UNIVERSIDAD INTERNACIONAL SEK

DIGITAL SCHOOL

Trabajo de investigación titulado:

Diseño de un Modelo de Ciberseguridad basado en la Norma ISO/IEC 27002:2017 para el Sistema de Gestión Académica Ignug del Instituto Superior Tecnológico Yavirac

Realizado por:

Ing. Lorena Elizabeth Chulde Obando

Director del proyecto:

Ing. Verónica Elizabeth Rodríguez Arboleda, MBA.

Como requisito para la obtención del título de:

MÁSTER EN CIBERSEGURIDAD

Quito, marzo 2021

DECLARACION JURAMENTADA

Por la presente, yo, Lorena Elizabeth Chulde Obando, con cédula de ciudadanía Nº. 0401110481, 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 he consultado las referencias bibliográficas que se incluyen en este documento.

A través de esta declaración cedo mis derechos de propiedad intelectual de autora a la UNIVERSIDAD INTERNACIONAL SEK UISEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

_____

LORENA ELIZABETH CHULDE OBANDO

CC: 0401110481

DECLARACIÓN DE DIRECTOR DE TESIS

El presente que el presente trabajo de investigación titulado:

“Diseño de un Modelo de Ciberseguridad basado en la Norma ISO/IEC 27002:2017 para el Sistema de Gestión Académica Ignug del Instituto Superior Tecnológico Yavirac”

Realizado por:

Ing. Lorena Elizabeth Chulde Obando

Como requisito para la obtención del título de

MÁSTER EN CIBERSEGURIDAD

Ha sido dirigido por mi persona a través de reuniones periódicas con la estudiante y cumple con todas las disposiciones que rigen los trabajos de titulación.

_____

Ing. Verónica Rodríguez Arboleda, MBA.

DIRECTORA DEL PROYECTO

CC: 1707522312

LOS PROFESORES INFORMANTES

Los profesores informantes:

Ing. José Luis Medina Balseca, MSc

Ing. Joe Carrión Jumbo, PhD

Después de revisar el trabajo, lo han calificado

como apto para su defensa oral ante el tribunal examinador

El profesor informante:

Ing. José Luis Medina Balseca, MSc	Ing. Joe Carrión Jumbo, PhD

Quito, marzo de 2021

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es de mi autoría, que se han citado las fuentes correspondientes y que en su desarrollo se respetaron las disposiciones legales vigente, que protegen los derechos de autor.

_____

Lorena Elizabeth Chulde Obando

CC: 0401110481

AGRADECIMIENTO

A la Universidad Internacional SEK, a los docentes y a las autoridades de la Maestría de Ciberseguridad, por haber sido parte de mi formación profesional y transmitirme sus conocimientos con compromiso y ética profesional.

A la Ing. Verónica Rodríguez tutora de tesis, quien con su guía aportó para la estructuración y desarrollo exitoso de la investigación.

A mi madre Olga Obando, por su preocupación y colaboración con mis estudios de cuarto nivel.

A mi esposo Hugo Défaz, quien me ha respaldado continuamente para finalizar mis estudios de postgrado.

DEDICATORIA

El presente trabajo de titulación lo dedico a:

A Dios, por bendecirme y permitirme que me encuentre con toda mi familia con bienestar y salud.

A mi madre Olga Obando, quien ha sido un modelo de superación y esfuerzo, me ha inculcado valores y principios para ser una buena persona, buena hija y buena profesional.

A mi esposo Hugo Défaz, quien me ha apoyado en todo momento para finalizar exitosamente el postgrado de Máster en Ciberseguridad.

A mis hijos, Katherine, Anderson y Darla quienes, con su cariño y motivación, han sido un pilar fundamental para la culminación del proyecto de titulación.

A mi padre, quien desde el cielo me bendice y protege.

RESUMEN

En el Instituto Superior Tecnológico Yavirac, la gestión académica se la realiza, mediante procesos automatizados a través del Sistema de Gestión Académica Ignug, que procesa, almacena y transporta la información, obteniendo datos importantes con un volumen considerable. La plataforma alojada en un servidor virtual carece de seguridades estandarizadas, siendo proclive de sufrir un sinnúmero de ataques informáticos como: destrucción, divulgación, modificación y robo. El propósito del diseño del modelo de Ciberseguridad, es obtener una guía metódica que aporte con la gestión de riesgos mediante la aplicabilidad de la metodología Magerit y el uso de los dominios de la Norma ISO/IEC 27002:2017; con el fin de garantizar que la información del Sistema de Gestión Académica Ignug sea íntegra, confiable y esté disponible a los usuarios autorizados del Instituto Superior Tecnológico Yavirac.

Palabras clave: Política, Ciberseguridad, Norma ISO/IEC 27002:2017, Metodología Magerit, Instituto Superior Tecnológico Yavirac

ABSTRACT

At the Yavirac Higher Technological Institute, academic management is carried out, automated processes through the Ignug Academic Management System, which processes, stores and transports information, obtaining important data with a considerable volume. The platform hosted on a virtual server lacks standardized security, being prone to suffer countless computer attacks such as: destruction, disclosure, modification and theft. The purpose of designing the Cybersecurity model is to obtain a methodical guide that contributes to risk management through the applicability of the Magerit methodology and the use of the domains of the ISO / IEC 27002: 2017 Standard; in order to guarantee that the information in the Ignug Academic Management System is complete, reliable and available to authorized users of the Yavirac Higher Technological Institute.

Keywords: Policy, Cybersecurity, ISO / IEC 27002: 2017 Standard, Magerit Methodology, Yavirac Higher Technological Institute

ÍNDICE GENERAL

DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I

INTRODUCCIÓN

1. El problema de investigación

1.1. Planteamiento del problema

La información es el recurso estratégico más importante de las organizaciones, constituye el eje principal al momento de tomar decisiones en las entidades, es preciso salvaguardarla ante los posibles peligros que la pongan en riesgo.

Para acceder a la data en tiempo real y desde cualquier sitio, se usan herramientas tecnológicas que permiten ejecutar transacciones de grandes cantidades de datos, mediante sistemas de información, servicios electrónicos y redes de comunicaciones.

El Instituto Superior Tecnológico Yavirac, desarrolla las actividades académicas, mediante el uso de la tecnología; por tal razón, ha implementado el Sistema de Gestión Académica Ignug, que agiliza los procesos y facilita el acceso a los datos relevantes de la institución.

El Sistema Ignug, que se implementó a partir del primer período académico 2019, no cuenta con protección contra la ciberdelincuencia, existiendo problemas de vulnerabilidad y amenazas para su seguridad. La información está expuesta a sufrir modificaciones, a ser eliminada, hurtada y divulgada. Además, la plataforma corre el riesgo de quedar inoperativa, lo que puede ocasionar retrasos en los procesos institucionales.

1.2. Formulación del problema

La plataforma académica Ignug, los servicios informáticos, electrónicos y redes de comunicación del Instituto Superior Tecnológico Yavirac, carecen de controles estandarizados que resguarden la seguridad de la información, por lo que están expuestos a sufrir daños, fallos en el equipamiento, ataques de hacking o cracking, ya sean externos o internos a través de la propia aplicación, de la infraestructura informática, de los usuarios o de los administradores.

1.3. Objetivo general

Diseñar un modelo de ciberseguridad mediante el establecimiento de procedimientos y la aplicación de las directrices de la norma ISO/IEC 27002:2017, que sirva como guía de prevención contra ataques cibernéticos al Sistema de Gestión Académica Ignug, que garantice los tres principios esenciales de la seguridad de la información del Instituto Superior Tecnológico Yavirac.

1.3.1. Objetivos específicos

Analizar las investigaciones sobre políticas de seguridad desarrolladas por los estudiantes de la UISEK, mediante la elaboración de cuadros comparativos que sea un punto de referencia para el diseño del modelo de Ciberseguridad propuesto.

Analizar el estado de vulnerabilidad en el que se encuentra el Sistema Académico Ignug del Instituto Superior Tecnológico Yavirac, mediante la Metodología Magerit, que permita el reconocimiento de amenazas potenciales para la gestión de la seguridad.

Analizar los riesgos encontrados, priorizándolos de acuerdo a su criticidad y a las necesidades del sistema académico Ignug, que permita la selección de los dominios más adecuados de la Norma ISO/IEC 27002:2017.

Diseñar un modelo de ciberseguridad, mediante los controles elegidos de la Norma de seguridad ISO/IEC 27002:2017 que permita al personal del Área de Desarrollo de Software del Instituto Superior Tecnológico Yavirac, la mitigación de los riesgos encontrados en la plataforma y de esta manera se garantiza el normal funcionamiento del Sistema de Gestión Académica Ignug.

1.4. Justificación

Dado el crecimiento de la población institucional, el uso de la plataforma académica Ignug es indispensable; este sistema web, maneja información importante sobre las matrículas, certificados de estudios, notas de grados y títulos, registro de las notas, etc. con un volumen considerable de datos que se encuentran en la nube, siendo proclive de sufrir un sinnúmero de ataques informáticos como: destrucción, divulgación, modificación y robo de los datos.

La Norma ISO/ICE 27002:2017, guiará en el diseño el modelo de ciberseguridad y los procedimientos para la implementación de las reglas de seguridad, tiene una amplia visión de los problemas de seguridad en cuanto a la información digital y el personal encargado de gestionarla. Además, es un estándar internacional que proporciona controles que buscan optimizar los eventos de inseguridad que pueden sufrir las organizaciones.

Es obligación de las organizaciones velar por la seguridad de los servicios e información gestionados a través de medios tecnológicos, ya que pueden sufrir modificación, denegación, eliminación y robo, perdiendo tiempo y dinero. Por lo tanto, el uso de los controles de la norma serán los más adecuados para tomar las acciones requeridas en cuanto a la protección de los activos de la información.

A pesar de las inseguridades que se puedan presentar, ya sean deliberadas o no intencionales, se deben diseñar sistemas de gestión de seguridad, basados en mecanismos,

herramientas, métodos y protocolos que permitan defender la infraestructura informática ante cualquier malicia, error o desgracia; de esta manera se garantiza la disponibilidad y eficacia de los servicios que proporciona la entidad.

Al hacer uso los recursos de la red, existe un mayor riesgo en la transferencia de la información, puesto que puede ser interceptada y corrompida por terceros. Por lo tanto, es necesario la implementación de seguridad informática.

En el proceso de gestión de riesgos, se considera usar la guía metodológica de Magerit, puesto que es un estándar 100% enfocada a la unidad tecnológica de la información y comunicaciones. La metodología usa un modelo de estudios cualitativo y cuantitativo, es de fácil comprensión, soporta herramientas comerciales como EAR y PILAR.

1.5. Estado del arte

Se han revisado algunos artículos científicos, libros y tesis relacionadas con la presente investigación y se puede destacar los siguientes:

Barrio (2017) refiere que los riesgos generados por internet pueden reconducirse a dos categorías: primero, las amenazas sobre bienes jurídicos tradicionales derivadas del uso de las tecnologías, por ejemplo, la protección de datos sensibles, el uso de programas espía (*sniffers*), la supervisión de (*cookies, spyware*), la suplantación de identidad (*phishing*); segundo, los riesgos sobre las infraestructuras electrónicas propias, al ser atacadas para alterar el normal funcionamiento de los sistemas de información, por ejemplo, acceso no autorizado, difusión de programas maliciosos *(malware*) como: virus, bombas lógicas, caballos de troya, gusanos y ataques de denegación de servicio (*DoS*), perjudicando los servicios ofrecidos a través de la nube y causando daños a las entidades que han implementado negocios electrónicos.

Los ciberataques en otros países, se deben a que los riesgos están relacionados al ciberespacio, ya que éste es compartido por otros estados y organizaciones internacionales; lo que conllevan, a otros peligros que incorporan a áreas económicas, sociales, ambientales y geopolíticos. Según el informe "Riesgos Globales 2015", la sofisticación de ataques cibernéticos, el surgimiento de la hiperconectividad a internet, la vulnerabilidad que supone la provisión de los datos personales, incrementan los incidentes asociados a la privacidad y adecuado uso de los mismos (Villalba y Fernández, 2015).

En la siguiente Figura Nº 1, se observa la conexión directa de ciberataques con otros riegos tecnológicos como: la ruptura de la infraestructura de información crítica, el mal uso de las tecnologías, el fraude y robo de datos. Además, conexiones directas con otros riesgos como: geopolíticos, ataques terroristas, fallo de la gobernanza nacional y conflictos entre estados.

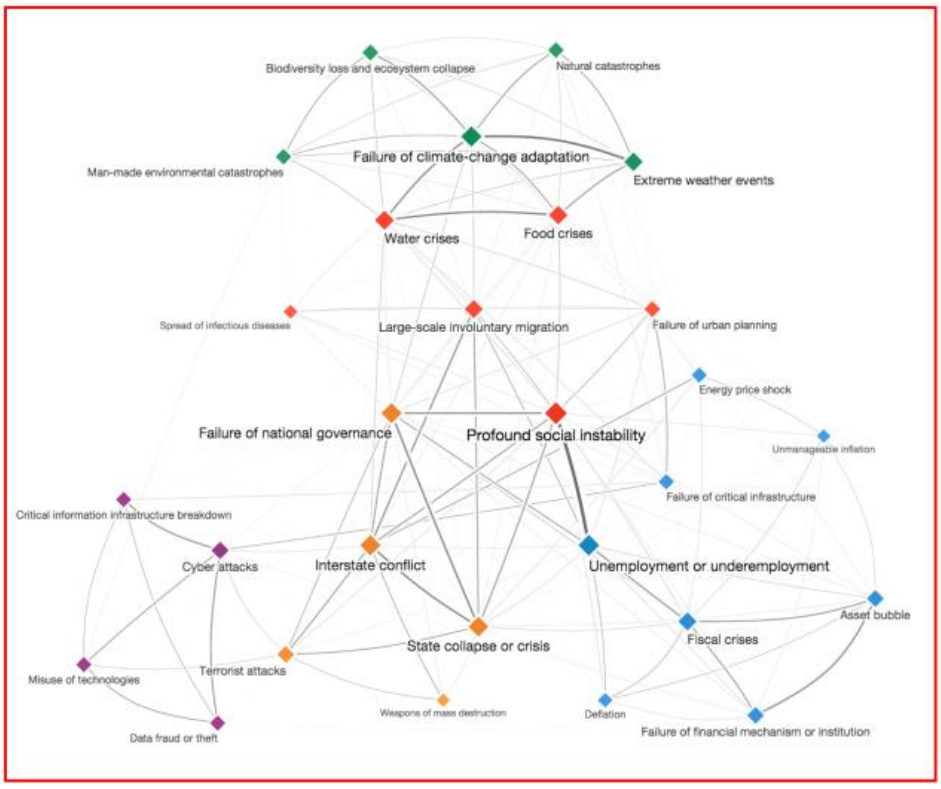

Figura 1: Mapa de interconexiones de riesgos globales (2015)
Fuente: World Economic Forum

Los ataques al sector de la educación, están aumentando cada vez más. Un grupo de *hackers* afirma haber atacado con éxito la Universidad de California de San Francisco en los últimos días. Cointelegraph pudo acceder a la información publicada por NetWalker en la dark web. En este blog, confirmaron el robo de la data confidencial, como: nombres, códigos de seguridad social y financiera de los estudiantes y de la entidad. Los ciberdelincuentes, solicitaron un pago con bitcoin para no filtrar los datos. El dato indica que Michigan State University, Columbia College of Chicago y la UCSF también fueron vulneradas (Erazo, 2020).

En la tesis realizada por Israel Cárdenas habla sobre "Diseño de una Política de Seguridad de la Información para la Unidad Educativa Borja 3 Canavis, basado en la Norma ISO/IEC 27002:2013", el autor indica que la implementación de los controles que sugiere en su trabajo, permitirá minimizar el riesgo que ocasionan las amenazas sobre los activos, considerado el presupuesto de la organización y el giro del negocio.

En el trabajo de investigación: "Política 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", la autora indica que los dominios de la política aportarán con la protección de la información, minimizando el riesgo de pérdida, garantizando el correcto funcionamiento de los procesos de la institución educativa (Torres, 2015).

En la tesis realizada sobre " Diseño de una política de seguridad para la infraestructura de red de la Universidad Central del Ecuador basada en la ISO / IEC 27002:2013 ", el autor trata sobre la actualización de la política existente, previo al análisis de riesgos realizada con la guía metodológica de Magerit, con la finalidad de reducir los riesgos de

seguridad de la información académica, de investigación y financiera de la institución mediante la aplicación de los controles de la política (Portilla, 2020).

Del análisis realizado a los trabajos citados, se concluye que es obligación de todas las organizaciones que hacen uso de sistemas web, diseñar un modelo de seguridad basado en estándares cualificados, que permita controlar y proteger la información y los servicios que son proporcionados mediante las aplicaciones web; debido a que éstas se encuentran implementadas en servidores intercomunicados a través de internet, por lo que son proclives de sufrir ciberataques como: interceptación, apropiación, borrado y alteración de los mensajes transmitidos.

El Sistema de Gestión Académica Ignug desarrollado con una arquitectura web, alojado en un servidor virtual en la nube, es propenso de ser atacado por ciberdelincuentes; por lo tanto, es primordial el diseño de un Modelo de Ciberseguridad basado en una guía de buenas prácticas como la Norma ISO/IEC 27002:2017, que garantice la integridad, disponibilidad y confidencialidad de la información y los servicios del Instituto Superior Tecnológico Yavirac.

CAPÍTULO II

MARCO TEÓRICO

2.1. Seguridad de la Información

La seguridad de la información son las medidas preventivas y reactivas, que resguardan y protegen la información impresa o digital, de las amenazas a las que se encuentra expuesta; para garantizar que ésta sea íntegra, confidencial y esté disponible en el momento indicado (ISOTools Excellence, 2017).

En el Instituto Superior Tecnológico Yavirac los procesos son automatizados, por lo tanto, es primordial implementar seguridad para resguardarlos.

Seguridad

Es la ausencia o reducción del riesgo de la información y de los activos de una entidad; involucra las siguientes acciones: prevención, transferencia, mitigación y aceptar del riesgo (Romero, et al., 2018).

Datos/Información

Es considerado el principal activo de la entidad que debe protegerse adecuadamente y tiene que estar a salvo; mediante su análisis se pueden tomar decisiones estratégicas, generando valor para la organización (Romero, et al., 2018).

2.2. La Ciberseguridad

Protege los datos digitales, la infraestructura computacional, software, bases de datos, archivos, etc., mediante la aplicación de protocolos, estándares, métodos, reglas, leyes y

herramientas, con el fin de reducir las amenazas y ataques cibernéticos, para garantizar la seguridad informática.

Disciplina que, en base a políticas y normas internas y externas de las organizaciones, se encarga de proteger la integridad y privacidad de la información procesada y almacenada en un sistema informático, frente a cualquier tipo de peligros, minimizando los riesgos físicos y lógicos (Baca, 2016).

Por otra parte, la seguridad es la capacidad de resistencia a los accidentes o ataques malintencionados que pueden comprometer la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos a través de las redes o de los sistemas informáticos, con un determinado nivel de confianza (Magerit, 2012).

Sánchez (2018) indica:

> La información segura debe cumplir con tres principios fundamentales:
>
> - **Integridad:** Se trata de garantizar la precisión de la información.
> - **Confidencialidad:** Avala que la información sea accedida únicamente por los usuarios autorizados.
> - **Disponibilidad:** La política de seguridad y las herramientas de comunicación deben funcionar correctamente para que la información esté siempre disponible. (p. 192)

2.3. Seguridad de Software

Desarrollar e implementar sistemas informáticos, es cada vez más complejo, puesto que el producto final debe contener calidad y seguridad. Incorporar los principios y buenas prácticas de seguridad desde la primera etapa del ciclo de vida de desarrollo de software SDLC, logra que las aplicaciones tengan menos fallas en el diseño, en la

programación o en la configuración; lo que protege de posibles interrupciones o alteraciones del funcionamiento normal de un programa o la toma de su control; también previene del robo, modificación o destrucción de la información.

Cuando se efectúa una incidencia en producción, se deben contemplar planes de recuperación tomando en cuenta el tiempo de reacción ante los desastres, puesto que la institución no se puede quedar sin servicios por mucho tiempo, ya que se paralizarían las actividades académicas y la imagen del instituto se vería afectada frente a la comunidad educativa y a externos.

Para prevenir que las aplicaciones web sean vulnerables frente a posibles ataques, se debe implementar seguridad durante el período de desarrollo de los sistemas, en la implementación y operación, para garantizar que el software cumpla con las siguientes propiedades: integridad, disponibilidad, confidencialidad, fiabilidad, autenticación, trazabilidad, robustez, resiliencia y tolerancia.

Además, existen elementos que intervienen en la implementación de la seguridad en el software como: herramientas, componentes adquiridos, conocimiento profesional, configuraciones desplegadas, ambiente de operación, principios y prácticas de mejora en desarrollo (Dawson, et al., 2010).

2.4. Gestión de Riesgos

Conlleva a realizar el análisis de los riesgos, adoptando las medidas necesarias para proteger los datos y los servicios; es preciso investigar el nivel del riesgo para hacer un adecuado tratamiento a través de la implementación de salvaguardas.

En la Figura Nº 2, se visualiza la estructura formal de la gestión de riesgos de acuerdo a las Normas ISO.

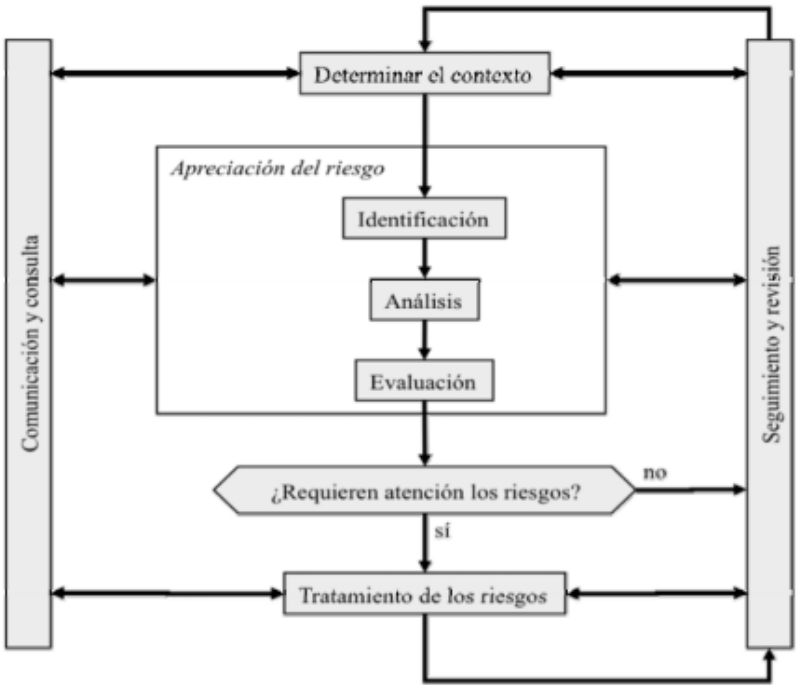

Figura 2: Proceso de gestión de riesgos
Fuente: ISO 31000

En la Figura Nº 3, se visualiza la combinación de dos actividades: análisis y tratamiento de los riesgos.

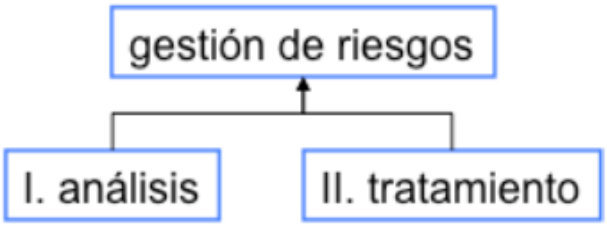

Figura 3: Estructura de gestión de riesgos
Fuente: Metodología de MAGERIT, v 3.0 (2012)

2.5. Análisis de Riesgos

Las organizaciones que hacen uso de la tecnología, no desean que sus sistemas informáticos sean atacados interna o externamente; sin embargo, es inevitable que los ataques sucedan y las amenazas son mayores cuando las aplicaciones presentan puntos débiles llamados “vulnerabilidades”, provocando daños y pérdidas en los activos dependiendo de la cantidad y número de vulnerabilidades reportadas (Baca, 2016).

Magerit (2012) afirma: “el análisis de riesgos es el proceso sistemático para estimar la magnitud de los riesgos al que está expuesta una Organización” (p. 9).

La comprensión del Análisis de Riesgos, ayudará a distinguir las actividades y entregables a realizarse en el desarrollo del proyecto; considerando los activos, las amenazas y la protección, con el objeto de estimar el impacto y el riesgo.

A continuación, se definen los términos antes mencionados, incluido vulnerabilidad y probabilidad.

Activos de la Información

Un activo es un bien significativo que la empresa posee. Los tipos de activos de acuerdo a la categoría informática pueden ser: datos, información, software, hardware, redes de comunicaciones relacionado con la conectividad, personal involucrado en actividades de seguridad y en los procesos, ubicaciones físicas como centro de datos, de oficinas en las cuales se ejecutan cada uno de los procesos, servicios de electricidad, de internet, servicios tercerizados dentro de la entidad, intangibles la reputación e imagen (Norma ISO 9000, cláusula 7.3.1).

Magerit (2012) en su Libro I menciona: “Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [UNE 71504:2008]” (p.22).

Existen dos activos esenciales la información y los servicios; además, se identifican otros activos de los cuales dependen:

- **Activos esenciales**

- Información: se considera la información que se maneja, se toman en cuenta características de carácter personal, su categorización, con requisitos legales y normativos.
- Servicios: Servicios que prestan los sistemas de información.

