UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE ARQUITECTURA E INGENIERÍAS

TRABAJO DE INVESTIGACIÓN DE FIN DE CARRERA

TITULADO:

DISEÑO DE UN MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL SISTEMA ACADÉMICO DE LA UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ

REALIZADO POR:

Ing. Carlos Conforme Sornoza

DIRECTOR DEL PROYECTO

Ing. Edison Estrella, MBA

COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE:

MASTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD Y REDES

Quito, 20 de noviembre del 2018

DECLARACIÓN JURAMENTADA

Yo, CARLOS EMILIO CONFORME SORNOZA, con cédula de identidad número 131189260-6, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y, que ha consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido en por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

Carlos Emilio Conforme Sornoza

C.C: 1311892606

DECLARATORIA

El presente trabajo de investigación titulado:

“DISEÑO DE UN MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL SISTEMA ACADÉMICO DE LA UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ”

Realizado por:

CARLOS EMILIO CONFORME SORNOZA

como Requisito para la Obtención del Título de:

MASTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD Y REDES

Ha sido dirigido por el profesor

Ing. Edison Estrella, MBA

quien considera que constituye un trabajo original de su autor

Ing. Edison Estrella, MBA

DIRECTOR

Los Profesores Informantes:

Ing. Verónica Rodríguez, MBA

Ing. Christian Pazmiño, MGS

Después de revisar el trabajo presentado,

lo han calificado como apto para su defensa oral ante el tribunal examinador

Ing. Verónica Rodríguez, MBA

Ing. Christian Pazmiño, MGS

Quito, 20 de noviembre del 2018

DEDICATORIA

A mi familia; quienes con su apoyo incondicional han motivado la superación profesional y personal en este arduo y complicado camino, deseándome siempre lo mejor a cada paso.

A mis profesores; quienes mantuvieron siempre la ideología de apoyarme incondicionalmente en cada ciclo de estudios cursado.

A mis compañeros maestrantes; quienes mostrando esfuerzo me motivaron a seguirlos acompañando en este sueño ahora hecho realidad.

AGRADECIMIENTO

Al Docente Ing. Edison Estrella quien, con su acertada dirección en este proyecto de investigación, mostro un excelente profesionalismo en el desarrollo este documento.

A los Docentes Ing. Christian Pazmiño, Ing. Verónica Rodríguez quienes, gracias a su gran experiencia, conocimientos y dedicación a la revisión de este trabajo aportaron acertados criterios para mejora del mismo.

Índice General de Contenido

CAPÍTULO I 12

INTRODUCCIÓN 12

1.1. EL PROBLEMA DE INVESTIGACIÓN 13
1.1.1. Planteamiento del Problema 13
1.1.2. Formulación del Problema 18
1.1.3. Sistematización del Problema 18
1.1.4. Objetivo General 18
1.1.5. Objetivos Específicos 18
1.1.6. Justificaciones 19
1.1.7. Estado del Arte 21

CAPÍTULO II 25

MARCO TEÓRICO 25

2.1. Consejo de Educación Superior 25
2.2. Base Legal UNESUM 25
2.3. Contraloría General del Estado 26
2.4. Información 27
2.5. Amenaza Informática 27
2.6. Incidentes Naturales 27
2.7. Incidentes Humanos 28
2.8. Ataques Informáticos 29
Estructura de un Ataque informático 29
2.9. Sistema de Información Académico 30
2.10. Sistema de Gestión de Seguridad de la Información (SGSI) 30
2.10.1. Ciclo de Mejora Continua - PDCA 30
2.11. Seguridad de la Información 34
2.12. ISO/IEC 27002 35

CAPÍTULO III 38

ANÁLISIS SITUACIONAL 38

3.1. SITUACIÓN ACTUAL 38
3.1.1. Descripción técnica 41
3.1.1.1. Servidores 41
3.1.1.2. Sistemas de Información 41
3.2. Análisis de Riesgos 42
3.2.1. Propósito 42
3.2.2. Alcance 42
3.2.3. Identificación y Clasificación de Activos de Información 43
3.2.3.1. Valoración de Activos de Información 12
3.2.3.2. Identificación de Amenazas y Vulnerabilidades 13
3.2.4. Evaluación del Riesgo 14
3.3. Análisis de controles de la norma ISO 27002:2017 17

3.3.1. MAPA DE CONTROLES ISO 27002:2017 18
3.3.2. IDENTIFICACIÓN DE CONTROLES ISO 27002:2017 26
CAPÍTULO IV 27
PROPUESTA 27
4.1. MODELO SISTEMA DE GESTIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN 27
4.2. FASE I: PLANIFICACIÓN 28
4.2.1. ALCANCE DEL SGSI 28
4.2.2. MARCO REGULATORIO 28
4.2.3. ANÁLISIS Y EVALUACIÓN DEL RIESGO 31
4.2.4. IDENTIFICACIÓN Y SELECCIÓN DE CONTROLES ISO 27002:2017 31
4.2.5. IMPLEMENTACIÓN DE LOS CONTROLES ISO 27002:2017 SELECCIONADOS 32
4.2.6. APROBACIÓN DEL INMEDIATO SUPERIOR 38
4.2.7. AUTORIZACIÓN PARA LA IMPLEMENTACIÓN DEL SGSI 38
4.2.8. ELABORACIÓN DE LA DECLARACIÓN DE APLICABILIDAD 39
4.3. FASE II: IMPLEMENTACIÓN Y UTILIZACIÓN DEL SGSI 39
4.4. FASE III: MONITORIZAR Y REVISAR EL SGSI 41
4.4.1. LINEAMIENTOS PARA EL MONITOREO DEL SGSI 41
4.5. FASE IV: MANTENER Y MEJORAR EL SGSI 41
4.5.1. LINEAMIENTOS PARA LA MEJORA DEL SGSI 41
4.5.1.1. ACCIONES CORRECTIVAS 42
CAPÍTULO V 43
CONCLUSIONES Y RECOMENDACIONES 43
5.1. CONCLUSIONES 43
5.2. RECOMENDACIONES 44
BIBLIOGRAFÍA 46

Índice de Tablas

Tabla 1 Descripción Técnica de Servidores. 41
Tabla 2 Matriz Identificación Valoración de Activos de información. 12
Tabla 3 Valoración de Activos. 12
Tabla 4 Valoración de los Activos de Información. 13
Tabla 5 Matriz para la identificación de Amenazas y Vulnerabilidades. 14
Tabla 6 Probabilidad de que ocurra la amenaza. 15
Tabla 7 Impacto causado por la probabilidad de amenaza. 15
Tabla 8 Valores para Estimación del Riesgo. 16
Tabla 9 Matriz Identificación Nivel de Riesgo expuesto. 16
Tabla 10 Mapa Controles ISO 27002:2017. 18
Tabla 11 Matriz para la identificación de Controles ISO 27002. 26
Tabla 12 Identificación y selección de Controles ISO 27002. 32
Tabla 13 Matriz sugerida para la elaboración de la Declaración de Aplicabilidad. 39

Índice de Figuras

Figura 1: Árbol del Problema. 17
Figura 2: Amenazas Informáticas. 29
Figura 3: Ciclo Deming 34
Figura 4 Sistema Académico Unesum. 38
Figura 5 Esquema Servidores UNESUM. 39

Índice de Anexos

ANEXO A 49
ANEXO B 51
ANEXO C 53

Resumen

Los sistemas de información se han convertido en una necesidad para las instituciones sean estas públicas o privadas, mismas que se ven beneficiadas manteniendo el acceso a la información en tiempo real hacia sus usuarios finales.

Las universidades del país optan por desarrollar sistemas informáticos para agilizar sus procesos académicos y así brindar facilidades a sus estudiantes mediante el acceso a su información en cualquier momento y lugar, los mismos contienen información relevante para los procesos internos de cada una. Manteniendo presente que la protección de la información debe ser primordial nace la investigación aquí presentada.

El desarrollo de la misma contempla un análisis de la situación actual de la gestión de la seguridad de la información (SGSI), la identificación de las amenazas de mayor impacto en cuanto a la gestión de la seguridad de la información, el análisis de la norma ISO/IEC 27002:2017, para finalmente lograr el desarrollo de un modelo SGSI como herramienta guía para la aplicación de lineamientos de seguridad en el sistema académico de la Universidad Estatal del Sur de Manabí.

El análisis de la situación actual previa revisión documental determina que la gestión de la seguridad de la información tiene muy poca acogida, evidenciando la no existencia de normativas de seguridad de información para el sistema académico.

La identificación de las amenazas de mayor impacto del sistema académico mediante un análisis de riesgos determina que producto de la falta de normativas ha dado lugar a incidentes de seguridad afectando la integridad, confidencialidad y seguridad de la información.

Los resultados del análisis de riesgos conllevaron al análisis de la norma ISO/IEC 27002:2017 la cual contiene controles de seguridad de la información permitiendo identificar los más acordes a ser tomados en consideración para mitigar los vacíos de seguridad revelados.

Todo el proceso descrito ha permitido desarrollar un modelo de sistema de gestión de seguridad de la información para el sistema de información académico basado en el estándar internacional ISO/IEC 27002:2017 como apoyo al personal informático de la Universidad Estatal del Sur de Manabí permitiéndoles desarrollar sus lineamientos de seguridad de la información acordes a la necesidad institucional, mismo que permitirá incorporar integridad, confidencialidad y seguridad.

Palabras claves: Seguridad informática, Gestión, SGSI, ISO 27002:2017

Summary

Information systems have become a necessity for institutions, whether public or private, which benefit from maintaining access to information in real time to their end users.

The universities of the country choose to develop computer systems to streamline their academic processes and thus provide facilities to their students by accessing their information at any time and place; they contain relevant information to the internal processes of each one of them. Keeping in mind that the protection of information must be paramount, the research presented here is born.

The development of the same one contemplates an analysis of the current situation of the management of the security of the information (SMSI), the identification of the threats of greater impact regarding the management of the security of the information, the analysis of the norm ISO / IEC 27002: 2017, to finally achieve the development of an SMSI as a guide tool for the application of safety guidelines in the academic system of the Southern State University of Manabí.

The analysis of the current situation after documentary review determines that the management of information security has very little reception, evidencing the absence of information security regulations for the academic system.

The identification of threats with the greatest impact of the academic system through a risk analysis determines that product of the lack of regulations has led to security incidents affecting the integrity, confidentiality and security of information.

The results of the risk analysis led to the analysis of the ISO / IEC 27002: 2017 standard, which contains information security controls allowing the identification of the most appropriate to be taken into consideration to mitigate the security gaps revealed.

The entire process described has allowed the development of an information security management system for the academic information system based on the international standard ISO / IEC 27002: 2017 as a support to the computer staff of the Southern State University of Manabí, allowing them to develop their guidelines of information security according to the institutional need, which will allow incorporating integrity, confidentiality and security.

Keywords: Computing Security, Management, ISMS, ISO 27002: 2017

CAPÍTULO I

INTRODUCCIÓN

Actualmente la tecnología se ha convertido en un instrumento esencial para las organizaciones en general, concibiendo información digital con ayuda de las diferentes herramientas informáticas que se desarrollan o se adquieren, manteniendo el oportuno acceso a los datos desde cualquier lugar del mundo, ocasionando que la información tome un valor incalculable para las organizaciones y se considere como el activo más importante a ser protegido frente a delitos informáticos.

La Universidad Estatal del Sur de Manabí es un centro de educación superior, sus procesos académicos y administrativos están evolucionando gracias a las tecnologías de Información fortaleciendo su operatividad institucional. Los sistemas informáticos: sistema académico UNESUM-S@U, sistema de evaluación de la gestión al Docente-SIEGDD, sistema de seguimiento a graduados-SSGU, Biblioteca Virtual, Aulas Virtuales, entre otros, se encuentran alojados en un pequeño centro de datos improvisado, donde los usuarios acceden con ayuda de internet.

El problema al mantener estos servicios en internet es que necesitan siempre contar con un monitoreo recurrente para identificar violaciones de seguridad, debido a que se pueden presentar dificultades en el acceso a los datos, y muchas veces los técnicos mantienen pocos criterios con respecto a la seguridad de la información.

Esto hace imprescindible que se cuente con sistemas de gestión de seguridad de la información que permitan al personal informático prevenir posibles pérdidas de información a causa de imprevistos o eventos catastróficos como: virus, ataques informáticos, caídas eléctricas, desastres naturales o medioambientales; ya que, del tiempo que tarde en reaccionar

la institución para recuperar y restaurar la información crítica, dependerá el impacto en el ámbito educativo, social y económico de la universidad, logrando así que la disponibilidad, integridad y confidencialidad de la información prevalezca ante cualquier evento que se presente.

1.1. EL PROBLEMA DE INVESTIGACIÓN

1.1.1. Planteamiento del Problema

La información digital ha pasado a adquirir un valor incalculable y actualmente es considerada el activo más importante para las organizaciones, se pude puntualizar que la seguridad de la información "Es el conjunto de sistemas y procedimientos que garantizan: la confidencialidad, la integridad y la disponibilidad de la información" (Navarro, 2000, p. 34).

En el Ecuador, las universidades alojan un sinnúmero de información digital concerniente a datos académicos de estudiantes, la misma es almacenada en su centro de datos y mediante un sistema informático, personal administrativo, docentes y estudiantes con los debidos accesos pueden hacer uso de esta herramienta de manera local o mediante Internet.

El sistema informático, dentro de las universidades es denominado comúnmente sistema académico y en muchos casos sin considerar buenas prácticas sobre gestión de seguridad de la información es puesto a consideración de los usuarios finales exponiéndose a sinnúmero de amenazas, las cuales pueden causar el robo, destrucción, divulgación y modificación de los datos.

Tal es el caso de la Universidad Estatal del Sur de Manabí (de aquí en adelante UNESUM), institución de educación superior que mediante su sistema académico (S@U) maneja un volumen de datos considerable, entre ellos se puede destacar: información de grados y títulos, certificados de estudios y registro de las notas que se otorgan a los estudiantes por parte de los docentes luego de cumplir con el programa de estudios, las cuales

acreditan su aprobación, reprobación o pérdida del mismo, todos estos datos se vuelven confidenciales y de vital importancia para el correcto desempeño de los procesos académicos.

Entonces, es aquí donde la gestión de la seguridad de la información puede volverse muy compleja desde el punto de vista organizativo. Al ser una universidad bajo gran demanda estudiantil necesita incorporar una planta docente y administrativa significativa, asignando diferentes funciones en su sistema académico.

Pues bien, mirando un poco más el lado organizativo se presentan las siguientes interrogantes tomando como ejemplo; el acceso al sistema académico depende de Internet , entonces ¿Quién debe gestionar que el recurso sea de buena calidad?, ¿Cómo se gestionan los incidentes causados por las amenazas informáticas?, ¿Cómo se gestiona la pérdida de los datos?, ¿Cómo se gestiona la seguridad sobre el acceso al sistema académico?, evidentemente el personal informático no ha considerado definir una manera de gestionar las respuestas a estas interrogantes, mientras que, desde el punto de vista técnico como un ejemplo generalizado, eliminar, bloquear, instalar actualizaciones dentro del mismo sistema académico no implica ninguna dificultad ya que el administrador toma las precauciones necesarias de forma inmediata.

