orientada a preservar todos los activos de información de la universidad.

4. CUMPLIMIENTO Y CONFORMIDAD

Es de forma responsable y obligatoria para todos los involucrados en el cumplimiento de las Políticas de Seguridad de la información.

Si algún individuo viola las siguientes disposiciones, se tomarán las medidas del caso y las acciones correspondientes.

5. MARCO LEGAL

Ley N" 27927: Ley de Transparencia y Acceso a la Información Pública

Ley N° 29733: Ley de protección de los datos

6. MARCO REFERENCIAL

Los objetivos de control establecen las políticas de seguridad de la

información para la Universidad Nacional Intercultural “Fabiola Salazar Leguía” Bagua.

7. OBJETIVOS DE CONTROL Y CONTROLES

a. Protección de los activos de información

Se debe definir el acceso a los sistemas de información para resguardar los activos de información única y exclusivamente al personal autorizado.

b. Autenticación

Verificar accesos, tipo de autorizaciones conforme a los niveles de autorización.

c. Autorización

La autorización se define en las políticas de seguridad de la información, el cual para obtener acceso a los recursos de información se debe tener los permisos o autorización necesaria.

d. Integridad de la información

Todo proceso que se realice, la información debe mantenerse íntegra, como la integridad del sistema, datos, confidencialidad.

e. Auditoría de actividades de seguridad

Supervisar los eventos relevantes para la seguridad de la información de forma que podamos prevenir los incidentes no deseados.

8. POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

La Universidad Nacional Intercultural “Fabiola Salazar Leguía” Bagua deberá definir y tomar las medidas de control necesarios para proteger la información contra los 3 principios esenciales: confidencialidad, integridad y disponibilidad.

POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

A.1. Política de control de acceso

Se implanta como control de seguridad de la información, el control de acceso para que de tal manera el personal obtenga un apropiado acceso a

los sistemas de información y recursos de tecnología, aprobando antes que su acceso sea autenticado, autorizado y auditado.

Objetivo

Especificar los controles respectivos para el acceso a la información.

Aplicabilidad:

Dirigido a todo el personal de la universidad.

Directrices

1. Se especificará en el área de Tecnologías de la Información de la UNIFSL-Bagua el programa para la dirección y aplicación de los aplicativos tecnológicos de los usuarios, haciendo uso de los métodos de menor riesgo e impacto para la universidad.
2. Está absolutamente prohibido el ingreso a los suministros computacionales y de comunicaciones empleando las cuentas de otros (funcionarios, servidores, CAS, locadores de servicios y otros) de la UNIFSL-Bagua o de alguna otra persona (jurídica, natural, de consultoría, por contrato o terceros).
3. Los niveles de acceso pueden ser determinado por cada función específica en todos los programas informáticos y para todos los usuarios, donde todo el personal de la UNIFSL-Bagua (funcionarios, CAS, locación de servicios y otros) obtendrá un código identificador único frente al sistema y quedará bajo responsabilidad ante cualquier designación registrada.
4. Elaboración, cancelación y evaluación de privilegios de los usuarios de red y los programas Informáticos de la UNIFSL-Bagua, habrán de ser evaluados con regularidad mediante una programación de actividades por el área de Tecnologías de la Información.
5. El control para obtener accesos a la información mediante los distintos sistemas de información que tiene la universidad se efectúa mediante roles administrando los privilegios del usuario dentro del sistema de información.

6. Las áreas correspondientes deberán enviar al área de Tecnologías de la Información, un detalle actualizado de vacaciones, discapacidad, licencia, encargaturas, consultorías, servicios, etc. del personal que labora en la UNIFSL-Bagua (funcionarios, servidores, CAS, locadores de servicios y otros) esto con la finalidad de dirigir el control de cuentas de usuario como corresponde según proceda.

A.2. Política de clasificación y manejo de la información

La información de la UNIFSL-Bagua se especifica conforme a su valoración e importancia de ésta.

Objetivo:

Realizar una clasificación de la información procedente de la universidad para su correspondiente acceso y almacenamiento de parte de los usuarios.

Aplicabilidad:

Tecnologías de la Información y todo el personal en general de la institución.

Directrices

A.2.1. Clasificación de la Información:

1. Cualquier información manejada por la UNIFSL-Bagua y el personal (funcionarios, CAS, locación de servicios y otros), se deberá realizar su clasificación y administración conforme a los niveles que establece la universidad donde se detallen en el documento referente al clasificado de activos de la Información.
2. Cada activo de información, propiedad de la UNIFSL-Bagua, tiene que asignarse a un propietario, personal de la universidad, el cual se hará responsable (funcionarios, servidores CAS, locadores de servicios y otros)

A.2.2. Manejo de la Información:

1. La UNIFSL-Bagua custodiará todos sus activos de información identificados e inventariados, al cual se le realizará una actualización constante.

2. Toda adquisición que realice la universidad, de hardware, software, servicios informáticos e información, debe tener un control mediante el área de Tecnologías de la Información.

A.3. Política de seguridad física y ambiental

Objetivo

Definir los respectivos controles para la seguridad física y ambiental garantizando la seguridad de la información de la universidad.

Aplicabilidad: Dirigido a todo el personal de la universidad.

A.3.1. Controles de acceso perimetral

a) Identificación del personal de la UNIFSL-Bagua (funcionarios, CAS, locación de servicios y otros) portando un fotocheck.

b) Toda persona (natural, jurídica, contratistas, consultores, temporales o terceras personas) que realicen su ingreso a las instalaciones de la institución habrán de identificarse e informar su llegada mediante el personal de vigilancia de las instalaciones el cual proceda a realizar el registro que le corresponde.

c) Deberán mantenerse cerradas las puertas de ingreso a las áreas de operación o manipular información privada o reservada, permanentemente para evitar posibles amenazas.

d) Para la salida de cualquier elemento de la institución se deberá diligenciar formatos de autorización que tiene determinada por la universidad con el registro completado de la información requerida.

A.3.2. Controles ambientales

a) La UNIFSL-Bagua conservará los ambientes de las instalaciones en condiciones óptimas de seguridad, mantenimiento y funcionalidad de todos los componentes que conforman el centro de cómputo y

el resguardo de los backups de la información.

b) La UNIFSL-Bagua facilitará un ambiente apropiado para conservar dispositivos magnéticos, laboratorio de cómputo, biblioteca y equipamientos tecnológicos.

A.4. Política de temas finales orientados al usuario, tales como:

A.4.1. Política de uso aceptable de activos

Tiene responsabilidad el personal de la UNIFSL-Bagua para dar un uso razonable y eficiente los recursos encomendados, que utilicen activos de información que sea propiedad de la institución.

Objetivo:

Responsabilizar a los usuarios por el manejo permisible de los activos de información.

Aplicabilidad:

Dirigido a todo el personal de la universidad.

Directrices

A.4.1.1. Correo electrónico.

El usuario se responsabilizará por el buen empleo de su cuenta de correo electrónico institucional, velando por su seguridad y protegiendo su clave de acceso.

En consecuencia el usuario se compromete a:

1. El uso de correos electrónicos institucionales, deberá ser usado solamente para fines propios de la universidad, haciendo uso de manera responsable y relacionada con las actividades propias de su trabajo que se le tenga asignada.
2. Realizar el mantenimiento de los correos institucionales periódicamente, cuando el sistema le haga advertencias de liberación de espacio.
3. El respeto de la privacidad de cuentas institucionales de otros

usuarios, dentro y fuera de la institución.

A.4.1.2. Navegación en Internet.

1. El uso de Internet debe estar destinado exclusivamente a la ejecución de actividades propias de la institución para realizar funciones establecidas para el cargo que se le asigne.
2. Está absolutamente prohibido la descarga de software no autorizado, y/o descargar información ajena al desempeño institucional.

A.4.2. Política de escritorio y pantalla limpios

Tiene la finalidad de mitigar los riesgos de accesos sin autorización, pérdidas y/o daños de la información.

Objetivo

Reducir riesgos en la presentación de búsquedas en escritorios y equipos computacionales.

Aplicabilidad: Dirigido a todo el personal de la universidad.

Directrices

1. Proteger los documentos impresos y los dispositivos de almacenamiento extraíbles bajo llave, cuando no están siendo utilizados.
2. Hacer uso del protector de pantalla cuando no se está haciendo uso del equipo, configurar para que la activación sea de manera automática posterior a diez (10) minutos de inactividad.
3. La información sensible, una vez impresa, debe archivarse inmediatamente en lugares seguros establecidos para su protección adecuada.
4. El escritorio de los equipos computacionales no debe tener acceso directo a archivos de interés de la institución.

A.4.3. Política de dispositivos móviles y teletrabajo

Restricción de la utilización de los equipos de la institución afuera de las instalaciones de la universidad, solo se aprueban los dispositivos móviles autorizados teniendo cuidado de no poner en riesgo la Seguridad de la Información de la institución.

Objetivo

Garantizar la seguridad de la información de los equipos fuera de las instalaciones de la universidad.

Aplicabilidad: Dirigido a todo el personal de la universidad.

Directrices

1. Realizar cuentas de usuario y contraseñas para acceder a los dispositivos móviles.
2. Garantizar el adecuado uso del dispositivo móvil, es responsabilidad del usuario conectarlo a redes confiables, para evitar se propague cualquier amenaza.
3. El software instalado en los equipos móviles debe tener íntegramente licencia y autorización del área de Tecnologías de la información (TI).
4. El trabajo remoto solo será autorizado a través la Oficina de Tecnologías de la información (OTI) después de verificar las condiciones de seguridad del entorno laboral.
5. Solo se podrá tener acceso a la red de la universidad el personal autorizado mediante túneles SSL o VPN y empleando los dispositivos móviles de la institución que se le han sido asignados para realizar funciones encomendadas en la institución.

A.4.4. Política de restricciones a las instalaciones y uso del software

Aplicar controles de seguridad de uso de software para la protección de la información administrando una adecuada protección de su disponibilidad e integridad.

Objetivo

Establecer medidas necesarias de seguridad para el uso de software.

Aplicabilidad: Dirigido a todo el personal de la universidad.

Directrices

1. La UNIFSL-Bagua prohíbe la instalación o utilización de software sin licencias autorizadas por la universidad, verificando constantes revisiones al cumplimiento de las normativas relacionado con la propiedad intelectual, con excepción del software con licencia de libre utilización o que sean sustentados con certificado de propiedad de licencia de terceros.
2. Todo el personal de la UNIFSL-Bagua (funcionarios, CAS, locación de servicios y otros) que requieran la instalación de software debe ser gestionada y conseguida a través del área de Tecnologías de la Información.

A.4.5. Política de copia de seguridad

Aplicar controles de copias de seguridad para proteger la información administrando una adecuada protección de su disponibilidad e integridad.

Objetivo

Establecer copias de seguridad necesarias para la protección de la información.

Aplicabilidad: Dirigido al personal de Tecnologías de la Información (TI).

Directrices

1. Toda información de la UNIFSL-Bagua tiene que ser protegida a través de backups de seguridad de la información, imágenes, software o cualquier otra información de relevancia para la universidad siguiendo el procedimiento adecuado. Este procedimiento incluye información de las diferentes áreas de trabajo en coordinación con la persona encargada del área de Tecnologías de la Información para incluirlos en el procedimiento de backups.
2. El personal de la UNIFSL-Bagua (funcionarios, CAS, locación de

servicios y otros) es responsable de ubicar en una unidad de red, la información referida solamente a la Universidad que requiera ser respaldada por el área de TI.