- **Servicios internos**

  Organiza el sistema de información.

- **Equipamiento informático**

- Aplicaciones: mediante las cual se realizan los procesos y tareas de una organización.
- Equipos informáticos: hardware de soporte de las aplicaciones, servicios y datos.
- Comunicaciones: servicios de comunicaciones contratados a terceros, que transportan la data entre dispositivos electrónico.
- Soportes de información: unidades físicas que almacenan datos permanentemente como: discos, cintas, tarjetas de memoria, etc.

- **Entorno:** lugar en el que se alojan las aplicaciones para su operación

- Equipamiento y suministros: equipos y suministros de energía, climatización, etc.
- Mobiliario: armarios, etc.

- **Servicios subcontratados a terceros**:

- **Instalaciones físicas**

  Sitios físicos que alojan los sistemas informáticos y de comunicación

- **Personal**

  Personal relacionado con el uso y administración de los sistemas de informáticos.

- Usuarios: externos e internos que hacen uso del software.
- Operadores y administradores: de aplicaciones, bases de datos, redes.

- Desarrolladores: de los sistemas de información, diseñadores de bases de datos, arquitectura web (Magerit, 2012).

La identificación de los activos, guiará con la ejecución de las actividades a realizar en el análisis de riesgos en el desarrollo del proyecto; se identificarán los activos, las dependencias entre ellos para valorarlos, considerando las dimensiones de seguridad.

Amenaza

Baca (2016) asegura: "Es una condición del entorno de los sistemas, áreas o dispositivos que contienen información importante, que podría dar lugar a que se produjese una violación de seguridad afectando parte de la información y de la TI de la organización" (p. 30).

Existen varios tipos de amenazas que afectan a los activos de un sistema informático:

- **[N] Desastres Naturales:** Eventos que suceden sin que los seres humanos intervengan.
- **[I] De origen industrial:** hechos que suceden accidentalmente, de origen humano de tipo industrial.
- **[E] Errores y fallos no intencionados:** incidencias que las personan causan de forma accidental.
- **[A] Ataques intencionados:** Provocados por las personas de forma deliberada

Una vulnerabilidad producida puede ser una amenaza para que se ocasione un evento de ataque, afectando a un activo en el sentido de la degradación y la probabilidad de que se materialice el peligro (Magerit, 2012).

En la Tabla Nº 1, se visualiza la escala cualitativa de la degradación del valor del activo.

Tabla 1
Degradación del valor del activo

Valoración		**Probabilidad de ocurrencia**	**Degradación**
MA	Muy alta	Casi seguro	Fácil
A	Alta	Muy alto	Medio
M	Media	Posible	Difícil
B	Baja	Poco probable	Muy difícil
MB	Muy baja	Muy raro	Extremadamente difícil

Fuente*:* Elaborado por el autor, en referencia a la Metodología de MAGERIT, Libro I "Método" (2012)

En la Tabla Nº 2, se observa la probabilidad de ocurrencia de la amenaza, de manera cuantitativa, tomando como referencia 1 año.

Tabla 2
Probabilidad de ocurrencia

MA	100	Muy frecuente	A diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco frecuente	Cada varios años
MB	1/100	Muy poco frecuente	Siglos

Fuente*:* Elaborado por el autor, en referencia a la Metodología MAGERIT, Libro I "Método" (2012)

El paso 2 del Análisis de Riesgos, aportará a identificar las amenazas y valorarlas, tomando en cuenta las dimensiones de seguridad afectadas de los activos y su influencia en la degradación y la probabilidad en caso de llegar a materializarse los peligros a las que está expuesto el Sistema Ignug.

Determinación del impacto potencial

Sánchez (2018) manifiesta: "El impacto es el peligro relativo (bajo, medio o alto) de una amenaza para la organización, se puede expresar en términos de dinero o estatus social" (p. 208). Se lo cuantifica para poder realizar un adecuado cálculo del riesgo.

En el Libro I, Método de Magerit (2012) manifiesta que el impacto es el grado de daño que sufre el activo como consecuencia de la ejecución de una amenaza; se lo puede calcular mediante el valor de los activos y la degradación que ejercen las amenazas.

Se puede calcular el impacto tomando en cuenta, las variables: valoración y degradación de los activos. Ver Tabla Nº 3.

Tabla 3
Estimación del impacto

Impacto		**Degradación**		
		1%	10%	100%
Valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Fuente: Elaborado por el autor, en referencia a la Metodología MAGERIT, . Libro III "Guía de Técnicas" (2012)

La determinación del impacto, aportará al desarrollo del trabajo, tomando en cuenta el valor de información y los servicios que presta el Sistema de Gestión Académica Ignug y las amenazas a las que están expuestos. Se podrá agregar el resultado del impacto y el acumulado sobre cada activo de forma independiente, en diferentes dimensiones.

Determinación del riesgo potencial

Es la evaluación del nivel de despliegue de la materialización de la amenaza sobre los activos, dañándolos y perjudicando a la Organización. Para gestionar los riesgos, es necesario conocerlos para poder afrontarlos y controlarlos (Magerit, 2012).

Para calcular el riesgo se usa la siguiente fórmula:

Riesgo = Probabilidad de ocurrencia de las amenazas x Impacto

En la Tabla Nº 4, se listan las escalas a considerar para la estimación del impacto.

Tabla 4

Escalas cualitativas para la estimación del riesgo

Escalas					
Impacto		**Probabilidad**		**Riesgo**	
MA	Muy alto	**MA**	Prácticamente seguro	**MA**	Crítico
A	Alto	**A**	Probable	**A**	Importante
M	Medio	**M**	Posible	**M**	Apreciable
B	Bajo	**B**	Poco probable	**B**	Bajo
MB	Muy bajo	**MB**	Muy raro	**MB**	despreciable

Fuente: Elaborado por el autor, en referencia a la Metodología MAGERIT, Libro III "Guía de Técnicas" (2012)

Tabla 5

Estimación del riesgo

		Probabilidad				
Riesgo		**MB**	**B**	**M**	**A**	**MA**
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: Elaborado por el autor, en referencia a la Metodología MAGERIT, Libro III – Guía de Técnicas - versión 3.0 (2012)

La estimación del impacto, ayudará a calcular el nivel de riesgo al que está expuesto cada activo de información y servicio del Sistema de Gestión Académica Ignug, con el fin de priorizar la atención a los activos críticos que se encuentren en la zona roja.

Salvaguardas

Una vez identificados los riesgos, se toman medidas de protección que se plasman en el diseño del modelo de seguridad para posteriormente implementarlas (Sánchez, 2018).

En el Libro I, Método, Magerit (2012) refiere que los controles son formas tecnológicas que minimizan el riesgo; para seleccionarlas, se debe tener en cuenta: el tipo de activo, las

dimensiones a prevenir, las amenazas de las que se necesitan defender; finalmente, se verificará si existen salvaguardas alternativas.

La determinación de las salvaguardas, paso 3 del Análisis de Riesgos, contribuirá con el reconocimiento de las protecciones adecuadas para cada tipo de activo del Sistema de Gestión Académica Ignug; las mismas que se plasman en el Libro II, "Catálogo de Elementos" de Magerit 2012.

Vulnerabilidad

Los sistemas informáticos de las organizaciones, corren el riesgo de sufrir ciberataques, a través de las debilidades existentes, comprometiendo a los activos de la información.

Baca, G. (2016) manifiesta:

> Constituye un hecho o una actividad que permite concretar una amenaza. Se es vulnerable en la medida en que no hay suficiente protección como para evitar que llegue a suceder una amenaza. La primera vulnerabilidad que puede suceder es que los diseñadores del sistema no sean capaces de prever todas las amenazas que existen o que pueden existir en el futuro, y como es imposible predecir el futuro, los sistemas siempre serán vulnerables. (p.30)

Las aplicaciones web, al ser implementadas en la red para su disponibilidad 24/7, son vulnerables y corren el riesgo de ser atacadas a través de la infraestructura de comunicaciones.

Probabilidad de Ocurrencia

Es el evento de que ocurra un ataque; se debe analizar la agresión para determinar con estudios estadísticos o predictivos, cuando una amenaza puede llegar a ejecutarse dentro de la organización. (ISO 27005, 2008).

2.6. Tratamiento de los riesgos

Permite organizar la defensa de los activos de forma concienzuda y prudente, previniendo y mitigando las amenazas, con el fin de resistir los accidentes y seguir el proceso operacional en excelentes entornos; la seguridad no se la pueda tratar completamente quedando un riesgo residual (Magerit,2012).

2.7. ISO/IEC 27002

De acuerdo con el sitio web (2017), la Norma ISO/IEC 27002, es un estándar que suministra lineamientos enfocados a la implementación de controles de la seguridad informática; el objetivo que persigue, es que la organización independiente del tamaño, tipo o naturaleza, reconozca los activos de información con los que cuenta y los riesgos que puedan existir en los diferentes dispositivos en los que se procesan.

ISO/IEC 27002:2017

La Norma EN ISO/IEC 2700:2017, aprobada por CEN sin ninguna modificación, fue desarrollada en base a la ISO/IEC 27002:2013 que incluye el Cor 1:2014 y Cor 2:2015; construida por el Comité Técnico ISO/IEC JTC 1 Tecnología de la Información de la Organización Internacional de Normalización (ISO) y de la Comisión Electrónica Internacional (IEC) acogida como de la EN ISO/IEC 27002:2017. Esta norma se encuentra vigente a partir de agosto de 2017, anulando a las normas UNE-ISO/IEC 27002:2009 y UNE-ISO/IEC 27002:2015 (Norma ISO/IEC 27002:2017, 2017).

Sobre el objeto y campo de aplicación la ISO/IEC (2017) manifiesta lo siguiente:

> Este modelo establece lineamientos para la implementación y gestión de seguridad de la información en las entidades; incluye la selección, la puesta en marcha y la gestión de los estándares considerando entorno de los riesgos de seguridad.

de la información de la organización. Se lo plantea para las empresas desarrollen sus propias directrices de seguridad a ser utilizada. (p. 9)

La norma, consta de 14 capítulos, conteniendo 35 categorías de seguridad y 114 controles. Sirven para organizar la información a alto nivel dentro del ámbito de la conectividad. Ver Anexo 1 “Controles ISO/IEC 27002:2017”.

De acuerdo a lo que manifiesta la Norma, es importante entender el funcionamiento de cada uno de los 114 controles existentes, con el fin de seleccionarlos y tomarlos en cuenta en el diseño de la política para preservar la información y los sistemas informáticos, de acuerdo a las necesidades del Sistema de Gestión Académica Ignug.

2.8. Magerit

Magerit, es una guía desarrollada por el gobierno español, de uso público para efectos de cálculos de indecencias tecnológicas, valora los activos digitales y de infraestructura técnica. Cuenta con tres Libros establecidos de la siguiente manera:

- **Libro 1 del Método. -** Describe la estructura del modelo de gestión de riesgos, catálogo de elementos de riegos.
- **Libro 2 Catálogo de Elementos. -** Contiene la clasificación de los activos de información a tomar en cuenta, lo cual permite valorar los activos identificarlos; además de un listado con las amenazas y controles que deben considerarse.
- **Libro 3 Guía de Técnicas. -** Aporta con una guía de técnicas para su aplicación, sin ayudas automatizadas; mediante notación textual y /o gráfica de cada procedimiento. Considera el uso de tablas, algorítmicas, árboles de ataque, técnicas gráficas, sesiones de trabajo como entrevistas, reuniones y presentaciones, valoración Delphi.

Se basa en analizar las vulnerabilidades que son aprovechadas por las amenazas y el impacto de la violación de seguridad que puede sufrir la empresa; de esa manera se

identifican las medidas preventivas y correctivas adecuadas para controlar y mitigar los ataques (Magerit, 2012).

En la Figura Nº4, se observa la fase en la que interviene la metodología, tomando en cuenta los riesgos al usar la tecnología.

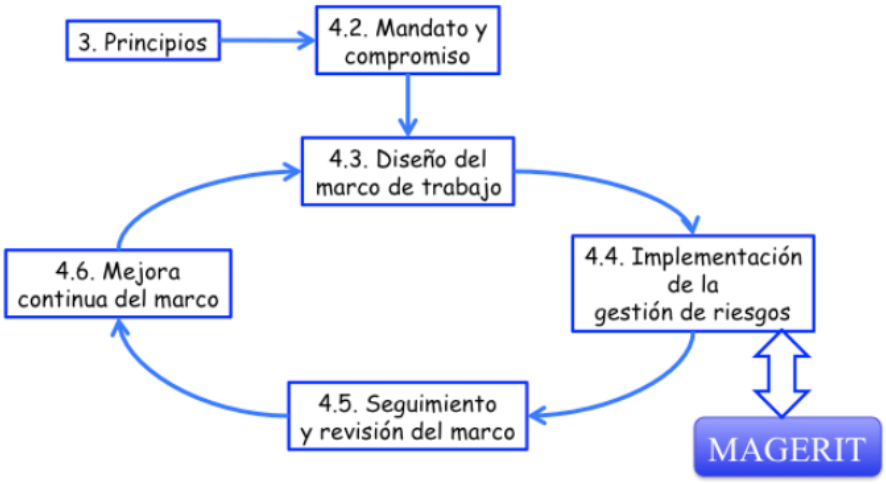

Figura 4: ISO 31000
Fuente: Metodología de MAGERIT, Libro I –Método- v 3.0 (2012)

La guía busca cumplir con los objetivos directos para concienciar a las personas de que los riesgos existen y se los debe gestionar mediante hallazgos, planificación y tratamiento, para mitigarlos; los indirectos para que las entidades se preparen ante evaluaciones, auditorías certificaciones, acreditaciones (Magerit, 2012).

En la Tabla Nº 6, se describen las actividades de análisis y gestión de riesgos que se ejecutan, con el fin de estandarizar los hallazgos y las conclusiones de los informes:

Tabla 6
Actividades de análisis y gestión de riesgos

Actividades de análisis y gestión de riesgos	Descripción
Modelo de valor	Estima el valor de los activos y las dependencias entre ellos.
Mapa de Riesgos	Relación de las amenazas a que están expuestos los activos.
Declaración de la aplicabilidad	Se analiza la aplicabilidad de las salvaguardas de acuerdo a la amenaza sobre el activo.

Actividades de análisis y gestión de riesgos	Descripción
Evaluación de salvaguardas	Verificar si las salvaguardas son eficaces respecto al riesgo.
Estado de riesgo	Lo que les puede pasar a los activos considerando las salvaguardas adoptadas.
Informe de insuficiencias	Recopila las vulnerabilidades del sistema, puntos débilmente protegidos provocando la materialización de las amenazas.
Cumplimiento de la normativa	Declaración de satisfacción de la normativa correspondiente.
Plan de seguridad	Proyectos de seguridad que permiten materializar las decisiones de tratamiento de riesgos

Fuente*:* Elaborado por el autor, en referencia a la Metodología MAGERIT, Libro I "Método" (2012)

Magerit se integra con las metodologías ISO 31000 o ISO 27005, puesto el procedimiento de la gestión de riesgos es prácticamente el mismo; sin embargo, para el efecto del desarrollo del proyecto, se eligió trabajar con esta metodología, debido a que Magerit orienta el qué hacer y cómo hacerlo.

CAPÍTULO III

ANALISIS DE POLÍTICAS DE SEGURIDAD DESARROLLADAS EN LA UISEK

3.1. Antecedentes

La Universidad Internacional SEK, oferta el programa de Maestría en Ciberseguridad, busca formar profesionales mediante un proceso de aprendizaje teórico-práctico de estrategias y herramientas de seguridad, aportando a la implementación de la seguridad de la información (UISEK, 2020).

3.2. Análisis

Se analizan las investigaciones sobre políticas de seguridad de los trabajos de tesis realizadas por los estudiantes de la UISEK; se elaboran cuadros comparativos, lo que aportará a la mejora del diseño de la política de Ciberseguridad propuesto; para proteger los activos del Sistema de Gestión Académica Ignug del Instituto Superior Tecnológico Yavirac.

Tesis: "Diseño de una Política de Seguridad de la Información para la Unidad Educativa Borja 3 Canavis, basado en la Norma ISO/IEC 27002:2013".

Autor: Ing. Israel Alejandro Cárdenas Calderón

Fecha: enero 2020

En el trabajo realizado de Israel Cárdenas en el 2020, estructura el modelo de seguridad referente a los dominios de la Norma ISO/IEC 27002:2013, selecciona el 70% de los controles según las necesidades de la entidad; redacta la política de forma clara y concisa con el fin de garantizar la protección de la información de la Institución Educativa.

Tabla 7
Análisis del trabajo del Ing. Israel Cárdenas

Nº	Trabajo Ing. Israel Cárdenas	Trabajo propuesto
1	**Norma ISO/IEC 27002:2013:** Usa el estándar ISO / IEC 27002: 2013 / Cor.1: 2014: en esta 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."	**Norma ISO/IEC 27002:2017:** - Se usará la Norma ISO/IEC 27002:2017 / incluyendo Cor 1:2014 y Cor 2:2015 fue aprobado por CEN como Norma EN ISO/IEC 2700:2017 sin ninguna modificación. - La norma establece los controles, acorde al SGA Ignug, con el objeto que la Comisión Ejecutiva del IST Yavirac los implemente.
2	**Política:** - Selecciona el 70% de los controles según las necesidades de la entidad; redacta la política de forma clara y concisa con el fin de garantizar la protección de la información de la institución. - No contiene controles sobre desarrollo de software, en vista que en la Unidad Educativa Borja 3 Cavanis no desarrollan sistemas. - Registra los controles sin detallar cómo se los va a implementar.	**Política:** - El IST Yavirac a través de la Unidad de TIC, implementó el SGA Ignug, en la actualidad sigue desarrollando nuevos módulos para integrarlos a la plataforma, por lo tanto, es indispensable que se propongan controles de seguridad para el desarrollo seguro del software. - Se propone diseñar la política aplicando principios y buenas prácticas de seguridad, como una guía clara para que el Comité de Seguridad la implemente.

Fuente*:* Elaborado por el autor, basado en la tesis realizada por el Ing. Israel Cárdenas

Tesis: "Diseño de una política de seguridad de la información para SWEADEN Compañía de Seguros S.A, basado en la norma ISO/IEC 27002:2013".

Autor: Ing. Jaime Andrés Almeida Bajaña

Fecha: 2019

En el trabajo realizado de Jaime Almeida en el 2019, diseña una política de seguridad para la Compañía de Seguros SWEADEN, en referencia al estándar ISO/IEC 27002:2013, con el objeto de implementarla y mitigar los riesgos y debilidades presentes seguridad de la información de la entidad. Almeida identifica los activos de forma global, sin especificar detalles de cada tipo de activo; sin embargo, en la identificación de las amenazas análisis la hace identificando cada tipo de activo.

Tabla 8
Análisis del trabajo del Ing. Jaime Almeida

Nº	Trabajo Ing. Jaime Almeida	Trabajo propuesto
1	**Dependencias de activos:** - En el análisis de riesgos, identifica los activos de forma global, sin especificar las dependencias; sin embargo, en la selección de las amenazas, sí considera la estructura del conjunto de activos en capas, puesto que los ataques se pueden realizar de diferentes maneras para cada activo.	**Dependencias de activos:** - Se identificarán los activos mediante una estructura en capas, donde unos activos dependan de otros con el fin de reconocer los controles a implementar para proteger a los activos de la capa superior del grafo.
2	**Norma ISO/IEC 27002:2013:** - Usa el estándar ISO / IEC 27002: 2013 / Cor.1: 2014: en esta renueva el contenido en la página 10, subcláusula 7.1.2 Guía de Implementación numeral c); Página 13, Subcláusula 8.1.1	**Norma ISO/IEC 27002:2017**: - Se usará la versión 2017, en cada control se especificarán principios y buenas prácticas para la implementación. - Se establecerán los controles, acorde al SGA Ignug, con el objeto que la Comisión Ejecutiva en conjunto con el Comité de Seguridad de la Información del IST Yavirac implemente los controles.
3	**Política:** - Plasma los controles de la política, sin detallar las indicaciones para que el área de TIC los implemente.	**Política:** - Los artículos de la política, además de contener el control, plasmarán los principios, buenas prácticas y recomendaciones para que la

Nº	Trabajo Ing. Jaime Almeida	Trabajo propuesto
		Unidad de TIC del IST Yavirac, comprenda y ejecute la implementación de los controles.

Fuente*:* Elaborado por el autor, basado en la tesis realizada por el Ing. Jaime Almeida

Tesis: "Diseño de un Modelo de Seguridad de la Información, basado en OSSTMMV3, NIST SP 800-30 E ISO 27001, para centros de Educación: caso de Estudio Universidad Regional Autónoma de los Andes, Extensión Tulcán".

Autor: Ing. Elva Gioconda Lara Guijarro

Fecha: febrero 2019

En el trabajo realizado de Elva Lara en el 2019, diseña una guía de seguridad de la información, en referencia a OSSTMMv3, NIST SP 800-30 e ISO 27001, personalizándolos de acuerdo a los requerimientos institucionales, lo cual le permitirá solventar los problemas que presenta la gestión de recursos, acceso a la información y gestión administrativa de la Universidad Regional Autónoma de los Andes, extensión

Tabla 9
Análisis del trabajo de la Ing. Elva Lara

Nº	Trabajo Ing. Elva Lara	Trabajo propuesto
1	**Metodología:** - Usa el manual de la metodología Abierta de Testeo de Seguridad, OSSTMMv3, para contemplar el cumplimiento de estándares y buenas prácticas de en la actualidad cumple la intuición, que están establecidas en el NIST, ISO 27001, para el diseño del modelo y que TIC lo implemente en la Universidad Regional Autónoma de los Andes, extensión Tulcán.	**Metodología:** - Se usará la metodología Magerit, debido a que la implementación del sistema Ignug es reciente, por lo que no se cuenta con estándares y procedimientos de seguridad. - Se ejecutarán todas las actividades que el método lo indica: se iniciará con el análisis de los riesgos mediante Magerit, con el objetivo de identificar los activos, valorarlos de acuerdo a las dimensiones de seguridad, reconocer las

Nº	Trabajo Ing. Elva Lara	Trabajo propuesto
		amenazas y seleccionar las salvaguardas por cada activo.
2	**Análisis de Riesgos:** - A partir de los resultados de las encuestas realizadas en uno de los capítulos, plantea el modelo de SGSI, identifica los activos según el tipo, se salta a evaluar los riesgos identificando las vulnerabilidades y estima el riesgo. - No se observa la valoración de los activos, tampoco la estimación del impacto y la probabilidad, variables fundamentales para la estimación del peligro.	**Análisis de Riesgos:** - Se identificarán las dependencias entre los activos, se los estructura en capas, con el fin de reconocerlos, valorarlos de acuerdo a la dimensión, identificar las amenazas a los que están expuestos, estimar el impacto y la probabilidad de ocurrencia para calcular el riesgo e implementar las salvaguardas necesarias para cada activo.
3	**Norma ISO/IEC 27001 y NIST 800:** - La usa para crear la estructura del SGSI.	**Norma ISO/IEC 27002:2017**: - Se usará la última versión, para implementar los controles, debido a que en cada control se específica la forma de ponerlo en marcha.
4	- **La política:** - Plasma algunos controles de la política, sin detallar las indicaciones para que el área de TIC los implemente. - La mayoría de los controles propuestos no son detallados, mientras que pocos controles explican las prácticas que se deben tomar en cuenta al momento de implementarse.	**La política:** - Se considerarán todos los dominios tomando en cuenta el 90 % de controles, debido a que van orientados a proteger a los activos de la información, servicios, equipamiento en donde se alojan los módulos y las personas relacionadas con los servicios que proporciona el SGA Ignug. - Cada control de la política constará con principios y buenas prácticas a tomarse en cuenta para que la implementación sea fácil.

Fuente*:* Elaborado por el autor, basado en la tesis realizada por la Ing. Elva Lara

Tesis: "Diseño de una política de seguridad de la información basada en la norma ISO 27002:2013, para el Sistema de Botones de Seguridad del Ministerio del Interior".

Autor: Ing. Wáshington Marcelo Contero Ramos

Fecha: marzo 2019

En el trabajo realizado de Wáshington Contero en el 2019, diseña una política de seguridad de la información, basado en de seguridad de la información de la norma ISO 27002:2013, para el establecimiento de las medidas necesarias que garanticen la protección de la información de la aplicación "Botones de Seguridad del Ministerio del Interior".

Tabla 10
Análisis del trabajo del Ing. Wáshington Contero

Nº	Trabajo Ing. Wáshington Contero	Trabajo propuesto
1	**Metodología:** - Usa la metodología Magerit, realiza el análisis de los riesgos identificando los activos, valorarlos de acuerdo a las dimensiones de seguridad, reconocer las amenazas y seleccionar las salvaguardas por cada activo.	**Metodología:** - Se ejecutarán todas las actividades del método. - Se iniciará con el análisis de los riesgos mediante Magerit, con el objetivo de identificar los activos, valorarlos de acuerdo a las dimensiones de seguridad, reconocer las amenazas y seleccionar las salvaguardas por cada activo.
2	**Análisis de inseguridades:** - El reconocimiento de los activos la realiza de acuerdo a la categoría recomendada en la metodología, - Valora a los activos mediante las dimensiones integridad, confidencialidad y disponibilidad, asigna un valor bajo a las aplicaciones informáticas. - Identifica las amenazas, vulnerabilidades y el impacto en una sola matriz; calcula el riesgo y asigna los controles según el peligro del activo.	**Análisis de inseguridades:** - Se analizarán a los activos de acuerdo a la dependencia entre ellos, se los clasificará y estructurará por capas, para reconocerlos absolutamente a todos, valorarlos considerando la dimensión de afectación, identificar las amenazas a los que están expuestos, estimar el impacto y la probabilidad de ocurrencia para calcular el riesgo e implementar las salvaguardas necesarias para cada activo.
3	**Norma ISO/IEC 27002:2013:** Usa el estándar ISO / IEC 27002: 2013 / Cor.1: 2014: en esta renueva el contenido en la página 10, subcláusula 7.1.2 Guía de	**Norma ISO/IEC 27002:2017**: - Se usará la última versión de la ISO/IEC 27002:2017; para establecer los controles acorde al SGA Ignug, con el objetivo de que la

Nº	Trabajo Ing. Wáshington Contero	Trabajo propuesto
	Implementación numeral c); Página 13, Subcláusula 8.1.1 "Controlar", Página 14, Subcláusula 8.1.3 "Guía de Implementación."	Comisión Ejecutiva del IST Yavirac los implemente.