Las amenazas están presentes y crecen año tras año, ocasionando, que todo entorno informático sea público o privado se vea afectado si su personal no tiene o adquiere conocimiento sobre la gestión de seguridad de la información, causando que los inconvenientes sean mayores al no tener el juicio para tratarlos.

Actualmente hay que tomar en consideración que las amenazas y riesgos de la información tales como sabotaje, violación de privacidad, hackers, interrupción de servicios, virus, y las futuras que se presenten tendrán como objetivo el secuestro, robo o pérdida de información.

Finalmente, la problemática radica en la falta de un modelo para la gestión de incidentes de seguridad de la información acorde a las necesidades del sistema académico de la UNESUM

que ayude al personal informático a considerar estrategias que abarquen el uso de buenas prácticas sobre seguridad de información reconocidas a nivel internacional, mismas que permiten la identificación de los riesgos críticos a los que se encuentra expuesto el sistema académico de la institución.

1.1.1.1. Diagnóstico del Problema

La revisión documental de tesis, libros y la norma ISO 27002:2017, permitió desarrollar un criterio ante la problemática. Se mantuvieron conversaciones con el jefe informático y se le solicito el respectivo permiso con el propósito de percibir la situación real, de la problemática que se presenta en la UNESUM, se visitaron dos sedes denominadas “Complejo Universitario” y “Campus los Ángeles” considerado el principal.

Con la ayuda de la herramienta ficha de observación (véase ANEXO B) se conoció lo siguiente:

- La administración y el acceso al sistema académico de la UNESUM se realiza vía Internet.
- No existen registros sobre incidentes informáticos.
- La base de datos se encuentra alojada en los mismos servidores virtuales donde están los servicios web encontrándose expuesta directamente a Internet.
- Los trabajos de mantenimiento al sistema académico se ejecutan de manera remota, dejando al mismo en ocasiones inoperativo.
- El servicio de Internet no es óptimo y se otorga mediante fibra óptica entre las sedes “Edificio Central”, “Complejo Universitario” y “Campus Los Ángeles”.
- El registro interno de datos en el sistema académico se realiza mediante Internet.
- Se presentan modificaciones en los registros de la base de datos del sistema académico producto de acceso no controlados o indebidos.

- No se mantiene un registro o historial de quienes acceden al sistema académico.
- No existe un manual de responsabilidades claro que permitan identificar cuál es el rol de cada usuario en la administración y uso del sistema académico.
- No se documentan los incidentes con respecto a la modificación no autorizada de la información.

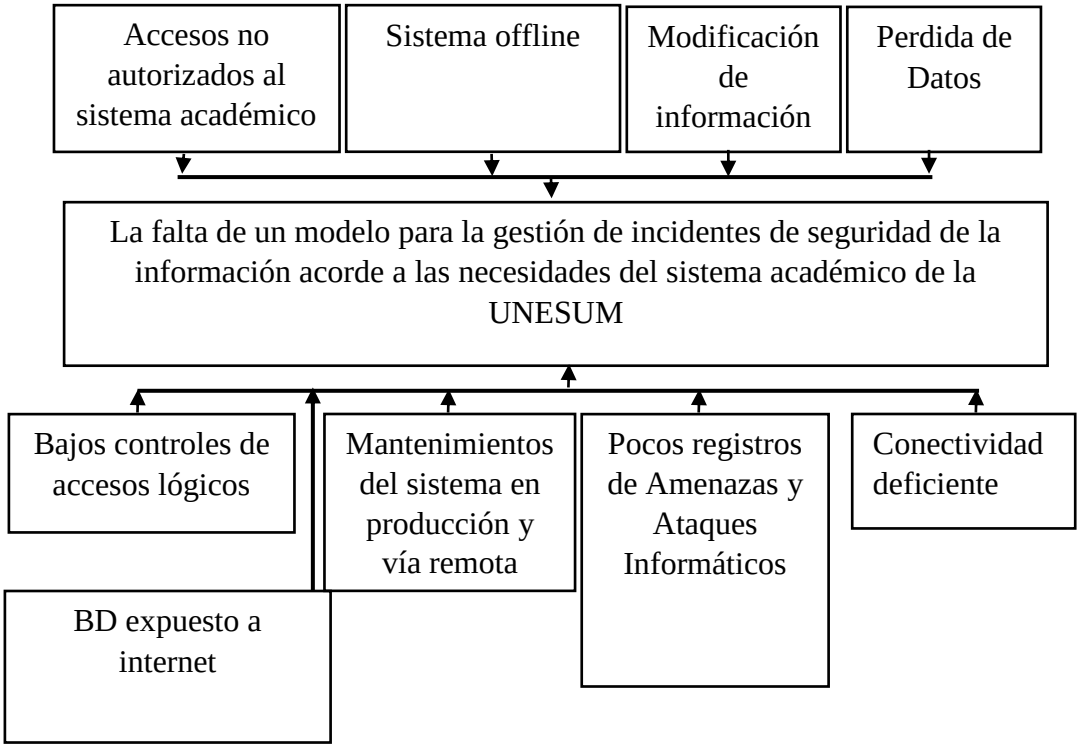
De igual manera se realizó una entrevista al jefe de informática (véase ANEXO C) con el objetivo de conocer los métodos aplicados en el manejo de la seguridad de la información, la misma reveló de manera general que a pesar de haberse presentado con frecuencia la modificación de los datos no se consideró aplicar alguna metodología que permita minimizar esta amenaza.

Así mismo se aplicó una encuesta sobre gestión de seguridad de la información (véase ANEXO A) a una muestra de doce técnicos de la unidad informática con el objetivo de determinar si existe un conocimiento básico sobre seguridad de la información.

Finalmente se diagnostica en base a lo expuesto que la falta de un modelo para la gestión de incidentes de seguridad de la información acorde a las necesidades del sistema académico de la UNESUM ocasiona que el personal informático no desarrolle una política para la seguridad de la información y esta pueda ser aplicada en el uso de su aplicación informática.

La Figura 1 muestra en resumen las causas y efectos de acuerdo al diagnóstico establecido anteriormente.

Figura 1: Árbol del Problema.
Fuente: Elaboración Autor



1.1.1.2. Pronóstico

Se pronostica que, de no adoptar un modelo para la gestión de incidentes de seguridad de la información acorde a las necesidades del sistema académico de la UNESUM, la información del mismo estará expuesta al robo, destrucción, divulgación y manipulación de sus datos.

1.1.1.3. Control del Pronóstico

Considerando que el sistema académico es de vital importancia para la UNESUM y la información a la que se accede mediante el mismo debe mantenerse siempre disponible, integra y confidencial, para el control del pronóstico será necesario:

Aportar con lineamientos para la adopción de un modelo que permita al personal informático implantar una política de seguridad de la información, incorporando buenas prácticas orientadas a la protección de los datos, y así gestionar los incidentes de seguridad del sistema académico de mejor manera.

1.1.2. Formulación del Problema

La falta de un modelo de gestión para incidentes de seguridad de la información como apoyo al personal informático de la UNESUM provoca que el sistema académico sea vulnerable.

1.1.3. Sistematización del Problema

¿Cómo determinar la situación actual sobre la gestión de seguridad de la información aplicada al sistema académico de la UNESUM?

¿Cómo identificar las amenazas a las que está expuesto el sistema académico de la UNESUM?

¿Cómo proteger al sistema académico de la UNESUM de las amenazas informáticas identificadas?

¿Cómo proveer un modelo de gestión de seguridad de la información para el apoyo personal de la unidad informática de la UNESUM?

1.1.4. Objetivo General

Diseñar un modelo de gestión de seguridad de la información para el sistema académico de la UNESUM mediante la aplicación de la norma ISO 27002:2017 que permita al personal informático implantar una política de seguridad.

1.1.5. Objetivos Específicos

- Analizar la situación actual del sistema académico de la UNESUM mediante el uso de técnicas de investigación que permitan la determinación de su proceso de gestión de seguridad.
- Identificar las amenazas a las que se expone el sistema académico de la UNESUM mediante un análisis de riesgos que permita reconocer las de mayor impacto.

- Elaborar un mapa de los controles mediante el análisis de la norma ISO 27002:2017 que permita escoger los más acordes a la necesidad del sistema académico de la UNESUM.
- Desarrollar un modelo de gestión para la seguridad de la información mediante el análisis de la norma ISO 27002:2017 que permita al personal informático establecer la política de seguridad para el sistema académico de la UNESUM.

1.1.6. Justificaciones

Legal:

Esta investigación se realiza en base al Acuerdo 039 - CG - 2009 expedido por la Contraloría general del Estado la cual expresa textualmente "Expedir las normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos" (CGE, 2009, p. 3), dicha norma en su apartado 410 TECNOLOGÍA DE LA INFORMACIÓN subsección 410-10 en donde expresa los lineamientos que se deben aplicar en los departamentos tecnológicos de entidades estatales con respecto a la seguridad de la información.

De la misma manera el modelo de evaluación institucional de universidades y escuelas politécnicas 2018 en su versión preliminar emitido por el Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior (CEAACES) en su criterio de evaluación 5.1.3 Sistemas Informáticos pone a consideración como uno de sus puntos fundamentales la aplicación de políticas, protocolos de seguridad y gestión de la información, que garantizan la confiabilidad y la confidencialidad de la información (CEAACES, 2018, p. 22).

Teórica:

Esta investigación se realiza con el objetivo de ofrecer un modelo de gestión de seguridad de la información que permita tratar incidentes de seguridad basado en una norma

internacional mediante la implantación de una política de seguridad dentro de las instituciones de educación superior, manteniendo como referencia las buenas prácticas internacionales con el fin de generar un mejor criterio ante los directivos de las instituciones en cuanto a la protección de la información.

Metodológica:

Para lograr el objetivo de la investigación se consideró usar la metodología PDCA la cual ha sido considerada en varias investigaciones ya realizadas por otros autores obteniendo resultados favorables y a su vez permitió desarrollar criterio sobre sus cuatro fases, permitiendo:

- Planificar diversas actividades en cuanto al desarrollo del sistema de gestión,
- Comprender como utilizar el sistema de gestión.
- Monitorear el sistema de gestión considerando la eficiencia y eficacia de sus componentes.
- Mantener la mejora continua del sistema de gestión de seguridad de la información.

Así mismo se consideró incorporar buenas prácticas de seguridad de la información basadas en la estándar internacional ISO 27002:2017; mismo que se ha aplicado a organizaciones a nivel internacional logrando controlar los incidentes informáticos presentados, se analizaron los controles y los mismos se asociaron a la problemática planteada.

Práctica:

Esta investigación se efectúa porque existe la necesidad de proveer un modelo de gestión de seguridad de la información como apoyo al personal informático de la UNESUM, mismo que debe ser aplicado para minimizar los incidentes de seguridad mediante el desarrollo de políticas acordes a las necesidades institucionales.

Se resalta que por solicitud interna de los directivos en esta investigación solo se desarrollan los lineamientos de seguridad y posteriormente el personal informático interno por seguridad a su información desarrollará la política de seguridad mediante los lineamientos descritos en este documento.

1.1.7. Estado del Arte

En el último año las investigaciones sobre implementación de sistemas de gestión de seguridad de la información (de aquí en adelante SGSI) basados en controles de seguridad han tomado un cuantioso impulso dentro de las organizaciones, debido a que las amenazas a las que se exponen los sistemas de información son cada vez más sofisticadas teniendo como objetivo el robo, destrucción, divulgación y manipulación de la información, orientadas generalmente a organizaciones públicas y privadas; pero existe poca información específica sobre su aplicación en las instituciones de educación superior.

Los lineamientos que propone la Organización Internacional de Estandarización (2017) son acogidos por las organizaciones, introducen cambio y mejor gestión de los activos de información, pero no se especifica una metodológica que pueda ser acogida como modelo para el ámbito universitario.

Por un lado, se considera a un SGSI como un proceso sistemático y documentado que debe ser conocido por toda la organización, según el portal ISO 27001(2012) conlleva a la preservación de confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Por otro lado, los controles ISO 27002 complementan la gestión de ISO 27001 poniendo a disposición los dominios de control.

Así mismo, existen estándares específicos para determinados sectores. Muchos de ellos cuentan con el aval de la misma ISO/IEC, considerados como buenas prácticas.

En este ámbito se puede señalar casos de estudios relacionados con la implementación del SGSI, como, por ejemplo:

Nieves (2017), en el estudio Diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI) basados en la Norma ISO/IEC 27001:2013, busca gestionar riesgos mediante la metodología MAGERIT la cual permite realizar la evaluación del impacto que una violación de la seguridad tiene en la organización, siendo específico en una de sus conclusiones expresa "(…) permitió identificar que el desconocimiento del tema pone en riesgo los procesos que se desarrollan en cuanto a disponibilidad, integridad y confidencialidad" (2017, p. 34).

Otro estudio realizado por Tur Hartman (2016), denominado Plan de Implementación del SGSI basado en la norma ISO 27001:2013, busca evaluar el estado de sus procesos, los cuales en ese momento se enfocaban en ISO 9001 y no estaban orientados a la seguridad, usando la metodología modelo de madurez de la capacidad (CCMM) logran mantener un análisis de madurez en la implementación del SGSI incorporando los controles de la norma ISO/IEC 27002:2013. Y expresa como uno de sus resultados "La implementación de un sistema de gestión de seguridad de la información SGSI, conformará un mecanismo de optimización de recursos, ahorro de costos y mejora continua que permitirá a Textilera S.A alcanzar los objetivos y metas planteadas" (2016, p. 157).

En ambos casos el SGSI se volvió una herramienta de muy importante y ha permitido la gestión de riesgos y a su vez la incorporación de controles de seguridad específicos para cada caso.

El estudio Diseño de un Sistema de Gestión de Seguridad de la Información - SGSI basado en la norma ISO27001 para el Colegio Procolombiano de la Ciudad de Bogotá, que incluye: Asesoría y Planeación desarrollado por Riaño y Herley (2017), de acuerdo a su problemática estipula que la información se encuentra con un riesgo muy alto ya que los datos

son manipulados sin ninguna política de seguridad a casusa de lo no implementación de un SGSI, su estudio utiliza la metodología MAGERIT para la evaluación de riesgos, de acuerdo a sus conclusiones confirma que es necesaria la implementación de un SGSI debido a los altos riesgos y vulnerabilidades identificados.

Así mismo Sarmiento y Arias (2016), en la investigación Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para la EMPRESA AGILITY S.A.S dedicada a la publicidad y mercadeo ha experimentado pérdida y alteración de información propia de negocio, ante esta problemática Sarmiento y Arias consideraron establecer la metodología PHVA del cual expresan textualmente “Es la concepción básica que dinamiza la relación entre las personas y los procesos y entre los procesos y los resultados" (2016, p. 27). Al ser un ciclo dinámico se asocia con la planificación, implementación y mejora continua, este método ayudó a manejar la problemática según como lo expresa el investigador en una de sus conclusiones donde claramente ratifica que se definió los controles y la respectiva política para la seguridad de la información.