A.4.6. Política de protección contra software malicioso

Se utilizan controles de seguridad de protección contra software malicioso, con la finalidad de administrar una protección apropiada de su disponibilidad e integridad.

Objetivo

Aplicar controles para brindar protección a la disponibilidad e integridad de la información.

Aplicabilidad: Dirigido a todo el personal de la universidad.

Directrices

1. La universidad caso de estudio tendrá establemente un sistema seguro de antivirus, antimalware, antispam, antispyware que conserve las últimas actualizaciones y parches de seguridad administrado y bajo el compromiso de personal responsable del área de Tecnologías de la Información.

2. La parte usuaria deberá cumplir con las mejores prácticas establecidas por la universidad caso de estudio con respecto al uso del Antivirus garantizando que los archivos descargados proceden de fuentes fiables para impedir contaminación de virus informáticos y/o instalación de software maliciosos en los recursos tecnológicos.

3. Es responsabilidad de todo el personal de la universidad caso de estudio la ejecución de software de antivirus sobre archivos que se ejecutan por vez primera, información que se hallan en medios de almacenamiento externo o que proceden de correos electrónicos. Realizar la revisión de medios magnéticos extraíbles que sean examinados con un antivirus suministrado por la institución previamente a su procesamiento en los computadores personales o

servidores de la institución.

4. Es responsabilidad del área de Tecnologías de la Información conservar en estado óptimo el funcionamiento los sistemas el cual permite la prevención, detección y corrección de los ingresos o intentos de ingresos sin autorización, evitando así cualquier alteración y acceso no autorizado.

A.4.7. Política de Gestión de Vulnerabilidades

Se realizan revisiones de manera periódica a las debilidades técnicas acerca de los recursos de la plataforma tecnológica mediante pruebas.

Objetivo

Efectuar la correlación sobre hallazgos encontrados

Aplicabilidad: Dirigida al personal de Tecnologías de la Información (TI).

Directrices

1. Revisión periódica de la manifestación de nuevas vulnerabilidades técnicas y proporcionar al personal administrativo de la plataforma, con el propósito de advertir la expuesta al riesgo.

2. Establecer lineamientos y estándares para la ejecución segura de la plataforma tecnológica, tomando medidas de restricción y los límites a fin de instalar software en los equipos computacionales.
3. Establecer y realizar el monitoreo de los planes de acción para minimizar debilidades técnicas encontradas en la plataforma tecnológica.

A.4.8. Política de controles criptográficos

Manejo de métodos y conocimientos criptográficos para brindar protección a la información, con el objetivo de facilitar una apropiada salvaguarda de su confidencialidad e integridad.

Objetivo

Aplicación de controles criptográficos con el fin de proteger la integridad y confidencialidad de la información.

Aplicabilidad: Dirigida a todo el personal de la institución.

Directrices

Se utilizarán controles criptográficos en los casos siguientes:

1. El área de Tecnologías de la Información es responsable de administrar e implementar los controles criptográficos de acceso a sistemas y aplicaciones informáticas que necesiten autenticación.
2 Servicio institucional que seleccionen información de terceras personas. Uso de correo electrónico institucional, vía web.
2. Se forma el servicio de certificación digital cerrado, para administrar la integridad, autenticidad y aprobación de la información digital organizacional.
3. Protocolos establecidos relacionado con administrar las claves de cifrado, reparación de información encriptada cuando exista extravío, responsabilidad o perjuicio de las claves de cifrado.

A.4.9. Política de seguridad de las comunicaciones

Se utilizan controles de seguridad de las comunicaciones dentro de las instalaciones de la universidad, para proteger la seguridad de la Información de la institución.

Objetivo:

Garantizar la seguridad de las comunicaciones dentro de las instalaciones de la universidad.

Aplicabilidad: Dirigida a todo el personal de la universidad.

Directrices

1. Todos los procedimientos operativos de la UNIFSL-Bagua estarán

debidamente acreditados, protegidos y disponible al usuario a quien corresponde.

2. El área de Tecnologías de la Información es responsable de conservar apropiadamente la documentación actualizada correspondiente a la plataforma tecnológica de la universidad.
3. Es responsabilidad del área de Tecnologías de la Información garantizar un adecuado modelo de seguridad proporcionando tecnologías de acceso remoto al personal de la UNIFSL-Bagua (funcionarios, CAS, locación de servicios y otros), previa evaluación y autorización del área correspondiente.
4. La UNIFSL-Bagua conservará un monitoreo constante acerca de la red interna, con la implementación de herramientas necesarias que autoricen la detección, prevención y recuperación del código malintencionado hallado en la plataforma tecnológica.
5. La UNIFSL-Bagua mantendrá actualizada mediante la debida aprobación del área de Tecnologías de la Información, un listado de las categorías de acceso no autorizado para la navegación en Internet vigilando el cumplimiento de los compromisos de seguridad de la página https://www.unibagua.edu.pe/, a través de la revisión periódica de los informes de vulnerabilidades entregados a la universidad.

A.4.10. Política de relación con los proveedores

La Universidad dispone los mecanismos de control en sus relaciones con el personal externo que le suministran bienes o servicios.

El personal responsable de la elaboración y/o firma de contrataciones, acuerdos o licitaciones con personal externo debe respaldar la ejecución de las políticas de seguridad de la información por parte de estos.

Objetivo

Examinar los servicios contratados con personal externo para que realicen la ejecución de las políticas de seguridad de la información determinadas en la organización.

Aplicabilidad: Personal externo, contratistas y proveedores.

Directrices

1. Gestionar y firmar el formato declaración de confidencialidad y participación en la seguridad de la información contratistas o terceros y acuerdos para la revelar la información confidencial bajo el compromiso de reserva.
2. La UNIFSL-Bagua, mediante el área de TI, asegurará la mejor selección de los proveedores de servicios, para los componentes y el equipo que conforman los equipos computacionales, informáticos que así lo requiera la institución.
3. El área de Gestión del Talento Humano debe especificar la supervisión del personal externo encargado por el personal responsable, que efectúen trabajos en las instalaciones en la universidad, comprobando que los documentos se hallen correctamente ejecutados, también estará encargado juntamente con el supervisor del contrato en la coordinación, teniendo en consideración aquellas medidas de seguridad que tiene la entidad.

5. POLÍTICAS PARA LA SEGURIDAD DE LOS RECURSOS HUMANOS.

Uno de los activos más valiosos es el recurso humano, es por ello que la universidad debe tener el personal capacitado para ejercer las funciones para las cuales han sido contratados; del mismo modo requerir del compromiso y conocimiento con relación a la información y su seguridad.

Objetivo:

Asegurar la ejecución de las políticas de seguridad de la información por parte del personal contratado.

Aplicabilidad: Dirigida al área de Gestión del Talento Humano de la universidad.

Directrices

1. Se debe seleccionar el personal de una manera coherente siguiendo a

cabalidad los Términos de Referencia que la universidad estipula, siguiendo el procedimiento para la confirmación de la credibilidad de la información brindada por el personal postulante para el ingreso a la universidad antes de su vinculación definitiva.

2. Todo el personal de la UNIFSL-Bagua (funcionarios, CAS, locación de servicios y otros), previa evaluación y autorización del área de Gestión del Talento Humano le corresponde gestionar los formatos Declaración de Confidencialidad y Compromiso con la Seguridad de la Información.
3. El personal externo (natural, jurídico, consultores, contratistas, temporal o terceros), previa evaluación y autorización del área Recursos Humanos le corresponde gestionar los formatos Declaración de Confidencialidad, asimismo comprometerse con la Seguridad de la Información adjuntándose con las hojas de vida en la oficina del área de Gestión del Talento Humano de la universidad caso de estudio.

Elaborado por: Mavila Segura Huaman	Aprobado por:
Firma:	Firma:
Cargo:	Cargo:

Tratamiento de riesgos

Activos de información	Responsable del activo	Amenazas	Vulnerabilidades	Tratamiento del riesgo	
				Opción de tratamiento del riesgo	Controles o Salvaguardas
-Resoluciones Presidenciales. -Directivas	Secretaría Gral.	Robo de documentos	Falta de concientización por parte del personal.	Mitigar	1 Política de control de acceso
		Mal uso de privilegios de acceso por el personal interno	Acceso de personal sin previa autorización.		3 Política de seguridad física y ambiental 3.1 Controles de acceso perimetral
		Pérdida de documentos			4.7 Políticas de controles criptográficos
Documentos de trámite documentario	Trámite Docum.	Divulgación de información	Ausencia de permisos de accesos. Ingreso de personal externo a las instalaciones.	Mitigar	4.8 Política de seguridad de las comunicaciones
		Robo de documentos			1 Política de control de acceso
		Pérdida de documentos			3 Seguridad física y ambiental
		Datos de fuentes no confiables			2 Políticas de clasificación y manejo de la información
Información de Gestión del Talento Humano	RRHH	Divulgación de información	Falta de cultura y buenas prácticas.	Mitigar	1 Políticas de control de acceso. 4.9 Políticas de relación con los proveedores. 5 Política de los recursos humanos.
		Pérdida de documentos			
		Modificación deliberada de	Fácil acceso y seguridad de documentos.		

		información			
Información de DGA.	DGA	Divulgación de información	Uso de dispositivos extraíbles (pen drives)	Mitigar	1 Políticas de control de acceso. 5 Política de los recursos humanos.
		Modificación o alteración de la información	Introducción de información errónea		
		Manipulación de datos	Ausencia de control de contenidos transferidos en la red		
Información de secretaría general	Secretaría General	Datos de fuentes poco fiables	Uso de dispositivos extraíbles (pen drives) Abuso de confianza por parte del personal interno.	Mitigar	1 Políticas de control de acceso.
		Divulgación de información			2 Política y clasificación y manejo de la información.
		Documentos fácilmente extraíbles por personal interno.			4.8 Política de seguridad de las comunicaciones.
-Correos electrónico. -Contraseñas SIGA. -Contraseñas SIAF. -Contraseña página Web. -Contraseñas correos institucionales. -Contraseñas de	TI	Accesos no autorizados. Desconexión física o lógica. Falla de generador eléctrico. Fallas de conexión	Falta de seguridad y uso de controles adecuados de acceso a las áreas de acceso restringido.	Mitigar	1 Políticas de control de acceso. 4.1 Política de uso aceptable de activos. 4.5 Políticas de copias de seguridad. 4.7 Políticas de controles criptográficos.

aplicaciones informáticas.		de internet. Fuga de información. Repudio.			
Servicios académicos.	Área académica	Accesos no autorizados	No se tienen definidos los accesos. Uso de dispositivos extraíbles (pen drives) Por parte de personal interno.	Mitigar	1 Políticas de control de acceso.
		Divulgación de información			4.1 Política de uso aceptable de activos.
Servicios institucionales	Área admin.	Accesos no autorizados		Mitigar	1 Políticas de control de acceso.
		Divulgación de información			4.5 Políticas de copia de seguridad.
-Sistema Akademico. -Sistema de planilla. -Sistema de admisión. -Sistema biblioteca. -SW de control de asistencia. -SW de cámaras de video vigilancia. -SIGA. -SIAF.	TI	Acceso no autorizado	No se tienen definidos los accesos.	Mitigar	1 Políticas de control de acceso. 4.1 Política de uso aceptable de activos. 4.6 Política de protección contra SW malicioso. 4.7 Políticas de controles criptográficos. 4.9 Política de relación con los proveedores.
		Fallo informático por recursos agotados	Agotamiento de recursos.		
		Infección por código malicioso, virus, troyanos, gusanos. Modificación deliberada de información. Destrucción de información	Presencia de bases de datos y antivirus desactualizadas. Ausencia de revisiones periódicas de privilegios de acceso		
-Servidor Data Center. - Servidor de base de datos. -Servidor HPE	TI	Accesos no autorizados.	No se tienen definidos los accesos.	Mitigar	A.1 Políticas de control de acceso. A.3 Políticas de seguridad
		Falla de generador eléctrico	Falta de sistemas de ventilación o		