Fuente*:* Elaborado por el autor, basado en la tesis realizada por el Ing. Wáshington Contero

Tesis: "Diseño de un modelo de gestión de seguridad de la información para el sistema académico de la Universidad Estatal del Sur de Manabí".

Autor: Ing. Carlos Conforme Sornoza

Fecha: noviembre 2018

En el trabajo realizado de Carlos Conforme Sornoza en el 2018, diseña un modelo de gestión para la seguridad de la información mediante el análisis de la norma ISO 27002:2017; aplica la metodología del Ciclo de mejora continua PDCA, que consta de las etapas: planificar, hacer, verificar y actuar, la que apoya al modelo en mención e incorpora controles de seguridad de la información de la norma internacional ISO 27002:2017. Carlos, plasma en un mapa los controles de la Norma ISO 27002:2017, con el fin de que la Unidad de Sistemas Informáticos de la UNESUM, diseñe la política de seguridad seleccionando los controles adecuados conforme las necesidades del sistema académico de la institución.

Tabla 11
Análisis del trabajo del Ing. Carlos Conforme

Nº	Trabajo Ing. Carlos Conforme	Trabajo propuesto
1	**Política:** - No diseña la política, debido a que la propuesta es el diseño de un SGSI, únicamente plasma en un mapa el estándar	**Política:** - Se propone el diseño de la política aplicando los dominios del estándar ISO/IEC 27002:2017.

Nº	Trabajo Ing. Carlos Conforme	Trabajo propuesto
	ISO/IEC 27002:2017, para que la Unidad de Sistemas Informáticos de la UNESUM diseñe la política.	- Se darán directrices para su implementación basada en buenas prácticas y recomendaciones para que la Unidad de TIC del IST Yavirac, comprenda y ejecute la implementación de los controles.
2	**Norma ISO/IEC 27002:2017:** - Usa la Norma ISO/IEC 27002:2017 para proponer los controles de la misma; sin embargo, no realiza la política.	**Norma ISO/IEC 27002:2017:** - Se usará la Norma ISO/IEC 27002:2017, guía que contiene buenas prácticas que describen los objetivos de los controles, para que la Comisión Ejecutiva en conjunto con el Comité de Seguridad de la Información del IST Yavirac implementen los controles.
3	**Metodología PDCA:** - Para el diseño del SGSI, aplica la metodología PDCA, estándar usado por la ISO/IEC 27001.	**Metodología Magerit:** - Para el diseño de la política se realizará un análisis de riesgos usando la metodología Magerit, previo al diseño de la política.

Fuente*:* Elaborado por el autor, basado en la tesis realizada por el Ing. Carlos Conforme

Tesis: "Diseño y creación de una política de seguridad de la Información (SGSI basado en la normativa ISO 27000 para la Cooperativa Construcción, Comercio y Producción."

Autor: Ing. Jean Pierre Rodríguez Guerra

Fecha: junio 2016

En el trabajo realizado de Jean Pierre Rodríguez en el 2016, diseña una nueva política de seguridad de la información, basado la norma ISO 27002-2005 para la Cooperativa de Ahorro y Crédito Construcción, Comercio y Producción COOPCCP, en base a los levantamientos de información, el ERM y diccionario de controles para mejorar los procesos, procedimientos y el manejo de información aplicando medidas preventivas y correctivas.

Tabla 12

Análisis del trabajo del Ing. Jean Pierre Rodríguez

Nº	Trabajo Ing. Jean Pierre Rodríguez	Trabajo propuesto
1	**Metodología:** - Usa la metodología Magerit, realiza el análisis de los riesgos identificando los activos, valorarlos de acuerdo a las dimensiones de seguridad, reconocer las amenazas y seleccionar las salvaguardas por cada activo.	**Metodología:** - Se ejecutarán todas las actividades que el método lo indica: se iniciará con el análisis de los riesgos mediante Magerit, con el objetivo de identificar los activos, valorarlos de acuerdo a las dimensiones de seguridad, reconocer las amenazas y seleccionar las salvaguardas por cada activo.
2	**Análisis de Peligros:** - La identificación de los activos la realiza de acuerdo a la categoría recomendada en la metodología, los valora mediante las dimensiones integridad, confidencialidad y disponibilidad, se observa que asigna un valor bajo a las aplicaciones informáticas; identifica las amenazas, vulnerabilidades y el impacto en una sola matriz; calcula el riesgo y asigna los controles según el peligro del activo.	**Análisis de Peligros:** - Se identificarán los activos de acuerdo a la dependencia entre ellos, se los clasificará y estructurará por capas, para reconocerlos absolutamente a todos, valorarlos considerando la dimensión de afectación, identificar las amenazas a los que están expuestos, estimar el impacto y la probabilidad de ocurrencia para calcular el riesgo e implementar las salvaguardas necesarias para cada activo.
3	**Norma ISO/IEC 27002:2005:** - La norma usa 11 capítulos, 39 categorías y 114 controles	**Norma ISO/IEC 27002:2017**: Se usará la última versión de la ISO/IEC 27002:2017, consta de 14 dominios de controles, conteniendo 35 categorías y 114 controles.

Fuente*:* Elaborado por el autor, basado en la tesis realizada por el Ing. Jean Pierre Rodríguez

Tesis: "Diseño de una política de seguridad de la información para el área de TICs del Instituto Tecnológico Superior Central Técnico, basado en la Norma de seguridad ISO/IEC 27002:2013"

Autor: Ing. Hilda Yecenia Cevallos Jarro

Fecha: marzo 2019

En la tesis realizada por Hilda Cevallos en el 2019, diseña una política de seguridad de la información para el Instituto Tecnológico Superior Central Técnico, mediante los controles de la norma de seguridad ISO/IEC 27002:2013, guía que permitirá al área de TICs proteger la información contra posibles amenazas que puedan afectar la confidencialidad, integridad y disponibilidad.

Tabla 13
Análisis del trabajo de la Ing. Hilda Cevallos

Nº	Trabajo Ing. Hilda Cevallos	Trabajo propuesto
1	**Metodología Magerit:** - Para el análisis de riesgos de la información del instituto, sigue la guía metodológica de Magerit, ejecutando las actividades recomendadas, sin embargo, la identificación de los activos es breve, no se analiza detalladamente el inventario de activos reales.	**Metodología Magerit:** - Para realizar el análisis de riesgos, se ejecutarán las tareas indicadas por la metodología, especificando minuciosamente cada uno de los activos de información y de servicios del Sistema Ignug. con el fin de protegerlos para asegurar la gestión de continuidad a los procesos del instituto.
2	**Norma ISO/IEC 27002:2013:** - Diseña la política basándose en los controles de la Norma ISO/IEC 27002:2013.	**Norma ISO/IEC 27002:2017:** - Para el diseño de la política se aplicarán los dominios del estándar ISO/IEC 27002:2017, guía de buenas prácticas que describen los objetivos de los controles.
3	**Política:** - Diseña la política, de forma breve y concisa, sin explicar las directrices de cómo ejecutar cada uno de los controles.	**Política:** - Se considerarán todos los dominios y la mayoría de los controles. - Se mencionarán directrices para su implementación basada en buenas prácticas y recomendaciones para que la Unidad de TIC del IST Yavirac, comprenda y ejecute la implementación de los controles.

Fuente*:* Elaborado por el autor, basado en la tesis realizada por la Ing. Hilda Cevallos

Una vez realizado el análisis a los trabajos de diseño de políticas de los estudiantes de la Universidad Internacional SEK, se distingue que fueron realizados con la Norma ISO / IEC 27002:2013, Norma ISO / IEC 27002:2005; la tesis en desarrollo propone el uso de Norma ISO / IEC 27002:2017, estándar que sirve como punto de partida para el desarrollo de la política con especificaciones y directrices de buenas prácticas, que aportarán claridad a la implementación de la seguridad de los activos de información y servicios que provee el Sistema de Gestión Académicas Ignug del Instituto Superior Tecnológico Yavirac.

CAPÍTULO IV

ANÁLISIS Y SITUACIÓN ACTUAL DEL SGA Ignug

4.1 Situación Actual del Sistema de Gestión Académica Ignug

Antecedentes

El Instituto Superior Tecnológico Yavirac, es una institución comprometida en la ejecución del Plan Nacional de Desarrollo "Toda una Vida", busca fortalecer las competencias de los estudiantes, en los ámbitos teórico-práctico, enfatizando la creatividad y la innovación. La IES oferta carreras técnicas-tecnológicas reconocidas por la LOES como de tercer nivel en un ambiente adecuado orientado al sector de turístico, tecnológico y de patrimonio (Yavirac, 2019).

Esta entidad del sector público, regida por la Secretaría de Educación Superior Ciencia, Tecnología e Innovación (SENESCYT), mantiene contacto permanente con entidades nacionales e internacionales, de tal forma que, la actualización y orientación académica potencializan la pertinencia y la calidad educativa de docentes y estudiantes.

En la actualidad el Instituto Yavirac, se encuentra en proceso de fusión con los Institutos Tecnológicos Superiores Gran Colombia, Benito Juárez y 24 de Mayo, siendo el MSc. Iván Borja, Rector de todas las instituciones. La población estudiantil, supera las 1300 personas, con una planta docentes de 93 profesores. Para su organización administrativa y gestión académica, se encuentra estructurado de acuerdo al Anexo 2 "Organigrama Estructural".

La comunidad educativa actualmente cuenta con procesos automatizados y muchas de las actividades las realizan mediante el uso del Sistema de Gestión Académico Ignug, por

lo que es indispensable que la información digital sea protegida contra amenazas internas y externas.

Figura 5: Pantalla de autenticación del SGA Ignug
Fuente: http://Ignug.yavirac.edu.ec/#/login

Unidad de Tecnologías de la Información y Telecomunicaciones

La Unidad de TICs, fue creada durante el primer período lectivo de 2020; al ser un área relativamente nueva, no consta en el organigrama estructural de la institución. Está conformada por el Ing. Mauricio Tamayo, Coordinador; Ing. Pablo Robayo, Vicecoordinador; Ing. Maritza Tituaña, Administradora de Aplicaciones; Ing. Yogledis Herrera, Administradora de Base de Datos; Ing. Luis Chipuxi, Administrador del Data Center; docentes de la Carrera de Desarrollo de Software, Líderes de Proyectos de los nuevos módulos del Ignug. Tiene como misión, automatizar los procesos académicos y administrativos del instituto, administrar otras herramientas informáticas como Moodle, *Git Hub*, correo electrónico de *Google*, servidor virtual de Contabo; además, gestiona la conectividad con internet y con el servicio de alojamiento del Ignug, da soporte a los laboratorios de informática, capacitar a los docentes de la comunidad educativa con respecto a herramientas informáticas de educación virtual, soporte académico, etc.; por

lo cual, es de vital importancia identificar los peligros y amenazas a los que está expuesta la información y la infraestructura.

Es imperativo la implementación de normas, controles y la aplicación de buenas prácticas, que permitan preveer los posibles ciberataques que puede sufrir la plataforma tecnológica Ignug.

La Comisión Ejecutiva con el Comité de Seguridad, son los responsables de desarrollar, implementar, administrar y mantener los sistemas de información que se integran con Ignug.

4.2 Análisis de Riesgos aplicando Magerit

En el Instituto Superior Tecnológico Yavirac, los registros estudiantiles, notas, pases de año, récords académicos, etc., se los procesa, almacena y transporta, mediante el Sistema de Gestión Académica Ignug, que permite el registro de la data estudiantil, procesa y proporciona resultados con rapidez y exactitud; brindando un servicio automatizado a estudiantes y docentes de la comunidad educativa.

La información procesada a través de los recursos tecnológicos contratados por el instituto, corre el riesgo de ser atacada, por lo que es indispensable gestionar el análisis de riesgos como paso necesario para el diseño del modelo de ciberseguridad.

Mediante la técnica general “Sesiones de Trabajo”, que recomienda Magerit en el Libro 3, se mantuvieron reuniones y entrevistas con la Unidad de Tecnologías de la Información y Comunicación, se recolectó la información sobre los activos automatizados del instituto.

Para cumplir con el objetivo planteado en el presente proyecto, se consideró el modelo de catálogo de elementos, en el que manifiesta que para la determinación del riesgo se

deben reconocer los activos, la interrelación entre ellos y su valor; también determinar las salvaguardas y estimar el impacto y el riesgo (Magerit, 2012).

4.3 Determinación de los activos relevantes del instituto

Para determinar el riesgo, se levantó la información que se opera y los servicios que brinda el instituto, mediante la Plataforma de Gestión Académica Ignug, activos esenciales para el desarrollo de las actividades académicas. Además, se identificaron otros activos de los cuales depende como son:

- **[esencial] Activos esenciales**

- **[D] Datos/[info]Información:** información almacenada en las bases de datos del Sistema Ignug y la descripción del servidor virtual**.**
- **[serv] Servicios:** Servicios que satisfacen las necesidades de los usuarios del Sistema Ignug

- **[S] Servicios internos**: Organizan la estructura de los componentes del sistema Ignug.
- **[HW] Equipamiento informático:** Consta de las aplicaciones informáticas, los equipos físicos y virtuales, los dispositivos de comunicación y de almacenamiento.

- **[SW] Aplicaciones:** Módulos del Ignug desarrollados para automatizar los procesos académicos
- **[HW] Equipos informáticos**: Equipos en los cuales se encuentran las aplicaciones y datos del Sistema Ignug
- **[COM] Comunicaciones:** Incluyen los dispositivos intermediarios que transportan los datos de un equipo a otro como los *routers* y los servicios contratados como internet.
- **[Media] Soportes de información:** Equipos de la red, discos externos, en los que se almacena información de respaldo del Sistema Ignug, de forma permanente.

- **[SERVST] Servicios subcontratados a terceros**: Se toma en cuenta el servicio de host virtual Contabo, en el cual se encuentra alojada la plataforma Ignug y su base de datos.
- **[P] Personal**: Personas que usan el sistema y son encargadas de administrar la plataforma Ignug, la base de datos, el data center, desarrolladores y proveedores de internet y hosting virtual.

Infraestructura

El Instituto Yavirac, cuenta con un centro de datos administrado por la SENESCYT, con el fin de mantener en red y proveer de internet a los cuatro laboratorios informáticos de la institución; sin embargo, no está autorizado de implementar las aplicaciones creadas por la Unidad de Tecnología en dicha infraestructura.

Ignug, al ser un programa web, está implementado en un servidor de aplicaciones web en la nube, mediante el proveedor de servicios tecnológicos Contabo; el hosting virtual ofrece servicios de almacenamiento, servidores, alojamiento de aplicaciones web, bases de datos, redes, etc. De igual manera, la información procesada en él, se guarda en la nube; además, usa un gestor de base de datos Postgres.

En el siguiente diagrama, se observa la arquitectura cliente-servidor de la infraestructura virtual en la que se encuentra implementada la plataforma Ignug.

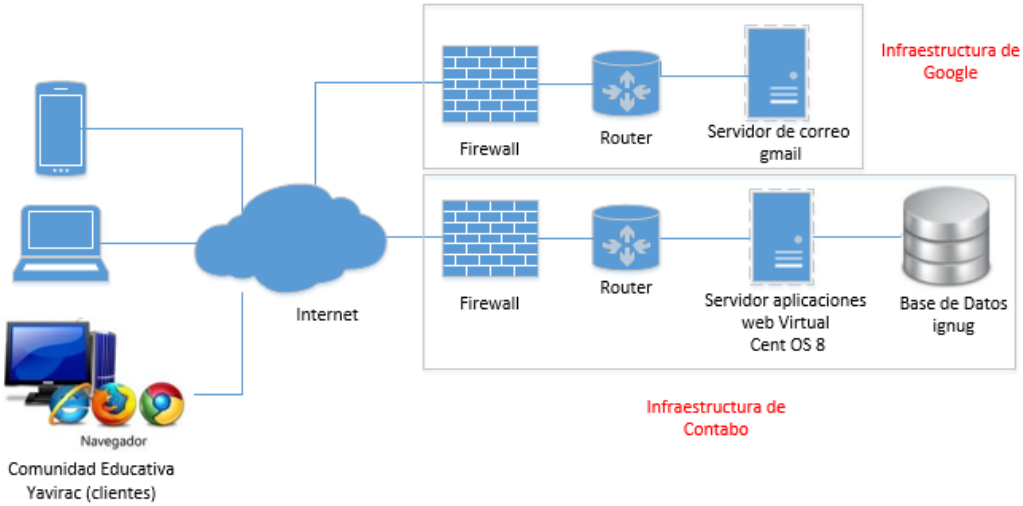

Figura 6: Esquema de la arquitectura cliente-servidor del Sistema Ignug
Fuente: Elaborado por el autor

Se le realizó una entrevista al Ing. Mauricio Tamayo, responsable de administrar el servidor web de aplicaciones, con la finalidad de levantar el inventario de las propiedades y características del servidor virtual. Ver Anexo 3 “Entrevista de Infraestructura”.

En la Tabla Nº 14, se observa el detalle técnico de los servicios contratados por la institución.

Tabla 14
Especificación técnica del servidor virtual

Servidor Virtual	**Detalle de los Recursos**
Componentes básicos en hardware	– 10 núcleos de CPU
	– 60 GB de RAM
	– 1600 GB de espacio en disco SSD
	– 100% de espacio en disco SSD
	– Tráfico ILIMITADO
	– Puerto de 1 Gbit / s
	– Protección DDoS
	– Acceso VNC
	– 1 dirección IP incluida
	– / 64 red IPv6 incluida
	– 4 instantáneas incluidas
Sistema Operativo	– Ubuntu Server 20

Servidor Virtual	Detalle de los Recursos
	– Reinicio y reinstalación del sistema operativo a través de la interfaz web
Centro de Administración	– Acceso root
Complementos	– Soporte en vivo todos los días, 365 días al año por correo electrónico y teléfono

Fuente: Elaborado por el autor, en referencia a la entrevista realizada al Coordinador de la Unidad de TIC

- Las bases de datos se encuentran alojadas en el mismo servidor que hospeda a las aplicaciones web, por tal razón, se encuentran directamente expuestas a Internet, lo cual conlleva a ser vulnerable de ataques cibernéticos.
- La velocidad de acceso a internet es de 70 Megas, cuyo proveedor es la Corporación Nacional de Telecomunicaciones CNT, el mismo que es costeado por el instituto.
- Para acceder al servidor de Contabo, únicamente se tiene un usuario genérico con el que ingresa el coordinador de la Unidad de TICs; sin embargo, cuando alguien más necesita acceder debe autenticarse con las mismas credenciales.
- No existe un inventario de aplicaciones y esquemas de base de datos que se encuentran alojados en el servidor alquilado.
- Los trabajos de mantenimiento al sistema académico, se los ejecuta de manera remota, dejándolo inoperativo por varias horas, causando denegación de servicio.
- No se ha implementado un protocolo de transferencia de hipertexto seguro, puesto que no posee certificado de seguridad, lo que hace que el sitio sea vulnerable de hackeo.
- No se cuenta con redundancia, si el servidor se baja, se cae el servicio.
- Se depende 100% de internet para tener acceso al servidor y al sistema.

- No existen logs de registros de incidentes informáticos con respecto a la infraestructura.

Aplicaciones informáticas

Ignug está conformada por los siguientes módulos: Matriculación, Asistencia y Notas, Administración, Registro y Asistencia de Docentes, Bolsa de Empleo. Está desarrollada con el framework Angular para el *front-end* y Laravel en el *back-end.*

En la Tabla Nº 15, se listan los módulos que conforman la plataforma web Ignug.

Tabla 15

Módulos que conforman el Sistema de Gestión Académica Ignug

Sistemas de Informáticos	Descripción
Módulo de Gestión de Matriculación	En esta aplicación web, se realiza la matriculación de forma automatizada, se cargan archivos y se generan reportes con la información de los estudiantes. Se tienen los siguientes perfiles: estudiante, docente, secretaria, coordinador de carrera y vicerrector. Se integra con el esquema de la base de datos Ignug.
Módulo de Gestión de Notas y Asistencia	Sistema web en la que se registran las notas, la asistencia, el historial académico de los estudiantes
Módulo de Administración	Aplicación web, que es administrada por el coordinador de TIC, para gestionar usuarios, carga de asignaturas, distributivo docente, etc.
Módulo de Registro de Asistencia de Docentes	Sistema Web, para registrar la jornada diaria, emite registros de la asistencia de los docentes.
Módulo de Bolsa de Empleo	Programa web en el cual se registran los estudiantes y empresas, para publicar sus perfil profesional y ofertas laborales, para la inserción laboral de los graduados del instituto.
Portal Web Yavirac	Página web institucional que contiene la oferta académica de las carreras del instituto.

Fuente: Elaborado por el autor, en referencia a la reunión con el Coordinador de la Unidad de TIC

Debido a que el sistema fue implementado hace tres períodos lectivos, tiene pocas seguridades contra la ciberdelincuencia. A continuación, se mencionan los siguientes problemas:

- El sistema no cuenta con temporizador de sesión que defina el tiempo que se mantendrá en el firewall cuando esté inactiva. Los estudiantes dejan abierta la cuenta del Ignug, por lo que, otros alumnos suplantan la identidad, alterando la información del propietario.
- Las bases de datos, no constan con un esquema de auditoría, no se tiene conocimiento de los usuarios que realizaron actualizaciones sobre ella.
- Se presentan modificaciones en los registros de la base de datos “ignug-bdd”, producto de accesos no controlados o indebidos.
- La creación de la cuenta de los graduados en la Bolsa de Empleo, se realiza mediante Internet, permitiendo ingreso de datos a usuarios externos a la institución, quienes pueden llenar con información basura la base de datos.
- No existe un manual de responsabilidades en el que se identifique el rol de cada usuario en la administración y uso del sistema académico.
- Los administradores de la plataforma, al desconocer sobre ciberseguridad, son vulnerables a ataques de ingeniería social, existiendo peligro para la custodia de las credenciales de administración tanto de los esquemas de bases de datos como de módulos del Ignug.
- No se mantiene un historial de quienes acceden al sistema académico.
- No se documentan los incidentes con respecto a la modificación no autorizada de la información.
- No se cuentan con técnicas de monitorización, que permitan al software detectar cualquier anomalía y error.
- Al hacer uso de una plataforma virtual como servidor, no existe redundancia ni funciones de recuperación.

- Las credenciales de acceso al sistema son predecibles, por lo general, se forma del correo electrónico para el usuario y el número de cédula como *password*; mientras el usuario no cambie sus credenciales de autenticación, se encuentra vulnerables de suplantación.

Uno de los principales retos del instituto, es la Ausencia de desarrolladores que se dediquen a tiempo completo a programar los diferentes módulos del Sistema Ignug, puesto que, los profesionales en el área ejercen sus funciones como docentes; además, de desempeñar funciones administrativas, vinculación con la sociedad, investigación, gestión empresarial, etc.; de esta manera, se reducen las horas de desarrollo y más aún, la aplicación de técnicas de protección frente a ataques en la red, en el Sistema Ignug y en las bases de datos implementados. Finalmente, tampoco posee políticas de seguridad informática.

Datos de información

Se realizó la recolección de datos, para lo cual se mantuvo una reunión con el coordinador de la Unidad de TIC, responsable de la administración del Sistema Ignug del instituto. Ver Anexo 4 “Acta de reunión”.

La información que se transacciona mediante los módulos que conforman el Sistema Ignug es la siguiente:

Módulo de Gestión de Matriculación

- Formularios de datos personales, académicos y socio-económicos, de los estudiantes.
- Solicitudes de matrículas.
- Archivos del Sistema Inteligente de Atención al Usuario de la SENESCYT, para identificar quienes cancelan rubros económicos y quiénes no adeudan al instituto.
- Registros de Matrículas.

- Reportes con la información antes indicada.

Módulo de Notas y Asistencia

- Matrices de rendimiento académico del alumnado.
- Registros de asistencia de estudiantes.
- Registros de notas por asignatura.
- Pases de año, récords académicos, etc.
- Informes de asistencia y calificaciones.

Módulo de Registro de Asistencia de Docentes

- Registros de asistencia de docentes y administrativos.
- Catálogo de actividades académicas, administrativas, de vinculación y de investigación que los docentes cumplen diariamente.
- Calendario semestral de vacaciones del personal de apoyo, docentes y directivos
- Reportes por fechas y por institutos, con la data de asistencia y actividades del personal.

Módulo de Administración

- Credenciales de autenticación de cuentas de usuarios y contraseñas de estudiantes, docentes y personal administrativo.
- Asignaturas de las diferentes mallas de cada carrera.
- Distributivo docente con la carga horaria.

Módulo de Bolsa de Empleo

- Datos personales, académicos, capacitaciones, experiencia laboral, etc. de los graduados de todas las carreras del Yavirac.