Las investigaciones antes descritas de acuerdo a sus resultados corroboran que la gestión de seguridad de la información se vuelve cada vez más indispensable en las empresas y en otros países está incorporándose en las instituciones educativas internacionales como lo expresa uno de los casos revisados.

En relación a la gestión de la seguridad basada en ISO 27002:2013, Núñez (2015), efectuó un estudio denominado Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002: 2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato, se encuentran con una problemática no muy diferente a los casos antes mencionados; la inseguridad que el investigar evidencia en cuanto a la manipulación de la información es grave, ante esto se aplica la metodología de análisis de riesgo con el fin de identificar las vulnerabilidades. Se evidencia en una de sus conclusiones

que es importante implementar los controles de ISO 27002:2013 para prevenir la "pérdida de información garantizando el correcto funcionamiento de los procesos" (2015, p. 107).

De la misma manera, Zatán en su investigación denominada Plan de Seguridad Informática Basada en la Norma ISO 27002 para el Control de Accesos Indebidos a la Red de UNIANDES PUYO, hace enfatizar su investigación es saber si a pesar de mantener políticas de seguridad estas son aplicadas, evidentemente el SGSI debe poder evaluar esta situación y a su vez los controles que se han usado, en una de sus conclusiones el investigador expresa "El personal, conjuntamente con la información son los activos más importantes con que cuenta UNIANDES Puyo. Tener pocos controles y políticas que garanticen su seguridad traerán consecuencias negativas al momento de cumplir los objetivos institucionales" (2017, p. 118). Es evidente en estos dos casos que no es muy aceptado la incorporación de un SGSI, esto estaría hiendo en contra de lo que manda la norma 410 de la contraloría general del estado.

Estos estudios, aunque con enfoques diferentes, para llegar a sus resultados proponen usar los controles 27002 en su versión más reciente.

La norma es tan flexible que permite ser aprovechada tanto a la resolución de accesos indebidos a los sistemas de información, mantener lineamientos sobre inventario de activos, control de accesos físicos, entre otros.

Finalmente, es necesario hacer notar que dentro de los casos nacionales revisados en esta sección no se ha encontrado un caso específico que hable de la problemática planteada en esta investigación.

CAPÍTULO II

MARCO TEÓRICO

2.1. Consejo de Educación Superior

El Consejo de Educación Superior (CES) tiene como su razón de ser planificar, regular y coordinar el Sistema de Educación Superior, y la relación entre sus distintos actores con la Función Ejecutiva y la sociedad ecuatoriana; para así garantizar a toda la ciudadanía una Educación Superior de calidad (CES, 2018).

2.2. Base Legal UNESUM

De acuerdo a la gaceta oficial electrónica del Consejo de Educación Superior donde reposa el estatuto de la UNIVERSIDAD ESTATAL DEL SUR DE MANABI (de aquí en adelante UNESUM), en su base legal indica textualmente Art. 1.- Naturaleza:

La Universidad Estatal del Sur de Manabí, es una Institución de Educación Superior Pública creada mediante Ley No. 38 publicada en el Registro Oficial No. 261 de 7 de febrero de 2001, tiene su domicilio en la ciudad de Jipijapa, provincia de Manabí, constituida por el Estado como persona jurídica sin fines de lucro, por lo que sin lesionar su autonomía constitucionalmente establecida, debe articular sus actividades con el Sistema de Educación Superior, el Plan Nacional de Desarrollo y el Plan Nacional del Buen Vivir. Por su naturaleza jurídica, la Universidad Estatal del Sur de Manabí, orientará sus actividades de docencia, investigación, postgrado, vinculación con la sociedad y gestión, a servir a la población del sur de Manabí y buscará trascender sus servicios al contexto nacional. Se rige por la Constitución de la República del Ecuador, la Ley Orgánica de Educación Superior y su Reglamento, los Reglamentos y las Resoluciones expedidas por el organismo público de planificación, regulación y coordinación del sistema de educación superior, el presente Estatuto, los

Reglamentos que se expidan por los órganos propios de su gobierno y demás resoluciones de sus autoridades (Gaceta Oficial, 2017).

En la actualidad la UNESUM ha tenido un crecimiento estudiantil significativo, esto promueve el uso de sistemas de información para agilizar sus procesos.

2.3. Contraloría General del Estado

Al ser una Institución Pública es regulada por todos los organismos del estado encargados de este control, uno de ellos es la Contraloría General del Estado la cual es su página web expresa textualmente:

La Constitución de la República del Ecuador, en el artículo 211, establece que la Contraloría General del Estado es un organismo técnico, encargado del control de la utilización de los recursos estatales, y de las personas jurídicas de derecho privado que dispongan de recursos públicos (Moreno, 2016).

La contraloría general del estado enmarcada en el control de los recursos públicos con la finalidad de precautelar el buen uso para beneficio de la sociedad, considero necesario desarrollar un marco normativo denominado NORMAS DE CONTROL INTERNO DE LA CONTRALORIA GENERAL DEL ESTADO emitido mediante acuerdo N° 039, con registro oficial suplemento 87 del 14 de diciembre del 2009 y modificado por última vez el 16 de diciembre del 2014 (2009), permitiendo el desarrollo para alcanzar los objetivos institucionales y maximizar los servicios públicos que deben proporcionar a la comunidad.

Normas de Control Interno de la Contraloría General del Estado

Dicha norma, expresa “El control interno será responsabilidad de cada institución” (CGE, 2009, p. 3), partiendo de este punto las tecnologías de información se encuentran consideradas dentro de este documento en un apartado denominado 410 TECNOLOGÍA DE LA INFORMACIÓN, agrupadas en diferentes ámbitos.

Uno de estos ámbitos se refiere a la seguridad de la información expresado claramente en el apartado "410-10 Seguridad de tecnología de información. La Unidad de Tecnología de Información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos" (2009, p. 73).

De acuerdo a esto la UNESUM se encuentra en la obligación de adoptar métodos de gestión que permitan salvaguardar los datos del sistema académico y a su vez cumplir con lo que demandan las leyes del país.

Entonces, tomando como referencia lo descrito es preciso tomar en consideración los siguientes conceptos:

2.4. Información

Se puede conceptualizar como el conjunto organizado de datos procesados, que generan un mensaje. Toda información constituye un gran valor sea tangible o intangible sin concernir la forma en la que se muestre, sea esta recolectada, de manera digital o impresa, entregada por medios electrónicos, cedida por video o concebida en conversación.

2.5. Amenaza Informática

De acuerdo al sitio web de la Universidad Nacional de Lujan "Se puede definir como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información" (de Luján, 2018).

Las amenazas dependen fuertemente de las vulnerabilidades que existan y puedan ser aprovechadas independientemente de que se comprometa o no la información.

2.6. Incidentes Naturales

Hace referencia a todo evento ocasionado por fenómenos naturales donde no interviene el ser humano entre ellos tenemos: terremotos, inundaciones, tormentas eléctricas, entre otros provocando un impacto negativo.

2.7. Incidentes Humanos

"Surge por ignorancia en el manejo de la información, por descuido, por negligencia o por inconformidad" (de Luján, 2018).

El personal humano por diversas situaciones suele cometer errores muy perjudiciales que provocan la caída de los sistemas de información o pérdida de la misma, entre las amenazas más relevantes se consideran:

Ingeniería Social: es considerada como la manipulación de personas con el fin de lograr que realicen acciones o actos que revelen información para superar entornos de seguridad.

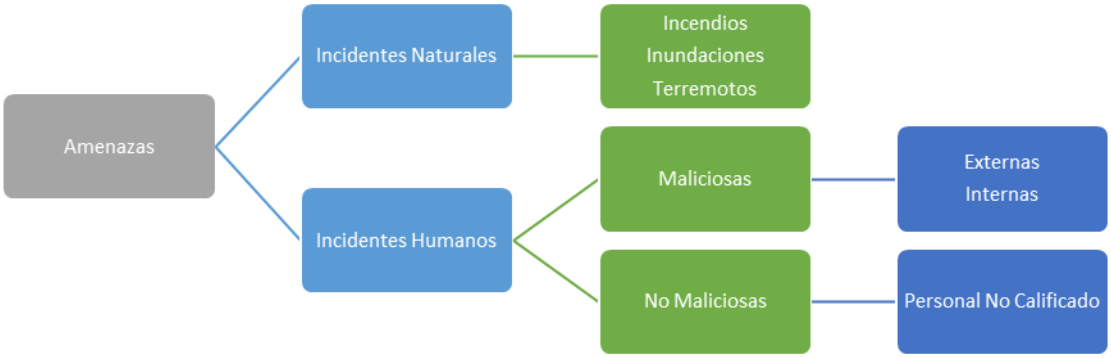
Fraude: los ordenadores son utilizados con frecuencia para engañar al usuario y realizar alguna transacción indebida, con el fin de ocasionar algún perjuicio económico patrimonial realizado con ánimo de lucro.

Robo: consiste en hurtar el equipamiento informático ya sea para obtener la información o el equipo tecnológico.

Sabotaje: se produce con la finalidad de causar un daño o destrucción intencionalmente a los servicios o información.

La Figura 2 muestra en resumen general las amenazas.

Figura 2: Amenazas Informáticas.
Fuente: Elaboración Autor



2.8. Ataques Informáticos

Mieres, califica a los ataques informáticos como una manera de "obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización" (2009, p. 4).

Estructura de un Ataque informático

Se organiza por pasos estructurados para obtener el mayor conocimiento del objetivo y con la finalidad de lanzar un ataque más preciso. Sus fases:

Fase 1: Reconocimiento. se acude a los diferentes medios (google, redes sociales, entre otros) disponibles para obtener la mayor cantidad de información de la víctima.

Fase 2: Exploración. En esta fase se utiliza la información obtenida en la fase 1 para analizar el objetivo, valiéndose de herramientas que permitan realizar escaneo de puertos, escaneo de redes, etc. Con la finalidad de obtener información del sistema, por ejemplo: direccionamiento IP, nombre de host, credenciales de acceso y otros.

Fase 3: Obtener Acceso. Es aquí donde se comienza a plasmar el ataque a través de la explotación de vulnerabilidades descubiertas en la fase 1 y 2.

Fase 4: Mantener el Acceso. Cuando el atacante ha logrado ingresar al sistema usando cualquier herramienta buscara instalar software que le permita tener el control del equipo en cualquier momento (*backdoors, rootkits y troyanos*).

Fase 5: Borrar Huellas. El atacante intentará borrar todos los rastros que dejo durante la intrusión con el fin de no ser descubierto.

2.9. Sistema de Información Académico

Se puede definir como "Un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo" (Laudon, 1996, p. 1).

Son la herramienta perfecta para cualquier organización que desee conceder accesos a sus datos, volviéndose un claro ejemplo la UNESUM quien a través de las tecnologías de información puso a disposición de la comunidad universitaria su información académica.

2.10. Sistema de Gestión de Seguridad de la Información (SGSI)

De acuerdo a la página web de ISO el SGSI consiste, en preservar la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y dar confianza a las partes interesadas para que los riesgos se gestionen adecuadamente (ISO, 2013).

De acuerdo con ISO es imprescindible incorporar modelos gestión de seguridad de la información ya que gran parte de su implementación está orientada a identificar deficiencias y fortalecerlas de acuerdo a las necesidades de la institución.

2.10.1. Ciclo de Mejora Continua - PDCA

Según Gómez y Álvarez el ciclo PDCA es:

Un concepto ideado originalmente por Shewhart, pero adaptado a lo largo del tiempo por algunos de los más sobresalientes personajes del mundo de la calidad. Esta metodología ha

demostrado su aplicabilidad y ha permitido establecer la mejora continua en organizaciones de todas clases (2012, p. 14).

El ciclo PDCA, contiene una serie de fases y acciones que facilitan desarrollar indicadores y métricas de manera que se pueda evaluar el avance de mejora en la institución, a continuación, se detallan estas fases:

Plan: Establecer una Planificación

En esta fase se define el alcance del SGSI su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.

Do: Implementar y Utilizar el SGSI

En esta segunda fase se procede con la implementación de todas las tareas establecidas en la fase de PLAN. Por lo general suele ser la fase más larga en términos de tiempo y complejidad.

Se considera:

Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.

Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.

Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.

Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.

Gestionar las operaciones del SGSI.

Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.

Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones

Check: Monitorizar y Revisar

Esta fase conlleva la realización de diferentes tipos de revisión en los que se comprobarán la correcta implementación del Sistema de Gestión de Seguridad de la Información. Para esto se considera ejecutar procedimientos de monitorización y revisión para:

Detectar a tiempo los errores en los resultados generados por el procesamiento de la información; identificar brechas e incidentes de seguridad; ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto; detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores; determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

Revisar regularmente la efectividad del SGSI.

Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.

Revisar regularmente en intervalos planificados las evaluaciones de riesgo.

Realizar periódicamente auditorías internas del SGSI.

Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado.

Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados.

Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

Act: Mantener y Mejorar

El resultado obtenido de las revisiones debe quedar reflejado en la definición e implementación de las diferentes acciones correctivas, preventivas o de mejora con las que se consigue avanzar en la consecución del Sistema de Gestión de Seguridad de la Información siendo un sistema eficaz y eficiente.

La organización deberá regularmente: Implantar en el SGSI las mejoras identificadas.

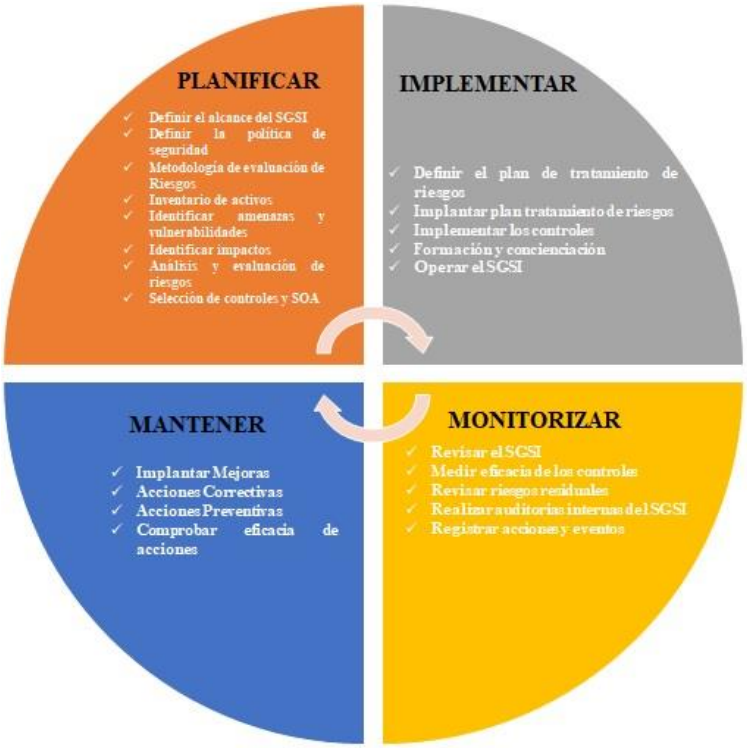
Realizar las acciones preventivas y correctivas adecuadas para prevenir potenciales no conformidades antes de que se produzcan.

Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.

Asegurarse que las mejoras introducidas alcanzan los objetivos previstos: la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

Luego de conocer estos pasos es necesario recordar que al ser un ciclo continuo deberá iniciar de nuevo en la primera fase (PLANIFICAR). A continuación, en la ilustración 4 se presentan las cuatro fases, en resumen.

Figura 3: Ciclo Deming
Fuente: Elaboración Autor



2.11. Seguridad de la Información

La información es esencial en la toma de medidas, pues, cuanto más completa y exacta sea ayudara a una mejor toma de decisiones.

De acuerdo con el sitio web QUISEC "La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente. Esto es especialmente importante en el ambiente comercial cada vez más interconectado" (QUISEC, 2017).

Objetivos en la Seguridad de la Información

Apoyar las tareas mediante el cumplimiento de metas u objetivos tiende a proporcionar buenos resultados dentro del campo de acción que sea requerido, pues en el ámbito informático se prevé mantener los datos lo más seguros posibles, ante esto los objetivos principales según Chamorro (2015) buscan:

Confidencialidad

Es el principio en el cual solo individuos, procesos o sistemas autorizados pueden acceder a la información en función de sus necesidades. El principio de la confidencialidad se debe aplicar en los tres estados de la información es decir en almacenamiento, en procesamiento y en tránsito. Para aplicar el principio de confidencialidad se puede usar identificación, autenticación, autorización a través de controles de acceso, pero esto no garantiza 100% de confidencialidad porque usuarios autorizados también son un riesgo ya que pueden acceder a la información con fines maliciosos (2015, p. 4).

Integridad

Es el principio en el cual la información que se encuentra en almacenamiento, procesamiento y en tránsito solo debe ser alterada de una manera específica (procedimiento) y por sujetos autorizados. El principio de integridad depende del principio de confidencialidad ya que sin confidencialidad la integridad no puede ser mantenida (2015, p. 4).

Disponibilidad

"Es el principio en el cual la información que se encuentra en almacenamiento, procesamiento y en tránsito debe estar accesible en cualquier momento y en cualquier lugar solo para los sujetos autorizados" (2015, p. 5).

2.12. ISO/IEC 27002

La Organización Internacional de Normalización (ISO) en conjunto con la Comisión Electrotécnica Internacional (IEC) conforman el grupo especializado para el desarrollo de estándares por medio de comités técnicos establecidos para tratar materia en campos particulares con actividad técnica.

De acuerdo con el sitio web (ISO, 2013) el cual expresa textualmente "Este Estándar Internacional está diseñado para que las organizaciones lo utilicen como referencia para

seleccionar controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO / IEC 27001 o como documento guía para organizaciones que implementan controles de seguridad de la información comúnmente aceptados".

El estándar ISO/IEC 27002 (de aquí en adelante norma 27002), suministra pautas para las normas de seguridad de la información y prácticas de gestión de seguridad de la información teniendo en cuenta los ambientes de riesgo.

La norma 27002 está en constante actualización por parte de sus desarrolladores, en la actualidad se consideran dos versiones las cuales toman el nombre de ISO/IEC 27002:2013 y ISO/IEC 27002:2017.

ISO/IEC 27002:2013

Es producto de la revisión de su antecesora, se publicó oficialmente en el 2013 manejando el mismo criterio para el que fue desarrollada, su actualización recae en la reducción de 133(27002:2005, 2013) a 111 controles y estos a su vez se presentan en 14 dominios y 34 objetivos de control.

Las misma hasta la actual fecha ha tenido dos actualizaciones las cuales se describen a continuación:

ISO / IEC 27002: 2013 / Cor.1: 2014: en esta actualización se renueva el contenido en la página 10, subcláusula 7.1.2 Guía de Implementación numeral c); Página 13, Subcláusula 8.1.1 "Controlar", Página 14, Subcláusula 8.1.3 "Guía de Implementación." Para una lectura más a fondo se recomienda visitar el sitio web:

https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:cor:1:v1:en

ISO/IEC 27002:2013/Cor.2:2015: en esta actualización se renueva el contenido en la página 61, Subcláusula 14. Guía de Implementación. Para una lectura más a fondo se recomienda visitar el sitio web:

https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:cor:2:v1:en

ISO/IEC 27002:2017

De acuerdo con El Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services(ILNAS, 2017),(International Organization for Standardization (ISO, 2017), la actualización para la norma se basa específicamente en la presentación rediseñada con los cambios descritos en el apartado anterior.

Realizando un análisis de las dos actualizaciones descritas podríamos considerar que no se alteraría en ninguna instancia al usar tanto la norma ISO/IEC 27002:2013 o la norma ISO/IEC 27002:2017 siempre que se mantengan presentes los cambios realizados por la entidad internacional autorizada.

CAPÍTULO III

ANÁLISIS SITUACIONAL

3.1. SITUACIÓN ACTUAL

La Universidad Estatal del Sur de Manabí de acuerdo a su naturaleza jurídica es una institución de educación superior creada para formar profesionales que ayuden a la resolución de problemas de la sociedad.

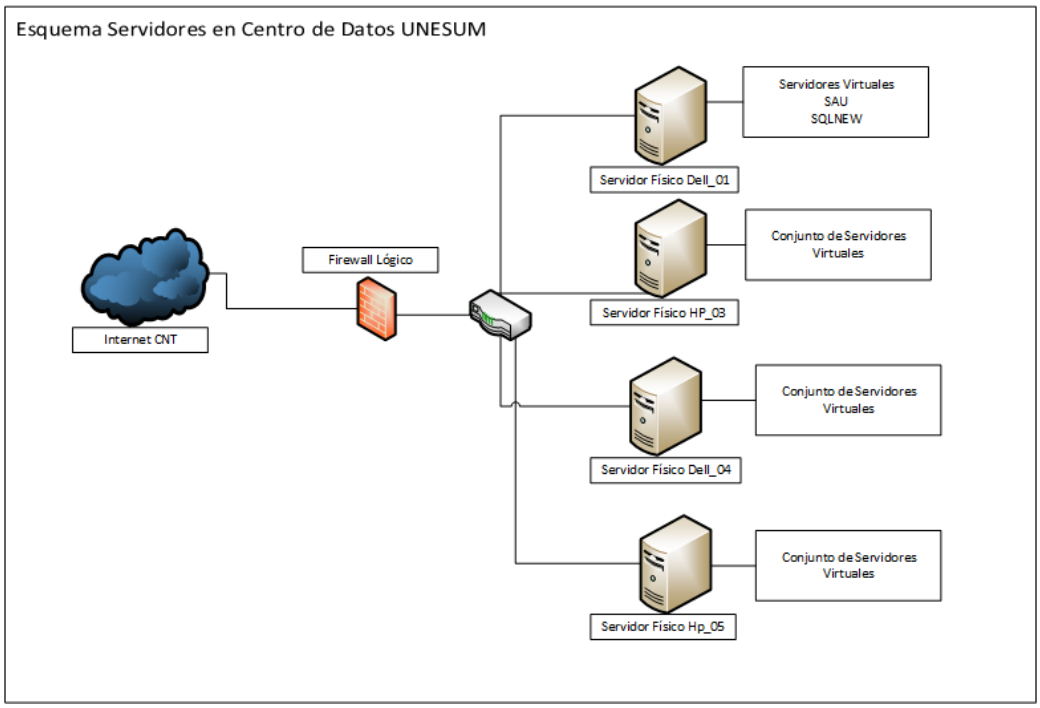
Su principal actividad institucional es la gestión y administración de información académica, proceso que actualmente se encuentra sistematizado, el acceso a la información se realiza mediante una plataforma web denominada "*Sistema Académico UNESUM-S@U",* el cual es accesible solo mediante internet.

Figura 4 Sistema Académico Unesum.
Fuente: http://sistsau.unesum.edu.ec/inicio.php

La información se encuentra almacenada en un servidor con un sistema base Linux el cual a su vez maneja software interno denominado MySql como gestor de base de datos.

Los equipos que soportan los sistemas de información se encuentran alojados en un pequeño centro de datos el cual cuenta con acceso a internet para que los mismos puedan estar disponibles para la comunidad universitaria y público en general.

Figura 5 Esquema Servidores UNESUM.
Fuente: Elaboración Autor



A continuación, una descripción del esquema anterior:

- La granja de servidores está compuesta por cuatro (4) servidores físicos que a su vez mantienen servidores virtuales los cuales alojan los sistemas de información tales como: sistema académico UNESUM-S@U, sistema de evaluación de la gestión al Docente-SIEGDD, sistema de seguimiento a graduados-SSGU, Biblioteca Virtual, Aulas Virtuales, Evaluación Institucional.
- Se cuenta con un acceso a internet de 450 MEGAS contratados con el proveedor de servicios Corporación Nacional de Telecomunicaciones – CNT, distribuidos en las sedes Campus lo Ángeles, Complejo y Edificio Central, el cual no se recibe en su totalidad.
- En cuanto al control de acceso al centro de datos (CD) solo se mantiene una puerta de metal con seguridad.
- El personal técnico informático cumple con sus horas laborables dentro del CD, teniendo acceso a todos los servidores sin ningún control.

- Se mantiene un inventario del equipamiento del CD manual que muy pocas veces se actualiza.
- No existe un control en los accesos asignados a los usuarios del sistema académico.
- El personal informático desconoce sobre medidas de protección de la información.
- No se documentan los ataques, modificaciones, accesos indebidos a la plataforma web del sistema académico.
- La administración y el acceso al sistema académico de la UNESUM se realiza vía web.
- La base de datos se encuentra alojada en el mismo servidor físico donde está el sistema web académico.
- EL acceso a los sistemas depende totalmente del servicio de internet.
- Se realizan trabajos de mantenimiento al sistema de manera remota, dejando en ocasiones los sistemas offline o fuera de línea ocasionando retardo en los procesos.
- No se evidencia ningún documento que le permita al personal informático seguir una guía para la implementación de medidas de seguridad para la protección de la información del sistema académico.
- La base de datos maneja un registro académico de a próximamente 7000 usuarios con una proyección de crecimiento de alrededor de 1000 por año

3.1.1. Descripción técnica

3.1.1.1. Servidores

Tabla 1 Descripción Técnica de Servidores.
Fuente: Elaboración Autor

ID_Server_Físico (SF)	Nombre_SF	ID_Server_Virtuales (SV)	Nombre_SV	Recursos Asignados
ID_Server_Físico (SF)	Server Dell_01	SV_01	Graduados	1 núcleos, 4096 MB de RAM asignada
		SV_02	Evaluación	2 núcleos, 4096 MB de RAM asignada
		SV_03	Aula Virtual	2 núcleos, 4096 MB de RAM asignada
		SV_04	SIU-GLPI	2 núcleos, 4096 MB de RAM asignada
		SV_06	SAU	4 núcleos, 32768 MB de RAM asignada
		SV_07	SQLNEW	4 núcleos, 32768 MB de RAM asignada
		SV_08	Investigación	1 núcleos, 4096 MB de RAM asignada
SF_03	Server HP_03	SV_01	PBX	3 núcleos, 3072 MB de RAM asignada
SF_04	Server Dell_04	SV_01	DSPACE	4 núcleos, 4096 MB de RAM asignada
SF_05	Server HP_05	SV_01	OJS	1 núcleos, 1024 MB de RAM asignada
		SV_02	PMB Biblioteca	1 núcleos, 2048 MB de RAM asignada
		SV_03	Bodega	1 núcleos, 2048 MB de RAM asignada
		SV_04	Web UNESUM	2 núcleos, 4096 MB de RAM asignada

3.1.1.2. Sistemas de Información

Sistema Académico UNESUM-S@U: Aplicación web que permite el registro de matrículas, notas, cargas horarias, historial académico de estudiantes, datos personales y académicos de docentes, colabora en conjunto con el servidor de base de datos, actualmente mantiene información relevante de alrededor de 7000 usuarios.

Sistema de Evaluación de la Gestión del desempeño Docente - SIEGDD: Permite realizar la actividad de evaluación al Docentes a los estudiantes de cada facultad.

Sistema de Seguimientos a Graduados – SSGU: Mantiene información relevante con respecto al registro de graduados de la institución.

Portal Web Institucional: Sitio en Internet bajo el dominio unesum.edu.ec que permite mantener información actualizada para las consultas del caso ante los organismos de control del estado.

Al autor se le indico de manera interna que se darían las facilidades para que se realice el trabajo de investigación y a su vez se le solicitó respetar las sugerencias realizadas por cada encargado de los departamentos a los cuales se permitiría el acceso, por lo tanto, el análisis de riesgos solo **presentará datos de manera general** respetando el acuerdo pactado y **la no divulgación de información sensible**, de la misma manera se aclaró por parte de las autoridades que ellos tomarían los correctivos de manera interna.

3.2. Análisis de Riesgos

3.2.1. Propósito

El análisis de riesgos de seguridad de la información se desarrolla con el **propósito de conocer a que amenazas están expuestos los activos de información** más relevantes que permiten la conexión al sistema académico UNESUM, alojado el centro de datos de la institución.

Para cumplir con el propósito se tomó como referencia la guía de análisis de riesgos del Instituto Nacional de Ciberseguridad Español, el cual trabaja para afianzar la seguridad digital (INCIBE, 2016) .

3.2.2. Alcance

Se desarrollará solo el modelo para la implementación del sistema de gestión de seguridad de la información debido a que será el personal de la unidad informática quienes basados en los lineamientos que se presentaran desarrollaran la política de seguridad.

Comprende el centro de datos de la UNESUM y todo el equipamiento informático administrativo principal del personal de la Unidad de Sistemas usados para la administración y gestión del sistema académico UNESUM repartidos en el campus Los Ángeles. En este documento **NO** se dará a conocer las amenazas y vulnerabilidades identificadas por seguridad de la institución, pero si explicara cómo se realizó incorporando ejemplos que permitan tener una idea de las mismas.

3.2.3. Identificación y Clasificación de Activos de Información

Una vez definido el alcance se procedió a la identificación y valoración de los activos de información la cual se logró mediante las visitas in situ al objeto de estudio, se desarrolló una matriz la cual abarca los criterios más relevantes con respecto al sitio de estudio. La Tabla 2 muestra un ejemplo de cada activo identificado.