ProLiant DL 360. -Servidor Prolian 390. -Servidor DELL. -PCs portátiles.		Sobrecalentamiento de equipos.	aire acondicionado adecuados.		física y ambiental. A.3.1 Controles de acceso perimetral. 3.2 Controles ambientales.
		Fallas de origen físico.	Partes defectuosas de fábrica		
Cableado de red. -Router. -Switch -Hub -Disco Duro Externo. -Cámaras de seguridad. -Reloj Biométrico.	TI	Falla eléctrica	Falta de sistemas de ventilación o aire acondicionado adecuados.	Mitigar	A.1 Políticas de control de acceso. A.3 Políticas de seguridad física y ambiental. A.3.1 Controles de acceso perimetral. A.3.2 Controles ambientales.
		Sobrecalentamiento de los equipos.			
		Manipulación de equipos tecnológicos. Fallas de origen físico. Fallas de origen lógico.	Ausencia de permisos de accesos. Presencia de polvo en los equipos.		
Local administrativo	Área admin.	Accesos no autorizados.	Falta de concientización por parte del personal.	Mitigar	A.1 Política de control de acceso. A.3.1 Controles de acceso perimetral. A.4.4 Política de restricciones a las instalaciones y uso de software A.4.7 Políticas de controles criptográficos
Presidencia	Área admin.	Pérdida de documentos	Ausencia de permisos de accesos. Uso de dispositivos extraíbles (pen drives)	Mitigar	
Vicepresidencia de Investigación	Área admin.	Accesos no autorizados			
Vicepresidencia Académica.	Área Académica	Accesos no autorizados			
Personal	Área Admin.	Fuga/divulgación de la información de parte del personal interno.	Ausencia de concientización por parte del personal.	Mitigar	A.1 Políticas de control de acceso. A.2 Políticas de seguridad física y

		Pérdida de documentos			ambiental. A.4.2 Política de escritorio y pantalla limpia. A.4.3 Política de dispositivos móviles y teletrabajo.
	Área Académica	Accesos no autorizados. Fuga/divulgación de la información de parte del personal interno.	Ausencia de permisos de accesos.	Mitigar	

Declaración de aplicabilidad

DECLARACIÓN DE APLICABILIDAD

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN			
A.1	**Control de acceso**		
A.1	Políticas de control de acceso	**SI**	La legalidad para los controles de acceso está documentado en las Políticas de la Seguridad de Información. Este documento estará a disponibilidad del personal de la institución caso de estudio.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.2	**CLASIFICACCIÓN Y MANEJO DE LA INFORMACIÓN**		
A.2.1	**Clasificación de la información**		
A.2.1.1	Políticas de Clasificación de la información	**SI**	Clasificación y administración de toda información por un propietario quien se responsabilizará por el mismo.
A.2.2	**manejo de la información**		
A.2.2.1	Políticas de manejo de la información	**SI**	Toda averiguación tiene que estar identificada e inventariados, al cual se le realizará una actualización constante. Debe tener un control mediante el área de Tecnologías de la Información.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.3	**SEGURIDAD FÍSICA Y AMBIENTAL**		
A.3.1	**Controles de acceso perimetral**		
A.3.1.1	Políticas de acceso perimetral	**SI**	Todo el personal de la universidad que haga su ingreso a las instalaciones de deberán identificarse por medio del personal de vigilancia portando un fotocheck que lo identifique como personal de la universidad.
A.3.2	**Controles ambientales**		
A.3.2.1	Políticas de controles ambientales	**SI**	Toda información debe ser identificada e inventariados, al cual se le realizará una actualización constante. Debe tener un control a través del área de Tecnologías de la Información.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.4	**SEGURIDAD ORIENTADOS AL USUARIO**		
A.4.1	**USO ACEPTABLE DE ACTIVOS**		
A.4.1.1	**Correo electrónico**		
A.4.1.1	Políticas de uso aceptable de activos	**SI**	El usuario se responsabilizará por el uso correcto de su cuenta de correo electrónico institucional, velando por su seguridad y protegiendo su clave de acceso.
A.4.1.2	**Navegación en internet**		
A.4.1.2	Políticas de uso aceptable de activos	**SI**	El uso de Internet debe estar destinado exclusivamente a la ejecución de actividades propias de la universidad para

			realizar funciones establecidas para el cargo que se le asigne.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.4	**SEGURIDAD ORIENTADOS AL USUARIO**		
A.4.2	**Escritorio y pantalla limpia**		
A.4.2.1	Políticas de escritorio y pantalla limpia	**SI**	Este documento está a disposición del personal de la universidad caso de estudio con la finalidad de mitigar los riesgos de accesos no permitidos, pérdidas y/o daños de la información expuesta en escritorios y equipos computacionales.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.4	**SEGURIDAD ORIENTADOS AL USUARIO**		
A.4.3	**Dispositivos móviles y teletrabajo**		
A.4.3.1	Políticas de dispositivos móviles y teletrabajo	**SI**	Restricción del uso de equipos institucionales para respaldar la protección de la información de los equipos afuera de las instalaciones de la universidad.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.4	**SEGURIDAD ORIENTADOS AL USUARIO**		
A.4.4	**Restricciones a las instalaciones y uso de software**		
A.4.4.1	Políticas de restricciones a las instalaciones y uso de software	**SI**	Aplicar controles de seguridad de uso de software para la protección de la información administrando una adecuada protección de su disponibilidad e integridad.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.4	**SEGURIDAD ORIENTADOS AL USUARIO**		
A.4.5	**Copia y seguridad**		
A.4.5.1	Políticas de copia y seguridad	**SI**	Aplicar controles de copias de seguridad para la protección de la información administrando una adecuada protección de su disponibilidad e integridad.
CONTROL_ID	**CONTROL**	**APLICABLE**	**IMPLEMENTACIÓN**
A.4	**SEGURIDAD ORIENTADOS AL USUARIO**		
A.4.6	**Protección contra software malicioso**		
A.4.6.1	Políticas contra software malicioso	**SI**	Aplicar controles de protección contra software malicioso, con la finalidad de proporcionar una adecuada protección de su disponibilidad e integridad.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.4	**SEGURIDAD ORIENTADOS AL USUARIO**		
A.4.7	**Gestión de vulnerabilidades**		
A.4.7.1	Políticas de gestión de vulnerabilidades	**SI**	Realizar revisiones periódicamente a las vulnerabilidades técnicas acerca del recurso de la plataforma tecnológica a través de pruebas.
CONTROL_ID	**CONTROL**	**APLICABLE**	**IMPLEMENTACIÓN**
A.4	**SEGURIDAD ORIENTADOS AL USUARIO**		
A.4.8	***Controles criptográficos***		
A.4.8.1	Políticas de controles criptográficos	**SI**	Aplicar controles de seguridad donde se emplean sistemas y técnicas criptográficas para el resguardo de la información,

			con la finalidad de proporcionar una protección apropiada de su confidencialidad e integridad.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.4	**SEGURIDAD ORIENTADOS AL USUARIO**		
A.4.9	**Seguridad de las comunicaciones**		
A.4.9.1	Políticas de seguridad de las comunicaciones	**SI**	Aplicar controles de seguridad para garantizar y proteger el aseguramiento de la información de las comunicaciones dentro de las instalaciones de la universidad

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.4	**SEGURIDAD ORIENTADOS AL USUARIO**		
A.4.10	**Relación con los proveedores**		
A.4.10.1	Políticas de relación con los proveedores	**SI**	Aplicar controles de seguridad de información relacionado con el personal externo que le proporcionan bienes o servicios, asegurando el cumplimiento de las políticas de seguridad de relación con los proveedores.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.5	**SEGURIDAD DE LOS RECURSOS HUMANOS**		
A.5.1	**Seguridad para los Recursos Humanos**		
A.5.1.1	Políticas para la seguridad de los recursos humanos	**SI**	Aplicar controles de selección de personal capacitado para desempeñar las funciones por los cuales son contratadas, de igual forma necesita de su compromiso y conocimiento relacionado con la seguridad de la información.

Plan de Auditoría

PLAN DE AUDITORÍA	
OBJETIVO	
Realizar el seguimiento al Sistema de Gestión de Seguridad de la Información caso de estudio Universidad Nacional Intercultural “Fabiola Salazar Leguía” Bagua para garantizar el cumplimiento de las políticas de seguridad de la información del modelo planteado.	
ALCANCE	
Sede administrativa y sede académica	
RESPONSABLE	**ÁREAS INVOLUCRADAS**
Equipo auditor de la Seguridad de la Información	Todas las áreas de la universidad

COSTO APROXIMADO	S/. 30,000
PLAZO DE CONSECUCIÓN	Largo plazo
TIEMPO ESTIMADO DE EJECUCIÓN	6 meses
ACTIVIDADES	

- Formación del equipo auditor interno
- Planificación del plan de auditorías
- Planteamiento de acciones de mejora
- Revisión del cumplimiento de las No conformidades

Seguimiento

SEGUIMIENTO DE LAS POLÍTICAS DE SEGURIDAD			
DOMINIO / OBJETIVO DE CONTROL	**DÍA**	**INTERLOCUTOR**	**OBSERVACIONES**
Control de acceso	1	Determinar en la reunión inicial	A.1 Políticas de control de acceso
Clasificación y manejo de la Información	1	Determinar en la reunión inicial	A.2; A.2.1 Clasificación de la información, A.2.2 Manejo de la información..
Seguridad física y ambiental	1	Determinar en la reunión inicial	A.3; A.3.1. Controles de acceso perimetral, A.3.2 Controles ambientales.
Seguridad orientados al usuario	1	Determinar en la reunión inicial	A.4; A.4.1. Políticas de uso aceptable de activos, A.4.2 Políticas de escritorio limpio A.4.3 Política de dispositivos móviles y teletrabajo, A.4.4 Políticas de restricciones a las instalaciones y uso de software, A.4.5 Política de copias de seguridad, A.4.6 Políticas de protección contra software malicioso, A.4.7 Políticas de gestión de vulnerabilidades, A.4.8 Políticas de controles criptográficos, A.4.9 Políticas de seguridad de las comunicaciones, A.4.10 Políticas de relación con los proveedores,
Seguridad para los recursos humanos	1	Determinar en la reunión inicial	A.5.1 Políticas para la seguridad de la información.