- Información general de las empresas como: razón social, RUC, actividad laboral, área de conocimiento, dirección, teléfono, etc. de las empresas.
- Ofertas laborales de las entidades registradas en la aplicación.

Portal Web Yavirac

- Datos del instituto y sus carreras.
- Información sobre la admisión a oferta académica y el proceso de postulación.
- Evidencias de fotos de las diferentes actividades del instituto.
- Calendario académico.
- Reglamentos interinstitucionales.
- Horarios de docentes, aulas, laboratorios, cursos.
- Autoevaluación institucional.
- Trabajos de investigación realizados por los docentes.

Personal

- Administrador del sistema web Ignug.
- Administrador de la base de datos “ignug-bdd”.
- Apoyo de administración del sistema web Ignug.
- Apoyo de administración de la base de datos “ignug-bdd”.
- Administrador de comunicaciones.
- Equipo de desarrollo: Docentes y estudiantes.

Desarrollo de Sistemas

En la actualidad, con la colaboración de estudiantes de la Unidad de Integración Curricular, se encuentran desarrollando los módulos de Capacitación Continua, Proceso de Titulación, Evaluación Docente, Vinculación con la Sociedad, que se integrarán al Sistema de Gestión Académico Ignug.

En reunión mantenida con el Ing. Tamayo, coordinador de TIC, se detectó que, durante el desarrollo de las aplicaciones, no se toma en consideración lo siguiente:

- El diseño del sistema en algunos casos es complejo, puesto que, en varios módulos se usan plantillas de front-end diferentes.
- Para la fase de *testing*, no se cuenta con un servidor exclusivo de pruebas, las mismas las realizan en el mismo servidor en otro directorio.
- Los archivos de datos, las configuraciones y los programas se almacenan en los mismos directorios separados del sistema de archivos.
- No se aplican validaciones en las entradas provenientes de fuentes no autorizadas.
- No se cuentan con entornos de desarrollo y pruebas exclusivos para estas actividades.
- No se han implementado temporizadores como *watchdog*.
- Existen problemas de sincronización y secuenciación causados por el uso compartido con los estudiantes.
- No se ocultan las carpetas del código fuente en el servidor web.

En cambio, sí se toma en cuenta los siguientes principios de seguridad:

- La arquitectura de los proyectos se la hace en tres capas, cumpliendo con el principio de defensa en profundidad.
- Se aplica el principio de mínimo privilegio, puesto que se otorgan permisos de las funcionalidades necesarias para el desempeño de las tareas autorizadas por usuario de acuerdo a su perfil.
- Asignación de roles a los usuarios para acceder únicamente al subconjunto de funciones y datos necesarios del sistema.
- Se observa que el código fuente, tiene implementado una lógica de control de excepciones.

Dependencias de los activos

En la siguiente imagen, se visualiza la estructura de los activos de la capa superior: esenciales, equipamiento informático y personal, relacionados con el Sistema de Gestión Académica Ignug, en base al análisis de dependencias del Libro I de Magerit 2012.

Figura 7: Activos del SGA Ignug
Fuente: Elaborado por el autor

Como se observa en la Figura Nº 6, los activos que se categorizaron en la primera capa son:

- [esencial] Activos esenciales
- [HW] Equipamiento informático
- [P] Personal

[esencial] Activos esenciales

Conforme al Libro II, "Catálogo de Elementos" de Magerit 2012, se clasificaron los activos esenciales, donde las capas superiores dependen de los activos inferiores.

En la siguiente imagen se observa la estructura de los activos esenciales y los dependientes, que se identificaron respecto al Sistema de Gestión Académico Ignug.

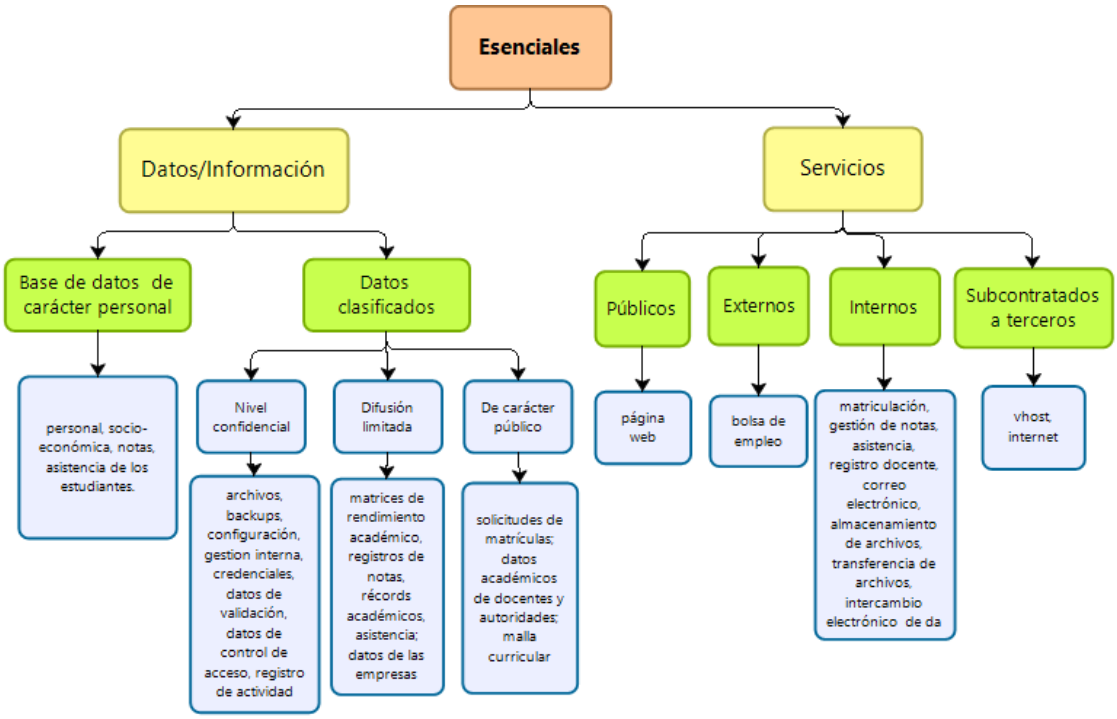

Figura 8: Activos esenciales
Fuente: Elaborado por el autor

En la Tabla Nº 16, se listan los activos esenciales de forma detallada.

Tabla 16

Activos esenciales

[esencial]Activos esenciales		
[D] Datos/[info]Información:		
[per] Datos personales	[per]	Bases de datos con información personal, socio-económica, notas, asistencia de los estudiantes.
[clas] Datos clasificados:	[C]	**Nivel confidencial**:
	[fich]	Archivos
	[backup]	Copias de respaldo
	[conf]	Datos de configuración del sistema
	[int]	Datos de gestión interna
	[paswd]	Credenciales: contraseñas
	[auth]	Datos de validación de credenciales
	[acl]	Datos de control de acceso
	[log]	Registro de actividad
	[codf]	Código fuente
	[exe]	Código ejecutable
	[R]	**Difusión limitada:** matrices de rendimiento académico, registros de notas, récords académicos, asistencia; datos de las empresas
	[pub]	**De carácter público:** solicitudes de matrículas; datos académicos de docentes y autoridades; malla curricular, información del portal.
[S] Servicios prestados:		
[S.pub] Públicos	[pub]	Público: página web
[S.ext] Externos	[ext]	Usuarios externos: bolsa de empleo

[esencial]Activos esenciales		
[S.int] Internos	[int]	Interno: matriculación, gestión de notas, asistencia, registro docente.
	[email]	Gmail de *Google*
	[file]	Almacenamiento de archivos
	[ftp]	Transferencia de archivos
	[edi]	Intercambio electrónico de datos
	[gesu]	Gestión de usuarios
	[idm]	Gestión de identidades
	[ipm]	Gestión de privilegios
[S.sub] Subcontratados a terceros	[vhost]	Hosting virtual Contabo
	[Internet]	Internet

Fuente: Elaborado por el autor, en referencia a la Metodología MAGERIT. Libro II "Catálogo de Elementos" (2012)

[HW] Equipamiento informático

Se estructuró el árbol de dependencias del equipamiento informático, donde las capas superiores dependen de los activos inferiores, de acuerdo al Libro II, "Catálogo de Elementos" de Magerit 2012, se encontraron los activos: aplicaciones, equipos informáticos, redes de comunicaciones, soportes de información. En la siguiente imagen, se observa la estructura de los activos del equipamiento informático que dependen unos de otros.

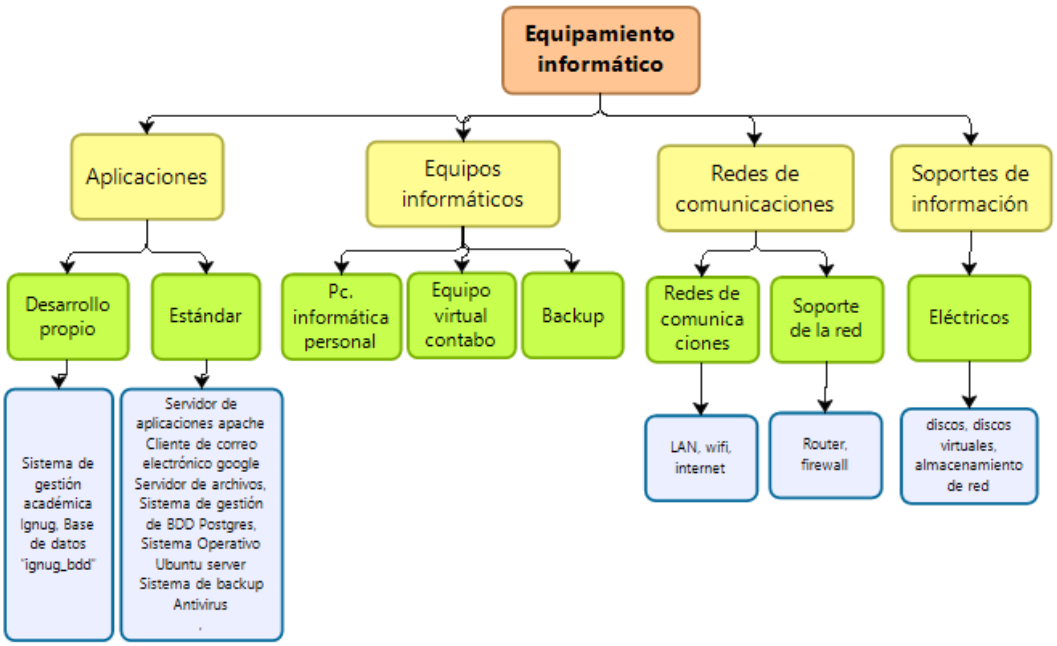

Figura 9: Activos equipamiento informático
Fuente: Elaborado por el autor

En la Tabla Nº 17, se listan los activos del equipamiento informático de forma detallada.

Tabla 17

Equipamiento informático

[HW] Equipamiento Informático		
[SW] Aplicaciones:		
[prp] Desarrollo propio	[sgai]	Sistema de gestión académica Ignug
	[bddi]	Base de datos ““ignug_bdd””
[std] Estándar	[app]	Servidor de aplicaciones web “Apache”
	[email-cliente]	Cliente de correo electrónico *Google*
	[file]	Servidor de archivos
	[dmbs]	Sistema de gestión de BDD Postgres
	[os]	Sistema Operativo Ubuntu server
	[backup]	Sistema de backup
[HW] Equipos informáticos:		
[HW] Equipos informáticos	[pc]	Informática personal
	[vhost]	Equipo virtual
	[backup]	Equipamiento de respaldo
[COM] Redes de comunicaciones:		
[COM] Redes de comunicaciones:	[LAN]	Red local
	[wifi]	Red inalámbrica
	[Internet]	Internet
[network] Soporte de la red	[firewall]	cortafuegos
	[router]	encaminadores
[Media] Soportes de información:		
[elect] electrónicos	[disk]	Discos
	[vdisk]	Discos virtuales
	[san]	Almacenamiento en red

Fuente: Elaborado por el autor, en referencia a la Metodología MAGERIT. Libro II “Catálogo de Elementos” (2012)

[P] Personal

A continuación, se detalla la estructura del personal relacionado con el uso, administración, desarrollo y proveedores de los servicios, donde las capas superiores dependen de los activos inferiores. En la Figura Nº 10, se visualizan los activos de acuerdo a la dependencia.

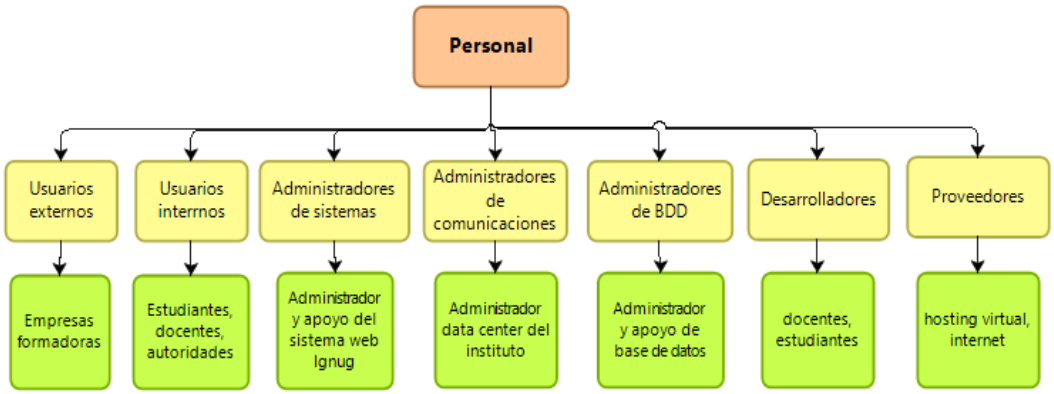

Figura 10: Activo personal
Fuente: Elaborado por el autor

Las dependencias de los datos son: bases de datos de carácter personal y datos clasificados y las dependencias de los servicios son: públicos, externos, internos, subcontratados a terceros.

En la Tabla Nº 18, se listan los activos del equipamiento informático de forma detallada.

Tabla 18
Personal

[P] Personal		
[ue] Usuarios externos	[ue]	Empresas formadoras
[ui] Usuarios internos	[uest]	Estudiantes
	[ud]	Docentes
	[ua]	Autoridades
[adm]	[adm]	Administrador del sistema web Ignug
Administradores de sistemas	[adma]	Apoyo de administración del sistema Ignug
[com] Administradores de comunicaciones	[com]	Administrador data center del instituto
[dba]	[adba]	Administrador de la BDD “ignug_bdd”
Administradores de BDD		
	[adbap]	Apoyo de administración bbdd “ignug_bdd”
[des]	[desd]	Desarrolladores docentes
Equipo de desarrollo	[dese]	Desarrolladores estudiantes
[prov]	[provi]	Proveedores de internet
Proveedores	[provhv]	Proveedores de hosting virtual

Fuente: Elaborado por el autor, en referencia a la Metodología MAGERIT. Libro II “Catálogo de Elementos” (2012)

Modelo de Valor

Para valorar a los activos listados en el ítem anterior, se consideraron las características básicas de seguridad:

- [D] disponibilidad del servicio,
- [I] integridad de los datos
- [C] confidencialidad de la información

También, se tomaron en cuenta dimensiones que preservan la integridad y confidencialidad de ciertos activos como:

- [A] autenticidad, y
- [T] trazabilidad

Además, se usó la escala de valor, que se indica en la Tabla Nº 19:

Tabla 19

Escala de valor para los activos

Valor		Criterio
5	MA Muy alto	Daño extremadamente grave
4	A Alto	Daño muy grave
3	M Medio	Daño grave
2	B Bajo	Daño importante
1	MB Muy bajo	Daño menor
0	D	Irrelevante a efectos prácticos

Fuente*:* Elaborado por el autor, en referencia a la Metodología MAGERIT. Libro II "Catálogo de Elementos" (2012)

Se eligió una escala del 1 al 10 conforme lo recomienda la metodología aplicada, en donde 0 es un valor que se asignan a los activos no relevantes; es decir, si fuesen afectados no causarían ningún daño y 10 la escala más alta, significa que el activo es muy importante, es decir, si una amenaza llegase a materializarse produciría un daño grave y posiblemente irreparable al instituto; por lo tanto, debería ser objeto de atención

inmediata. La valoración se realizó en función del impacto que una amenaza puede causarle a la información y a los servicios de la institución.

Para estimar el valor de los activos de información y de los servicios que proporciona el Sistema de Gestión Académica Ignug, se usó la fórmula siguiente:

$$\boldsymbol{VA} = \frac{\boldsymbol{C} + \boldsymbol{I} + \boldsymbol{D} + \boldsymbol{A} + \boldsymbol{T}}{\mathbf{5}}$$

Donde:

VA: promedio de las dimensiones de la seguridad

C, I, D, A, T: las dimensiones de seguridad

En las matrices siguientes, se estima el valor de los activos esenciales, equipamiento informático y personal relacionado con el Sistema Ignug tomando en cuenta las dimensiones básicas de seguridad.

Tabla 20

Valoración de los activos esenciales del Sistema Ignug tomando en cuenta las dimensiones básicas de seguridad

		[esencial] Activos esenciales	Valoración de acuerdo a las dimensiones de seguridad					Valor final	Tipo de valoración
			[I]	[C]	[D]	[A]	[T]		
[D] Datos/[info]Información:									
[per] Datos personales	[per]	Bases de datos con información personal, socio-económica, notas, asistencia de los estudiantes.	5	2	3	5	3	3	Medio
[clas] Datos clasificados:	[C]	**Nivel confidencial**:							
	[fich]	Archivos	5	5	5	5	5	5	Muy alto
	[backup]	Copias de respaldo	5	5	5	5	5	5	Muy alto
	[conf]	Datos de configuración del sistema	5	5	5	5	5	5	Muy alto
	[int]	Datos de gestión interna	5	5	5	5	5	5	Muy alto
	[paswd]	Credenciales: contraseñas	5	5	5	5	5	5	Muy alto
	[auth]	Datos de validación de credenciales	5	5	5	5	5	5	Muy alto
	[acl]	Datos de control de acceso	5	5	5	5	5	5	Muy alto
	[log]	Registro de actividad	5	5	5	5	5	5	Muy alto
	[codf]	Código fuente	5	5	5	5	5	5	Muy alto
	[exe]	Código ejecutable	5	5	5	5	5	5	Muy alto
	[R]	**Difusión limitada:** matrices de rendimiento académico, registros de notas, récords académicos, asistencia; datos de las empresas	5	2	5	3	5	4	Alto
	[pub]	**De carácter público:** solicitudes de matrículas; datos académicos de docentes y autoridades; malla curricular	5	-	3	.	2	3	Medio
[S] Servicios prestados:									
[S.pub] Públicos	[pub]	Público: página web	5	-	3	-	2	3	Medio
[S.ext] Externos	[ext]	Usuarios externos: bolsa de empleo	5	3	4	5	3	4	Alto
[S.int] Internos	[int]	Interno: matriculación, gestión de notas, asistencia, registro docente.	5	5	5	5	5	5	Muy Alto
	[email]	Gmail de google	5	5	4	5	4	5	Muy Alto
	[file]	Almacenamiento de archivos	5	5	5	5	5	5	Muy Alto
	[ftp]	Transferencia de archivos	5	5	5	5	5	5	Muy Alto
	[edi]	Intercambio electrónico de datos	5	5	5	5	5	5	Muy Alto
	[gesu]	Gestión de usuarios	5	5	5	5	5	5	Muy Alto
	[idm]	Gestión de identidades	5	5	5	5	5	5	Muy Alto
	[ipm]	Gestión de privilegios	5	5	5	5	5	5	Muy Alto

[esencial] Activos esenciales			Valoración de acuerdo a las dimensiones de seguridad					Valor final	Tipo de valoración
[S.sub]	[vhost]	Hosting virtual Contabo	5	5	5	5	5	5	Muy Alto
Subcontratados a terceros	[Internet]	Internet	5	5	3	5	3	4	Alto

Fuente: Elaborado por el autor, en referencia a la Metodología MAGERIT. Libro II "Catálogo de Elementos" (2012)

Tabla 21

Valoración del equipamiento informático del instituto tomando en cuenta las dimensiones de seguridad

[HW] Equipamiento informático			Valoración de acuerdo a las dimensiones de seguridad					Valor final	Tipo de valoración
			[I]	**[C]**	**[D]**	**[A]**	**[T]**		
[SW] Aplicaciones:									
[prp]	[sgai]	Sistema de gestión académica Ignug	5	5	5	5	5	5	Muy Alto
Desarrollo propio	[bddi]	Base de datos "ignug_bdd"	5	5	5	5	5	5	Muy Alto
[std] Estándar	[app]	Servidor de aplicaciones apache	5	5	5	5	5	5	Muy Alto
	[email-cliente]	Cliente de correo electrónico google	5	5	5	5	5	5	Muy Alto
	[file]	Servidor de archivos	5	5	5	5	5	5	Muy Alto
	[dmbs]	Sistema de gestión de BDD Postgres	5	5	5	5	5	5	Muy Alto
	[os]	Sistema Operativo Ubuntu server	5	5	5	5	5	5	Muy Alto
	[backup]	Sistema de backup	5	5	5	5	5	5	Muy Alto
[HW] Equipos informáticos:									
[HW] Equipos	[pc]	Informática personal	4	3	2	4	-	3	Medio
informáticos	[vhost]	Equipo virtual	5	5	5	5	5	5	Muy Alto
	[backup]	Equipamiento de respaldo	5	5	4	5	3	4	Alto
[COM] Redes de comunicaciones:									
[COM] Redes de	[LAN]	Red local	-	5	4	5	5	4	Alto
comunicaciones:	[wifi]	Red inalámbrica	-	5	4	5	5	4	Alto
	[Internet]	Internet	-	5	4	5	5	4	Alto
[network]	[firewall]	cortafuegos	5	5	3	5	3	4	Alto
Soporte de la red	[router]	encaminadores	5	5	3	5	3	4	Alto

[HW] Equipamiento informático			Valoración de acuerdo a las dimensiones de seguridad					Valor final	Tipo de valoración
			[I]	[C]	[D]	[A]	[T]		
[Media] Soportes de información:									
[elect] electrónicos	[disk]	Discos	5	5	3	3	3	4	Alto
	[vdisk]	Discos virtuales	5	5	4	5	3	4	Alto
	[san]	Almacenamiento en red	5	5	4	5	3	4	Alto

Fuente: Elaborado por el autor, en referencia a la Metodología MAGERIT. Libro II "Catálogo de Elementos" (2012)

Tabla 22

Valoración del personal relacionado con las aplicaciones e infraestructura del Ignug, tomando en cuenta las dimensiones de seguridad

[P] Personal			Valoración de acuerdo a las dimensiones de seguridad					Valor final	Tipo de valoración
			[I]	[C]	[D]	[A]	[T]		
[ue] Usuarios externos	[ue]	Empresas formadoras	5	3	3	5	3	3	Medio
[ui]	[uest]	Estudiantes	5	4	4	5	4	4	Alto
Usuarios internos	[ud]	Docentes	5	4	4	5	4	4	Alto
	[ua]	Autoridades	5	4	4	5	4	4	Alto
[adm] Administradores de sistemas	[adm]	Administrador del sistema web Ignug	5	5	5	5	5	5	Muy Alto
	[adma]	Apoyo de administración del sistema Ignug	5	5	5	5	5	5	Muy Alto
com] Administradores de comunicaciones	[com]	Administrador data center del instituto	5	5	5	5	5	5	Muy Alto
[dba] Administradores de BDD	[adba]	Administrador de la BDD "ignug_bdd"	5	5	5	5	5	5	Muy Alto
	[adbap]	Apoyo de administración bbdd "ignug_bdd"	5	5	5	5	5	5	Muy Alto
[des]	[desd]	Desarrolladores docentes	5	5	4	4	3	4	Alto
Equipo de desarrollo	[dese]	Desarrolladores estudiantes	5	5	4	4	3	4	Alto
[prov]	[provi]	Proveedores de internet	5	4	4	5	4	4	Alto
Proveedores	[provhv]	Proveedores de hosting virtual	5	5	5	5	5	5	Muy Alto

Fuente: Elaborado por el autor, en referencia a la Metodología MAGERIT. Libro II "Catálogo de Elementos" (2012)

4.4 Determinación de las amenazas

Se reconocieron y valoraron las amenazas que pueden sufrir los elementos en estudio, considerando la afectación a las dimensiones de seguridad.

La seguridad informática no considera las amenazas o desastres naturales, por lo que, del "Catálogo de Elementos" de Magerit, se tomaron en cuenta las siguientes amenazas:

- [I] De origen industrial
- [E] Errores y fallos no intencionados
- [A] Ataques intencionados

[esencial] Activos esenciales

En la Tabla Nº 22, se plasman las amenazas a las que están expuestos los activos esenciales como los datos, servicios ya sean prestados, internos y de acceso, que proporciona la plataforma Ignug; así como, los medios físicos y virtuales, en los que se transporta y almacena la información, tomando en cuenta las dimensiones de seguridad.