Tabla 2 Matriz Identificación Valoración de Activos de información.
Fuente: Elaboración Autor

MATRIZ ANÁLISIS DE RIESGOS							
INSTITUCIÓN	UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ						
OBJETIVO	Clasificación e Identificación de Activos de Información						
UNIDAD	Centro de Datos / Sistemas Informáticos						
IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN							
ID ACTIVO	**NOMBRE ACTIVO**	**DESCRIPCIÓN ACTIVO**	**PROPIETARIO ACTIVO**	**TIPO ACTIVO**	**UBICACIÓN ACTIVO**	**OBSERVACIONES**	**CLASIFICACIÓN**
I_1	Datos Académicos	Información digital de los estudiantes, profesores.	Dirección académica, Vicerrectorado, Decanos Coordinadores, Unidad de Sistemas Informáticos-USI	Digital	Centro de Datos-DC	La información sirve como medio de consulta para usuarios con accesos concedidos(Administrativos, Docentes y Estudiantes)	Datos e Información
S_1	Internet	Red Externa de enlace mundial	Unidad de Sistemas Informáticos	digital	Centro de Datos-DC	El servicio de internet permite el acceso a los sistemas de información que mantiene la Institución	Servicios
SV_07	SQLNEW	Base de Datos general de la Unesum	Unidad de Sistemas Informáticos	Servidor Virtual	Centro de Datos-DC	Sostiene el Servicios de Bases de datos donde se Almacenan los Registros ingresados por medio de la Aplicación web S@U.	Equipamiento Informático

3.2.3.1. Valoración de Activos de Información

Luego de la identificación y clasificación de los activos de información se consideró valorarlos con el objetivo de establecer el nivel de afectación en cuanto a la utilidad del servicio que proporciona. El criterio con el cual se realizó la valoración es el costo en el que se cae debido a la pérdida de la confidencialidad integridad y disponibilidad como resultado de un suceso.

Las reuniones mantenidas con el personal de tecnologías permitieron identificar si los activos tienen alguna dependencia que afecte al sistema académico vulnerando su Integridad, Confidencialidad y Disponibilidad. Esto ayudó a la elaboración de la matriz de valores. A continuación, la Tabla 3 muestra la escala de valoración.

Tabla 3 Valoración de Activos.
Fuente: Elaboración Autor

CALIFICACIÓN	VALOR	DEPENDIENTE	TECNOLOGIA	INTEGRIDAD/CONFIDENCIALIDAD/ DISPONIBILIDAD
1	CRÍTICO	Todos los activos dependen de este la entrega de los servicios.	Última Generación	Si se compromete afectaría totalmente sistema académico.
2	ALTO	Considerable número de activos dependen de este para la entrega del servicio.	Muy Avanzada	Si se compromete afectaría gravemente al sistema académico.
3	MEDIO	Mínimos activos dependen de este activo para la entrega del servicio.	Avanzada	Si se compromete afectaría significativamente al sistema académico.
4	BAJO	Este activo tiene poca dependencia de para otros activos en la entrega de servicios.	Limitada	Si se compromete afectaría en parte al sistema académico.
5	MUY BAJO	Este activo no depende de ninguno para la entrega del servicio.	Muy limitada	Si se compromete afecta de manera insignificante al sistema académico.

Consiguientemente se ubicó un casillero con la descripción “OBSERVACIÓN” el cual identifica la función de cada activo para proceder a la respectiva valoración del mismo y determinar críticamente en las reuniones de trabajo mantenidas con el equipo informático que activo es considerando critico en cuanto a la pérdida de Disponibilidad, integridad y confidencialidad con respecto al suceso de algún incidente. La Tabla 4 muestra un detalle de lo explicado.

Tabla 4 Valoración de los Activos de Información.
Fuente: Elaboración Autor

CLASIFICACIÓN	NOMBRE DEL ACTIVO	OBSERVACIÓN	CALIFICACIÓN FINAL
Datos e Información	Datos Académicos	La información sirve como medio de consulta para usuarios con accesos concedidos(Administrativos, Docentes y Estudiantes)	1
Equipamiento Informático	Dell_01	Aloja Servidores Virtuales entre ellos la base de datos y el aplicativo web del sistema académico.	1
Equipamiento Informático	SAU	Sostiene el Servicio web para el acceso al sistema Académico UNESUM(S@U)	1
Equipamiento Informático	SQLNEW	Sostiene el sistema base de la Base de datos donde se guardan y almacenan los registros ingresados por medio de la Aplicación web S@U.	1
Software Aplicaciones	Aplicación Web Sistema Académico - S@U	La aplicación permite a la comunidad universitaria realizar actividades tales como: Matricula. Notas. Carga Horaria. Historial Académico Estudiantes. Datos Personales y Académicos Docentes.	1

Las visitas in situ, revisión documental y reuniones de trabajo fueron fundamentales a la hora de valorar e identificar los activos de mayor relevancia.

3.2.3.2. Identificación de Amenazas y Vulnerabilidades

Una vez identificado los activos, se procedió a la identificación de las amenazas y vulnerabilidades a las que se encuentran expuestos los activos más relevantes, es necesario tener en consideración que la presencia de una vulnerabilidad va de la mano con la amenaza para que esta pueda ser explotada, es decir que una vulnerabilidad que no cuente con una amenaza no requiere la aplicación de un control.

Amenaza: suceso ocasionado de manera accidental o intencional de cualquier tipo, capaz de causar daño a un sistema informático, utilizando sus vulnerabilidades para tomar control sobre el u originar un impacto considerable a la institución.

Vulnerabilidad: Son las debilidades de un sistema informático que pueda permitir el ingreso de amenazas que pueda causar daños y perdida en una organización, Por lo tanto, Las vulnerabilidades son fallas en los sistemas ya sean por una mala instalación o configuración, por la falta de capacitación del personal con los recursos del sistema, también por equipos de

cómputo donde los programas y herramientas no son seguras para la información (Bautista, 2018, p. 40).

Para una mejor identificación fue necesario desarrollar una tabla donde se registren las vulnerabilidades y amenazas. A continuación, la Tabla 5 muestra un resumen de lo indicado.

Tabla 5 Matriz para la identificación de Amenazas y Vulnerabilidades.
Fuente: Elaboración Autor

			AFECTA A LA:		
CLASIFICACIÓN ACTIVO	**VULNERABILIDADES**	**AMENAZAS**	**INTEGRIDAD**	**DISPONIBILIDAD**	**CONFIDENCIALIDAD**
Datos e Información	Borrado de Información	Bajo control en el acceso a los datos	X		X
Equipamiento Informático	Bajo registro de equipos informáticos	Bajo control en el Centro de Datos	X	X	X
Software Aplicaciones	Denegación de Servicios	Información no disponible		X	

Es necesario acotar que durante la investigación documental que se realizó no se pudo evidenciar una propuesta o aplicación de controles para minimizar las amenazas.

3.2.4. Evaluación del Riesgo

Riesgo: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización (MAGERIT, 2012, p. 9).

La identificación de las amenazas y vulnerabilidades conllevo a estimar la probabilidad de que las mismas se materialicen y así conocer que tan grave es el impacto que se produciría cuando la amenaza permita explotar la vulnerabilidad. Pues bien, se asigna un valor de 3 cuando la probabilidad de que la amenaza permita explotar la vulnerabilidad sea BAJA, un valor de 5 cuando la probabilidad de que la amenaza permita con poca frecuencia explotar la vulnerabilidad clasificándola como MEDIA y un valor 9 cuando la probabilidad de que la amenaza permita explotar vulnerabilidades frecuentemente clasificándola como ALTA.

En el caso del impacto, se asigna un valor de 4 cuando el daño producto de la amenaza no tiene consecuencias notables clasificándolo como Bajo, un valor de 6 cuando el daño

producto de la amenaza tiene consecuencias significativas clasificándolo como Medio y un valor de 8 cuando el daño producto de la amenaza tiene consecuencias graves clasificándolo como Alto.

A continuación, la Tabla 6 y

Tabla 7 muestran los criterios desarrollados para la evaluación del riesgo, mismos que permitieron ser identificados mediante las reuniones de trabajo mantenidas con el personal de tecnologías de la institución.

Tabla 6 Probabilidad de que ocurra la amenaza.
Fuente: Elaboración Autor

PROBABILIDAD DE QUE OCURRA LA AMENAZA

Clasificación	Descripción	Valor
BAJA	La probabilidad de que la amenaza permita explotar la vulnerabilidad es muy baja	3
MEDIA	La probabilidad de que la amenaza permita con poca frecuencia explotar vulnerabilidades	5
ALTA	Probabilidad de que la amenaza permita explotar vulnerabilidades frecuentemente.	9

Tabla 7 Impacto causado por la probabilidad de amenaza.
Fuente: Elaboración Autor

IMPACTO

Clasificación	Descripción	Valor
Bajo	EL daño producto de la amenaza no tiene consecuencias notables para la Institución	4
Medio	EL daño producto de la amenaza tiene consecuencias significativas para la Institución	6
Alto	EL daño producto de la amenaza tiene consecuencias graves para la Institución	8

Una vez que se mantuvo un claro criterio sobre la evaluación del riesgo se realiza el cálculo del mismo multiplicando la probabilidad de ocurrencia por el impacto, es decir:

RIESGO = PROBABILIDAD DE OCURRENCIA x IMPACTO

Estimación del Riesgo

Aplicando la formula anterior se puede conocer la escala de valores asignados para la estimación del riesgo, a continuación la Tabla 8 muestra en resumen el cálculo realizado.

Tabla 8 Valores para Estimación del Riesgo.
Fuente: Elaboración Autor

		IMPACTO		
		Bajo (4)	**Medio (6)**	**Alto (8)**
Probabilidad de ocurrencia	**BAJA (3)**	12 a 20 Bajo	12 a 20 Bajo	24 a 36 Medio
	MEDIA (5)	12 a 20 Bajo	24 a 36 Medio	40 a 54 Alto
	ALTA (9)	24 a 36 Medio	40 a 54 Alto	60 a 72 Muy Alto

Riesgos sobre los Activos de Información

A este punto se ha recolectado información muy valiosa para lograr el propósito propuesto. La agrupación de los activos de información, la identificación de las amenazas y vulnerabilidades existentes sobre los activos de información, la asignación de valor para la probabilidad de ocurrencia de amenazas y el impacto junto a la escala de valores para la estimación del riesgo se constatan en el desarrollo de una matriz con el fin de identificar el nivel de riesgo al que se encuentra expuesto cada activo. La Tabla 9 muestra un ejemplo de lo descrito.

Tabla 9 Matriz Identificación Nivel de Riesgo expuesto.
Fuente: Elaboración Autor

			EVALUACIÓN DEL RIESGO	
Clasificación de activo	**Tipo Activo**	**Nombre Activo**	**Amenazas**	**Nivel de Riesgo**
Datos e Información	Información	Información Académica	Bajo control en el acceso a los datos	MUY ALTO
Equipamiento Informático	Servidor	Base de datos	Deficiente inventario de activos	MUY ALTO
Software Aplicaciones	Aplicación	Aplicación web	Deficientes lineamientos de seguridad en el acceso	MUY ALTO

3.3. Análisis de controles de la norma ISO 27002:2017

De acuerdo con el sitio web (ISO2700, 2018) la norma ISO 27002 es una guía de buenas prácticas donde se describen controles y objetivos de control referentes a la seguridad de la información.

Su aplicación dependerá de la necesidad de la institución, pues la norma se ha desarrollado para que se escojan sus controles de acuerdo a su necesidad considerándose particularmente en la implementación de modelos de gestión para la seguridad de la información.

Su última actualización pone a disposición 114 dominios de control, mismos que se organizan en 14 dominios y 35 objetivos de control.

El análisis realizado a los dominios y objetivos de control tiene como pieza clave escoger los más acordes a la necesidad del sistema académico de la UNESUM para así proveer lineamientos que puedan seguir los técnicos informáticos de la institución y desarrollar su política de seguridad.

A continuación, la Tabla 10 muestra en resumen general cada control y su posible ámbito de aplicación.

3.3.1. Mapa de controles ISO 27002:2017

Tabla 10 Mapa Controles ISO 27002:2017.
Fuente: Elaboración Autor

DOMINIO	OBJETIVOS DE CONTROL	CONTROL	APLICA (A) / NO APLICA(N.A.)	DESCRIPCIÓN
a) Políticas de seguridad	1. Directrices de la Dirección en seguridad de la información.	1.1 Documento de Políticas de seguridad de la Información.		Orientar y Soportar a la gestión de la seguridad de la Información, mediante el desarrollo de un Documento denominado Política de Seguridad, el cual deberá tener una intención e instrucción formal expresada por la Dirección acorde a las leyes vigentes.
		1.2 Revisión de las Políticas para la seguridad de la Información		
b) Aspectos organizativos de la seguridad.	2. Organización interna.	2.1 Asignación de responsabilidades para la seguridad de la información.		Conformar un esquema directivo para la administración de la seguridad de la información como pilar principal de Objetivos y actividades de la Institución, con la finalidad de iniciar y controlar la implementación de la seguridad de la información.
		2.2 Segregación de Tareas.		
		2.3 Contacto con las Autoridades		
		2.4 Contacto con grupos de interés especial.		
		2.5 Seguridad de la información en la gestión de proyectos.		
	3. Dispositivos para movilidad y teletrabajo.	3.1 Política de uso de dispositivos para movilidad.		
		3.2 Teletrabajo		
c) Seguridad ligada a los recursos humanos	4. Antes de la contratación.	4.1 Investigación de antecedentes.		Asegurar que el personal que labora en la institución, contratistas y usuarios terceros comprendan las responsabilidades, y corroborar que sean actos para el desarrollo de las funciones que se asignen, buscando incorporar
		4.2 Términos y condiciones de contratación.		
	5. Durante la contratación.	5.1 Responsabilidades de gestión.		
		5.2 Concienciación, educación y capacitación en segur. de la información.		

				lineamientos de seguridad en asuntos de confidencialidad logrando así reducir: el error humano, cometer actos ilícitos o un manejo no autorizado de información.
		5.3 Proceso disciplinario.		
	6. Cese o cambio de puesto de trabajo.	6.1 Cese o cambio de puesto de trabajo.		
d) Gestión de activos	7. Responsabilidad sobre los activos.	7.1 Inventario de activos.		Mantener un preciso conocimiento de los activos de la organización para la identificación y definición de responsabilidades para así conseguir la aplicación de niveles de seguridad acordes a la protección de la información evitando la divulgación, modificación o destrucción en su almacenamiento.
		7.2 Propiedad de los activos.		
		7.3 Uso aceptable de los activos.		
		7.4 Devolución de activos.		
	8. Clasificación de la información.	8.1 Directrices de clasificación.		
		8.2 Etiquetado y manipulado de la información.		
		8.3 Manipulación de activos.		
	9. 8.3 Manejo de los soportes de almacenamiento.	9.1 Gestión de soportes extraíbles.		
		9.2 Eliminación de soportes.		
		9.3 Soportes físicos en tránsito.		
e) Control de accesos.	10. Requisitos de negocio para el control de accesos.	10.1 Política de control de accesos.		Controlar los accesos por medio de un sistema de excepciones y prohibiciones a la información, aplicada a las instalaciones que realicen procesamiento de datos con la finalidad
		10.2 Control de acceso a las redes y servicios asociados.		
	11. Gestión de acceso de usuario.	11.1 Gestión de altas/bajas en el registro de usuarios.		
		11.2 Gestión de los derechos de acceso asignados a usuarios.		