Matriz RACI

RESPONSABILIDADES	
RESPONSABLE	**R**
ADMINISTRADOR (SUPERVISOR)	**A**
CONSULTAR	**C**
INFORMAR	**I**

ACTIVIDADES	Comisión Organizadora	Equipo del proyecto	Jefe de Tecnologías de la Información	Personal
Definir y actualizar políticas y plan de seguridad de información	A	R	C	C
Implementación de protocolos y controles de seguridad establecidos en plan	A	R	C	I
Socialización y divulgación de medidas de seguridad y responsabilidades	A	R	C	I
Evaluación de controles de seguridad y procesos de gestión de la seguridad de información	A	R	C	C
Verificación de la gestión de la seguridad	A	R	A	I
Actualización y mejora continua de políticas y plan de seguridad de información	A	R	A	I

Informe Final de Auditoría

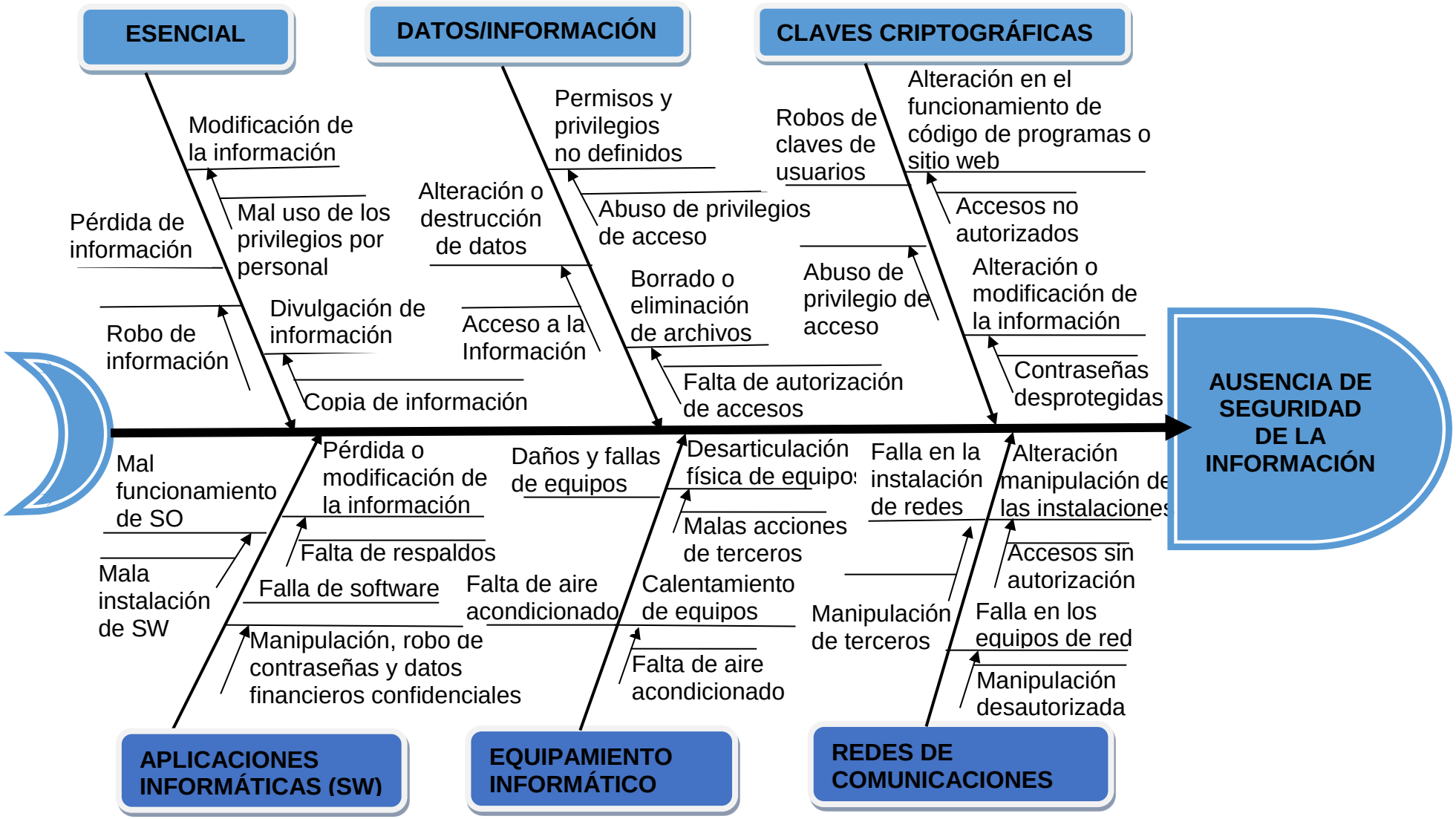
INFORME DE AUDITORÍA INTERNA			
Proceso(s) Auditado(s):	Procesos de Matrícula Procesos de Admisión Procesos de Notas		
Alcance de la auditoria:			
Norma(s) de referencia para la realización de la auditoria:			
Auditor Principal:	Auditor	**Equipo Auditor:**	Equipo auditor
Fecha de realización de la auditoria:	**19/08/2019**	**Fecha de presentación del informe:**	**21/08/2019**
Auditado(s):	**UNIFSL-BAGUA**		
Documento(s) Revisados			**Ref. Cláusula/ Control**
Documento de Políticas de seguridad de la información			**Anexo 15**
Documento de tratamiento de riesgo			**Anexo 16**
Documento de Declaración de aplicabilidad			**Anexo 17**
Fortalezas:			
Oportunidades de Mejora:			
No conformidades:	**No conformidades menores:** Las no conformidades menores convienen ser solucionadas en un periodo no mayor de 5 meses, estas son:		

	- Dominio afectado: Control de acceso - Dominio afectado: Seguridad física y del entorno - Dominio afectado: Seguridad de las operaciones **No conformidades mayores:** Las conformidades mayores se deben resolver de forma inmediata, afectando los siguientes dominios: **-** Dominio afectado: Seguridad de las comunicaciones **-** Dominio afectado: Seguridad relativa a los recursos humanos

Conclusiones:
Se observa que se han desarrollado 16 políticas de seguridad de la información como propuesta de Gestión de seguridad de la información para la universidad caso de estudio el cual debe obtener mejoras de manera continua la efectividad del SGSI por medio del uso de las políticas de seguridad con el propósito de dar protección a los activos de información.

Firma del auditor principal:		**Fecha:**	**20/08/2019**

Diagrama Causa Efecto



Tratamiento de No Conformidades

LOGO	INFORME DE NO CONFORMIDAD	
	PROCEDENTE DE:	**N° No Conformidad:**
		Fecha:

IDENTIFICACIÓN DE LA NO CONFORMIDAD
PROCESO/S: Procesos de Matrícula Procesos de Admisión Procesos de Notas
DESCRIPCIÓN: **Evidencias:** **No conformidades menores:** - Dominio afectado: Control de acceso - Dominio afectado: Seguridad física y del entorno - Dominio afectado: Seguridad de las operaciones **No conformidades mayores:** **-** Dominio afectado: Seguridad de las comunicaciones - Dominio afectado: Seguridad relativa a los recursos humanos 1. Se producirá un análisis luego de la identificación de una no conformidad y, en funcionalidad del alcance del no cumplimiento de los requerimientos, se decidirá y tomarán las acciones correspondientes en concordancia con el sistema de responsabilidad y participaciones del SGSI. 2. En términos generales se disponen, conforme corresponda, las siguientes acciones:

<table>
<tr><td colspan="2">a) Identificar las acciones para la eliminación de la no conformidad mostrada: de las correcciones de manera inmediata asimismo de aquella que elimine los motivos de la no conformidad.
b) Practicar acciones para evitar prestaciones de servicios o producto para utilización o aplicación inicialmente no previsto.
c) Verificado por el responsable del área de Tecnologías de la Información donde las acciones adoptadas autorizan la prestación de servicios o productos que cumplan con las necesidades especificadas para los mismos.</td></tr>
<tr><td>DETECTADA POR:</td><td>FIRMA RESPONSABLE PROCESO AUDITADO:</td></tr>
<tr><td>Jefe de Tecnologías de la Información.</td><td>Jefe de TI</td></tr>
<tr><td>Auditor Jefe:
La firma se lleva a cabo en caso de no conformidades registradas en auditoría o seguimiento elaborados por auditores internos.</td><td>Nombre:
Jefe de Tecnologías de la Información</td></tr>
<tr><td colspan="2">observación:
Las acciones correctivas practicadas se expondrán a un seguimiento de verificación de acuerdo con lo estipulado en la Auditorías Interna.</td></tr>
</table>

Plan de Mejora Continua

PLAN DE MEJORA CONTINUA			Fecha: 19/08/2019 Edición: 1	
Elaborado por:	Revisado por :		Aprobado por :	
Mavila Segura Huaman				

I. OBJETIVO

Especificar un procedimiento para establecer normas generales a continuar y mediante el cual el personal de la universidad logre formar las acciones que contribuyan un mejoramiento continuo a los procesos de la institución.

II. APLICACIÓN (x)General () Específica

Este proceso es aplicado a cada una de las áreas de la universidad.

III. ALCANCE

A partir del análisis de información incluso los resultados obtenidos para ser presentado a la alta Dirección.

IV. DEFINICIONES

MEJORA CONTINUA: Es una actividad frecuente para incrementar la facultad de realizar el cumplimiento con los requerimientos determinados por la universidad.

V. RESPONSABILIDADES

El jefe del área de Tecnologías de la Información es responsable de realizar de forma estable este proceso en cada una de las áreas de la universidad.

La Alta Dirección es responsable de promocionar, asistir con los recursos necesarios y dar el seguimiento que corresponde a cada una de las acciones de mejoramiento de la institución y estimular al personal involucrado por sus metas.

VI. DESCRIPCIÓN DE LAS ACTIVIDADES

1. Invitación a crear sugerencias y/o proyectos de mejoramiento al personal, estos productos o resultados quedarán comunicados por el personal encargado de las

áreas autorizadas.

2. En el caso de que surja sugerencias de mejoramiento antes, durante y después de la comprobación, se realiza una propuesta de mejoras y una documentación o registro de la información.
3. En el caso de que se autorice la propuesta se realiza la especificación de la metodología para el proyecto de mejoras por el contribuyente quien realizó la propuesta, teniendo en consideración los siguientes aspectos:

   Definición de objetivos a obtener.

   Definición de etapas.

   Definición de responsables.

   Definición de tiempos.
4. Se publica su ejecución en cada una de las áreas que tengan mayor susceptibilidad de atención.
5. Registro de los productos a cargo de la Alta Dirección al personal involucrado en el proyecto.

3.2. Consideraciones finales

3.2.1. Conclusiones

a. Después de haber realizado un análisis exhaustivo de los modelos para administrar la seguridad de la información, se tomó la determinación de elegir las destacadas normativas que se adecuan al desarrollo de la administración de seguridad de la información.

   La norma ISO/IEC 27001 mediante los lineamientos de este estándar internacional de seguridad de la información ISO/IEC 27001 apoyado en los lineamientos de COBIT 5, ITIL, PMBOK, de las cuales se concluye y considera que son herramientas de gran beneficio en la de toma de decisiones a fin de efectuar y de constituir un modelo de seguridad de la información y uno de las ventajas fundamentales que plantea es que pueden ser adaptable a metodologías de evaluación de análisis de riesgos.