Tabla 23

Amenazas afectan a las dimensiones de seguridad de los activos esenciales del Sistema Ignug

[esencial] Activos esenciales			**Amenaza**		**Dimensión comprometida**
[D] Datos / [info] Información:					
[per] Datos personales	[per]	Bases de datos con información personal, académica y socio-económica, de los estudiantes; certificado SIAU.	[E.1]	Errores de los usuarios	[I], [D], [C]
			[E.2]	Errores del administrador	[I],[D],[C],[A]
			[E.15]	Alteración accidental de la información	[I]
			[E.18]	Destrucción de información	[D]
			[E.19]	Fugas de información	[C]
			[A.6]	Abuso de privilegio de acceso	[I],[D],[C]
			[A.7]	Uso no previsto	[I],[D],[C],[A]
			[A.11]	Acceso no autorizado	[I], [C], [A]
			[A.15]	Modificación deliberada de la información	[I]
			[A.18]	Destrucción de información	[D]
			[A.19]	Divulgación de información	[C]

[esencial] Activos esenciales			Amenaza		Dimensión comprometida
[clas] Datos clasificados	**[C]**	**Nivel confidencial**:			
	[fich]	Archivos	[E.1]	Errores de los usuarios	[I], [D], [C]
	[backup]	Copias de respaldo	[E.15]	Alteración accidental de la información	[I]
	[int]	Datos de gestión interna	[E.18]	Destrucción de información	[D]
			[E.19]	Fugas de información	[C]
			[A.7]	Uso no previsto	[I],[D],[C],[A]
			[A.11]	Acceso no autorizado	[I], [C], [A]
			[A.15]	Modificación deliberada de la información	[I]
			[A.18]	Destrucción de información	[D]
			[A.19]	Divulgación de información	[C]
	[conf]	Datos de configuración del sistema	[E.4]	Errores de configuración	[I]
			[E.15]	Alteración accidental de la información	[I]
			[E.18]	Destrucción de información	[D]
			[E.19]	Fugas de información	[C]
			[A.11]	Acceso no autorizado	[I], [C], [A]
			[A.15]	Modificación deliberada de la información	[I]
			[A.18]	Destrucción de información	[D]
			[A.19]	Divulgación de información	[C]
	[paswd]	Credenciales: contraseñas	[E.15]	Alteración accidental de la información	[I]
	[auth]	Datos de validación de credenciales	[E.18]	Destrucción de información	[D]
			[E.19]	Fugas de información	[C]
	[acl]	Datos de control de acceso	[A.11]	Acceso no autorizado	[I], [C], [A]
	[codf]	Código fuente	[A.15]	Modificación deliberada de la información	[I]
			[A.18]	Destrucción de información	[D]
			[A.19]	Divulgación de información	[C]
	[log]	Registro de actividad	[E.3]	Errores de monitorización (log)	[I], [T]
			[E.19]	Fugas de información	[C]
			[A.3]	Manipulación de los registros de actividad (log)	[I], [T]
			[A.4]	Manipulación de la configuración	[I], [T]
			[A.13]	Repudio	[I], [T]
			[A.15]	Modificación deliberada de la información	[I]
			[A.18]	Destrucción de información	[D]
	[exe]	Código ejecutable	[E.18]	Destrucción de información	[D]
			[E.19]	Fugas de información	[C]
			[A.11]	Acceso no autorizado	[I], [C], [A]
			[A.18]	Destrucción de información	[D]
			[A.19]	Divulgación de información	[C]
	[R]	**Difusión limitada:** matrices de rendimiento académico, registros de notas, récords	[E.1]	Errores de los usuarios	[I], [D], [C]
			[E.15]	Alteración accidental de la información	[I]
			[E.18]	Destrucción de información	[D]
			[E.19]	Fugas de información	[C]

[esencial] Activos esenciales			Amenaza		Dimensión comprometida
		académicos, asistencia; datos de las empresas,	[A.11]	Acceso no autorizado	[I], [C], [A]
			[A.15]	Modificación deliberada de la información	[I]
			[A.18]	Destrucción de información	[D]
			[A.19]	Divulgación de información	[C]
	[pub]	**De carácter público:** solicitudes de matrículas	[E.15]	Alteración accidental de la información	[I]
		datos académicos de docentes y autoridades;	[A.15]	Modificación deliberada de la información	[I]
		malla curricular	[A.18]	Destrucción de información	[D]
[serv] Servicios:					
[S.pub] Públicos	[pub]	Público	[A.12]	Análisis de tráfico	[D], [C]
			[A.15]	Modificación deliberada de la información	[I]
[S.ext] Externos	[ext]	Usuarios externos: empresas formadoras	[E.1]	Errores de los usuarios	[I], [D], [C]
			[E.19]	Fugas de información	[C]
			[A.7]	Uso no previsto	[I],[D],[C][A]
			[A.11]	Acceso no autorizado	[I], [C], [A]
			[A.13]	Repudio	[I], [T]
[S.int] Internos	[int] Usuarios Internos:	matriculación, gestión de notas, registro docente, bolsa de empleo.	[E.1]	Errores de los usuarios	[I], [D], [C]
			[E.19]	Fugas de información	[C]
			[A.5]	Suplantación de la identidad del usuario	[I],[D],[C] [A]
			[A.11]	Acceso no autorizado	[I], [C], [A]
			[A.13]	Repudio	[I], [T]
	[email]	Correo electrónico	[E.1]	Errores de los usuarios	[I], [D], [C]
			[E.9]	Errores de re encaminamiento	[C]
			[E.10]	Errores de secuencia	[I]
			[E.18]	Destrucción de información	[D]
			[E.19]	Fugas de información	[C]
			[E.24]	Caída del sistema por agotamiento de recursos	[D]
			A.5]	Suplantación de la identidad del usuario	[I],[D],[C], [A]
			[A.9]	Re encaminamiento de mensajes	[C]
			[A.10]	Alteración de secuencia	[I]
			[A.11]	Acceso no autorizado	[I], [C], [A]
			[A.13]	Repudio	[I], [T]
			[A.15]	Modificación deliberada de la información	[I]
			[A.18]	Destrucción de información	[D]
			[A.19]	Divulgación de información	[C]
	[file]	Almacenamiento de archivos	[E.1]	Errores de los usuarios	[I], [D], [C]
			[E.2]	Errores del administrador	[I], [D], [C]
			[E.10]	Errores de secuencia	[I]
			[E.18]	Destrucción de información	[D]
			[E.19]	Fugas de información	[C]
			[E.20]	Vulnerabilidades de los programas (software)	[I], [D], [C], [A], [T]
			[E.24]	Caída del sistema por agotamiento de recursos	[D]

[esencial] Activos esenciales			Amenaza		Dimensión comprometida
			[A.7]	Uso no previsto	[I],[D],[C],[A]
			[A.9]	Re encaminamiento de mensajes	[C]
			[A.10]	Alteración de secuencia	[I]
			[A.15]	Modificación deliberada de la información	[I]
			[A.18]	Destrucción de información	[D]
			[A.19]	Divulgación de información	[C]
	[ftp]	Transferencia de archivos	[E.1]	Errores de los usuarios	[I], [D], [C]
			[E.2]	Errores del administrador	[I], [D], [C]
			[E.9]	Errores de re encaminamiento	[C]
			[E.10]	Errores de secuencia	[I]
			[E.18]	Destrucción de información	[D]
			[E.19]	Fugas de información	[C]
			[E.20]	Vulnerabilidades de los programas (software)	[I], [D], [C], [A], [T]
			[E.24]	Caída del sistema por agotamiento de recursos	[D]
			[A.5]	Suplantación de la identidad del usuario	[I], [D], [C], [A]
			[A.9]	Re encaminamiento de mensajes	[C]
			[A.10]	Alteración de secuencia	[I]
			[A.11]	Acceso no autorizado	[I], [C], [A]
			[A.13]	Repudio	[I], [T]
			[A.15]	Modificación deliberada de la información	[I]
			[A.18]	Destrucción de información	[D]
	[edi]	Intercambio electrónico de datos	[E.1]	Errores de los usuarios	[I], [D], [C]
			[E.2]	Errores del administrador	[I], [D], [C]
			[E.9]	Errores de re encaminamiento	[C]
			[E.10]	Errores de secuencia	[I]
			[E.18]	Destrucción de información	[D]
			[E.19]	Fugas de información	[C]
			[E.20]	Vulnerabilidades de los programas (software)	[I], [D], [C], [A], [T]
			[E.24]	Caída del sistema por agotamiento de recursos	[D]
			[A.5]	Suplantación de la identidad del usuario	[I], [D], [C], [A]
			[A.9]	Re encaminamiento de mensajes	[C]
			[A.10]	Alteración de secuencia	[I]
			[A.11]	Acceso no autorizado	[I], [C], [A]
			[A.13]	Repudio	[I], [T]
			[A.18]	Destrucción de información	[D]
			[A.19]	Divulgación de información	[C]
	[gesu] [idm] [ipm]	Gestión usuarios Gestión identidades Gestión privilegios	[E.2]	Errores del administrador	[I], [D], [C]
			[A.5]	Suplantación de la identidad del usuario	[I], [D], [C], [A]
			[A.11]	Acceso no autorizado	[I], [C], [A]
[S.sub] Subcontra	[vhost]	Hosting virtual Contabo	[I.5]	Avería de origen físico o lógico	[D]
			[E.2]	Errores del administrador	[I], [D], [C]
			[E.19]	Fugas de información	[C]

[esencial] Activos esenciales			Amenaza		Dimensión comprometida
tados a terceros	[Internet]	Internet	[A.6]	Abuso de privilegios de acceso	[I], [D], [C], [A]

Fuente: Elaborado por el autor, en referencia a la Metodología MAGERIT. Libro II "Catálogo de Elementos" (2012)

Como se observa en la tabla anterior, las amenazas con respecto a errores y fallos no intencionados y ataques intencionados, perjudican a los activos esenciales datos y servicios que proporciona el Sistema de Gestión Académica Ignug, comprometiendo las características de la seguridad informática como la disponibilidad integridad, confidencialidad, autenticación y trazabilidad.

[Hw] El equipamiento informático

En la Tabla Nº 23, se reconocen las amenazas que puede sufrir el equipamiento informático en el cual está alojado el Sistema de Gestión Académica Ignug; así como, los medios físicos y virtuales, en los que se transporta y almacena la información, tomando en cuenta las dimensiones de seguridad.

Tabla 24

Amenazas que afectan a las dimensiones de seguridad del equipamiento informático en el cual se encuentra alojado el Sistema Ignug

[HW] Equipamiento informático			Amenaza		Dimensión comprometida
[SW] Aplicaciones:					
[prp] Desarrollo propio	[sgai]	Sistema de gestión académica Ignug	[I.5]	Avería de origen físico o lógico	[D]
			[E.1]	Errores de los usuarios	[I], [D], [C]
			[E.2]	Errores del administrador	[I], [D], [C]
			[E.10]	Errores de secuencia	[I]
	[bddi]	Base de datos "ignug_bdd"	[E.15]	Alteración accidental de la información	[I]
			[E.18]	Destrucción de información	[D]
			[E.19]	Fugas de información	[C]
			[E.20]	Vulnerabilidades de los programas (software)	[I],[D],[C],[A],[T]
			[E.24]	Caída del sistema por agotamiento de recursos	[D]
			[A.5]	Suplantación de la identidad del usuario	[I], [D], [C], [A]
			[A.6]	Abuso de privilegios de acceso	[I], [D], [C], [A]

[HW] Equipamiento informático			Amenaza		Dimensión comprometida
			[A.9]	Re encaminamiento de mensajes	[C]
			[A.10]	Alteración de secuencia	[I]
			[A.11]	Acceso no autorizado	[I], [C], [A]
			[A.15]	Modificación deliberada de la información	[I]
			[A.18]	Destrucción de información	[D]
			[A.19]	Divulgación de información	[C]
			[A.24]	Denegación de servicio	[D]
[std] Estándar	[app]	Servidor de aplicaciones apache	[E.1]	Errores de los usuarios	[I], [D], [C]
			[E.2]	Errores del administrador	[I], [D], [C]
			[E.15]	Alteración accidental de la información	[I]
	[dmbs]	Sistema de gestión de base de Datos Postgres	[E.18]	Destrucción de información	[D]
			[E.19]	Fugas de información	[C]
			[E.20]	Vulnerabilidades de los programas (software)	[I],[D],[C],[A],[T]
	[file]	Servidor de archivos	[E.24]	Caída del sistema por agotamiento de recursos	[D]
	[os]	Sistema Operativo Ubuntu server	[A.5]	Suplantación de la identidad del usuario	[I], [D], [C], [A]
			[A.6]	Abuso de privilegios de acceso	[I], [D], [C], [A]
			[A.7]	Uso no previsto	[I], [D], [C], [A]
	[backup]	Sistema de backup	[A.10]	Alteración de secuencia	[I]
			[A.11]	Acceso no autorizado	[I], [C], [A]
			[A.15]	Modificación deliberada de la información	[I]
			[A.18]	Destrucción de información	[D]
			[A.24]	Denegación de servicio	[D]
	[email-cleinte]	Cliente de correo electrónico *Google*	[E.9]	Errores de re encaminamiento	[C]
			[E.10]	Errores de secuencia	[I]
			[E.19]	Fugas de información	[C]
			[E.20]	Vulnerabilidades de los programas (software)	[I],[D],[C],[A],[T]
			[A.5]	Suplantación de la identidad del usuario	[I], [D], [C], [A]
			[A.6]	Abuso de privilegios de acceso	[I], [D], [C], [A]
			[A.7]	Uso no previsto	[I], [D], [C], [A]
			[A.9]	Re encaminamiento de mensajes	[C]
			[A.10]	Alteración de secuencia	[I]
			[A.11]	Acceso no autorizado	[I], [C], [A]
			[A.15]	Modificación deliberada de la información	[I]
			[A.18]	Destrucción de información	[D]
			[A.19]	Divulgación de información	[C]
			[A.24]	Denegación de servicio	[D]
[HW] Equipos informáticos:					
[HW] Equipos informáticos	[pc]	Informática personal	[I.1]	Fuego	[D]
			[I.3]	Contaminación mecánica	[D]
			[I.5]	Avería de origen físico o lógico	[D]
			[I.6]	Corte de suministro eléctrico	[D]

[HW] Equipamiento informático			Amenaza		Dimensión comprometida
			[I.7]	Condiciones inadecuadas de temperatura o humedad	[D]
			[I.11]	Emanaciones electromagnéticas	[C]
			[E.2]	Errores del administrador	[I], [D], [C]
			[E.19]	Fugas de información	[C]
	[backup]	Equipamiento de respaldo	[I.5]	Avería de origen físico o lógico	[D]
			[I.7]	Condiciones inadecuadas de temperatura o humedad	[D]
			[E.2]	Errores del administrador	[I], [D], [C]
			[E.19]	Fugas de información	[C]
			[A.6]	Abuso de privilegios de acceso	[I], [D], [C], [A
			[A.7]	Uso no previsto	[I], [D], [C], [A]
[COM] Redes de comunicaciones:					
[COM] Servicios subcontratados	[LAN]	Red local	[I.5]	Avería de origen físico o lógico	[D]
	[wifi]	Red inalámbrica	[I.8]	Fallo de servicios de comunicaciones	[D]
			[E.2]	Errores del administrador	[I], [D], [C]
			[E.9]	Errores de re encaminamiento	[C]
			[E.10]	Errores de secuencia	[I]
			[E.19]	Fugas de información	[C]
			[A.6]	Abuso de privilegios de acceso	[I], [D], [C], [A]
			[A.7]	Uso no previsto	[I], [D], [C], [A]
[network] Soporte de la red	[firewall]	Cortafuegos	[I.1]	Fuego	[D]
	[router]	Encaminadores	[I.3]	Contaminación mecánica	[D]
			[I.5]	Avería de origen físico o lógico	[D]
			[I.6]	Corte de suministro eléctrico	[D]
			[I.7]	Condiciones inadecuadas de temperatura o humedad	[D]
			[I.8]	Fallo de servicios de comunicaciones	[D]
			[I.11]	Emanaciones electromagnéticas	[C]
			[E.2]	Errores del administrador	[I], [D], [C]
			[E.9]	Errores de re encaminamiento	[C]
			[E.10]	Errores de secuencia	[I]
			[A.6]	Abuso de privilegios de acceso	[I], [D], [C], [A]
			[A.9]	Re encaminamiento de mensajes	[C]
[Media] Soportes de información:					
[elect] electrónicos	[disk]	Discos	[I.1]	Fuego	[D]
			[I.3]	Contaminación mecánica	[D]
	[vdisk]	Discos virtuales	[I.4]	Contaminación electromagnética	[D]
			[I.5]	Avería de origen físico o lógico	[D]
	[san]	Almacenamiento en red	[E.19]	Fugas de información	[C]
			[A.6]	Abuso de privilegios de acceso	[I], [D], [C], [A]
			[A.7]	Uso no previsto	[I], [D], [C], [A]

Fuente: Elaborado por el autor, en referencia a la Metodología MAGERIT. Libro II "Catálogo de Elementos" (2012)

En la tabla anterior, se visualizan las amenazas con carácter industrial, errores y fallos involuntarios y ataques deliberados, que afectan al equipamiento informático afines a las aplicaciones, equipos informáticos, redes de comunicaciones y soportes de información de la plataforma Ignug, perjudicando la disponibilidad integridad, confidencialidad, autenticación y trazabilidad.

[P] Personal

En la siguiente matriz, se reconocen las amenazas a las que se puede enfrentar el Sistema de Gestión Académica Ignug, relacionado con el personal interno del instituto, tomando en cuenta las dimensiones de seguridad.

Tabla 25

Amenazas que afectan a las dimensiones de seguridad del personal relacionado con el uso y administración del SGA Ignug

Activo: [P] Personal			**Amenaza**		**Dimensión comprometida**
[ue]Usuarios externos	[ue]	Empresas formadoras	[A.5]	Suplantación de la identidad usuario	[I], [C], [A]
			[A.11]	Acceso no autorizado	[I], [C], [A]
[ui] Usuarios internos	[uest]	Estudiantes	[E.1]	Errores de los usuarios	[I], [D], [C]
			[E.19]	Fugas de información	[C]
	[ud]	Docentes	[A.5]	Suplantación de la identidad del usuario	[I], [C], [A]
	[ua]	Autoridades	[A.6]	Abuso de privilegios de acceso	[I], [D], [C]
			[A.11]	Acceso no autorizado	[I], [C], [A]
			[A.19]	Divulgación de información	[C]
[adm] Administradores de sistemas	[adm]	Admin. sistema Ignug	[E.2]	Errores del administrador	[I], [D], [C]
	[adma]	Apoyo de admin. Ignug	[E.19]	Fugas de información	[C]
[dba] Administradores BDD.	[adba]	Admin.BDD	[A.5]	Suplantación de la identidad del usuario	[I], [C], [A]
	[adbap]	Apoyo de admin. BDD	[A.19]	Divulgación de información	[C]
[com] Administradores comuni.	[adcom]	Admin. data center			
[des] Equipo de desarrollo	[desd]	desarrolladores docentes	[E.2]	Errores del administrador	[I], [D], [C]
			[E.19]	Fugas de información	[C]
	[dese]	desarrolladores estudiantes	[A.5]	Suplantación de la identidad del usuario	[I], [C], [A]
			[A.6]	Abuso de privilegios de acceso	[I], [D], [C]
			[A.19]	Divulgación de información	[C]
[prov]	[provi]		[E.19]	Fugas de información	[C]

Activo: [P] Personal			Amenaza		Dimensión comprometida
Proveedores	[provhv]	proveedores de internet	[A.5]	Suplantación de la identidad del usuario	[I], [C], [A]
		proveedores de hosting virtual	[E.19]	Fugas de información	[C]
			[A.5]	Suplantación de la identidad del usuario	[I], [C], [A]
			[A.6]	Abuso de privilegios de acceso	[I], [D], [C]
			[A.19]	Divulgación de información	[C]

Fuente: Elaborado por el autor, en referencia a la Metodología MAGERIT. Libro II "Catálogo de Elementos" (2012)

Como se observa en la tabla anterior, las amenazas en relación al personal interno que administra los módulos del Ignug, tiene que ver con errores y fallos involuntarios y ataques delibrados, los que afectan a los pilares fundamentales de la seguridad del Sistema de Gestión Académica Ignug.

Valoración de las amenazas

Posterior a la identificación de las amenazas a las que están expuestos los activos del Sistema de Gestión Académica Ignug, se valoró la amenaza en los sentidos de la degradación y la probabilidad de ocurrencia que se puedan materializar; se tomó en cuenta los indicadores cualitativos de la Tabla Nº 1 del Capítulo II referente al Marco Teórico. Cabe indicar que, los peligros producidos a través incidencias involuntarias pesan menos que los ataques deliberados, debido a, que la primera amenaza se puede ejecutar en menor grado de afectación con respecto a la segunda, causando mucho daño a un elemento específico (Magerit, 2012).

[esencial] Activos esenciales

En la matriz Nº 26, se visualiza la valoraron de las amenazas relevantes sobre cada activo esencial como los datos y los servicios que presta el Sistema Ignug, con respecto a las variables degradación y probabilidad de ocurrencia. Se usó la Tabla Nº 1 del Capítulo II referente al Marco Teórico.

Tabla 26

Valoración de las amenazas de acuerdo a la degradación de los activos esenciales

[esencial] Activos esenciales		Amenaza		Vulnerabilidad	Degradación		Probabilidad	
[D] Datos /[info] Información:								
[per] Datos personales								
[per]	Bases de datos con información personal, académica y socio-económica, de los estudiantes; certificado SIAU.	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	M	Media	Posible	Difícil
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración				
		[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	A	Alta	Muy alto	Medio
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	Muy alta	Casi seguro	Fácil
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario				
		[A.6]	Abuso de privilegio de acceso	Ausencia de control de eventos *logs*				
		[A.7]	Uso no previsto	Ausencia de registro de control en el acceso a los datos	A	Alta	Muy alto	Medio
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Muy alta	Casi seguro	Fácil
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	Muy alta	Casi seguro	Fácil
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Muy alta	Casi seguro	Fácil
		[A.19]	Divulgación de información	Falta control en las cuentas dadas de baja de los usuarios	A	Alta	Muy alto	Medio
[clas] Datos clasificados:								
[C] Nivel confidencial:								
[fich]	Archivos	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	MA	Muy alta	Casi seguro	Fácil
		[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	MA	Muy alta	Casi seguro	Fácil
[backup]	Copias de respaldo	[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	Muy alta	Casi seguro	Fácil
[int]	Datos de gestión interna	[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	A	Alta	Muy alto	Medio
		[A.7]	Uso no previsto	Ausencia de registro de control en el acceso a los datos	A	Alta	Muy alto	Medio
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Muy alta	Casi seguro	Fácil
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	Muy alta	Casi seguro	Fácil
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Muy alta	Casi seguro	Fácil

[esencial] Activos esenciales		Amenaza		Vulnerabilidad	Degradación		Probabilidad	
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja	A	Alta	Muy alto	Medio
[conf]	Datos de configuración del sistema	[E.4]	Errores de configuración	Ausencia de manuales de instalación y configuración	MA	Muy alta	Casi seguro	Fácil
		[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	MA	Muy alta	Casi seguro	Fácil
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	Muy alta	Casi seguro	Fácil
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	Muy alta	Casi seguro	Fácil
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Muy alta	Casi seguro	Fácil
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	Muy alta	Casi seguro	Fácil
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Muy alta	Casi seguro	Fácil
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja	MA	Muy alta	Casi seguro	Fácil
[paswd]	Credenciales: contraseñas	[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	MA	Muy alta	Casi seguro	Fácil
[auth]	Datos de validación de credenciales	[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	Muy alta	Casi seguro	Fácil
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	Muy alta	Casi seguro	Fácil
	Datos de control de	[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Muy alta	Casi seguro	Fácil
[acl]	acceso	[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	Muy alta	Casi seguro	Fácil
	Código fuente							
[codf]		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Muy alta	Casi seguro	Fácil
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja	MA	Muy alta	Casi seguro	Fácil
[log]	Registro de actividad	[E.3]	Errores de monitorización (log)	Ausencia de implementación, seguimiento y lectura a *logs*	A	Alta	Muy alto	Medio
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	A	Alta	Muy alto	Medio
		[A.3]	Manipulación de los registros de actividad (log)	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información	MA	Muy alta	Casi seguro	Fácil
		[A.4]	Manipulación de la configuración	Falta de procedimiento formal para la supervisión del registro del SGSI	MA	Muy alta	Casi seguro	Fácil
		[A.13]	Repudio	Ausencia de implementación de firmas digitales	MA	Muy alta	Casi seguro	Fácil
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	Muy alta	Casi seguro	Fácil
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Muy alta	Casi seguro	Fácil
[exe]	Código ejecutable	[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	Muy alta	Casi seguro	Fácil
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	A	Alta	Muy alto	Medio

[esencial] Activos esenciales		Amenaza		Vulnerabilidad	Degradación		Probabilidad	
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Muy alta	Casi seguro	Fácil
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Muy alta	Casi seguro	Fácil
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja	A	Alta	Muy alto	Medio
[R] **Difusión limitada:**								
[R]	matrices de rendimiento académico, registros de notas, récords académicos, asistencia; datos de las empresas,	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	A	Alta	Muy alto	Medio
		[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	A	Alta	Muy alto	Medio
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	Muy alta	Casi seguro	Fácil
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	A	Alta	Muy alto	Medio
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	A	Alta	Muy alto	Medio
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	Muy alta	Casi seguro	Fácil
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Muy alta	Casi seguro	Fácil
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja	A	Alta	Muy alto	Medio
[pub] **De carácter público:**								
[pub]	solicitudes de matrículas; datos académicos de docentes y autoridades; malla curricular	[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	A	Alta	Muy alto	Medio
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	Muy alta	Casi seguro	Fácil
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Muy alta	Casi seguro	Fácil
[serv] Servicios:								
[pub]	Público	[A.12]	Análisis de tráfico	Puerto abiertos innecesariamente	MB	Muy baja	Muy raro	Ext. difícil
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	M	Media	Posible	Difícil
[ext]	Usuarios externos: empresas formadoras	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	M	Media	Posible	Difícil
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	A	Alta	Muy alto	Medio
		[A.7]	Uso no previsto	Ausencia de registro de control en el acceso a los datos	A	Alta	Muy alto	Medio
		[A.11]	Acceso no autorizado	Contraseñas inseguras	MA	Muy alta	Casi seguro	Fácil
		[A.13]	Repudio	Ausencia de implementación de firmas digitales	MA	Muy alta	Casi seguro	Fácil
[int]	Usuarios Internos: matriculación,	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	M	Media	Posible	Difícil
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	A	Alta	Muy alto	Medio