		11.3 Gestión de los derechos de acceso con privilegios especiales.		de garantizar el acceso autorizado e impedir accesos no autorizados a los sistemas de informáticos y servicios asignando responsabilidades a los usuario para la seguridad de la información.
		11.4 Gestión de información confidencial de autenticación de usuarios.		
		11.5 Revisión de los derechos de acceso de los usuarios.		
		11.6 Retirada o adaptación de los derechos de acceso		
	12. Responsabilidades del usuario.	12.1 Uso de información confidencial para la autenticación.		
	13. Control de acceso a sistemas y aplicaciones.	13.1 Restricción del acceso a la información.		
		13.2 Procedimientos seguros de inicio de sesión.		
		13.3 Gestión de contraseñas de usuario.		
		13.4 Uso de herramientas de administración de sistemas.		
		13.5 Control de acceso al código fuente de los programas.		
f) Cifrado.	14. Controles criptográficos.	14.1 Política de uso de los controles criptográficos.		Proteger el acceso a la información por medio de métodos criptográficos con la finalidad de garantizar la confidencialidad, autenticidad e integridad de la información.
		14.2 Gestión de claves.		
g) Seguridad física y ambiental.	15. Áreas seguras.	15.1 Perímetro de seguridad física.		Minimizar en lo posible los riesgos de la información y operaciones otorgando acceso a los entornos físicos solo a personal autorizado con la sana intención de prevenir el robo,
		15.2 Controles físicos de entrada.		
		15.3 Seguridad de oficinas, despachos y recursos.		

		15.4 Protección contra las amenazas externas y ambientales.		perdida o daños de la información y la interrupción de las operaciones.
		15.5 El trabajo en áreas seguras.		
		15.6 Áreas de acceso público, carga y descarga.		
	16. Seguridad de los equipos.	16.1 Emplazamiento y protección de equipos.		
		16.2 Instalaciones de suministro.		
		16.3 Seguridad del cableado.		
		16.4 Mantenimiento de los equipos.		
		16.5 Salida de activos fuera de las dependencias de la empresa.		
		16.6 Seguridad de los equipos y activos fuera de las instalaciones.		
		16.7 Reutilización o retirada segura de dispositivos de almacenamient11.2.8 Equipo informático de usuario desatendido.		
		16.8 Política de puesto de trabajo despejado y bloqueo de pantalla.		
h) Seguridad en la Operativa.	17. Responsabilidades y procedimientos de operación.	17.1 Documentación de procedimientos de operación.		Evidenciar y controlar la existencia de procedimientos de operaciones, mantenimiento y actualización de la documentación relacionada evitando el acceso no autorizado a las instalaciones físicas y daños a la información donde se realice procesamiento de la misma y
		17.2 Gestión de cambios.		
		17.3 Gestión de capacidades.		
		17.4 Separación de entornos de desarrollo, prueba y producción.		

	18. Protección contra código malicioso.	18.1 Controles contra el código malicioso.		así garantizar que el espacio donde se procesa la información esté protegida contra código malicioso evitando la perdida de datos mediante copias de seguridad seguras y en el caso de existir algún evento registrarlo con la evidencia necesaria garantizando la integridad de los sistemas informáticos para evitar el aprovechamiento de alguna vulnerabilidad. Todo esto conlleva a disminuir el impacto de las auditorias en los sistemas informáticos.
	19. 12.3 Copias de seguridad.	19.1 Copias de seguridad de la información.		
	20. 12.4 Registro de actividad y supervisión.	20.1 Registro y gestión de eventos de actividad.		
		20.2 Protección de los registros de información.		
		20.3 Registros de actividad del administrador y operador del sistema.		
	21. 12.5 Control del software en explotación.	21.1 Gestión de las vulnerabilidades técnicas.		
		21.2 Restricciones en la instalación de software.		
	22. Consideraciones de las auditorías de los sistemas de información.	22.1 Controles de auditoría de los sistemas de información.		
i) Seguridad en las Telecomunicaciones.	23. Gestión de la seguridad en las redes.	23.1 Controles de red.		Brindar protección a la información que circula por redes de datos y a su vez a la infraestructura que soporta esta actividad evitando accesos no autorizados a la infraestructura para mantener un sistema de intercambio de información seguro hacia instituciones externas.
		23.2 Mecanismos de seguridad asociados a servicios en red.		
		23.3 Segregación de redes.		
	24. Intercambio de información con partes externas.	24.1 Políticas y procedimientos de intercambio de información.		
		24.2 Acuerdos de intercambio.		
		24.3 Mensajería electrónica.		
		24.4 Acuerdos de confidencialidad y secreto.		

j) Adquisición, desarrollo y mantenimiento de los sistemas de información.	25. Requisitos de seguridad de los sistemas de información.	25.1 Análisis y especificación de los requisitos de seguridad.		Definir y documentar procedimientos y normativas a usar durante la vigencia de las aplicaciones y en infraestructura que los soporta logrando que la seguridad de la información se considere parte integral de los sistemas en todo el ciclo de uso incluyéndose los servicios de telecomunicaciones arrendados a terceros permitiendo garantizar protección a la información que se usa como base para pruebas.
		25.2 Seguridad de las comunicaciones en servicios accesibles públicas.		
		25.3 Protección de las transacciones por redes telemáticas.		
	26. Seguridad en los procesos de desarrollo y soporte.	26.1 Política de desarrollo seguro de software.		
		26.2 Procedimientos de control de cambios en los sistemas.		
		26.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.		
		26.4 Restricciones a los cambios en los paquetes de software.		
		26.5 Uso de principios de ingeniería en protección de sistemas.		
		26.6 Seguridad en entornos de desarrollo.		
		26.7 Externalización del desarrollo de software.		
		26.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.		
		26.9 Pruebas de aceptación.		
	27. Datos de prueba.	27.1 Protección de los datos utilizados en pruebas.		
k) Relaciones con suministradores.	28. Seguridad de la información en las	28.1 Política de seguridad de la información para suministradores.		Lograr mantener niveles apropiados de

	relaciones con suministradores.			seguridad de la información en servicios contratados para garantizar protección de activos a los cuales accederán los distribuidores respetando los acuerdos de entrega de servicios de terceros.
		28.2 Tratamiento del riesgo dentro de acuerdos de suministradores.		
		28.3 Cadena de suministro en tecnologías de la información y comunicaciones.		
	29. Gestión de la prestación del servicio por suministradores.	29.1 Supervisión y revisión de los servicios prestados por terceros.		
		29.2 Gestión de cambios en los servicios prestados por terceros.		
l) Gestión de incidentes en la seguridad de la información.	30. Gestión de incidentes de seguridad de la información y mejoras.	30.1 Responsabilidades y procedimientos.		Mantener un monitoreo constante sobre los eventos de seguridad de la información y las debilidades en los sistemas de información, manteniendo una buena comunicación de los mismos para en el caso de considerarse necesario aplicar las sanciones del caso a tiempo.
		30.2 Notificación de los eventos de seguridad de la información.		
		30.3 Notificación de puntos débiles de la seguridad.		
		30.4 Valoración de eventos de seguridad de la información y toma de decisiones.		
		30.5 Respuesta a los incidentes de seguridad.		
		30.6 Aprendizaje de los incidentes de seguridad de la información.		
		30.7 Recopilación de evidencias.		
m) Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	31. Continuidad de la seguridad de la información.	31.1 Planificación de la continuidad de la seguridad de la información.		Preservar los lineamiento de la seguridad de la información durante su inicio de aplicación, desarrollo de procesos, normativas y planes de continuidad de manera integral dentro de cada proceso de la organización para así garantizar la disponibilidad de los centros de procesamiento de información.
		31.2 Implantación de la continuidad de la seguridad de la información.		
		31.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.		
	32. Redundancias.	32.1 Disponibilidad de instalaciones para el procesamiento de la información.		

n) Cumplimiento.	33. Cumplimiento de los requisitos legales y contractuales.	33.1 Identificación de la legislación aplicable.		La operación, administración y uso de los sistemas de información deben estar regulados por las normativas vigentes, obligaciones legales o contractuales para garantizar que se implementa y opera un sistema de gestión de seguridad de la información de acuerdo a los procedimientos, políticas y normativas institucionales.
		33.2 Derechos de propiedad intelectual (DPI).		
		33.3 Protección de los registros de la organización.		
		33.4 Protección de datos y privacidad de la información personal.		
		33.5 Regulación de los controles criptográficos.		
	34. Revisiones de la seguridad de la información.	34.1 Revisión independiente de la seguridad de la información.		
		34.2 Cumplimiento de las políticas y normas de seguridad.		
		34. Comprobación del cumplimiento.		

3.3.2. Identificación de controles ISO 27002:2017

Este análisis corresponde a la identificación de medidas para anticipar, mitigar o minimizar las amenazas encontradas. Es importante resaltar que la norma 27002 está en constante actualización. Sus cambios más se radican en conceptos, los cuales identifican un espacio o más grande o más reducido, los mismos no afectan a los controles establecidos por la organización internacional de normalización por lo que responsablemente ISO sugiere usar tanto la norma 27002:2013 o 27002:2017 siempre que se mantengan presentes los cambios efectuados. La Tabla 11 muestra a manera de ejemplo la matriz que ayudo a la identificación de los controles acordes a las amenazas identificadas.

Tabla 11 Matriz para la identificación de Controles ISO 27002.
Fuente: Elaboración Autor

NOMBRE ACTIVO	AMENAZAS	DOMINIO CONTROL	OBJETIVO DE CONTROL	CONTROL
Información Académica	Bajo control en el acceso a los datos	Control de accesos	Control de acceso a sistemas y aplicaciones	Gestión de contraseñas de usuarios
Base de datos	Deficiente inventario de activos	Gestión de Activos	Responsabilidad sobre los activos	Inventario de Activos
Aplicación web	Deficientes lineamientos de seguridad en el acceso	Control de accesos	Control de acceso a sistemas y aplicaciones	Gestión de contraseñas de usuarios

cada control necesita un análisis crítico para comprender que es lo que se intenta anticipar, mitigar o minimizar.

CAPÍTULO IV

PROPUESTA

4.1. Modelo sistema de gestión para la seguridad de la información

La Universidad Estatal del Sur de Manabí – UNESUM por medio de la Unidad de Sistemas Informáticos debe implementar, operar, supervisar, revisar, mantener y mejorar el presente modelo de gestión para la seguridad de la información, aplicado al sistema académico.

Este modelo se apoya en el ciclo de mejora continua e incorpora controles de seguridad de la información, mismos que se encuentran descritos en la norma internacional ISO 27002:2001.

Actualmente el sistema académico es el eje principal de la institución brindando las facilidades a estudiantes, docentes y personal administrativo para realizar los diferentes procesos académicos que son exigidos por la universidad.

Considerando la fuerte dependencia de la UNESUM sobre el sistema Académico (S@U) se hace evidente la necesidad de contar con una herramienta de gestión como apoyo al personal informático, contando con lineamientos que les permita implantar una política de seguridad acorde a las necesidades del sistema descrito anteriormente.

A continuación, se indican los lineamientos a considerar para la implementación del sistema de gestión de seguridad de la información (de aquí en adelante SGSI) aplicado al sistema académico de la UNESUM.

4.2. FASE I: PLANIFICACIÓN

4.2.1. Alcance del SGSI

Se resalta que este alcance puede ser adaptado en caso de necesitar incorporar nuevos espacios para la implementación del SGSI.

El sistema de gestión para la seguridad de la información - SGSI incorpora lineamientos de seguridad de la información en el sistema académico S@U basados en el estándar internacional ISO 27002:2017 para así preservar la integridad, disponibilidad y confidencialidad de la información almacenada en el mismo.

“Se resalta que este alcance puede ser adaptado en caso de necesitar incorporar nuevos espacios para la implementación del SGSI”

4.2.2. Marco Regulatorio

En este apartado incorpora toda información concerniente a las leyes vigentes, proporcionando la base legal necesaria para sustentar la implementación del SGSI.

De acuerdo a las leyes vigentes:

- El numeral 3 del artículo 225 de la Constitución de la República del Ecuador, señala que el sector público comprende: los organismos y entidades creados por la Constitución o la ley para el ejercicio de la potestad estatal, para la prestación de servicios públicos o para desarrollar actividades económicas asumidas por el Estado.
- La Gaceta Oficial electrónica del Consejo de Educación Superior almacena el estatuto de la UNIVERSIDAD ESTATAL DEL SUR DE MANABI, mismo que en su base legal indica textualmente “Art. 1.- Naturaleza. - La Universidad Estatal del Sur de Manabí, es una Institución de Educación Superior Pública creada mediante Ley No. 38 publicada en el Registro Oficial No. 261 de 7 de febrero de 2001, tiene su domicilio en la ciudad de Jipijapa, provincia de Manabí, constituida por el Estado como persona

jurídica sin fines de lucro, por lo que sin lesionar su autonomía constitucionalmente establecida, debe articular sus actividades con el Sistema de Educación Superior, el Plan Nacional de Desarrollo y el Plan Nacional del Buen Vivir. Por su naturaleza jurídica, la Universidad Estatal del Sur de Manabí, orientará sus actividades de docencia, investigación, postgrado, vinculación con la sociedad y gestión, a servir a la población del sur de Manabí y buscará trascender sus servicios al contexto nacional. Se rige por la Constitución de la República del Ecuador, la Ley Orgánica de Educación Superior y su Reglamento, los Reglamentos y las Resoluciones expedidas por el organismo público de planificación, regulación y coordinación del sistema de educación superior, el presente Estatuto, los Reglamentos que se expidan por los órganos propios de su gobierno y demás resoluciones de sus autoridades.”.

- La Constitución de la República del Ecuador, en el artículo 211, establece que la Contraloría General del Estado es un organismo técnico, encargado del control de la utilización de los recursos estatales, y de las personas jurídicas de derecho privado que dispongan de recursos públicos.
- El numeral 3 del artículo 212 de la Constitución de la República del Ecuador, establece como función de la Contraloría General del Estado expedir la normativa para el cumplimiento de sus funciones.
- El artículo 7 numeral 1 de la Ley Orgánica de la Contraloría General del Estado, faculta al Organismo Técnico de Control, expedir y actualizar las Normas de Control Interno, que sirvan de marco básico para que las instituciones del Estado y sus servidoras y servidores establezcan y pongan en funcionamiento su propio control interno.
- Las Normas de Control Interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, contienen

el apartado 410 Tecnologías de la Información, el cual hace referencia a los diferentes puntos a tomar en consideración para la gestión de las tecnologías de acuerdo a las necesidades de la institución.

- De acuerdo a las normas de control interno de la Contraloría General del Estado en su apartado 410-10 Seguridad de tecnología de información expresa textualmente "La Unidad de Tecnología de Información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medidas:

  1. Ubicación adecuada y control de acceso físico a la Unidad de Tecnología de Información y en especial a las áreas de: servidores, desarrollo y bibliotecas.