   En cuanto a los distintos modelos de análisis de riesgos se ha tomado en cuenta la metodología de Análisis y Gestión de los Riesgos de los Sistemas de Información v3.0 (MAGERIT) y Octave, en donde se puede especificar que de los modelos que se ha tomado en cuenta, la ISO/IEC 27005 y la ISO/IEC 31000 son normativas dedicadas exclusivamente para administrar los riesgos y la seguridad de la información, de esta manera se concluye que mediante los modelos descritos en la presente investigación a través de un ciclo de mejora continua garantizó elaborar los documentos que necesita el modelo para administrar la seguridad de la información.

b. Se concluye que mediante la presente propuesta de gestión de seguridad de la información para la universidad caso de estudio sea tomado en cuenta al momento de tomar la decisión de establecer un modelo de seguridad de la información puesto que, de lograrse el objetivo de la propuesta, la universidad podrá lograr la sostenibilidad del Sistema de Gestión de Seguridad de la Información.

c. Después de haber realizado la propuesta a medida para la Universidad Nacional Intercultural “Fabiola Salazar Leguía” Bagua, se realizó la

implementación del modelo propuesto con datos reales de la universidad caso de estudio y se logró validar el modelo propuesto.

d. De las conclusiones anteriores el Sistema de Gestión de Seguridad de la Información permite salvaguardar los activos de la información, conocer los activos más relevantes, efectuar un análisis de riesgos, especificar salvaguardias, especificar las responsabilidades en la administración de la información y aprobar políticas de seguridad de la información para la protección de los activos en los procesos de: matrícula, admisión y notas de la universidad caso de estudio.

3.2.2. Recomendaciones

a. El presente modelo de investigación se basó en modelos de buenas prácticas, normas y metodologías relacionado con la gestión de riesgos que están señalados durante el desarrollo de la investigación caso de estudio.

b. Se propone emplear el modelo: Sistema de Gestión de Seguridad de la Información, en la Universidad Nacional Intercultural “Fabiola Salazar Leguía” Bagua y efectuar su posterior implementación y mantener el ciclo de vida de un SGSI permitiendo a tiempo detectar amenazas y vulnerabilidades.

REFERENCIAS

Ministerio de Hacienda , y. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. (M. d. Públicas, Ed.) Madrid, España: Centro de Publicaciones.

Pérez Villamizar, M. (30 de Noviembre de 2017). Aplicación de la metodología ITIL para impulsar la gestión de TI en empresas del Norte de Santander (Colombia). Espacios, Vol. 39(N° 9). Obtenido de https://www.revistaespacios.com/a18v39n09/18390917.html

Adobe. (22 de setiembre de 2017). Aspectos básicos de las aplicaciones web. Obtenido de https://helpx.adobe.com/es/dreamweaver/using/web-applications.html

Aguirre Cardona, J. D., & Aristizabal Betancourt, C. (15 de abril de 2013). Obtenido de http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf?sequence=1

Aguirre Mollehuanca, D. (30 de 10 de 2014). Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A. Obtenido de http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/5677

Alcántara, F. J. (28 de mayo de 2015). Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los Sistemas Informáticos de la Comisaria del Norte P.N.P en la ciudad de Chiclayo. La metodología empleada fue ISO /IEC 27001. Obtenido de http://tesis.usat.edu.pe/bitstream/usat/539/1/TL_Alcantara_Flores_JulioCesar.pdf

Arce, B. H. (28 de Agosto de 2008). Informática Jurídica. Obtenido de http://norbe1508.blogspot.pe/2008/

Avenía Delgado, C. (2017). Fundamentos de seguridad (Fondo editorial Areandino ed.). Colombia.

Barcos, S. (15 de enero de 2010). Reflexiones acerca de los sistemas de información universitarios ante los desafíos y cambios generados por los procesos de evaluación y acreditación. Obtenido de http://www.scielo.br/pdf/aval/v13n1/a12v13n1.pdf

Bernal Torres, C. A. (2010). Metología de la Investigación, administración, economía, humanidades y ciencias sociales (Tercera ed.). (O. F. Palma, Ed.) Bogotá, Colombia: Pearson Educación de Colombia Ltda. .

Cárdenas Solano, L., Martínez Ardila, H., & Becerra Ardila, L. (Noviembre de 2016). GESTIÓN DE SEGURIDAD DE LA INFORMACION: REVISION BIBLIOGRAFICA. El Profesional de la Información, 25(6).

Carolina Nieves, A. (2017). DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADOS EN LA NORMA ISO/IEC 27001:2013.

Casañ, R. M. (2015-2016). COBIT 5 y el Cuadro de Mando Integral. Obtenido de https://riunet.upv.es/bitstream/handle/10251/72620/MONFORT%20-%20COBIT%205%20y%20el%20Cuadro%20de%20Mando%20Integral%20como%20herramientas%20de%20Gobierno%20de%20TI.pdf?sequence=2

Chuna Chinga, G. I. (2018). Propuesta de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para la DRTPE - filial Piura". Repositorio de la Universidad César Vallejo.

Clarenc, C. A. (2011). nociones de cibercultura y periodismo. San Carlos de Bariloche, Río Negro, Argentina. Obtenido de https://www.humanodigital.com.ar/Publicaciones/Nociones-de-Cibercultura-y-Periodismo.pdf

Cobb, S. (15 de abril de 2017). La seguridad como rehen - Tendencias 2017. Obtenido de https://www.welivesecurity.com/wp-content/uploads/2016/12/Tendencias-2017-eset.pdf

Cuevas Riaño, E. (2015). La política de seguridad de la información y la conciencia humana. Revista Especializada en Ingeniería #ashtag(7).

Díaz Fonseca, D. A., & Ramírez Rodríguez, M. J. (17 de Abril de 2015). Inventario y Clasificación de Activos de Información de la Empresa XPERIA TECHNOLOGY CREDIT para Fortalecer los Procesos y Procedimientos asociados a la Tecnología Data LOSS PREVENTION - DLP.

Díaz Ricardo, Y., Pérez del Cerro, Y., & Proenza Pupo, D. (2 de junio de 2014). Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín. Obtenido de http://www.redalyc.org/pdf/1815/181531232002.pdf

Dinaluzf.blogspot. (2014). Metodologías para el análisis de riesgos. Obtenido de http://dinaluzf.blogspot.com/2014/12/margerit-metodologia-de-analisis.html

docplayer. (s.f.). 4.1 Entender la organización y su contexto A+ 5.3 Roles organizacionales, responsabilidades y autoridades. 5.1 Liderazgo y Compromiso. Obtenido de https://docplayer.es/16630761-4-1-entender-la-organizacion-y-su-contexto-a-5-3-roles-organizacionales-responsabilidades-y-autoridades-5-1-liderazgo-y-compromiso.html

Espinosa T., D., Martínez P., J., & Amador D., S. (2014). GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN CON BASE EN LA NORMA ISO/IEC 27005 DE 2011, PROPONIENDO UNA ADAPTACIÓN DE LA METODOLOGÍA OCTAVE-S. Ingenierías USBMed, 5(2), 33–43.

Fernández Parra, K., Garrido Saroza, A., Ramírez Martínez, Y., & Perdomo Bello, I. (Diciembre de 2015). PMBOK y PRINCE 2 similitudes y diferencias. Revista Científica, XXXIII, 111-123.

Freund, J., & Simon, G. (1992). Estadística elemental (8 ed.). México, México: Pearson.

Galdámez, P. (28 de mayo de 2017). Seguridad Informática. Obtenido de http://web.iti.upv.es/actualidadtic/2003/07/2003-07-seguridad.pdf

Gómes, Á. y. (2005). Sistemas de Información: herramientas prácticas para la gestión empresarial.

Hernández Sampieri, R., Collado Fernández, C., & Baptista Lucio, P. (29 de Enero de 2014). Metodología de la Investigación (Sexta ed.). (Interamericana, Ed.) Editorial mexicana. Recuperado el 22 de Marzo de 2016, de http://peru21.pe/economia/ccl-turismo-receptivo-creceria-6-2015-2210593

Hernández, Fernández y Baptista. (29 de Enero de 2010). CCL: Turismo receptivo en el Perú crecería 6% en 2015. Recuperado el 22 de Marzo de 2016, de http://peru21.pe/economia/ccl-turismo-receptivo-creceria-6-2015-2210593

Herrera , J., D'Armas , M., & Arzola, M. (2012). Análisis de los Diferentes Métodos de Mejora Continua. Obtenido de https://docplayer.es/1430239-Analisis-de-los-diferentes-metodos-de-mejora-continua.html

ISACA. (2012). Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. Obtenido de www.isaca.org/COBITuse.

iso27000. (2012). Sistema de Gestión de la Seguridad de la información. Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

Jímenez, R. J. (01 de febrero de 2010). Buenas prácticas de seguridad: Utiliza software de seguridad en tu(s) equipo(s) de cómputo. Obtenido de http://www.seguridad.unam.mx/descarga.dsc?arch=2164

Jimeno, B. J. (23 de Agosto de 2013). Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua. Obtenido de http://www.pdcahome.com/5202/ciclo-pdca/

LACHAPELLE, PECB, E., & BISLIMI, PECB, M. (2016). TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD. En P. Rreze HALILI (Ed.). Anders CARLSTEDT, Parabellum Cyber Security. Obtenido de www.pecb.com

Lara, M. (25 de abril de 2013). Investigación tecnológica. Obtenido de https://studylib.es/doc/5392952/investigacion-tecnologica

Ledezma Espin, D. N. (Diciembre de 2015). DESARROLLO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADAS EN LAS NORMAS ISO 27002 PARA UNA COORDINACIÓN ZONAL DEL INEC.

López. (Febrero de 2014). Actividades educativas. Recuperado el 31 de Enero de 2015, de Actividades educativas: ctaactividades.blogspot.com/2014_08_01archive.html

López Armendaris, D. (2017). Modelo de gestión de los servicios de tecnología de información basado en COBIT, ITIL e ISO/IEC 27000. Revista Tecnológica ESPOL – RTE, xxx(1), 51-69.

Merino Bada, C., & Cañizares Sales, R. (2014). AUDITORÍA DE SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI). Madrid, España: FUNDACION CONFEMETAL.

MINEDU, M. (23 de mayo de 2010). Estándares para el uso de herramientas de desarrollo de plataformas de aplicaciones web. Obtenido de http://www.minedu.gob.pe/ofin/xtras/EstndUsoHerramientDesarrolloAplicacionesWebV3.pdf

Monfort Casañ, R. (15 de Aosto de 2016). COBIT 5 y el Cuadro de Mando Integral como herramientas de Gobierno de TI. Repositorios UPV-Universidad Politécnica de Valencia, 12-14.

Montesino & Otros. (15 de abril de 2013). Gestión automatizada e integrada de controles de seguridad informática. Obtenido de Gestión automatizada e integrada de controles de seguridad informática: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1815-59282013000100004

Orrego, V. O. (Junio de 2011). La gestión en la seguridad de la información según Cobit, Itil e Iso 27000. Pensamiento Americano, 2(6), 21-23.

Otter, M., Sidi, J., & Hanaud, L. (200, 2009). Guide des Certifications SI (2e Édition ed.). Dunod, París.

Parra Alvernia, H., Contreras Navarro, J., Díaz Pacheco, D. Y., & López Ovalle, E. J. (10 de Abril de 2015). DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA COMUNITARIA DE ACUEDUCTO DE RÍO DE ORO, CESAR “EMCAR”. Repositorio ufpso.

Parra Alvernia, H., Contreras Navarro, J., Diaz Pacheco, D., & López Ovalle, E. (2015). DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA COMUNITARIA DE ACUEDUCTO DE RIO DE ORO, CESAR “EMCAR”. Repositorio UFPS.