[esencial] Activos esenciales		Amenaza		Vulnerabilidad	Degradación		Probabilidad	
	gestión de notas, registro docente, bolsa de empleo.	[A.5]	Suplantación de la identidad del usuario	Contraseñas predecibles o inseguras	MA	Muy alta	Casi seguro	Fácil
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Muy alta	Casi seguro	Fácil
		[A.13]	Repudio	Ausencia de implementación de firmas digitales	MA	Muy alta	Casi seguro	Fácil
[email]	Correo electrónico	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	M	Media	Posible	Difícil
		[E.9]	Errores de re encaminamiento	Configuraciones erróneas, Ausencia de monitoreo	MA	Muy alta	Casi seguro	Fácil
		[E.10]	Errores de secuencia	Ausencia de sincronización	MA	Muy alta	Casi seguro	Fácil
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	Muy alta	Casi seguro	Fácil
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	A	Alta	Muy alto	Medio
		[E.24]	Caída del sistema por agotamiento de recursos	Saturación de los recursos tecnológicos	A	Alta	Muy alto	Medio
		A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles	MA	Muy alta	Casi seguro	Fácil
		[A.9]	Re encaminamiento de mensajes	Ausencia de monitoreo	MA	Muy alta	Casi seguro	Fácil
		[A.10]	Alteración de secuencia	Ausencia de sincronización	MA	Muy alta	Casi seguro	Fácil
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Muy alta	Casi seguro	Fácil
		[A.13]	Repudio	Ausencia de implementación de firmas digitales	MA	Muy alta	Casi seguro	Fácil
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	Muy alta	Casi seguro	Fácil
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Muy alta	Casi seguro	Fácil
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja de los usuarios	MA	Muy alta	Casi seguro	Fácil
[file]	Almacenamiento de archivos	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	A	Alta	Muy alto	Medio
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	Muy alta	Casi seguro	Fácil
		[E.10]	Errores de secuencia	Ausencia de sincronización	MA	Muy alta	Casi seguro	Fácil
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	Muy alta	Casi seguro	Fácil
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	A	Alta	Muy alto	Medio
		[E.20]	Vulnerabilidades de los programas (software)	Ausencia de escaneo y actualizaciones	MA	Muy alta	Casi seguro	Fácil
		[E.24]	Caída del sistema por agotamiento de recursos	Saturación de los recursos tecnológicos	A	Alta	Muy alto	Medio

[esencial] Activos esenciales		Amenaza		Vulnerabilidad	Degradación		Probabilidad	
		[A.7]	Uso no previsto	Ausencia de registro de control en el acceso a los datos	MA	Muy alta	Casi seguro	Fácil
		[A.9]	Re encaminamiento de mensajes	Ausencia de monitoreo	MA	Muy alta	Casi seguro	Fácil
		[A.10]	Alteración de secuencia	Ausencia de sincronización	MA	Muy alta	Casi seguro	Fácil
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	Muy alta	Casi seguro	Fácil
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Muy alta	Casi seguro	Fácil
		[A.19]	Divulgación de información	Falta control en las cuentas dadas de baja de los usuarios	MA	Muy alta	Casi seguro	Fácil
[ftp]	Transferencia de archivos	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	A	Alta	Muy alto	Medio
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	Muy alta	Casi seguro	Fácil
		[E.9]	Errores de re encaminamiento	Configuraciones erróneas, Ausencia de monitoreo	MA	Muy alta	Casi seguro	Fácil
		[E.10]	Errores de secuencia	Ausencia de sincronización	MA	Muy alta	Casi seguro	Fácil
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	Muy alta	Casi seguro	Fácil
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	A	Alta	Muy alto	Medio
		[E.20]	Vulnerabilidades de los programas (software)	Ausencia de escaneo y actualizaciones	MA	Muy alta	Casi seguro	Fácil
		[E.24]	Caída del sistema por agotamiento de recursos	Saturación de los recursos tecnológicos	A	Alta	Muy alto	Medio
		[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles	MA	Muy alta	Casi seguro	Fácil
		[A.9]	Re encaminamiento de mensajes	Ausencia de monitoreo	MA	Muy alta	Casi seguro	Fácil
		[A.10]	Alteración de secuencia	Ausencia de sincronización	MA	Muy alta	Casi seguro	Fácil
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Muy alta	Casi seguro	Fácil
		[A.13]	Repudio	Ausencia de implementación de firmas digitales	MA	Muy alta	Casi seguro	Fácil
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	Muy alta	Casi seguro	Fácil
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Muy alta	Casi seguro	Fácil
[edi]	Intercambio electrónico de datos	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	A	Alta	Muy alto	Medio
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	Muy alta	Casi seguro	Fácil

[esencial] Activos esenciales		Amenaza		Vulnerabilidad	Degradación		Probabilidad	
		[E.9]	Errores de re encaminamiento	Configuraciones erróneas, Ausencia de monitoreo	MA	Muy alta	Casi seguro	Fácil
		[E.10]	Errores de secuencia	Ausencia de sincronización	MA	Muy alta	Casi seguro	Fácil
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	Muy alta	Casi seguro	Fácil
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	A	Alta	Muy alto	Medio
		[E.20]	Vulnerabilidades de los programas (software)	Ausencia de escaneo y actualizaciones	MA	Muy alta	Casi seguro	Fácil
		[E.24]	Caída del sistema por agotamiento de recursos	Saturación de los recursos tecnológicos	A	Alta	Muy alto	Medio
		[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles	MA	Muy alta	Casi seguro	Fácil
		[A.9]	Re encaminamiento de mensajes	Ausencia de monitoreo	MA	Muy alta	Casi seguro	Fácil
		[A.10]	Alteración de secuencia	Ausencia de sincronización	MA	Muy alta	Casi seguro	Fácil
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Muy alta	Casi seguro	Fácil
		[A.13]	Repudio	Ausencia de implementación de firmas digitales	MA	Muy alta	Casi seguro	Fácil
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Muy alta	Casi seguro	Fácil
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja	MA	Muy alta	Casi seguro	Fácil
[gesu]	Gestión usuarios	[E.2]	Errores del administrador	Ausencia de concienciación y control en las cuentas dadas de baja de los usuarios	MA	Muy alta	Casi seguro	Fácil
[idm]	Gestión identidades							
[ipm]	Gestión privilegios	[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles	MA	Muy alta	Casi seguro	Fácil
		[A.11]	Acceso no autorizado	Contraseñas inseguras	MA	Muy alta	Casi seguro	Fácil
[S.sub] Subcontratados a terceros								
[vhost]	Hosting virtual Contabo	[I.5]	Avería de origen físico o lógico	Fallo en los equipos informáticos	MA	Muy alta	Casi seguro	Fácil
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	Muy alta	Casi seguro	Fácil
[Internet]	Internet	[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	Muy alta	Casi seguro	Fácil
		[A.6]	Abuso de privilegio de acceso	Ausencia de control de eventos *logs*	MA	Muy alta	Casi seguro	Fácil

Fuente: Elaborado por el autor, en referencia a la Metodología MAGERIT. Libro II "Catálogo de Elementos" (2012)

Como se observa en el cuadro anterior, la degradación que pueden sufrir los activos esenciales es muy alta, puesto que la información y los servicios son la razón de ser del Instituto Yavirac.

[Hw] El equipamiento informático

En la Tabla Nº 25, se valoraron las amenazas sobre el equipamiento informático como: aplicaciones, equipos físicos y lógicos, comunicaciones, soportes de información, con respecto a las variables degradación y probabilidad de ocurrencia. Se usó la Tabla Nº 1 del Capítulo II referente al Marco Teórico.

Tabla 27

Valoración de la amenaza de acuerdo a la degradación del equipamiento informático

[HW]Equipamiento informático		**Amenaza**		**Vulnerabilidad**	**Degradación**		**Probabilidad**	
[SW] Aplicaciones:								
[prp] Desarrollo propio								
[sgai]	Sistema de gestión	[I.5]	Avería de origen físico o lógico	Fallo en las configuraciones de los equipos informáticos	MA	Muy alta	Casi seguro	Fácil
	académica	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	A	Alta	Muy alto	Medio
	Ignug	[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	Muy alta	Casi seguro	Fácil
[bddi]	Base de datos	[E.10]	Errores de secuencia	Ausencia de sincronización	MA	Muy alta	Casi seguro	Fácil
	“ignug_bdd”	[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	MA	Muy alta	Casi seguro	Fácil
[backup]	Respaldos	[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	Muy alta	Casi seguro	Fácil
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	Muy alta	Casi seguro	Fácil
		[E.20]	Vulnerabilidades de los programas (software)	Ausencia de escaneo y actualizaciones	MA	Muy alta	Casi seguro	Fácil

[HW]Equipamiento informático		Amenaza		Vulnerabilidad	Degradación		Probabilidad	
		[E.24]	Caída del sistema por agotamiento de recursos	Saturación de recursos tecnológicos	A	Alta	Muy alto	Medio
		[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles	MA	Muy alta	Casi seguro	Fácil
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	MA	Muy alta	Casi seguro	Fácil
		[A.9]	Re encaminamiento de mensajes	Ausencia de monitoreo	MA	Muy alta	Casi seguro	Fácil
		[A.10]	Alteración de secuencia	Ausencia de sincronización	MA	Muy alta	Casi seguro	Fácil
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Muy alta	Casi seguro	Fácil
		[A.15]	Modificación deliberada de la información	Ausencia de procedimientos de desvinculación de los empleados	MA	Muy alta	Casi seguro	Fácil
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Muy alta	Casi seguro	Fácil
		[A.19]	Divulgación de información	Falta control en las cuentas dadas de baja de los usuarios	A	Alta	Muy alto	Medio
		[A.24]	Denegación de servicio	Ausencia de control en las cuentas dadas de baja de recursos suficientes	A	Alta	Muy alto	Medio
[std] Estándar:								
[app]	Servidor de aplicaciones apache	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	A	Alta	Muy alto	Medio
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	Muy alta	Casi seguro	Fácil
[dmbs]		[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	A	Alta	Muy alto	Medio
	Sistema de gestión de	[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	Muy alta	Casi seguro	Fácil
[file]	base de Datos	[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	A	Alta	Muy alto	Medio
	Postgres	[E.20]	Vulnerabilidades de los programas (software)	Ausencia de escaneo y actualizaciones	MA	Muy alta	Casi seguro	Fácil
[os]	Sistema de backup	[E.24]	Caída del sistema por agotamiento de recursos	Saturación de los recursos tecnológicos	MA	Muy alta	Casi seguro	Fácil
		[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles	MA	Muy alta	Casi seguro	Fácil
	Servidor de archivos	[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	MA	Muy alta	Casi seguro	Fácil
		[A.7]	Uso no previsto	Ausencia de registro de eventos de control de accesos	MA	Muy alta	Casi seguro	Fácil
	Sistema Operativo	[A.10]	Alteración de secuencia	Ausencia de sincronización	MA	Muy alta	Casi seguro	Fácil
	Ubuntu server	[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Muy alta	Casi seguro	Fácil

[HW]Equipamiento informático		Amenaza		Vulnerabilidad	Degradación		Probabilidad	
		[A.15]	Modificación deliberada de la información	Ausencia de procedimientos de desvinculación de los empleados	MA	Muy alta	Casi seguro	Fácil
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Muy alta	Casi seguro	Fácil
		[A.24]	Denegación de servicio	Ausencia de control en las cuentas dadas de baja de recursos suficientes	MA	Muy alta	Casi seguro	Fácil
[email-cleinte]	Cliente de correo electrónico google	[E.9]	Errores de re encaminamiento	Configuraciones erróneas, Ausencia de monitoreo	MA	Muy alta	Casi seguro	Fácil
		[E.10]	Errores de secuencia	Ausencia de sincronización	MA	Muy alta	Casi seguro	Fácil
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	M	Media	Posible	Difícil
		[E.20]	Vulnerabilidades de los programas (software)	Ausencia de escaneo y actualizaciones	M	Media	Posible	Difícil
		[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles	M	Media	Posible	Difícil
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	A	Alta	Muy alto	Medio
		[A.7]	Uso no previsto	Ausencia de registro de eventos de acceso a servicios	A	Alta	Muy alto	Medio
		[A.9]	Re encaminamiento de mensajes	Ausencia de monitoreo	MA	Muy alta	Casi seguro	Fácil
		[A.10]	Alteración de secuencia	Ausencia de sincronización	MA	Muy alta	Casi seguro	Fácil
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	A	Alta	Muy alto	Medio
		[A.15]	Modificación deliberada de la información	Ausencia de procedimientos de desvinculación de los empleados	A	Alta	Muy alto	Medio
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Muy alta	Casi seguro	Fácil
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja de los usuarios	A	Alta	Muy alto	Medio
		[A.24]	Denegación de servicio	Ausencia de control en las cuentas dadas de baja de recursos suficientes	A	Alta	Muy alto	Medio
[HW] Equipos informáticos:								
[pc]	Informática personal	[I.1]	Fuego	Ausencia de capacitación sobre extintores	MB	Muy baja	Muy raro	Ext. difícil
		[I.3]	Contaminación mecánica	Ausencia de mantenimiento preventivo	MB	Muy baja	Muy raro	Ext. difícil
		[I.5]	Avería de origen físico o lógico	Fallo en los equipos informáticos	MB	Muy baja	Muy raro	Ext. difícil
[pc.backup]	Equipamiento de respaldo	[I.6]	Corte de suministro eléctrico	Ausencia de implementación de UPS	MB	Muy baja	Muy raro	Ext. difícil
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Ausencia de implementación del sistema de enfriamiento	MB	Muy baja	Muy raro	Ext. difícil
		[I.11]	Emanaciones electromagnéticas	Ausencia de monitoreo de señales externas	MB	Muy baja	Muy raro	Ext. difícil
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	A	Alta	Muy alto	Medio

[HW]Equipamiento informático		Amenaza		Vulnerabilidad	Degradación		Probabilidad	
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	MA	Muy alta	Casi seguro	Fácil
		[A.7]	Uso no previsto	Ausencia de registro de eventos de control de accesos	A	Alta	Muy alto	Medio
[COM] Redes de comunicaciones:								
[LAN]	Red local	[I.5]	Avería de origen físico o lógico	Fallo en los equipos informáticos	M	Media	Posible	Difícil
		[I.8]	Fallo de servicios de comunicaciones	Ausencia de registros de eventos del data center	M	Media	Posible	Difícil
[wifi]	Red inalámbrica	[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	A	Alta	Muy alto	Medio
		[E.9]	Errores de re encaminamiento	Configuraciones erróneas, Ausencia de monitoreo	MA	Muy alta	Casi seguro	Fácil
[Internet]	Internet	[E.10]	Errores de secuencia	Ausencia de sincronización	MA	Muy alta	Casi seguro	Fácil
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	A	Alta	Muy alto	Medio
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	A	Alta	Muy alto	Medio
		[A.7]	Uso no previsto	Ausencia de registro de eventos de control de accesos	A	Alta	Muy alto	Medio
[network] Soporte de la red								
[firewall]	Cortafuegos	[I.1]	Fuego	Ausencia de capacitación sobre extintores	A	Alta	Muy alto	Medio
		[I.3]	Contaminación mecánica	Ausencia de mantenimiento preventivo	A	Alta	Muy alto	Medio
[router]	Encaminadores	[I.5]	Avería de origen físico o lógico	Fallo en los equipos informáticos	A	Alta	Muy alto	Medio
		[I.6]	Corte de suministro eléctrico	Ausencia de implementación de UPS	A	Alta	Muy alto	Medio
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Ausencia de implementación del sistema de enfriamiento	A	Alta	Muy alto	Medio
		[I.8]	Fallo de servicios de comunic.	Ausencia de bitácoras de ingreso al data center	A	Alta	Muy alto	Medio
		[I.11]	Emanaciones electromagnéticas	Ausencia de monitoreo de señales externas	M	Media	Posible	Difícil
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	A	Alta	Muy alto	Medio
		[E.9]	Errores de re encaminamiento	Configuraciones erróneas, Ausencia de monitoreo	A	Alta	Muy alto	Medio
		[E.10]	Errores de secuencia	Ausencia de sincronización	MA	Muy alta	Casi seguro	Fácil
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	MA	Muy alta	Casi seguro	Fácil
[Media] Soportes de información:								
[disk]	Discos	[I.1]	Fuego	Ausencia de capacitación sobre extintores	A	Alta	Muy alto	Medio
		[I.3]	Contaminación mecánica	Ausencia de mantenimiento preventivo	A	Alta	Muy alto	Medio
	Discos	[I.5]	Avería de origen físico o lógico	Fallo en los equipos informáticos	A	Alta	Muy alto	Medio
[vdisk]	virtuales	[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	A	Alta	Muy alto	Medio
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	A	Alta	Muy alto	Medio

[HW]Equipamiento informático		Amenaza		Vulnerabilidad	Degradación		Probabilidad	
[san]	Almacenamiento en red	[A.7]	Uso no previsto	Ausencia de registro de eventos de control de accesos	A	Alta	Muy alto	Medio

Fuente: Elaborado por el autor, en referencia a la Metodología MAGERIT. Libro II "Catálogo de Elementos" (2012)

La matriz anterior refleja que las aplicaciones, sistema operativo y servidores, tienen una degradación muy alta con respecto a los dispositivos físicos, que tienen un perjuicio alto, medio y muy bajo; puesto que, la plataforma se aloja en un equipo virtual; por lo que, si el hosting virtual fuese atacado, la infraestructura física no se vería afectada.

[P] Personal

En el cuadro siguiente, se valoraron las amenazas sobre el personal relacionado con el uso y la administración de las aplicaciones, equipos de comunicaciones y desarrollo, tomado en cuenta las variables degradación y probabilidad de ocurrencia. Se usó la Tabla Nº 1 del Capítulo II referente al Marco Teórico.

Tabla 28

Valoración de las amenazas de acuerdo a la degradación relacionado con el personal que administra el Sistema Ignug

Activo: [P] Personal			Amenaza	Vulnerabilidad	Degradación		Probabilida	
[ue] Usuarios externos								
[ue]	Empresas formadoras	[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles, sin protección	M	Media	Posible	Difícil
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	M	Media	Posible	Difícil
[ui] Usuarios internos								
[uest]	Estudiantes	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	A	Alta	Muy alto	Medio
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	A	Alta	Muy alto	Medio

Activo: [P] Personal			Amenaza	Vulnerabilidad	Degradación		Probabilida	
[ud]	Docentes	[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles, sin protección	MA	Muy alta	Casi seguro	Fácil
[ua]	Autoridades	[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	MA	Muy alta	Casi seguro	Fácil
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Muy alta	Casi seguro	Fácil
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja de los usuarios	A	Alta	Muy alto	Medio
[adm] Administradores de sistemas; [dba] Administradores de base de datos: [com] administrador de comunicaciones								
[adm]	Admin. sistema Ignug	[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	Muy alta	Casi seguro	Fácil
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	A	Alta	Muy alto	Medio
[adma]	Apoyo de admin. Ignug	[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles, sin protección	MA	Muy alta	Casi seguro	Fácil
[adba]	Admin.BDD	[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	MA	Muy alta	Casi seguro	Fácil
[adbap]	Apoyo de admin.	[A.19]	Divulgación de información	Ausencia de acuerdos de confidencialidad	A	Alta	Muy alto	Medio
[adcom]	BDD Admin. data center							
[des] Equipo de desarrollo								
[desd]	desarrolladores docentes	[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	Muy alta	Casi seguro	Fácil
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	A	Alta	Muy alto	Medio
[dese]	desarrolladores estudiantes	[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles, sin protección	MA	Muy alta	Casi seguro	Fácil
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	MA	Muy alta	Casi seguro	Fácil
		[A.19]	Divulgación de información	Ausencia de acuerdos de confidencialidad	A	Alta	Muy alto	Medio
[prov] Proveedores								
[provi]	proveedores de internet	[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	A	Alta	Muy alto	Medio
		[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles, sin protección	MA	Muy alta	Casi seguro	Fácil
[provhv]	proveedores de hosting virtual	[E.19]	Fugas de información	Ausencia de acuerdos de confidencialidad	A	Alta	Muy alto	Medio
		[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles, sin protección	MA	Muy alta	Casi seguro	Fácil
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	MA	Muy alta	Casi seguro	Fácil
		[A.19]	Divulgación de información	Ausencia de acuerdos de confidencialidad	A	Alta	Muy alto	Medio

Fuente: Elaborado por el autor, en referencia a la Metodología MAGERIT. Libro II "Catálogo de Elementos" (2012)

Como se observa en la tabla anterior, la valoración de las amenazas sobre el personal que administra la plataforma, la base de datos y desarrolla los módulos del Sistema Ignug, es muy alta con respecto a los proveedores de internet y *hosting virtual* y a al personal que hace uso de los servicios.

Determinar el impacto potencial

Valoradas las amenazas, se calculó el impacto potencial que pueden sufrir la información y los servicios que brinda el Sistema de Gestión Académica Ignug, en el caso de ser atacados. Para determinar el impacto sobre los activos, se tomaron en cuenta las variables degradación y evaluación de los activos en referencia a la Tabla Nº 3 del Capítulo II referente al Marco Teórico. Los resultados del análisis, se los visualizan en las tablas de estimación del riesgo.

Identificación de los riesgos

Una vez establecido el impacto, se estimó el riesgo al que está expuesto el Sistema de Información Ignug, considerando el impacto y la probabilidad de ocurrencia de los activos en referencia a las escalas de la Tabla Nº 4 del Capítulo II del Marco Teórico.