  2. Definición de procedimientos de obtención periódica de respaldos en función a un cronograma definido y aprobado. 3. En los casos de actualización de tecnologías de soporte se migrará la información a los medios físicos adecuados y con estándares abiertos para garantizar la perpetuidad de los datos y su recuperación.

  4. Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización

  5. Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados.

  6. Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire controlado, disponer de energía acondicionada, esto es estabilizada y polarizada, entre otros;

  7. Consideración y disposición de sitios de procesamiento alternativos.

8. Definición de procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana."

- De acuerdo al Modelo de Evaluación Institucional de Universidades y Escuelas Politécnicas 2018 emitido por el Consejo de Educación Superior en su numeral 5.1.3. establece "La IES cuenta con sistemas informáticos, conectividad necesaria y procedimientos para la gestión de los procesos académicos, lo cual garantiza accesibilidad, disponibilidad, confiabilidad y transparencia de la información; y su estructura responde a la lógica de los procesos sustantivos."

4.2.3. Análisis y evaluación del Riesgo

En este apartado se incorpora el desarrollo del análisis de riesgos o en su defecto el resultado de la evaluación del mismo.

El personal de la Unidad de Sistemas Informáticos de la Universidad Estatal del Sur de Manabí (de aquí en adelante UNESUM) deberá tomar como punto de partida el análisis y evaluación de riesgos realizado al sistema académico de la institución, misma que se detalla en el numeral 3.2 y 3.2.43.2.1.

Como resultado de este análisis se identificó que el sistema Académico mantiene riesgos considerables que podrían comprometer información importante como notas parciales, notas finales, record académico, entre otros, los cuales representan a una población activa de alrededor de 7000 usuarios de acuerdo a los registros del mismo.

4.2.4. Identificación y selección de controles ISO 27002:2017

El personal de la Unidad de Sistemas Informáticos de la UNESUM analizará los controles de seguridad de la información ISO 27002:2017 descritos en el numeral 3.3.2 y escogerá los más necesarios acordes a la necesidad institucional, la siguiente tabla muestra a manera de ejemplo el resultado de esta actividad.

Tabla 12 Identificación y selección de Controles ISO 27002.
Fuente: Elaboración Autor

NOMBRE ACTIVO	AMENAZAS	DOMINIO CONTROL	OBJETIVO DE CONTROL	CONTROL
Información Académica	Bajo control en el acceso a los datos	Control de accesos	Control de acceso a sistemas y aplicaciones	Gestión de contraseñas de usuarios
Base de datos	Deficiente inventario de activos	Gestión de Activos	Responsabilidad sobre los activos	Inventario de Activos
Aplicación web	Deficientes lineamientos de seguridad en el acceso	Control de accesos	Control de acceso a sistemas y aplicaciones	Gestión de contraseñas de usuarios

4.2.5. Implementación de los controles ISO 27002:2017 seleccionados

El personal de la Unidad de Sistemas Informáticos de la UNESUM no distinguirá orden en el que se escojan e implementen los controles de seguridad dentro del SGSI debido a que no es necesario seguir un orden específico para la implementación de los mismos (los literales descritos a continuación corresponden a la Tabla 10 Mapa Controles ISO 27002:2017.), debido a que cada espacio será diferente y requerirá solo controles específicos, para el caso de estudio, a continuación, los lineamientos:

Política de seguridad de la información

El personal de la Unidad de Sistemas Informáticos de la UNESUM proporcionará orientación y soporte de acuerdo a los requisitos de la institución, las leyes vigentes y reglamentos que se consideren pertinentes para la protección del sistema académico.

El personal de la Unidad de Sistemas Informáticos de la UNESUM desarrollará el documento “política de seguridad de la información para el sistema académico” de la institución basados en el análisis de riesgos realizado, mismo que en su resultado representa la necesidad institucional (Véase numeral 3.2.4).

La política de seguridad deberá ser presentada a la Máxima Autoridad para su aprobación, publicada y comunicada a los empleados y partes externas relevantes. La misma podrá definirse al máximo nivel y su desarrollo debe contemplar:

- La estrategia de la Institución.

- Leyes, reglamentos y contratos.
- Un análisis actual y previsto de las amenazas para la seguridad de la información.
- Se debe incorporar explicaciones claras en torno a:
  - ✓ Definiciones y Objetivos para orientar la seguridad de la información.
  - ✓ Asignar responsabilidades específicas y generales considerando los roles definidos en torno a la gestión de seguridad de la información.
  - ✓ Ordenamientos para manejar los desvíos y alteraciones.

En caso de definirse a un nivel inferior, la política de seguridad de la información debe apoyarse en temas específicos que atiendan las necesidades de espacios internos de la institución cubriendo temas de interés, para ello se sugiere a manera de ejemplo:

- Política de control de accesos.
- Políticas para copias de seguridad controladas.
- Política de escritorio limpio, y las que se identifiquen de acuerdo a la necesidad de la UNESUM.

El personal de la Unidad de Sistemas Informáticos para este caso específico debe desarrollar la política de seguridad a un nivel inferior con un mínimo de tres controles.

Revisión de la política para la seguridad de la información

El personal de la Unidad de Sistemas Informáticos de la UNESUM revisará la política de seguridad de la información en intervalos de tiempo planificados cada 6 meses o en su defecto por cambios relevantes con el fin de asegurar su eficacia e idoneidad. Todo cambio deberá forzadamente ser socializado y publicado.

Aspectos organizativos de la seguridad de la información

Organización Interna

El personal de la Unidad de Sistemas Informáticos de la UNESUM incluirá un marco normativo el cual se orientará a ejercer control sobre la implementación y operación de la seguridad de la información dentro de la institución.

Asignación de responsabilidades para la seguridad de la información

El personal de la Unidad de Sistemas Informáticos de la UNESUM identificará y documentará toda(s) la(s) responsabilidades que se consideren pertinentes para la protección de la información del sistema académico.

Las responsabilidades podrán ser delegadas a subalternos por su principal, dicha delegación no los exime del compromiso adquirido, por lo tanto, se deberá mantener un estricto seguimiento a las tareas delegadas.

Las delegaciones de las responsabilidades deben quedar evidenciadas por escrito, debiendo considerar:

- Identificar y definir los activos y procesos de la seguridad de la información (de aquí en adelante S.I.)
- Asignar un responsable para cada activo o proceso de S.I. y documentar los detalles de las responsabilidades asignadas.
- Precisar y documentar los niveles de autorización de manera individual o grupal.
- Mantener actualizados los trabajos desarrollados.
- Desarrollar y documentar los roles de supervisión y coordinación de la S.I. cuando se mantengan relaciones con personal externo.

Segregación de tareas

El personal de la Unidad de Sistemas Informáticos de la UNESUM en los espacios de responsabilidad donde se asignen tareas que puedan generar conflictos en cuyos casos podría

existir modificación de datos no autorizada o sin intención o uso indebido de los activos de información, deberá garantizar que las mismas se realicen con la respectiva autorización, la cual debe ser impuesta por varias personas con la finalidad de no caer en errores.

Contacto con autoridades

El personal de la Unidad de Sistemas Informáticos de la UNESUM desarrollará e implementará procedimientos que especifiquen el protocolo para el contacto con las autoridades (legales, reglamentarias o de supervisión) y bajo qué circunstancias se informará sobre los eventos detectados, se puede puntualizar como ejemplo la sospecha de alguna indisciplina sea esta interna o externa.

Contacto con grupos de interés especial

El personal de la Unidad de Sistemas Informáticos de la UNESUM deberá mantener un contacto permanente con profesionales, organizaciones o asociaciones especializadas en seguridad de la información.

Una buena opción sería involucrarse como miembro activo en los grupos, foros, wikis electrónicas con la finalidad de:

- Actualizar o mejorar conocimientos sobre las practicas más sobresalientes en materia de seguridad de la información.
- Mantener un entendimiento del entorno de S.I. actualizado.
- Contar con avisos en el correo electrónico sobre los diferentes ataques de seguridad de ser posible a nivel global, alertas y soluciones encontradas.
- Los que más se ajusten al entorno de la institución.

Seguridad de la Información en la gestión de proyectos

El personal de la Unidad de Sistemas Informáticos de la UNESUM desarrollará normativas que obligadamente involucren su participación en los proyectos independientemente de la naturaleza de cada uno de ellos.

Con la finalidad de asegurar que los riesgos a los que se exponga la información sean identificados y tratados dentro del marco de un proyecto se deberá incluir seguridad para la información en el método o métodos de gestión de proyectos, estos deberán exigir que:

- Los objetivos de la S.I. sean incluidos en los del proyecto.
- Se realice una evaluación de riesgos de S.I. en una fase anticipada del proyecto con la finalidad de tener presente los controles con respecto a seguridad de la información que se requieran cuando se ejecute el proyecto.

Gestión de activos

Responsabilidad sobre los activos

El personal de la Unidad de Sistemas Informáticos de la UNESUM identificará los activos de la institución y puntualizará las responsabilidades de protección adecuados.

Inventario de activos

El personal de la Unidad de Sistemas Informáticos de la UNESUM evaluará e informará sobre las instalaciones usadas para el procesamiento de la información, los activos asociados a la misma y la propia información identificando, elaborando y manteniendo actualizado el inventario de los mismos.

El personal de la Unidad de Sistemas Informáticos de la UNESUM identificará cada activo relevante, considerando el ciclo de vida de la información y documentando la importancia de la misma. Se debe tener presente que la información debe incluir su creación u origen, almacenamiento, procesamiento, transmisión, destrucción y borrado, como ejemplo para la identificación de los activos se puede tomar como referencia la Tabla 2 del numeral 433.2.3 Identificación y Valoración de activos de información de este documento.

Propiedad de los activos

El personal de la Unidad de Sistemas Informáticos de la UNESUM habiendo identificado los activos deberá coordinar con la Unidad de Administración de bienes la asignación de los respectivos custodios finales.

Forzadamente deberá hacerse conocer a los custodios finales que el uso de los activos deberá realizarse de manera responsable considerando el ciclo de vida del mismo, para lo cual el custodio deberá:

- Recibir el bien correctamente inventariado.
- Velar que sus activos de información estén protegidos correctamente.
- Considerar las normativas internas y externas de su competencia vigente en caso de existir.

Control de accesos

Control de acceso a sistemas y aplicaciones

El personal de la Unidad de Sistemas Informáticos de la UNESUM deberá prevenir el acceso no autorizado a las aplicaciones y los sistemas de información.

Gestión de contraseñas de usuarios

El personal de la Unidad de Sistemas Informáticos de la UNESUM gestionará las contraseñas que permiten el acceso a los sistemas de información y aplicaciones web de manera interactiva, las mismas deben ser de calidad.

A conveniencia de la institución la gestión de contraseñas debería al menos contemplar lo siguiente:

- Las contraseñas deberán ser asignadas de manera individual en lo posible manejando identificadores de usuario (ID).

- El sistema de gestión de contraseñas deberá permitir a los usuarios cambiar la contraseña, este deberá incluir un procedimiento de aceptación que controle los errores de entrada.
- Se deberá solicitar al menos un requisito mínimo que contemple: un mínimo de ocho (8) caracteres, letras mayúsculas, letras minúsculas, números y los que se consideren necesarios.
- Deberá solicitar para el primer inicio de sesión obligatoriamente el cambio de contraseña.
- Deberá solicitar periódicamente a los usuarios el cambio de la contraseña.
- Deberá contar con una base de datos de contraseñas usadas e impedir el uso de la misma en un nuevo cambio.
- Deberá contar con un método de ocultamiento en pantalla para las contraseñas.
- Deberá contar con métodos de seguridad de transmisión de las contraseñas.

4.2.6. Aprobación del inmediato superior

El personal de la Unidad de Sistemas Informáticos de la UNESUM presentará un documento numerado, fechado y sellado mediante el cual presentará el borrador de la política de seguridad al inmediato superior de la Unidad Informática con la finalidad de obtener su aprobación en primera instancia.

4.2.7. Autorización para la Implementación del SGSI

El Responsable de la Unidad de Sistemas Informáticos de la UNESUM una vez generada, presentada y aprobada la documentación referente al Sistema de Gestión para la Seguridad de la Información deberá obligatoriamente contar con un documento fechado, numerado y sellado por la autoridad inmediata superior o quien ejerza, en el que se describa la **AUTORIZACIÓN** para la implementación del mismo.

4.2.8. Elaboración de la declaración de aplicabilidad

El personal de la Unidad de Sistemas Informáticos de la UNESUM deberá redactar un documento en el cual se detallen los objetivos de control aplicados, considerando responsabilidades contractuales, requisitos legales o de la institución para la seguridad de la información, la Tabla 13 puede ser un ejemplo donde:

RL: Requerimiento Regulatorio

OC: Obligación Contractual

AR: Análisis de Riesgos

Tabla 13 Matriz sugerida para la elaboración de la Declaración de Aplicabilidad.
Fuente: Elaboración Autor

ISO27002:2017					**Razones para la selección**		
Objetivos de control	**Control**	**Justificación para exclusión**	**Medidas existentes**	**Medidas planificadas**	**RL**	**OC**	**AR**
7. Gestión de activos	7.1 Responsabilidad sobre los activos			Realizar el inventario de los activos de información	X		

4.3. FASE II: Implementación y utilización del SGSI

El personal de la Unidad de Sistemas Informáticos de la UNESUM habiendo obtenido la aprobación y autorización por escrito de la autoridad competente para la implementación del SGSI, debe ejecutar lo siguiente para la implementación:

La Formulación del plan de tratamiento de riesgos: el cual deberá contener el compromiso del jefe inmediato superior, mismo que deberá proporcionar las evidencias necesarias para permitir la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora del modelo de gestión para la seguridad de la información del sistema académico UNESUM.

Así mismo se deberá comunicar a los directivos de la institución la importancia del cumplimiento de objetivos y la política de seguridad desarrollada, responsabilidades legales y la mejora continua.

Finalmente coordinar la provisión de los recursos necesarios y las revisiones del SGSI.

La implementación del plan de tratamiento de riesgos: con la finalidad de cumplir con la aplicación de los controles identificados el personal de Unidad de Sistemas Informáticos de la UNESUM deberá contar con el financiamiento, asignación de responsabilidades y las respectivas funciones.

La implementación de los controles: el personal de Unidad de Sistemas Informáticos de la UNESUM analizará y aplicará los controles de seguridad identificados (véase **¡Error! No se encuentra el origen de la referencia.**).

Medir la eficacia de los controles aplicados: el personal de Unidad de Sistemas Informáticos de la UNESUM investigará y aplicará un método para la medición de la eficacia en la aplicación del(os) los controles seleccionados.