Pdcahome. (1 de octubre de 2017). Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua. Obtenido de https://www.pdcahome.com/5202/ciclo-pdca/

Peñafiel, M. (15 de abril de 2013). Aplicaciones web. Obtenido de https://es.scribd.com/doc/136052164/APLICACIONES-WEB-pdf

PMG-SSI. (2015). ISO 27001: ¿Qué significa la Seguridad de la Información? Obtenido de https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

Puyol , J. (2016). Estrategias para hacer frente a las brechas de la seguridad de la información. Obtenido de https://confilegal.com/20160417-estrategias-frente-las-brechas-la-seguridad-la-informacion/

Ramírez Castro, A., & Ortiz Bayona, Z. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. 16(2), 56-66.

Siles, R. (15 de Marzo de 2008). Seguridad en aplicaciones Web: un enfoque práctico en el entorno universitario (UCLM). Obtenido de https://www.rediris.es/cert/doc/reuniones/fs2008/archivo/RedIRIS_VI_Seguridad_en_aplicaciones_Web_v1.0_RaulSiles.pdf

sis.se. (01 de 02 de 2010). https://www.sis.se/api/document/preview/911960/. Obtenido de https://www.sis.se/api/document/preview/911960/

Solarte Solarte, F., Enriquez Rosero, E., & Benavides Ruano, M. (Diciembre de 2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica ESPOL – RTE, Vol. 28(N. 5).

Suarez Gonzales, R. (18 de julio de 2018). ANALISIS DE ACTIVOS DE INFORMACION PARA UN SISTEMA MISIONAL BASADOS EN LA METODOLOGIA MAGERIT V3 Y LA NORMA ISO 27001:2013. Repositios UNAD.

Tristán. (29 de Enero de 2008). CCL: Turismo receptivo en el Perú crecería 6% en 2015. Recuperado el 22 de Marzo de 2016, de http://peru21.pe/economia/ccl-turismo-receptivo-creceria-6-2015-2210593

UNED. (28 de mayo de 2017). Aplicaciones WEB. Obtenido de http://meteo.ieec.uned.es/www_Usumeteo2/Memoria/Capitulo3.pdf

Uniovi. (s.f.). Seguridad)de)la)información. Obtenido de 2018: http://isa.uniovi.es/docencia/SIGC/pdf/certificados.pdf

urg.es. (2009). www.ugr.es. Obtenido de https://www.ugr.es/~rescate/practicum/el_m_todo_de_observaci_n.htm

Valencia Duque, F. J., & Orozco Alzate, M. (1 de Mayo de 2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. Revista Ibérica de Sistemas y Tecnologías de Información.

Vasirani, H. &. (15 de abril de 2000). Seguridad Informatica. Obtenido de http://www.ia.urjc.es/cms/sites/default/files/userfiles/file/SEG-I/2012/introduccion.pdf

Velasco, M. H. (15 de junio de 2011). El Derecho Informático y la Gestión de la Seguridad de la Información una perspectiva con base en la norma ISO 27001,. Obtenido de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-86972008000100013

Voutssas, J. (6 de abril de 2011). Preservación documental digital y seguridad informática. Obtenido de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008

Wang, C.-H. (2010). Integrated Installing ISO 9000 and ISO 27000 Management. New York: Princel.

Wigodski, J. (14 de Julio de 2014). jacquelinewigodski.bolgspot.com. Recuperado el 19 de Enero de 2015, de jacquelinewigodski.bolgspot.com: http://jacquelinewigodski.bolgspot.com

www.isotools.org. (s.f.). Norma ISO 31000: el valor de la gestión de riesgos en las organizaciones. Obtenido de https://www.isotools.org/pdfs-pro/ebook-iso-31000-gestion-riesgos-organizaciones.pdf

Zacarias Villafranca, J. C. (2017). MODELO DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA ISO/IEC 27001:2013 PARA MITIGAR LOS RIESGOS DE LOS ACTIVOS DE INFORMACIÓN EN LA CENTRAL DE OPERACIONES POLICIALES EN LA REGIÓN POLICIAL JUNÍN. Repositorio Institucional Continental.

ANEXO 01: Resolución de aprobación del proyecto de tesis

USS | UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N° 0651-2019/FIAU-USS

Chiclayo, 11 de junio de 2019

VISTO:

El Acta de Reunión N° 0606-2019/FIAU-IC-USS de fecha 06 de junio de 2019, del Comité Evaluador de la Escuela Académico Profesional de **INGENIERÍA DE SISTEMAS,** donde se propone la aprobación de la modificación de título de la tesis presentada por el(los) tesista(s) **SEGURA HUAMÁN MAVILA**; y

CONSIDERANDO:

Que, de conformidad con la Ley Universitaria N° 30220 en su artículo 48° que a la letra dice: *"La investigación constituye una función esencial y obligatoria de la universidad, que la fomenta y realiza, respondiendo a través de la producción de conocimiento y desarrollo de tecnologías a las necesidades de la sociedad, con especial énfasis en la realidad nacional. Los docente, estudiantes y graduados participan en la actividad investigadora en su propia institución o en redes de investigación nacional o internacional, creadas por las instituciones universitarias públicas o privadas.";*

Que, mediante Resolución de Facultad N° 0352-2017/FIAU-USS de fecha 04 de agosto de 2017 se aprobó el Proyecto de Tesis titulado "DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA PARA LAS APLICACIONES WEB DEL ÁREA DEL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA UNIVERSIDAD NACIONAL INTERCULTURAL ?FABIOLA SALAZAR LEGUÍA? - BAGUA", presentado por el(los) tesista(s) SEGURA HUAMÁN MAVILA;

Que, es necesario facilitar el adecuado desarrollo de las Tesis aprobadas con la finalidad de dar continuidad al proceso de investigación; y

Estando a lo expuesto, en uso de las atribuciones conferidas y de conformidad con las normas y reglamentos vigentes;

SE RESUELVE:

ARTÍCULO 1°: APROBAR la modificación de título de la Tesis denominada: *"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA PARA LAS APLICACIONES WEB DEL ÁREA DEL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA UNIVERSIDAD NACIONAL INTERCULTURAL ?FABIOLA SALAZAR LEGUÍA? - BAGUA",* por el siguiente: ***"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: CASO DE ESTUDIO UNIVERSIDAD NACIONAL INTERCULTURAL FABIOLA SALAZAR LEGUIA",*** presentada por el(los) tesista(s) **SEGURA HUAMÁN MAVILA,** de la Escuela Académico Profesional de **INGENIERÍA DE SISTEMAS.**

ARTÍCULO 2°: MODIFICAR la Resolución de Asesor Especialista N° 0333-2017/FIAU-USS de fecha 04 de agosto de 2017 y Resolución de Aprobación de Proyecto N° 0352-2017/FIAU-USS de fecha 04 de agosto de 2017, en el extremo que dice: *"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA PARA LAS APLICACIONES WEB DEL ÁREA DEL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA UNIVERSIDAD NACIONAL INTERCULTURAL ?FABIOLA SALAZAR LEGUÍA? - BAGUA",* por lo siguiente: ***"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: CASO DE ESTUDIO UNIVERSIDAD NACIONAL INTERCULTURAL FABIOLA SALAZAR LEGUIA".***

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

USS UNIVERSIDAD SEÑOR DE SIPÁN S.A.
Dr. Andrés Alberto Ruiz Gómez
DECANO DE LA FACULTAD DE INGENIERÍA ARQUITECTURA Y URBANISMO

UNIVERSIDAD SEÑOR DE SIPÁN S.A.C.
Mg. Luis Roberto Larrea Colchado
SEC. ACADEMICO FACULTAD DE INGENIERIA ARQUITECTURA Y URBANISMO

Cc: CPGYT, Interesados, Archivo

ADMISIÓN E INFORMES
074 481610 - 074 481632
CAMPUS USS
Km. 5, carretera a Pimentel
Chiclayo, **Perú**

www.uss.edu.pe

ANEXO 02: Autorización para la recolección de datos

Bagua, 04 de mayo de 2017

Carta Nº 10- 2017-UNFSL-B/CO/P

Señora,
MAVILA SEGURA HUAMÁN

Av. Mariscal Castilla Nº 1420, Sector Pueblo Libre
JAÉN.-

Asunto: Autoriza otorgar información exclusiva para desarrollar Tesis de Pre grado

---

Es muy grato dirigirme a usted, para expresarle mi cordial saludo y desearle muchos éxitos en su gestión, en representación de la Universidad Nacional Intercultural "Fabiola Salazar Leguía" de Bagua (UNIFSL-8) que me honro presidir. El motivo del presente, es para comunicarle que se autoriza otorgar información exclusiva para el desarrollo de la Tesis de Pre grado denominada "Diseño de un Sistema de Gestión de Seguridad de la Información: Caso de estudio Universidad Nacional intercultural Fabiola Salazar Leguía".

Por tal motivo, usted coordinará con el Ing. Luis Hebert Sánchez Sandoval, Jefe de la Oficina de Tecnologías de la Información de esta casa superior de estudios.

Es propicia la oportunidad, para desearle éxitos en su gestión y renovarle las muestras de afecto y estima personal.

Atentamente,

UNIVERSIDAD NACIONAL INTERCULTURAL
"FABIOLA SALAZAR LEGUIA" DE BAGUA
Dr. Jorge Alberto Che Piu Salazar
PRESIDENTE (e) COMISION ORGANIZADORA DE LA UNIFSL

PCO/JLAG/cwhv
e.e. /Archivo.

Anexos de documentos del SGSI:

ANEXO 03: Reunión inicial de proyecto

REUNIÓN INICIAL DEL PROYECTO	< Logo >

REUNION INICIAL DEL PROYECTO	REVISIÓN N°	CÓDIGO
	FECHA Y HORA DE REUNIÓN	PÁGINA

Asistencia a reunión inicial del proyecto

Área asistente a reunión	Nombre	Abrev.	Correo

Justificación de inasistencia

Área asistente a reunión	Nombre	Correo

Agenda de trabajo

Tema	Beneficiario	Hora inicio	Descripción

Presidencia

Jefe del Proyecto

ANEXO 04: Documento de Aprobación del proyecto

DOCUMENTO DE APROBACIÓN DEL PROYECTO

LOGOTIPO DE LA ORGANIZACIÓN	**PROYECTO:**
	NOMBRE DEL DOCUMENTO:
	FECHA DE CREACIÓN:
	AUTOR:
	REVISIÓN:

DESCRIPCIÓN DEL PROYECTO:
DESCRIPCIÓN DEL PRODUCTO:
OBJETIVOS:
CRITERIOS DE ÉXITO:
REQUISITOS DE APROBACIÓN DEL PROYECTO:
FINALIDAD DEL PROYECTO:
ENTREGABLES PRINCIPALES:

JUSTIFICACIÓN DEL PROYECTO:
PRINCIPALES INTERESADOS:
RIESGOS INICIALES:
DURACIÓN E HITOS :
PRESUPUESTO:
SPONSOR:
DIRECTOR DEL PROYECTO:

ANEXO 05: Entrevista con los Stakeholders

FORMATO DE PREGUNTAS REALIZADAS EN LA ENTREVISTA AL JEFE DE TECNOLOGÍAS DE LA INFORMACIÓN.
1. ¿Sabe usted si la institución cuenta con un departamento de seguridad de la información con personal especializado? **Rpta:** …… …… …….. **2. ¿En la actualidad se adoptan políticas de seguridad para administrar la información?** **Si ( ) Enunciar** **No (x)** **Rpta:** …… …… …… **3. ¿Conoce usted sobre las políticas concernientes a la seguridad de la información de su trabajo?** ( ) Sí, las conozco completamente ( ) No, pero sé que existen. ( ) No existen ( ) No sé Si su respuesta es sí, indique si estas políticas son lo suficientemente robustas para solventar los problemas de la seguridad de la información en la universidad: …… …… **4. ¿Las funciones y responsabilidades se encuentran adecuadamente establecidos y designados al personal debidamente capacitados?**

Rpta:

……

……

……

5. ¿Existe el conocimiento y respaldo apropiados acerca de la arquitectura de riesgo y seguridad de la información

Rpta:

……

……

……

6. ¿Existe un control acerca del acceso sin autorización de personal, con el objeto de protección del equipo y sistemas que se gestionan en la universidad?