En las siguientes matrices, se estima el riesgo con respecto a la valoración y degradación de los activos de la plataforma Ignug:

[esencial] Activos esenciales

Tabla 29

Evaluación del riesgo de los activos esenciales

[esencial] Activos esenciales		Amenaza		Vulnerabilidad	Valoración	Degradación	Impacto	Probabilidad	Evaluación Riesgo	Código
[D] Datos /[info] Información: [per] Datos personales										
[per]	Bases de datos con información personal, académica y socio-económica, de los estudiantes; certificado SIAU.	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	M	M	M	M	M	R1
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	MA	MA	MA	MA	R2
		[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	A	A	A	A	A	R3
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	A	MA	MA	MA	MA	R4
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	MA	MA	MA	MA	R5
		[A.6]	Abuso de privilegio de acceso	Ausencia de control de eventos *logs*	MA	MA	MA	MA	MA	R6
		[A.7]	Uso no previsto	Ausencia de registro de control en el acceso a los datos	A	A	A	A	A	R7
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	A	MA	MA	MA	MA	R8
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	A	MA	MA	MA	MA	R9
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	A	MA	MA	MA	MA	R10
		[A.19]	Divulgación de información	Ausencia de concienciación y control en las cuentas dadas de baja de los usuarios	A	A	A	A	A	R11
[clas] Datos clasificados: [C]		Nivel confidencial:								
[fich]	Archivos	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	MA	MA	MA	MA	MA	R12
		[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	MA	MA	MA	MA	MA	R13
[backup]	Copias de respaldo	[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	MA	MA	MA	MA	R14
[int]		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	A	MA	A	MA	R15
	Datos de gestión interna	[A.7]	Uso no previsto	Ausencia de registro de control en el acceso a los datos	MA	A	MA	A	MA	R16
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	MA	MA	MA	MA	R17
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	MA	MA	MA	MA	R18
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	MA	MA	MA	MA	R19

[esencial] esenciales	Activos	Amenaza		Vulnerabilidad	Valoración	Degradación	Impacto	Probabilidad	Evaluación Riesgo	Código
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja	MA	A	MA	A	MA	R20
[conf]	Datos de configuración del sistema	[E.4]	Errores de configuración	Ausencia de manuales de instalación y configuración	MA	MA	MA	MA	MA	R21
		[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	MA	MA	MA	MA	MA	R22
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	MA	MA	MA	MA	R23
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	MA	MA	MA	MA	R24
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	MA	MA	MA	MA	R25
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	MA	MA	MA	MA	R26
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	MA	MA	MA	MA	R27
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja	MA	MA	MA	MA	MA	R28
[paswd]	Credenciales: contraseñas	[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	MA	MA	MA	MA	MA	R29
[auth]	Datos de validación de credenciales	[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	MA	MA	MA	MA	R30
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	MA	MA	MA	MA	R31
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	MA	MA	MA	MA	R32
[acl]	Datos de control de acceso	[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	MA	MA	MA	MA	R33
[codf]	Código fuente	[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	MA	MA	MA	MA	R34
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja	MA	MA	MA	MA	MA	R35
[log]	Registro de actividad	[E.3]	Errores de monitorización (log)	Ausencia de implementación, seguimiento y lectura a logs	MA	A	MA	A	MA	R36
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	A	MA	A	MA	R37
		[A.3]	Manipulación de los registros de actividad (log)	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información	MA	MA	MA	MA	MA	R38
		[A.4]	Manipulación de la configuración	Falta de procedimiento formal para la supervisión del registro del SGSI	MA	MA	MA	MA	MA	R39
		[A.13]	Repudio	Ausencia de implementación de firmas digitales	MA	MA	MA	MA	MA	R40
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	MA	MA	MA	MA	R41
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	MA	MA	MA	MA	R42
[exe]	Código ejecutable	[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	MA	MA	MA	MA	R43
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	A	MA	A	MA	R44

[esencial] Activos esenciales		Amenaza		Vulnerabilidad	Valoración	Degradación	Impacto	Probabilidad	Evaluación Riesgo	Código
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	MA	MA	MA	MA	R45
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	MA	MA	MA	MA	R46
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja	MA	A	MA	A	MA	R47
[R] Difusión limitada:										
[R]	matrices de rendimiento académico, registros de notas, récords académicos, asistencia; datos de las empresas,	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	A	A	A	A	A	R48
		[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	A	A	A	A	A	R49
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	A	MA	MA	MA	MA	R50
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	A	A	A	A	A	R51
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	A	A	A	A	A	R52
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	A	MA	MA	MA	MA	R53
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	A	MA	MA	MA	MA	R54
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja	A	A	A	A	A	R55
[pub] De carácter público:										
[pub]	solicitudes de matrículas; datos académicos de docentes y autoridades; malla curricular	[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	B	A	M	A	A	R56
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	B	MA	MA	MA	MA	R57
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	B	MA	MA	MA	MA	R58
[serv] Servicios:										
[pub]	Público	[A.12]	Análisis de tráfico	Puerto abiertos innecesariamente	M	MB	B	M	M	R59
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	M	M	M	MA	MA	R60
[ext]	Usuarios externos: empresas formadoras	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	A	M	A	M	A	R61
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	A	A	A	A	A	R62
		[A.7]	Uso no previsto	Ausencia de registro de control en el acceso a los datos	A	A	A	A	A	R63
		[A.11]	Acceso no autorizado	Contraseñas inseguras	A	MA	MA	A	MA	R64
		[A.13]	Repudio	Ausencia de implementación de firmas digitales	A	MA	MA	MA	MA	R65
[int]	Usuarios Internos:	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	MA	M	MA	M	A	R66
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	A	MA	A	MA	R67

[esencial] Activos esenciales		Amenaza		Vulnerabilidad	Valoración	Degradación	Impacto	Probabilidad	Evaluación Riesgo	Código
	matriculación, gestión de	[A.5]	Suplantación de la identidad del usuario	Contraseñas predecibles o inseguras	MA	MA	MA	MA	MA	R68
	notas, registro	[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	MA	MA	MA	MA	R69
	docente, bolsa de empleo.	[A.13]	Repudio	Ausencia de implementación de firmas digitales	MA	MA	MA	MA	MA	R70
[email]	Correo electrónico	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	MA	M	MA	M	A	R71
		[E.9]	Errores de re encaminamiento	Configuraciones erróneas, Ausencia de monitoreo	MA	MA	MA	MA	MA	R72
		[E.10]	Errores de secuencia	Ausencia de sincronización	MA	MA	MA	MA	MA	R73
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	MA	MA	MA	MA	R74
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	A	MA	A	MA	R75
		[E.24]	Caída del sistema por agotamiento de recursos	Saturación de los recursos tecnológicos	MA	A	MA	A	MA	R76
		A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles	MA	MA	MA	MA	MA	R77
		[A.9]	Re encaminamiento de mensajes	Ausencia de monitoreo	MA	MA	MA	MA	MA	R78
		[A.10]	Alteración de secuencia	Ausencia de sincronización	MA	MA	MA	MA	MA	R79
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	MA	MA	MA	MA	R80
		[A.13]	Repudio	Ausencia de implementación de firmas digitales	MA	MA	MA	MA	MA	R81
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	MA	MA	MA	MA	R82
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	MA	MA	MA	MA	R83
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja de los usuarios	MA	MA	MA	MA	MA	R84
[file]	Almacenamiento de archivos	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	MA	A	MA	A	MA	R85
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	MA	MA	MA	MA	R86
		[E.10]	Errores de secuencia	Ausencia de sincronización	MA	MA	MA	MA	MA	R87
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	MA	MA	MA	MA	R88
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	A	MA	A	MA	R89
		[E.20]	Vulnerabilidades de los programas (software)	Ausencia de escaneo y actualizaciones	MA	MA	MA	MA	MA	R90
		[E.24]	Caída del sistema por agotamiento de recursos	Saturación de los recursos tecnológicos	MA	A	MA	A	MA	R91
		[A.7]	Uso no previsto	Ausencia de registro de control en el acceso a los datos	MA	MA	MA	MA	MA	R92

[esencial] Activos esenciales		Amenaza		Vulnerabilidad	Valoración	Degradación	Impacto	Probabilidad	Evaluación Riesgo	Código
		[A.9]	Re encaminamiento de mensajes	Ausencia de monitoreo	MA	MA	MA	MA	MA	R93
		[A.10]	Alteración de secuencia	Ausencia de sincronización	MA	MA	MA	MA	MA	R94
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	MA	MA	MA	MA	R95
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	MA	MA	MA	MA	R96
		[A.19]	Divulgación de información	Falta control en las cuentas dadas de baja de los usuarios	MA	MA	MA	MA	MA	R97
[ftp]	Transferencia de archivos	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	MA	A	MA	A	MA	R98
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	MA	MA	MA	MA	R99
		[E.9]	Errores de re encaminamiento	Configuraciones erróneas, Ausencia de monitoreo	MA	MA	MA	MA	MA	R100
		[E.10]	Errores de secuencia	Ausencia de sincronización	MA	MA	MA	MA	MA	R101
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	MA	MA	MA	MA	R102
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	A	MA	A	MA	R103
		[E.20]	Vulnerabilidades de los programas	Ausencia de escaneo y actualizaciones	MA	MA	MA	MA	MA	R104
		[E.24]	Caída del sistema por agotamiento de recursos	Saturación de los recursos tecnológicos	MA	A	MA	A	MA	R105
		[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles	MA	MA	MA	MA	MA	R106
		[A.9]	Re encaminamiento de mensajes	Ausencia de monitoreo	MA	MA	MA	MA	MA	R107
		[A.10]	Alteración de secuencia	Ausencia de sincronización	MA	MA	MA	MA	MA	R108
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	MA	MA	MA	MA	R109
		[A.13]	Repudio	Ausencia de implementación de firmas digitales	MA	MA	MA	MA	MA	R110
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	MA	MA	MA	MA	R111
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	MA	MA	MA	MA	R112
[edi]	Intercambio electrónico de datos	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	MA	A	MA	A	MA	R113
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	MA	MA	MA	MA	R114
		[E.9]	Errores de re encaminamiento	Configuraciones erróneas, Ausencia de monitoreo	MA	MA	MA	MA	MA	R115
		[E.10]	Errores de secuencia	Ausencia de sincronización	MA	MA	MA	MA	MA	R116
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	MA	MA	MA	MA	R117
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	A	MA	A	MA	R118
		[E.20]	Vulnerabilidades de los programas	Ausencia de escaneo y actualizaciones	MA	MA	MA	MA	MA	R119
		[E.24]	Caída del sistema por agotamiento de recursos	Saturación de los recursos tecnológicos	MA	A	MA	A	MA	R120

[esencial] Activos esenciales		Amenaza		Vulnerabilidad	Valoración	Degradación	Impacto	Probabilidad	Evaluación Riesgo	Código
		[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles	MA	MA	MA	MA	MA	R121
		[A.9]	Re encaminamiento de mensajes	Ausencia de monitoreo	MA	MA	MA	MA	MA	R122
		[A.10]	Alteración de secuencia	Ausencia de sincronización	MA	MA	MA	MA	MA	R123
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	MA	MA	MA	MA	R124
		[A.13]	Repudio	Ausencia de implementación de firmas digitales	MA	MA	MA	MA	MA	R125
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	MA	MA	MA	MA	R126
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja	MA	MA	MA	MA	MA	R127
[gesu]	Gestión usuarios	[E.2]	Errores del administrador	Ausencia de concienciación y control en las cuentas dadas de baja de los usuarios	MA	MA	MA	MA	MA	R128
[idm]	Gestión identidades	[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles	MA	MA	MA	MA	MA	R129
[ipm]	Gestión privilegios	[A.11]	Acceso no autorizado	Contraseñas inseguras	MA	MA	MA	MA	MA	R130
[S.sub] Subcontratados a terceros										
[vhost]	Hosting virtual Contabo	[I.5]	Avería de origen físico o lógico	Fallo en los equipos informáticos	MA	MA	MA	MA	MA	R131
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	MA	MA	MA	MA	R132
[Internet]		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	MA	MA	MA	MA	R133
	Internet	[A.6]	Abuso de privilegio de acceso	Ausencia de control de eventos *logs*	MA	MA	MA	MA	MA	R134

Fuente: Elaborado por el autor, en referencia a la Metodología MAGERIT. Libro III "Guía de Técnicas" (2012)

[HW] Equipamiento informático

Tabla 30

Evaluación del riesgo del equipamiento informático

[HW] Equipamiento informático		Amenaza		Vulnerabilidad	Valoración	Degradación	Impacto	Probabilidad	Evaluación Riesgo	Código
[SW] Aplicaciones: [prp] Desarrollo propio										
[sgai]	Sistema de gestión	[I.5]	Avería de origen físico o lógico	Fallo en las configuraciones de los equipos informáticos	MA	MA	MA	MA	MA	R135

[HW] Equipamiento informático		Amenaza		Vulnerabilidad	Valoración	Degradación	Impacto	Probabilidad	Evaluación Riesgo	Código
	académica	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	MA	A	MA	A	MA	R136
	Ignug	[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	MA	MA	MA	MA	R137
		[E.10]	Errores de secuencia	Ausencia de sincronización	MA	MA	MA	MA	MA	R138
[bddi]	Base de datos "ignug_bdd"	[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	MA	MA	MA	MA	MA	R139
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	MA	MA	MA	MA	R140
[backup]	Sistema de backup	[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	MA	MA	MA	MA	R141
		[E.20]	Vulnerabilidades de los programas (software)	Ausencia de escaneo y actualizaciones	MA	MA	MA	MA	MA	R142
		[E.24]	Caída del sistema por agotamiento de recursos	Saturación de recursos tecnológicos	MA	A	MA	A	MA	R143
		[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles	MA	MA	MA	MA	MA	R144
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	MA	MA	MA	MA	MA	R145
		[A.9]	Re encaminamiento de mensajes	Ausencia de monitoreo	MA	MA	MA	MA	MA	R146
		[A.10]	Alteración de secuencia	Ausencia de sincronización	MA	MA	MA	MA	MA	R147
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	MA	MA	MA	MA	R148
		[A.15]	Modificación deliberada de la información	Ausencia de procedimientos de desvinculación de los empleados	MA	MA	MA	MA	MA	R149
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	MA	MA	MA	MA	R150
		[A.19]	Divulgación de información	Falta control en las cuentas dadas de baja de los usuarios	MA	A	MA	A	MA	R151
		[A.24]	Denegación de servicio	Ausencia de control en las cuentas dadas de baja de recursos suficientes	MA	A	MA	A	MA	R152
[app]	Servidor de aplicaciones	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	MA	A	MA	A	MA	R153
	apache	[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	MA	**MA**	MA	**MA**	R154
[dmbs]		[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	MA	A	MA	A	MA	R155
	Sistema de gestión de base	[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	MA	MA	MA	MA	R156
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	A	MA	A	MA	R157
[file]	de Datos Postgres	[E.20]	Vulnerabilidades de los programas (software)	Ausencia de escaneo y actualizaciones	MA	MA	MA	MA	MA	R158
		[E.24]	Caída del sistema por agotamiento de recursos	Saturación de los recursos tecnológicos	MA	MA	MA	MA	MA	R159
[os]										

[HW] Equipamiento informático		Amenaza		Vulnerabilidad	Valoración	Degradación	Impacto	Probabilidad	Evaluación Riesgo	Código
	Servidor de archivos	[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles	MA	MA	MA	MA	MA	R160
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	MA	MA	MA	MA	MA	R161
	Sistema	[A.7]	Uso no previsto	Ausencia de registro de eventos de control de accesos	MA	MA	MA	MA	MA	R162
	Operativo	[A.10]	Alteración de secuencia	Ausencia de sincronización	MA	MA	MA	MA	MA	R163
	Ubuntu server	[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	MA	MA	MA	MA	R164
		[A.15]	Modificación deliberada de la información	Ausencia de procedimientos de desvinculación de los empleados	MA	MA	MA	MA	MA	R165
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	MA	MA	MA	MA	R166
		[A.24]	Denegación de servicio	Ausencia de control en las cuentas dadas de baja de recursos suficientes	MA	MA	MA	MA	MA	R167
[email-cleinte]	Cliente de correo electrónico google	[E.9]	Errores de re encaminamiento	Configuraciones erróneas, Ausencia de monitoreo	MA	MA	MA	MA	MA	R168
		[E.10]	Errores de secuencia	Ausencia de sincronización	MA	MA	MA	MA	MA	R169
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	M	**A**	M	**A**	R170
		[E.20]	Vulnerabilidades de los programas (software)	Ausencia de escaneo y actualizaciones	MA	M	A	M	A	R171
		[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles	MA	M	**A**	M	**A**	R172
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	MA	A	MA	A	MA	R173
		[A.7]	Uso no previsto	Ausencia de registro de eventos de acceso a servicios	MA	A	MA	A	MA	R174
		[A.9]	Re encaminamiento de mensajes	Ausencia de monitoreo	MA	MA	MA	MA	MA	R175
		[A.10]	Alteración de secuencia	Ausencia de sincronización	MA	MA	MA	MA	MA	R176
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	A	MA	A	MA	R177
		[A.15]	Modificación deliberada de la información	Ausencia de procedimientos de desvinculación de los empleados	MA	A	MA	A	MA	R178
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	MA	MA	MA	MA	R179
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja de los usuarios	MA	A	MA	A	MA	R180
		[A.24]	Denegación de servicio	Ausencia de control en las cuentas dadas de baja de recursos suficientes	MA	A	MA	A	MA	R181
[HW] Equipos informáticos:										
[pc]	Informática personal	[I.1]	Fuego	Ausencia de capacitación sobre extintores	**M**	MB	**B**	MB	**B**	R182
		[I.3]	Contaminación mecánica	Ausencia de mantenimiento preventivo	**M**	MB	**B**	MB	**B**	R183

[HW] Equipamiento informático		Amenaza		Vulnerabilidad	Valoración	Degradación	Impacto	Probabilidad	Evaluación Riesgo	Código
		[I.5]	Avería de origen físico o lógico	Fallo en los equipos informáticos	**M**	MB	**B**	MB	**B**	R184
[pc.backup]	Equipamiento de respaldo	[I.6]	Corte de suministro eléctrico	Ausencia de implementación de UPS	**M**	MB	**B**	MB	**B**	R185
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Ausencia de implementación del sistema de enfriamiento	**M**	MB	**B**	MB	**B**	R186
		[I.11]	Emanaciones electromagnéticas	Ausencia de monitoreo de señales externas	**M**	MB	**B**	MB	**B**	R187
[backup]	Equipamiento de respaldo virtual	[I.5]	Avería de origen físico o lógico	Fallo en los equipos informáticos	MA	A	**MA**	A	**MA**	R188
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	MA	**MA**	MA	**MA**	R189
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	A	**MA**	A	**MA**	R190
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	MA	MA	**MA**	MA	**MA**	R191
		[A.7]	Uso no previsto	Ausencia de registro de eventos de control de accesos	MA	A	**MA**	A	**MA**	R192
[COM] Redes de comunicaciones:										
[LAN]	Red local	[I.5]	Avería de origen físico o lógico	Fallo en los equipos informáticos	A	M	**A**	M	**A**	R193
		[I.8]	Fallo de servicios de comunicaciones	Ausencia de bitácoras de ingreso al data center	A	M	**A**	M	**A**	R194
[wifi]	Red inalámbrica	[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	A	A	**A**	A	**A**	R195
		[E.9]	Errores de re encaminamiento	Configuraciones erróneas, Ausencia de monitoreo	A	MA	MA	MA	**MA**	R196
	Internet	[E.10]	Errores de secuencia	Ausencia de sincronización	A	MA	MA	MA	**MA**	R197
[Internet]		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	A	A	**A**	A	**A**	R198
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	**A**	A	**A**	A	**A**	R199
		[A.7]	Uso no previsto	Ausencia de registro de eventos de control de accesos	**A**	A	**A**	A	**A**	R200
[**network] Soporte de la red**										
[firewall]	Cortafuegos	[I.1]	Fuego	Ausencia de capacitación sobre extintores	A	A	**A**	A	**A**	R201
		[I.3]	Contaminación mecánica	Ausencia de mantenimiento preventivo	A	A	**A**	A	**A**	R202
[router]	encaminadores	[I.5]	Avería de origen físico o lógico	Fallo en los equipos informáticos	A	A	**A**	A	**A**	R203
		[I.6]	Corte de suministro eléctrico	Ausencia de implementación de UPS	A	A	**A**	A	**A**	R204
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Ausencia de implementación del sistema de enfriamiento	A	A	**A**	A	**A**	R205
		[I.8]	Fallo de servicios de comunicaciones	Ausencia de bitácoras de ingreso al data center	A	A	**A**	A	**A**	R206
		[I.11]	Emanaciones electromagnéticas	Ausencia de monitoreo de señales externas	A	M	**A**	M	**A**	R207
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	A	A	**A**	A	**A**	R208
		[E.9]	Errores de re encaminamiento	Configuraciones erróneas, Ausencia de monitoreo	A	A	**A**	A	**A**	R209
		[E.10]	Errores de secuencia	Ausencia de sincronización	A	MA	MA	MA	**MA**	R210
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	**A**	MA	MA	MA	**MA**	R211

[HW] Equipamiento informático		Amenaza		Vulnerabilidad	Valoración	Degradación	Impacto	Probabilidad	Evaluación Riesgo	Evaluación Código
[Media] Soportes de información:										
[disk]	Discos	[I.1]	Fuego	Ausencia de capacitación sobre extintores	A	A	A	A	**A**	R212
		[I.3]	Contaminación mecánica	Ausencia de mantenimiento preventivo	A	A	A	A	**A**	R213
[vdisk]	Discos virtuales	[I.5]	Avería de origen físico o lógico	Fallo en los equipos informáticos	**A**	A	A	A	**A**	R214
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	**A**	A	A	A	**A**	R215
[san]	Almacenamiento en red	[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	**A**	A	A	A	**A**	R216
		[A.7]	Uso no previsto	Ausencia de registro de eventos de control de accesos	**A**	A	A	A	**A**	R217

Fuente: Elaborado por el autor, en referencia a la Metodología MAGERIT. Libro III "Guía de Técnicas" (2012)

Activo: [P] Personal

Tabla 31

Evaluación del riesgo del personal relacionando con el sistema Ignug

Activo: [P] Personal		Amenaza		Vulnerabilidad	Valoración	Degradación	Impacto	Probabilidad	Evaluación Riesgo	Evaluación Código
[ue] Usuarios externos										
[ue]	Empresas formadoras	[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles, sin protección	**M**	**M**	A	**M**	A	R218
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	**A**	**M**	A	**M**	A	R219
[ui] Usuarios internos										
[uest]	Estudiantes	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	**A**	A	A	A	A	R221
[ud]	Docentes	[E.19]	Fugas de información	Ausencia de controles en la asignación de perfiles de usuario	**A**	A	A	A	A	R222
[ua]	Autoridades	[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles, sin protección	**A**	MA	MA	MA	MA	R223
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	**A**	MA	MA	MA	MA	R224
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	**A**	MA	MA	MA	MA	R225

Activo: [P] Personal		Amenaza		Vulnerabilidad	Valoración	Degradación	Impacto	Probabilidad	Evaluación	
									Riesgo	Código
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja de los usuarios	**A**	A	A	A	A	R226
[adm] Administradores de sistemas; [dba] Administradores de base de datos: [com] administrador de comunicaciones										
[adm]	Admin. sistema Ignug	[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	MA	MA	MA	MA	R227
[adma]	Apoyo de admin. Ignug	[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	A	MA	A	MA	R228
[adba]	Admin.bdd	[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles, sin protección	MA	MA	MA	MA	MA	R229
[adbap]	Apoyo bdd	[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	MA	MA	MA	MA	MA	R230
[adcom]	Admin. data center	[A.19]	Divulgación de información	Ausencia de acuerdos de confidencialidad	MA	A	MA	A	**MA**	R231
[des] Equipo de desarrollo										
[desd]	desarrolladores	[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	**A**	MA	MA	MA	MA	R232
	docentes	[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	**A**	**A**	**A**	MA	MA	R233
[dese]	desarrolladores estudiantes	[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles, sin protección	**A**	MA	MA	MA	MA	R234
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	**A**	MA	MA	MA	MA	R235
		[A.19]	Divulgación de información	Ausencia de acuerdos de confidencialidad	**A**	A	**A**	A	**A**	R236
[prov] Proveedores										
[provi]	proveedores de internet	[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	**A**	A	**A**	A	**A**	R237
		[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles sin protección	**A**	MA	MA	MA	MA	R238
[provhv]	proveedores de hosting virtual	[E.19]	Fugas de información	Ausencia de acuerdos de confidencialidad	MA	A	MA	A	MA	R239
		[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles, sin protección	MA	MA	MA	MA	MA	R240
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	MA	MA	MA	MA	MA	R241
		[A.19]	Divulgación de información	Ausencia de acuerdos de confidencialidad	MA	A	MA	A	MA	R242

Fuente: Elaborado por el autor, en referencia a la Metodología MAGERIT. Libro III "Guía de Técnicas" (2012)

Tabla 32

Mapa de calor

Riesgo		Probabilidad				
		Muy Baja	Baja	Media	Alta	Muy Alta
Impacto	MA			R66, R71,	R15, R16, R20, R36, R37, R44, R47, R64, R67, R75, R76, R85, R89, R91, R98, R103, R105, R113, R118, R120, R136, R143, R151, R152, R153, R157, R157, R173, R174, R177, R178, R180, R181, R188, R190, R192, R228, R231, R239, R242	R2,R4, R5, R6, R8, R9, R10, R12, R13, R14, R17,R18, R19, R21, R22, R23, R24, R25,R26, R27, R28, R29, R30, R31, R32, R33, R34, R35, R38, R39, R40, R41, R42, R43, R45, R46, R50, R53, R54, R57, R58, R65, R68, R69, R70, R72, R73, R74, R77, R78, R79, R80, R81, R82, R83, R84, R86, R87, R88, R90, R92, R93, R94, R95, R96, R97, R99, R100, R101,R102, R104, R106, R107, R108, R109, R110, R111, R112, R114, R115, R116, R117, R119, R121, R122, R123, R124, R125, R126, R127, R128, R129, R130, R131, R132, R133, R134, R135, R137, R138, R139, R140, R141,R142, R144, R145, R146, R147, R148, R149, R150, R154, R156, R158, R159, R160, R161, R162, R163, R164, R165, R166, R167, R168, R169, R175, R176, 179, R189, R191, R196, R197, R210, R211, R223, R224, R225, R227, R229, R230, R232, R234, R235, R238, R240, R241
	A			R61, R170, R171, R172, R193, R194, R207, R218, R219	R3,R7, R11, R48, R49, R51, 52, R55, R62, R63, R195, R198, R199, R200, R201, R202, R203, R204, R205, R206, R208, R209, R212, R213,R214, R215, R216, R217, R221, R222, R226, R236, R237	R228
	M			R1,	R56	R60
	B	R182,R183, R184,R185, R186,R187		R59		
	MB					

Fuente: Elaborado por el autor, en referencia a la Metodología MAGERIT. Libro III "Guía de Técnicas" (2012)

En el Libro I, Método de Magerit (2012) muestra la imagen, en la cual se visualizan las zonas del riesgo en el que se encuentran los activos, tomando en cuenta que el riesgo crece a medida que el impacto y la probabilidad crecen.

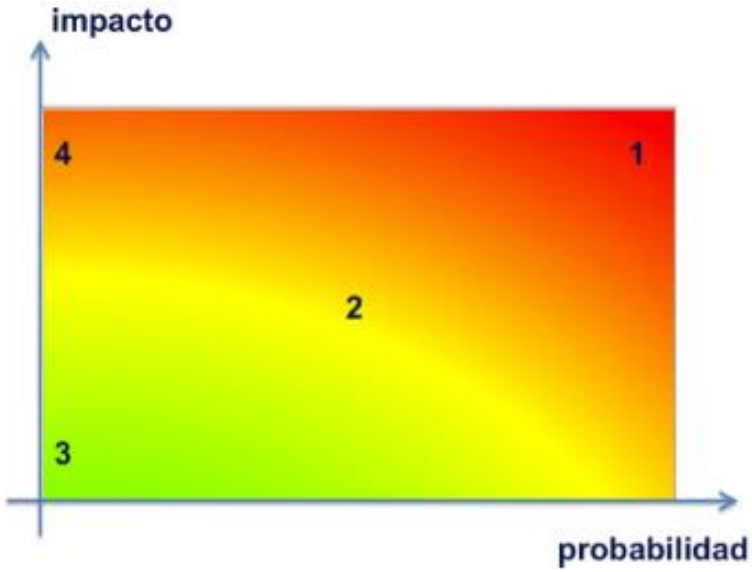

Figura 11: Zonas de riesgo
Fuente: Metodología de MAGERIT, Libro I –Método- v 3.0 (2012)

zona 1: riesgos muy probables y de muy alto impacto

zona 2: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables, pero de impacto bajo o muy bajo

zona 3: riesgos improbables y de bajo impacto

zona 4: riesgos improbables, pero de muy alto impacto

De acuerdo al mapa de calor resultante del análisis del riesgo de los activos de información y servicio del Sistema de Gestión Académica Ignug, se identifica lo siguiente:

Zona 1: los activos de muy alto impacto y riesgos muy probables, corresponden al conjunto más grande, los servicios, aplicaciones, sistemas y servidores de aplicaciones y de bases de datos y el personal; se encuentran dentro de la región de color rojo, por lo tanto, deben recibir una atención inmediata.