Desarrollar y aplicar un programa de concienciación: el personal de Unidad de Sistemas Informáticos de la UNESUM apoyados en la Dirección de Comunicación Social desarrollará y difundirá un programa de concienciación de la seguridad de la información con la finalidad de que todo el personal involucrado en el SGSI tenga claras sus competencias, considerando:

- Impartir charlas con respecto a la importancia de la seguridad de la información.
- Socializar los cambios realizados al SGSI y a la política de seguridad con respecto a su importancia y cumplimiento.
- Distribución de poster y trípticos sobre seguridad de la información.
- Consejos sobre seguridad mensuales, entre otros.

4.4. FASE III: Monitorizar y revisar el SGSI

4.4.1. Lineamientos para el monitoreo del SGSI

Con la finalidad de monitorear el SGSI y obtener resultados comparables que permitan conocer si se están cumpliendo los objetivos establecidos, el personal de la Unidad de Sistemas Informáticos deberá:

- Desarrollar y ejecutar operaciones de supervisión y revisión con el propósito de detectar lo antes posible errores.
- Identificar las deficiencias del SGSI, sus incidentes sea que se haya tenido éxito o no.
- Determinar qué tan efectivas son las acciones tomadas en la resolución de eventos de seguridad presentados.
- Realizar un control para conocer el nivel de cumplimiento de los objetivos de control seleccionados.
- Planificar una auditoria interna al SGSI.
- Revisar regularmente el SGSI identificando si su implementación ha sido adecuada y resaltar las mejoras obtenidas.
- Registrar las incidencias que pudieran afectar la eficiencia del SGSI.

4.5. FASE IV: Mantener y mejorar el SGSI

4.5.1. Lineamientos para la mejora del SGSI

Como operación vital del ciclo de mejora continua del modelo SGSI se obtiene retroalimentación y enmendación de posibles fallos dentro del SGSI, de igual manera permite el desarrollo sobre criterios de prevención a posibles eventos que se presenten, para ello el personal de la Unidad de Sistemas Informáticos aplicará al SGSI las mejoras detectadas en el proceso de monitoreo basándose en el uso de las políticas de seguridad y resultados de auditorías.

4.5.1.1. Acciones correctivas

El personal de la Unidad de Sistemas Informáticos de la UNESUM junto con la Autoridad competente analizará y aplicará acciones correctivas para separar las causas de posibles fallos en el SGSI, y que las mismas no vuelvan a ocurrir, para ello se tendrá presente lo siguiente:

- Valorar en caso de ser necesario las acciones para identificar las inconformidades que se puedan presentar.
- Valorar las causas que incitan a que las no satisfacciones surjan.
- Determinar las acciones correctivas necesarias consideradas convenientes para el SGSI.
- Realizar periódicamente una revisión de las acciones correctivas, estas pueden ser los controles de registros sean estas bitácoras, libros de informes de auditorías entre otras que se considere incorporar para mejora del SGSI.

Habiéndose ejecutado el SGSI basado en el modelo propuesto, la UNESUM contará con una herramienta de gestión que apoyará las actividades de los técnicos en la gestión de incidentes e implementará seguridad a el sistema académico, la experiencia obtenía permitirá ampliar el ámbito de aplicación a otros sistemas informáticos y esas mejoras apoyaran significativamente a la gestión departamental.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

La información del sistema académico se encuentra propensa al robo, destrucción, divulgación y manipulación, debido a la falta de gestión en incidentes de seguridad de la información.

El personal de la Unidad de Sistemas Informáticos de la UNESUM debe ser consciente que el sistema académico maneja la información de alrededor de siete mil usuarios, y es de vital importancia que se desarrollen medidas que protejan y salvaguarden la información que es procesada y almacenada con ayuda de este sistema de información.

Las leyes estatales son claras y su aplicabilidad es obligatoria a las instituciones públicas por lo tanto la Unidad de Sistemas Informáticos de la UNESUM deben tener presente que la no aplicación de las mismas traerá consecuencias legales muy graves a la institución.

El personal de la Unidad de Sistemas Informáticos de la UNESUM debe incorporar buenas prácticas de seguridad de la información a sus actividades diarias, una metodología a seguir, es el estándar internacional ISO 27002:2017.

El personal informático debe tener una participación más representativa en el desarrollo de mecanismos que ayuden a la protección del sistema académico de la Universidad Estatal del Sur de Manabí.

La implementación del modelo SGSI fortalecerá la gestión de incidentes de seguridad de la información y a su vez brindará protección a los sistemas de información en general de la institución.

5.2. RECOMENDACIONES

El personal de la Unidad de Sistemas Informáticos de la UNESUM debe aplicar el Modelo SGSI, mismo que les permitirá desarrollar mecanismos para la gestión de incidentes de seguridad de la información.

El personal de la Unidad informática de la UNESUM debe desarrollar la política de seguridad de la información orientada a la protección de su sistema académico.

Presentar el Modelo de Gestión de Seguridad de la Información-SGSI ante la máxima autoridad y explicar la importancia de su aplicación.

Lograr la aprobación y respaldo de la máxima autoridad, permitiendo que se aplique como política institucional en la gestión informática.

Una vez implementado el SGSI el personal de la Unidad de Sistemas Informáticos de la UNESUM debe evaluar con regularidad la gestión de la seguridad de la información con la consigna de anticiparse o detectar con antelación alguna vulnerabilidad que ponga en riesgo la seguridad, integridad y disponibilidad de la información.

Incorporar dentro del grupo informático al menos un especialista en seguridad de la información, con la finalidad de fortalecer la seguridad en sus procesos automatizados.

Capacitar al personal informático de la institución en el uso de la norma ISO 27002:2017 con respecto a la seguridad de la información para así contar con personal idóneo que apoye a la resolución de problemas que se presenten.

Comunicar a los usuarios sobre la seguridad a la información aplicada en el sistema académico con la finalidad de que conozcan que las ventajas, beneficios y sanciones a los están sujetos cuando se use el sistema académico.

El modelo sugerido es adaptable a diferentes entornos permitiendo a futuro implementar diferentes normas que fortalezcan la seguridad de la información en los sistemas informáticos.

A futuro cuando el modelo alcance un nivel de madurez confiable se aplique al entorno institucional como una política integral.

BIBLIOGRAFÍA

27002:2005. (2013). Introducción a ISO 27002 / ISO27002. Recuperado de http://www.27000.org/iso-27002.htm

Bautista, B. (2018). Diseño de un sistema de gestión de seguridad informática para la alcaldía municipal de la Jagua de Ibirico – Cesar basado en la Norma ISO 27001:2013. Recuperado de http://repository.unad.edu.co/handle/10596/14253

CEAACES. (2018). Modelo-evaluacion-preliminar-universidades-escuelas-politecnicas2018.pdf. Recuperado de http://ucsg.edu.ec/dmdocuments/Modelo-evaluacion-preliminar-universidades-escuelas-politecnicas2018.pdf

CES. (2018). Misión, visión y objetivos | CES - Consejo de Educación Superior | Ecuador. Recuperado de http://www.ces.gob.ec/index.php?option=com_content&view=article&id=1&Itemid=140

CGE. (2009). Normas de Control Interno de la Contraloría General del Estado. Quito: Contraloría General del Estado. Recuperado de http://www.gobiernoelectronico.gob.ec/wp-content/uploads/downloads/2017/09/Normas-de-control-interno-de-la-CGE.pdf

Chamorro, S., & Paul, D. (2015). Definición de las políticas de seguridad de la información para la red convergente de la Presidencia de la República del Ecuador basado en las normas ISO 27000. Recuperado de http://bibdigital.epn.edu.ec/handle/15000/11462

de Luján, U. N. (2018). Amenazas a la Seguridad de la Información | Universidad Nacional de Luján | Departamento de Seguridad Informática | Buenos Aires, Argentina. Recuperado de http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

Gaceta Oficial. (2017). C. E. S. - Consejo de Educación Superior - Gaceta Oficial. Recuperado de http://gaceta.ces.gob.ec/inicio.html

Gómez, L., & Álvarez, A. (2012). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para PYMES. Madrid: Asociación Española de Normalización y Certificación.

ILNAS. (2017). ILNAS-EN ISO/IEC 27002: PDF. Recuperado de http://docplayer.org/58470050-Ilnas-en-iso-iec-27002-2017.html

INCIBE. (2016, enero 27). Recuperado 26 de mayo de 2018, de https://www.incibe.es/que-es-incibe

ISO. (2017). ISO - International Organization for Standardization. Recuperado de https://www.iso.org/home.html

ISO, I. 27001. (2013). ISO/IEC 27001:2013(en), Information technology — Security techniques — Information security management systems — Requirements. Recuperado de https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27001:ed-2:v1:en

Laudon, F. (1996). Sistemas de Información. Editorial Diana, México.

MAGERIT. (2012). Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método, 127.

Mieres, J. (2009). Ataques informáticos. Debilidades de seguridad comúnmente explotadas). Recuperado http://proton. ucting. udg. mx/tutorial/hackers/hacking. pdf.

Moreno, E. (2016). Portal Web Oficial de la Contraloría General del Estado del Ecuador. Recuperado de http://www.contraloria.gob.ec/LaInstitucion/FundamentoLegal

Navarro, E. (2000). Ley de protección de datos: la nueva LORTAD. España: Ediciones Díaz de Santos.

Nieves, C. (2017). Diseño de un sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO/IEC 27001:2013. Recuperado de http://repository.poligran.edu.co/bitstream/handle/10823/994/Trabajo%20Final.pdf?sequence=1&isAllowed=y

Núñez, M. (2015). Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato. Recuperado de http://repositorio.uta.edu.ec/jspui/handle/123456789/13057

QUISEC. (2017). Seguridad de la Información de acuerdo a las ISO 27002/13. | QUISEG. Recuperado de https://www.quiseg.com.ar/seguridad-de-la-informacion-de-acuerdo-a-las-iso-2700213/

Riaño, Á., & Herley, J. (2017). Diseño de un sistema de gestión de seguridad de la información - SGSI basado en la norma ISO27001 para el colegio PRO-COLOMBIANO de la ciudad de Bogotá que incluye: asesoría, planeación. Recuperado de http://repository.unad.edu.co/handle/10596/11950

Sarmiento, P., & Arias, G. (2016). Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para la Empresa Agility S.A.S. Recuperado de http://repository.udistrital.edu.co/handle/11349/4709

Tur Hartmann, J. (2016). Elaboración de un plan de implementación de la ISO/IEC 27001: 2013 en un ayuntamiento. Universitat Oberta de Catalunya.

Zatán, G. (2017). Plan de seguridad informática basada en la norma Iso 27002 para el control de accesos indebidos a la red de Uniandes Puyo.

ANEXO A

ENCUESTA DIRIGIDA AL PERSONAL TÉCNICO DE LA UNIDAD DE SISTEMAS INFORMATICOS DE LA UNIVERSIDAD ESTATAL DEL SUR DE MANABI – UNESUM SOBRE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Pregunta 1: ¿Cómo considera usted a la información almacenada en el sistema académico de la UNESUM?

a. Importante
b. Poco Importante
c. Nada Importante
d. No sabe

Argumente su calificación

_____

Pregunta 2: ¿Cuál de los siguientes incidentes con respecto a los datos que se almacenan en el sistema académico se han presentado con frecuencia en la Institución?

a. Robo
b. Modificación
c. Perdida
d. Manipulación
e. Otro especifique _____
f. Desconoce

Pregunta 3: Con respecto a la respuesta de la pregunta 2 ¿Conoce usted el procedimiento con el cuál se gestiona el incidente presentado en la Institución?

a. Sí
b. No
c. No sabe

En el caso de que su respuesta sea positiva describa por favor

_____

Pregunta 4: ¿Cómo considera usted a la gestión de la seguridad de los datos del sistema académico de la UNESUM?

a. Buena
b. Mala
c. Regular

Pregunta 5: ¿Cómo califica usted al proceso de gestión de seguridad aplicado a la autenticación de accesos al sistema académico de la UNESUM?

a. Bueno
b. Regular
c. Malo

Pregunta 6: ¿Conoce usted alguna metodología sobre gestión de seguridad de la información que se haya implantado en el sistema académico de la UNESUM?

a. Sí
b. No
c. No sabe

En el caso de que su respuesta sea positiva describa cuál, caso contrario especifique las causas por las que cree usted que no conoce.

_____

Pregunta 7: ¿Conoce usted alguna metodología que ayude a mejorar o implantar una buena gestión en seguridad de la información para la protección del sistema académico de la UNESUM?

a. Sí
b. No
c. No sabe

En el caso de que su respuesta sea positiva describa por favor:

_____

Pregunta 8: Puede escoger más de una respuesta. De acuerdo a su criterio el estándar internacional ISO 27002 ayuda a:

a. Gestionar la seguridad de la Información
b. Identificar y valorar los riesgos
c. Implementar nuevas configuraciones en los servidores para mejorar la protección de los datos.
d. Todas las anteriores
e. Desconoce

Pregunta 9: Puede escoger más de una respuesta. De acuerdo a su criterio escoja los controles que pertenezcan al estándar internacional ISO 27002:2017

a. Política de seguridad
b. Leyes
c. Gestión de activos
d. Control de accesos
e. Todas las anteriores
f. Ninguna de las anteriores

Pregunta 10: ¿Considera usted que es importante contar con una herramienta de seguridad de la información basada en un estándar internacional que permita gestionar la protección del sistema académico de la UNESUM?

a. Sí
b. No
c. No sabe

Argumente su calificación _____

ANEXO B
FICHAS DE OBSERVACIÓN DIRECTA

Ficha de Observación directa #1

Tema:		Gestión de Seguridad del Sistema Académico
Subtema:		Seguridad de Información digital
Lugar:		UNESUM- Sede Complejo Universitario
Fuente:		Técnicos
Fecha:		Jipijapa, 9 octubre 2017
HORA	**AM** 9:30a10:30	
	PM 14:00a16:00	

Ficha de Observación directa #2

Tema:		Gestión de Seguridad del Sistema Académico
Subtema:		Seguridad de Información digital
Lugar:		UNESUM-Sede "Los Ángeles"
Fuente:		Técnicos
Fecha:		Jipijapa, 11 octubre 2017
HORA	**AM** 9:00a10:30 **PM** 14:00a16:00	

ANEXO C

ENTREVISTA DIRIGIDA A LA AUTORIDAD

Como jefe del Departamento informático cuénteme sobre las medidas de gestión de seguridad de la información adoptadas en el sistema académico web de la UNESUM.

Eso con respecto a la parte técnica, pero y en ¿en la parte de gestión?

¿Pero no considera usted que el proceso debe nacer del departamento informático?

¿Y sobre la gestión para tratar la perdida de datos?, producida por cualquier amenaza informática

Como gestiona la seguridad de la información sobre los accesos que manejan los usuarios al sistema académico web de la UNESUM.

existe algún manual con respecto a la gestión de seguridad de la información

Porque

Han tenido algún incidente con respecto a la información.

Con que frecuencia ocurre esto

Conoce sobre el proceso de gestión de seguridad de la información que se sigue para informar al responsable informático que una persona que tiene acceso al sistema académico ya no trabaja en la institución.

¿Existe un proceso?

Considera a la gestión de seguridad de la información necesaria para la UNESUM