Rpta:

……

……

……

7. ¿Se efectúa de manera periódica el mantenimiento de los equipos computacionales de la universidad?

Rpta:

……

……

……

8. ¿Se ha realizado simulacros relacionado con la caída de los sistemas de información y de comunicación?

Rpta:

……

……

…….

9. ¿Se efectúan funciones para monitorear los sistemas de información manejados en la universidad?

Rpta:

……

……

……

10. Seleccione una opción de acuerdo a la siguiente pregunta. ¿Con que frecuencia ha sido víctima la institución de amenazas que violenten contra la seguridad de la información?

Cada día ( )

Cada semana ( )

Cada mes ( )

Cada 2 meses ( )

Cada 4 meses ( )

Anual

Nunca

ANEXO 06: Matriz de Stakeholders

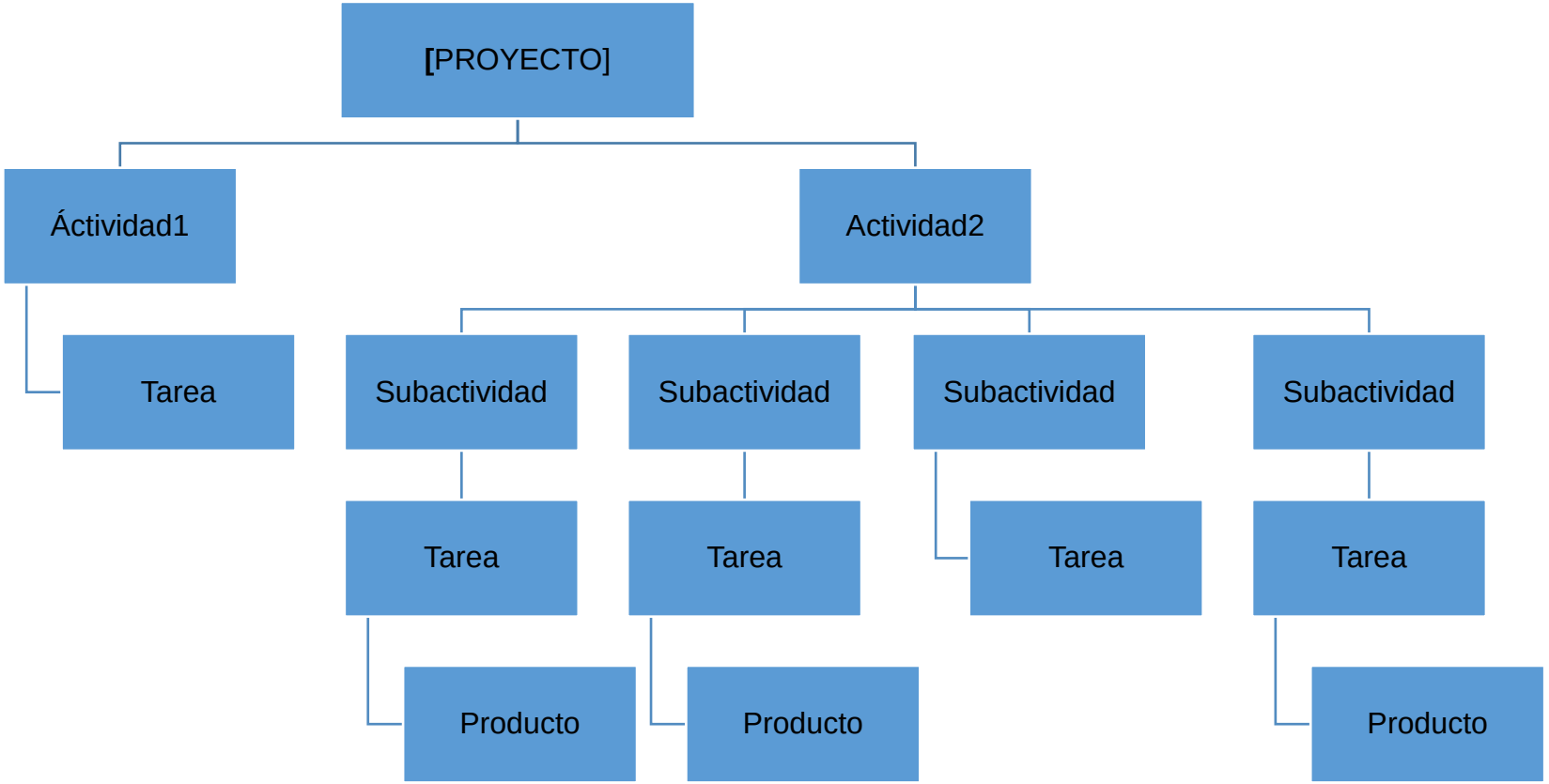
Matriz de Stakeholder					
Proyecto:					
Código:					
Fecha de Inicio:					
Stakeholder:					
Tipo:					
Objetivo o Resultados	**Nivel de Interés**	**Nivel de Influencia**	**Acciones Posibles**		**Estrategias**
			De impacto positivo	De impacto negativo	
Conclusiones:					

ANEXO 07: Plan del alcance del proyecto

<table>
<tr><td colspan="5">DOCUMENTO DEL ALCANCE DEL PROYECTO</td></tr>
<tr><td colspan="5">Estado Versión 0.0</td></tr>
<tr><td colspan="2">TITULO PROPUESTO DE PROYECTO: SGSI01</td><td colspan="3" rowspan="2">CLASIFICACION DE CONFIDENCIALIDAD
Uso General ☐ Uso interno Solamente ☐ Documento Confidencial ☐</td></tr>
<tr><td colspan="2">PATROCINANTE DEL PROYECTO:</td></tr>
<tr><td colspan="2">NUMERO DEL PROYECTO: 01</td><td colspan="3"></td></tr>
<tr><td colspan="5">ESPECIFICACIONES/PROPOSITO DEL PROYECTO:</td></tr>
<tr><td colspan="5">RESTRICCIONES DEL PROYECTO:</td></tr>
<tr><td colspan="5">FACTORES CRITICOS DE EXITO:</td></tr>
<tr><td colspan="5">SUPOSICIONES:</td></tr>
<tr><td colspan="5">DEPENDENCIAS:</td></tr>
<tr><td>PREPARADO POR:</td><td></td><td>FECHA</td><td>REVISIÓN</td><td>INICIALES</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>

ANEXO 08: EDT del Proyecto

PROYECTO	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO DE PROYECTO	
ELABORADO POR		FECHA DE ELABORACIÓN	



ANEXO 09: Identificación de activos

TIPO DE ACTIVO	
	[ ]
	[ ]
	[ ]
	[ ]
	[ ]
	[ ]
	[ ]
	[ ]
	[ ]
	[ ]
	[ ]
	[ ]
	[ ]
	[ ]
	[ ]

ANEXO 10: Inventario de activos

INVENTARIO DE ACTIVOS	CÓDIGO
[ESSENTIAL] ESENCIAL	
[D] DATOS/INFORMACIÓN	
[K] CLAVES CRIPTOGRÁFICAS	

[S] SERVICIOS	
[SW] APLICACIONES INFORMÁTICAS (SOFTWARE)	
[HW] EQUIPAMIENTO INFORMÁTICO (HARDWARE)	
[COM] REDES DE COMUNICACIONES	

[SI] SOPORTES DE INFORMACIÓN	
[AUX] EQUIPAMIENTO AUXILIAR	
[I] INSTALACIONES	
[P] PERSONAL	

ANEXO 11: Valoración de Activos

Valoración de activos teniendo en cuenta las dimensiones de seguridad

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

UNIFSL-BAGUA
Fecha elaboración: **Fecha aprobación:**

Inventario de activos								Valoración de activos			Valoración Final	Gestión	
N°	Nombre del activo	Descripción del activo	Tipo de activo	Ubicación	Unidad responsable	Responsable	Custodio	Disponibilidad	Integridad	Confidencialidad		Fecha de ingreso:	Fecha de salida:
1													
2													

3													
4													
5													
6													
7													
8													
9													
10													
11													
12													
13													
14													
15													
16													

17												
18												
19												
20												
21												
22												
23												
24												
25												
26												
27												
28												
29												
30												

31													
32													
33													
34													
35													
36													
37													
38													
39													
40													
41													
42													
43													
44													

45													
46													
47													
48													
49													
50													
51													
52													
53													
54													
55													

Elaborado por:

Firma:

_____

Cargo:

_____

Aprobado por:

Firma:

_____

Cargo:

_____

ANEXO 12: Identificación de Amenazas

Origen de las amenazas		
Deliberado	**D**	Acciones Voluntarias
Accidental	**A**	Acciones humanas
Ambiental	**E**	Acciones no humanas

Tipo	Amenaza	Origen
Daño Físico		
Eventos Naturales		
Fallo de Servicios esenciales		
Radiación		
Compromiso de la información		
Fallas técnicas		
Acciones no autorizadas		
Compromiso de funciones		

ANEXO 13: Identificación de Vulnerabilidades

LISTA DE VULNERABILIDADES

TIPO	Cod	VULNERABILIDAD
HARDWARE	H1	
	H2	
	H3	
	H4	
	H5	
	H6	
	H7	
	H8	
	H9	
SOFTWARE	S1	
	S2	
	S3	
	S4	
	S5	
	S6	
	S7	
	S8	
	S9	
	S10	
	S11	
	S12	
	S13	
	S14	
	S15	
	S16	
	S17	
	S18	
	S19	
	S20	

	S21	
RED	R1	
	R2	
	R3	
	R4	
	R5	
	R6	
	R7	
	R8	
	R9	
PERSONAL	P1	
	P2	
	P3	
	P4	
	P5	
	P6	
	P7	
	P8	
LUGAR	L1	
	L2	
	L3	
	L4	
ORGANIZACIÓN	O1	
	O2	
	O3	
	O4	
	O5	
	O6	
	O7	
	O8	
	O9	
	O10	

	O11	
	O12	
	O13	
	O14	
	O15	
	O16	
	O17	
	O18	
	O19	
	O20	

ANEXO 14: Identificación de Riesgos

LISTA DE RIESGOS

Lista de Riesgos potenciales	
Hardware	
Software	
Seguridad Física	
Seguridad Lógica	
Redes de Comunicaciones	
Personal	

TIPO DE RIESGOS	CÓD.	DESCRIPCIÓN
Hardware		
Software		

Seguridad Física		
Seguridad Lógica		
Redes de Comunicaciones		
Personal		

ANEXO 15: Análisis preliminar de riesgos

NOMBRE DEL PROYECTO:	
CÓDIGO DEL PROYECTO:	
DIRECTOR DEL PROYECTO:	
FECHA DE ELABORACIÓN:	

HISTORIAL DE VERSIONES			
FECHA Y HORA	**N° DE VERSIÓN**	**DESCRIPCIÓN**	**ELABORADO POR**

PROPÓSITO DEL PLAN DE GESTIÓN DE RIESGOS DEL PROYECTO

ROLES Y RESPONSABILIDADES

ROL	**RESPONSABILIDADES**
Interesado 1	
Interesado 2	
Interesado 3	
Interesado 4	
Interesado n	

SEGUIMIENTO Y AUDITORÍA

CONTROL DE LOS RIESGOS

APROBACIÓN

Nombre	Cargo	Firma	Fecha
	Iniciador/Patrocinador del Proyecto		
	Director del Proyecto		

ANEXO 16: Análisis de riesgos

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO

PROBABILIDAD	VALOR NUMÉRICO	IMPACTO	VALOR NUMÉRICO
Muy Improbable		Muy Bajo	
Relativamente Probable		Bajo	
Probable		Moderado	
Muy Probable		Alto	
Casi Certeza		Muy Alto	

TIPO DE RIESGO	PROBABILIDAD X IMPACTO
Muy Alto	
Alto	
Moderado	
Bajo	
Muy Bajo	

CÓDIGO DEL RIESGO	DESCRIPCIÓN DEL RIESGO	CAUSA RAIZ	TRIGGER	ESTIMACIÓN DE PROBABILIDAD	ESTIMACIÓN DE IMPACTO	PROB. X IMPACTO	TIPO DE RIESGO

ANEXO 17: Políticas de seguridad de la información

<table>
<tr><td rowspan="3">LOGO</td><td colspan="2">POLÍTICAS</td></tr>
<tr><td colspan="2">POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</td></tr>
<tr><td>No:</td><td>Página:</td></tr>
<tr><td colspan="3">
1. INTRODUCCIÓN

2. OBJETIVOS

3. ALCANCE

4. CUMPLIMIENTO Y CONFORMIDAD

5. MARCO LEGAL

6. MARCO REFERENCIAL

7. OBJETIVOS DE CONTROL Y CONTROLES

8. POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

Políticas Generales de Seguridad de la Información

• Política de control de acceso
• Política de clasificación y manejo de la información
• Política de seguridad física y ambiental
• Política de temas finales orientados al usuario, tales como:
</td></tr>
</table>

- Política de uso aceptable de activos
- Política de escritorio y pantalla limpios
- Política de transferencia de información
- Política de dispositivos móviles y teletrabajo
- Política de restricciones a las instalaciones y uso del software
- Política de copia de seguridad
- Política de protección contra software malicioso
- Política de gestión de vulnerabilidades
- Política de controles criptográficos
- Política de seguridad de las comunicaciones
- Política de relación con los proveedores

- Política para los recursos humanos

ANEXO 18: Tratamiento de Riesgos

Activos de información	Responsable del activo	Amenazas	Vulnerabilidades	Tratamiento del riesgo	
				Opción de tratamiento del riesgo	Controles o Salvaguardas

ANEXO 19: Declaración de aplicabilidad

DECLARACIÓN DE APLICABILIDAD

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN			
A.1	**Control de acceso**		

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.2	**CLASIFICACCIÓN Y MANEJO DE LA INFORMACIÓN**		
A.2.1	**Clasificación de la información**		
A.2.2	**manejo de la información**		

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.3	**SEGURIDAD FÍSICA Y AMBIENTAL**		
A.3.1	**Controles de acceso perimetral**		
A.3.2	**Controles ambientales**		

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.4	**SEGURIDAD ORIENTADOS AL USUARIO**		
A.4.1	**USO ACEPTABLE DE ACTIVOS**		
A.4.1.1	**Correo electrónico**		

A.4.1.2	Navegación en internet		

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.4	SEGURIDAD ORIENTADOS AL USUARIO		
A.4.2	Escritorio y pantalla limpia		

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.4	SEGURIDAD ORIENTADOS AL USUARIO		
A.4.3	Dispositivos móviles y teletrabajo		

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.4	SEGURIDAD ORIENTADOS AL USUARIO		
A.4.4	Restricciones a las instalaciones y uso de software		

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.4	SEGURIDAD ORIENTADOS AL USUARIO		
A.4.5	Copia y seguridad		

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.4	SEGURIDAD ORIENTADOS AL USUARIO		
A.4.6	Protección contra software malicioso		

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.4	SEGURIDAD ORIENTADOS AL USUARIO		
A.4.7	Controles criptográficos		

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.4	SEGURIDAD ORIENTADOS AL USUARIO		
A.4.8	Seguridad de las comunicaciones		

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.4	SEGURIDAD ORIENTADOS AL USUARIO		
A.4.9	Relación con los proveedores		
CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.5	SEGURIDAD DE LOS RECURSOS HUMANOS		
A.5.1	Seguridad para los Recursos Humanos		

ANEXO 20: Plan de Auditoría

PLAN DE AUDITORÍA	
OBJETIVO	
ALCANCE	
RESPONSABLE	**ÁREAS INVOLUCRADAS**

COSTO APROXIMADO	
PLAZO DE CONSECUCIÓN	
TIEMPO ESTIMADO DE EJECUCIÓN	
ACTIVIDADES	

ANEXO 21: Seguimiento

SEGUIMIENTO DE LAS POLÍTICAS DE SGURIDAD			
DOMINIO / OBJETIVO DE CONTROL	**DÍA**	**INTERLOCUTOR**	**OBSERVACIONES**
Control de acceso			
Clasificación y manejo de la Información			
Seguridad física y ambiental			
Seguridad orientados al usuario			
Seguridad para los recursos humanos			

ANEXO 22: Matriz RACI

RESPONSABILIDADES	
RESPONSABLE	**R**
ADMINISTRADOR (SUPERVISOR)	**A**
CONSULTAR	**C**
INFORMAR	**I**

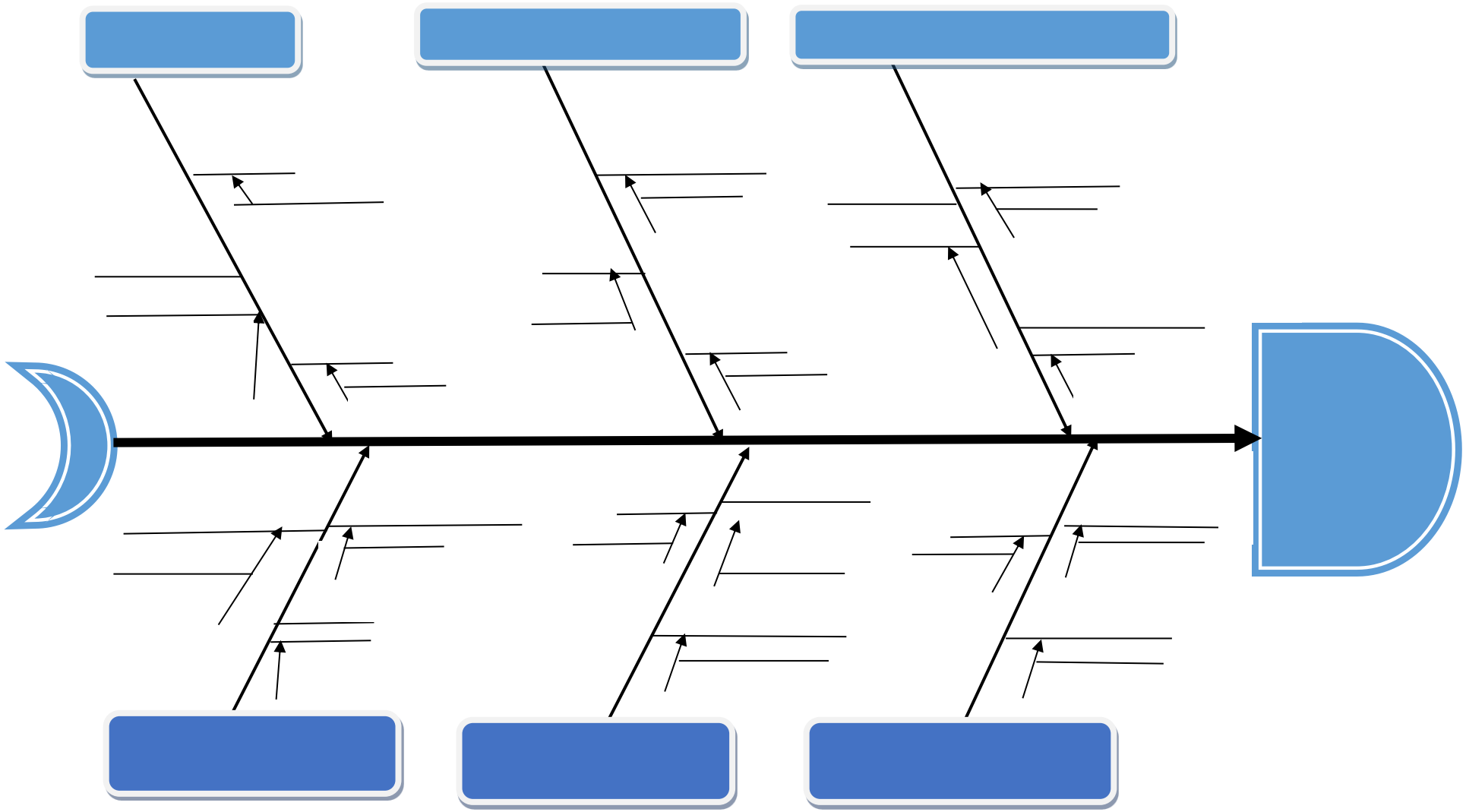
ACTIVIDADES	Comisión Organizadora	Equipo del proyecto	Jefe de Tecnologías de la Información	Personal

ANEXO 23: Informe Final de Auditoría

Informe de Auditoría			
Proceso(s) Auditado(s):			
Alcance de la auditoria:			
Norma(s) de referencia para la realización de la auditoria:			
Auditor Principal:		Equipo Auditor:	
Fecha de realización de la auditoria:		Fecha de presentación del informe:	
Auditado(s):			
Herramientas de trabajo utilizados en la auditoria:			

Documento(s) Revisados			Ref. Cláusula/ Control
Estado del Sistema de Gestión (Cantidad y Detalle):			
Fortalezas:			
Oportunidades de Mejora:			
No conformidades:			
Conclusiones:			
Firma del auditor principal:		Fecha:	

ANEXO 24: Diagrama causa efecto



ANEXO 25: Tratamiento de No Conformidades

LOGO	**INFORME DE NO CONFORMIDAD**	
	PROCEDENTE DE:	**N° No Conformidad:**
		Fecha:

IDENTIFICACIÓN DE LA NO CONFORMIDAD	
PROCESO/S:	
DESCRIPCIÓN: **Evidencias:**	
DETECTADA POR:	**FIRMA RESPONSABLE PROCESO AUDITADO:**
.	
Auditor Jefe:	**Nombre:**
observación:	

ANEXO 26: Plan de Mejora Continua

PLAN DE MEJORA CONTINUA			Fecha: Edición:	
Elaborado por:	Revisado por:		Aprobado por:	
I. OBJETIVO				
II. APLICACIÓN	() General		() Específica	
III. ALCANCE				
IV. DEFINICIONES				
V. RESPONSABILIDADES				
VI. DESCRIPCIÓN DE LAS ACTIVIDADES				