Zona 2: los usuarios pueden cometer errores involuntarios con respeto a los datos personales, cubren la zona de eventos muy probables de impacto bajo, lo cual amerita una atención a mediano plazo.

Zona 3: El perjuicio que pueden sufrir los equipos personales y de respaldo, debido a, contagio mecánico, deterior físico o lógico, falla de suministro eléctrico, ambiente con temperatura o humedad inadecuados, emanaciones electromagnéticas, son de bajo impacto por lo que el riesgo es bajo e improbable que ocurran, se los puede tratar a largo plazo.

Zona 4: los usuarios de las empresas formadoras pueden cometer errores involuntarios sobre los servicios que usan; el cliente de correo electrónico google, sufrir suplantación de identidades y ser vulnerable a fugas de información; por lo que el riesgo es improbable, pero de muy alto impacto, se debe dar una solución a corto plazo.

4.5 Determinación de salvaguardas

Se definieron las salvaguardas que permitirán enfrentar a las amenazas si llegaran a materializarse; se las calificó de acuerdo a la eficacia frente a los posibles peligros a mitigar en el Sistema de Gestión Académica Ignug.

Selección de las salvaguardas

Una vez definidas las salvaguardas, se las identificó de acuerdo al activo a proteger, con la finalidad de minimizar el riesgo y la degradación que pueden sufrir los elementos activos de información y servicios que provee el Sistema de Gestión Académica Ignug.

[esencial] Activos esenciales

Tabla 33

Selección de salvaguardas de los activos esenciales del Sistema Ignug

[esencial] Activos esenciales		Amenaza		Vulnerabilidad	Riesgo	Controles ISO/27002:2017	
[D] Datos /[info] Información:							
[per] Datos personales							
[per]	Bases de datos con información personal, académica y socio-económica, de los estudiantes; certificado SIAU.	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	M	Art. 47	Documentación de procedimientos de operación
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	Art. 47	Documentación de procedimientos de operación
		[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	A	Art. 30	Gestión de privilegios de acceso
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	Art. 30	Gestión de privilegios de acceso
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	Art. 67	Acuerdos de confidencialidad o no revelación
		[A.6]	Abuso de privilegio de acceso	Ausencia de control de eventos *logs*	MA	Art. 30	Gestión de privilegios de acceso
		[A.7]	Uso no previsto	Ausencia de registro de control en el acceso a los datos	A	Art. 30	Gestión de privilegios de acceso
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Art. 30	Gestión de privilegios de acceso
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	Art.32	Retirada o reasignación de los derechos de acceso
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Art.32	Retirada o reasignación de los derechos de acceso
		[A.19]	Divulgación de información	Falta de implementación del certificado SSL	A	Art.32	Retirada o reasignación de los derechos de acceso
[clas] Datos clasificados:							
[C] Nivel confidencial:							
[fich]	Archivos	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	MA	Art. 47	Documentación de procedimientos de operación
[backup]	Copias de respaldo	[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	MA	Art. 30	Gestión de privilegios de acceso

[esencial] Activos esenciales		Amenaza		Vulnerabilidad	Riesgo	Controles ISO/27002:2017	
[int]		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	Art. 30	Gestión de privilegios de acceso
	Datos de gestión interna	[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	Art. 67	Acuerdos de confidencialidad o no revelación
		[A.7]	Uso no previsto	Ausencia de registro de control en el acceso a los datos	MA	Art. 30	Gestión de privilegios de acceso
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Art. 30	Gestión de privilegios de acceso
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	Art.32	Retirada o reasignación de los derechos de acceso
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Art.32	Retirada o reasignación de los derechos de acceso
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja	MA	Art.32	Retirada o reasignación de los derechos de acceso
[conf]	Datos de configuración del sistema	[E.4]	Errores de configuración	Ausencia de manuales de instalación y configuración	MA	Art. 47	Documentación de procedimientos de operación
		[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	MA	Art. 30	Gestión de privilegios de acceso
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	Art. 30	Gestión de privilegios de acceso
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	Art. 67	Acuerdos de confidencialidad o no revelación
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Art. 30	Gestión de privilegios de acceso
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	Art.32	Retirada o reasignación de los derechos de acceso
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Art.32	Retirada o reasignación de los derechos de acceso
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja	MA	Art.32	Retirada o reasignación de los derechos de acceso
[paswd]	Credenciales: contraseñas	[E.15]	Alteración accidental de la información	Falta de implementación del certificado SSL	MA	Art. 30	Gestión de privilegios de acceso
[auth]	Datos de validación de credenciales	[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	Art. 30	Gestión de privilegios de acceso
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	Art. 67	Acuerdos de confidencialidad o no revelación
[acl]	Datos de control de acceso	[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Art. 30	Gestión de privilegios de acceso
[codf]		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	Art.32	Retirada o reasignación de los derechos de acceso

[esencial] Activos esenciales		Amenaza		Vulnerabilidad	Riesgo	Controles ISO/27002:2017	
	Código fuente	[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Art.32	Retirada o reasignación de los derechos de acceso
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja	MA	Art.32	Retirada o reasignación de los derechos de acceso
[log]	Registro de actividad	[E.3]	Errores de monitorización (log)	Ausencia de implementación, seguimiento y lectura a los *logs*	MA	Art. 63	Registro de eventos
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	Art. 67	Acuerdos de confidencialidad o no revelación
		[A.3]	Manipulación de los registros de actividad (log)	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información	MA	Art. 62	Seguridad de los servicios de red
		[A.4]	Manipulación de la configuración	Falta de procedimiento formal para la supervisión del registro del SGSI	MA	Art. 48	Gestión de cambios
		[A.13]	Repudio	Ausencia de implementación de firmas digitales	MA	Art. 53	Registro de eventos
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	Art.32	Retirada o reasignación de los derechos de acceso
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Art.32	Retirada o reasignación de los derechos de acceso
[exe]	Código ejecutable	[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	Art. 30	Gestión de privilegios de acceso
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	Art. 67	Acuerdos de confidencialidad o no revelación
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Art. 30	Gestión de privilegios de acceso
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Art.32	Retirada o reasignación de los derechos de acceso
		[A.19]	Divulgación de información	Falta de implementación del certificado SSL	MA	Art.32	Retirada o reasignación de los derechos de acceso
[R] Difusión limitada:							
[R]	matrices de rendimiento académico, registros de notas, récords académicos, asistencia;	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	A	Art. 47	Documentación de procedimientos de operación
		[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	A	Art. 30	Gestión de privilegios de acceso
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	**MA**	Art. 30	Gestión de privilegios de acceso
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	**A**	Art. 67	Acuerdos de confidencialidad o no revelación
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	**A**	Art. 30	Gestión de privilegios de acceso

[esencial] Activos esenciales		Amenaza		Vulnerabilidad	Riesgo	Controles ISO/27002:2017	
	datos de las empresas,	[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	**MA**	Art.32	Retirada o reasignación de los derechos de acceso
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	**MA**	Art.32	Retirada o reasignación de los derechos de acceso
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja	**A**	Art.32	Retirada o reasignación de los derechos de acceso
[pub] De carácter público:							
[pub]	solicitudes de matrículas;	[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	**A**	Art. 30	Gestión de privilegios de acceso
	datos académicos	[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	**MA**	Art.32	Retirada o reasignación de los derechos de acceso
	docentes y autoridades; malla curricular	[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	**MA**	Art.32	Retirada o reasignación de los derechos de acceso
[**serv] Servicios:**							
[pub]	Público	[A.12]	Análisis de tráfico	Puerto abiertos innecesariamente	**M**	Art. 61	Controles de red
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	**MA**	Art.32	Retirada o reasignación de los derechos de acceso
[ext]	Usuarios externos:	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	**A**	Art. 47	Documentación de procedimientos de operación
	empresas formadoras	[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	**A**	Art. 67	Acuerdos de confidencialidad o no revelación
		[A.7]	Uso no previsto	Ausencia de registro de control en el acceso a los datos	**A**	Art. 30	Gestión de privilegios de acceso
		[A.11]	Acceso no autorizado	Contraseñas inseguras	**MA**	Art. 30	Gestión de privilegios de acceso
		[A.13]	Repudio	Ausencia de implementación de firmas digitales	**MA**	Art. 53	Registro de eventos
[int]	Usuarios Internos:	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	**A**	Art. 47	Documentación de procedimientos de operación
	matriculación, gestión de	[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	**MA**	Art. 67	Acuerdos de confidencialidad o no revelación
	notas, registro docente, bolsa	[A.5]	Suplantación de la identidad del usuario	Contraseñas predecibles o inseguras	**MA**	Art. 26	“Política de Control de Acceso”
	de empleo.	[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	**MA**	Art. 30	Gestión de privilegios de acceso

[esencial] Activos esenciales		Amenaza		Vulnerabilidad	Riesgo	Controles ISO/27002:2017	
		[A.13]	Repudio	Ausencia de implementación de firmas digitales	**MA**	Art. 53	Registro de eventos
[email]	Correo electrónico	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	**A**	Art. 47	Documentación de procedimientos de operación
		[E.9]	Errores de re encaminamiento	Configuraciones erróneas, Ausencia de monitoreo	**MA**	Art. 64	Políticas y procedimientos de intercambio de información
		[E.10]	Errores de secuencia	Ausencia de sincronización	**MA**		
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	**MA**	Art. 30	Gestión de privilegios de acceso
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	**MA**	Art. 67	Acuerdos de confidencialidad o no revelación
		[E.24]	Caída del sistema por agotamiento de recursos	Saturación de los recursos tecnológicos	**MA**	Art. 92	Disponibilidad de los recursos de tratamiento de la información
		[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles	**MA**	Art. 26	"Política de Control de Acceso"
		[A.9]	Re encaminamiento de mensajes	Ausencia de monitoreo	**MA**	Art. 64	Políticas y procedimientos de intercambio de información
		[A.10]	Alteración de secuencia	Ausencia de sincronización	**MA**	Art. 64	Políticas y procedimientos de intercambio de información
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	**MA**	Art. 30	Gestión de privilegios de acceso
		[A.13]	Repudio	Ausencia de implementación de firmas digitales	**MA**	Art. 53	Registro de eventos
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	**MA**	Art.32	Retirada o reasignación de los derechos de acceso
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	**MA**	Art.32	Retirada o reasignación de los derechos de acceso
		[A.19]	Divulgación de información	Falta de implementación del certificado SSL	**MA**	Art.32	Retirada o reasignación de los derechos de acceso
[file]	Almacenamiento de archivos	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	**MA**	Art. 47	Documentación de procedimientos de operación
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	**MA**	Art. 47	Documentación de procedimientos de operación
		[E.10]	Errores de secuencia	Ausencia de sincronización	**MA**		
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	**MA**	Art. 30	Gestión de privilegios de acceso
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	**MA**	Art. 67	Acuerdos de confidencialidad o no revelación

[esencial] Activos esenciales		Amenaza		Vulnerabilidad	Riesgo	Controles ISO/27002:2017	
		[E.20]	Vulnerabilidades de los programas (software)	Ausencia de escaneo y actualizaciones	MA	Art. 58	Gestión de las vulnerabilidades técnicas
		[E.24]	Caída del sistema por agotamiento de recursos	Saturación de los recursos tecnológicos	MA	Art. 92	Disponibilidad de los recursos de tratamiento de la información
		[A.7]	Uso no previsto	Ausencia de registro de control en el acceso a los datos	MA	Art. 30	Gestión de privilegios de acceso
		[A.9]	Re encaminamiento de mensajes	Ausencia de monitoreo	MA	Art. 64	Políticas y procedimientos de intercambio de información
		[A.10]	Alteración de secuencia	Ausencia de sincronización	MA	Art. 64	Políticas y procedimientos de intercambio de información
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	Art.32	Retirada o reasignación de los derechos de acceso
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Art.32	Retirada o reasignación de los derechos de acceso
		[A.19]	Divulgación de información	Falta de implementación del certificado SSL	MA	Art.32	Retirada o reasignación de los derechos de acceso
[ftp]	Transferencia de archivos	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	MA	Art. 47	Documentación de procedimientos de operación
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	Art. 47	Documentación de procedimientos de operación
		[E.9]	Errores de re encaminamiento	Configuraciones erróneas, Ausencia de monitoreo	MA	Art. 64	Políticas y procedimientos de intercambio de información
		[E.10]	Errores de secuencia	Ausencia de sincronización	MA		
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	Art. 30	Gestión de privilegios de acceso
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	Art. 67	Acuerdos de confidencialidad o no revelación
		[E.20]	Vulnerabilidades de los programas (software)	Ausencia de escaneo y actualizaciones	MA	Art. 51	Controles contra el código malicioso
		[E.24]	Caída del sistema por agotamiento de recursos	Saturación de los recursos tecnológicos	MA	Art. 92	Disponibilidad de los recursos de tratamiento de la información
		[A.5]	Suplantación de la identidad del usuario	ñas débiles o predecibles	MA	Art. 26	“Política de Control de Acceso”
		[A.9]	Re encaminamiento de mensajes	Ausencia de monitoreo	MA	Art. 64	Políticas y procedimientos de intercambio de información

[esencial] Activos esenciales		Amenaza		Vulnerabilidad	Riesgo	Controles ISO/27002:2017	
		[A.10]	Alteración de secuencia	Ausencia de sincronización	MA	Art. 64	Políticas y procedimientos de intercambio de información
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Art. 30	Gestión de privilegios de acceso
		[A.13]	Repudio	Ausencia de implementación de firmas digitales	MA	Art. 53	Registro de eventos
		[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	MA	Art.32	Retirada o reasignación de los derechos de acceso
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Art.32	Retirada o reasignación de los derechos de acceso
[edi]	Intercambio electrónico de datos	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	MA	Art. 47	Documentación de procedimientos de operación
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	Art. 47	Documentación de procedimientos de operación
		[E.9]	Errores de re encaminamiento	Configuraciones erróneas, Ausencia de monitoreo	MA	Art. 64	Políticas y procedimientos de intercambio de información
		[E.10]	Errores de secuencia	Ausencia de sincronización	MA	Art. 64	Políticas y procedimientos de intercambio de información
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	Art. 30	Gestión de privilegios de acceso
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	Art. 67	Acuerdos de confidencialidad o no revelación
		[E.20]	Vulnerabilidades de los programas (software)	Ausencia de escaneo y actualizaciones	MA	Art. 58	Gestión de las vulnerabilidades técnicas
		[E.24]	Caída del sistema por agotamiento de recursos	Saturación de los recursos tecnológicos	MA	Art. 92	Disponibilidad de los recursos de tratamiento de la información
		[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles	MA	Art. 26	“Política de Control de Acceso”
		[A.9]	Re encaminamiento de mensajes	Ausencia de monitoreo	MA	Art. 64	Políticas y procedimientos de intercambio de información
		[A.10]	Alteración de secuencia	Ausencia de sincronización	MA	Art. 30	Gestión de privilegios de acceso
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Art. 53	Registro de eventos
		[A.13]	Repudio	Ausencia de implementación de firmas digitales	MA	Art. 53	Registro de eventos
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Art.32	Retirada o reasignación de los derechos de acceso
		[A.19]	Divulgación de información	Falta de implementación del certificado SSL	MA	Art.32	Retirada o reasignación de los derechos de acceso

[esencial] Activos esenciales		Amenaza		Vulnerabilidad	Riesgo	Controles ISO/27002:2017	
[gesu]	Gestión usuarios	[E.2]	Errores del administrador	Ausencia de concienciación y control en las cuentas dadas de baja de los usuarios	**MA**	Art. 47	Documentación de procedimientos de operación
[idm]	Gestión identidades	[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles	**MA**	Art. 26	"Política de Control de Acceso"
[ipm]	Gestión privilegios	[A.11]	Acceso no autorizado	Contraseñas inseguras	**MA**	Art. 30	Gestión de privilegios de acceso
[S.sub] Subcontratados a terceros							
[vhost]	Hosting virtual Contabo	[I.5]	Avería de origen físico o lógico	Fallo en los equipos informáticos	MA	Art. 44	Mantenimiento de los equipos
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	Art. 47	Documentación de procedimientos de operación
[Internet]	Internet	[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	Art. 67	Acuerdos de confidencialidad o no revelación
		[A.6]	Abuso de privilegio de acceso	Ausencia de control de eventos *logs*	MA	Art. 30	Gestión de privilegios de acceso

Fuente: Elaborado por el autor, en referencia a la Metodología MAGERIT, Libro II "Catálogo de Elementos" (2012)

[HW] Equipamiento informático

Tabla 34

Selección de las salvaguardas del equipamiento informático del Sistema Ignug

[HW] Equipamiento informático		Amenaza		Vulnerabilidad	Riesgo	Controles Norma ISO/27002:2017	
[SW] Aplicaciones:							
[prp] Desarrollo propio							
[sgai]	Sistema de gestión académica Ignug	[I.5]	Avería de origen físico o lógico	Fallo en las configuraciones de los equipos informáticos	MA	Art. 44	Mantenimiento de los equipos
		[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	MA	Art. 47	Documentación de procedimientos de operación

		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	Art. 47	Documentación de procedimientos de operación
[bddi]	Base de datos "ignug_bdd"	[E.10]	Errores de secuencia	Ausencia de sincronización	MA		
		[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	MA	Art. 30	Gestión de privilegios de acceso
[backup]	Sistema de backup	[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	Art. 30	Gestión de privilegios de acceso
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	Art. 67	Acuerdos de confidencialidad o no revelación
		[E.20]	Vulnerabilidades de los programas (software)	Ausencia de escaneo y actualizaciones	MA	Art. 58	Gestión de las vulnerabilidades técnicas
		[E.24]	Caída del sistema por agotamiento de recursos	Saturación de recursos tecnológicos	MA	Art. 92	Disponibilidad de los recursos de tratamiento de la información
		[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles	MA	Art. 26	"Política de Control de Acceso"
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	MA	Art. 30	Gestión de privilegios de acceso
		[A.9]	Re encaminamiento de mensajes	Ausencia de monitoreo	MA	Art. 64	Políticas y procedimientos de intercambio de información
		[A.10]	Alteración de secuencia	Ausencia de sincronización	MA	Art. 56	Sincronización del reloj
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Art. 30	Gestión de privilegios de acceso
		[A.15]	Modificación deliberada de la información	Ausencia de procedimientos de desvinculación de los empleados	MA	Art.32	Retirada o reasignación de los derechos de acceso
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Art.32	Retirada o reasignación de los derechos de acceso
		[A.19]	Divulgación de información	Falta de implementación del certificado SSL	MA	Art.32	Retirada o reasignación de los derechos de acceso
		[A.24]	Denegación de servicio	Ausencia de control en las cuentas dadas de baja de recursos suficientes	MA	Art. 62	Seguridad de los servicios de red
[std] Estándar:							
[app]	Servidor de aplicaciones apache	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	MA	Art. 47	Documentación de procedimientos de operación
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	**MA**	Art. 47	Documentación de procedimientos de operación
[dmbs]	Sistema de gestión de	[E.15]	Alteración accidental de la información	Ausencia de controles de procesos de modificación	MA	Art. 30	Gestión de privilegios de acceso

[file]	base de Datos Postgres	[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	MA	Art. 30	Gestión de privilegios de acceso
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	Art. 67	Acuerdos de confidencialidad o no revelación
[os]	Servidor de archivos	[E.20]	Vulnerabilidades de los programas (software)	Ausencia de escaneo y actualizaciones	MA	Art. 58	Gestión de las vulnerabilidades técnicas
	Sistema Operativo	[E.24]	Caída del sistema por agotamiento de recursos	Saturación de los recursos tecnológicos	MA	Art. 92	Disponibilidad de los recursos de tratamiento de la información
	Ubuntu server	[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles	MA	Art. 26	"Política de Control de Acceso"
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	MA	Art. 30	Gestión de privilegios de acceso
		[A.7]	Uso no previsto	Ausencia de registro de eventos de control de accesos	MA	Art. 30	Gestión de privilegios de acceso
		[A.10]	Alteración de secuencia	Ausencia de sincronización	MA	Art. 64	Políticas y procedimientos de intercambio de información
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Art. 30	Gestión de privilegios de acceso
		[A.15]	Modificación deliberada de la información	Ausencia de procedimientos de desvinculación de los empleados	MA	Art.32	Retirada o reasignación de los derechos de acceso
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Art.32	Retirada o reasignación de los derechos de acceso
		[A.24]	Denegación de servicio	Ausencia de control en las cuentas dadas de baja de recursos suficientes	MA	Art. 62	Seguridad de los servicios de red
[email-cleinte]	Cliente de correo electrónico google	[E.9]	Errores de re encaminamiento	Configuraciones erróneas, Ausencia de monitoreo	MA	Art. 64	Políticas y procedimientos de intercambio de información
		[E.10]	Errores de secuencia	Ausencia de sincronización	MA	Art. 63	Segregación en redes
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	**A**	Art. 67	Acuerdos de confidencialidad o no revelación
		[E.20]	Vulnerabilidades de los programas (software)	Ausencia de escaneo y actualizaciones	A	Art. 58	Gestión de las vulnerabilidades técnicas
		[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles	**A**	Art. 26	"Política de Control de Acceso"
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	MA	Art. 30	Gestión de privilegios de acceso
		[A.7]	Uso no previsto	Ausencia de *logs* de eventos control accesos	MA	Art. 30	Gestión de privilegios de acceso

		[A.9]	Re encaminamiento de mensajes	Ausencia de monitoreo	MA	Art. 64	Políticas y procedimientos de intercambio de información
		[A.10]	Alteración de secuencia	Ausencia de sincronización	MA	Art. 63	Segregación en redes
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Art. 30	Gestión de privilegios de acceso
		[A.15]	Modificación deliberada de la información	Ausencia de procedimientos de desvinculación de los empleados	MA	Art.32	Retirada o reasignación de los derechos de acceso
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	MA	Art.32	Retirada o reasignación de los derechos de acceso
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja de los usuarios	MA	Art.32	Retirada o reasignación de los derechos de acceso
		[A.24]	Denegación de servicio	Ausencia de control en las cuentas dadas de baja de recursos suficientes	MA	Art. 62	Seguridad de los servicios de red
[HW] Equipos informáticos:							
[pc]	Informática personal	[I.1]	Fuego	Ausencia de capacitación sobre extintores	**B**	Art. 41	Emplazamiento y protección de equipos
		[I.3]	Contaminación mecánica	Ausencia de mantenimiento preventivo	**B**	Art. 44	Mantenimiento de los equipos
[pc.back up]	Equipamiento de respaldo	[I.5]	Avería de origen físico o lógico	Fallo en los equipos informáticos	**B**	Art. 44	Mantenimiento de los equipos
		[I.6]	Corte de suministro eléctrico	Ausencia de implementación de UPS	**B**	Art. 42	Instalaciones de suministro
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Ausencia de implementación del sistema de enfriamiento	**B**	Art. 41	Emplazamiento y protección de equipos
		[I.11]	Emanaciones electromagnéticas	Ausencia de monitoreo de señales externas	**B**	Art. 41	Emplazamiento y protección de equipos
[backup]	Equipamiento de respaldo virtual	[I.5]	Avería de origen físico o lógico	Fallo en los equipos informáticos	**MA**	Art. 44	Mantenimiento de los equipos
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	**MA**	Art. 47	Documentación de procedimientos de operación
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	**MA**	Art. 67	Acuerdos de confidencialidad o no revelación
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	**MA**	Art. 30	Gestión de privilegios de acceso
		[A.7]	Uso no previsto	Ausencia de *logs* de eventos control accesos	**MA**	Art. 30	Gestión de privilegios de acceso
[COM] Redes de comunicaciones:							
[LAN]	Red local	[I.5]	Avería de origen físico o lógico	Fallo en los equipos informáticos	**A**	Art. 44	Mantenimiento de los equipos
[wifi]		[I.8]	Fallo de servicios de comunicaciones	Ausencia de bitácoras de quienes configuran el data center	**A**	Art. 62	Seguridad de los servicios de red

		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	**A**	Art. 47	Documentación de procedimientos de operación
[Internet]	Red inalámbrica	[E.9]	Errores de re encaminamiento	Configuraciones erróneas, Ausencia de monitoreo	**MA**	Art. 64	Políticas y procedimientos de intercambio de información
	Internet	[E.10]	Errores de secuencia	Ausencia de sincronización	**MA**	Art. 63	Segregación en redes
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	**A**	Art. 67	Acuerdos de confidencialidad o no revelación
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	**A**	Art. 30	Gestión de privilegios de acceso
		[A.7]	Uso no previsto	Ausencia de *logs* de eventos control accesos	**A**	Art. 30	Gestión de privilegios de acceso
[network] Soporte de la red							
[firewall]	Cortafuegos	[I.1]	Fuego	Ausencia de capacitación sobre extintores	**A**	Art. 41	Emplazamiento y protección de equipos
[router]	encaminadores	[I.3]	Contaminación mecánica	Ausencia de mantenimiento preventivo	**A**	Art. 44	Mantenimiento de los equipos
		[I.5]	Avería de origen físico o lógico	Fallo en los equipos informáticos	**A**	Art. 44	Mantenimiento de los equipos
		[I.6]	Corte de suministro eléctrico	Ausencia de implementación de UPS	**A**	Art. 42	Instalaciones de suministro
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Ausencia de implementación del sistema de enfriamiento	**A**	Art. 41	Emplazamiento y protección de equipos
		[I.8]	Fallo de servicios de comunicaciones	Ausencia de bitácoras de quienes ingresan al data center	**A**	Art. 65	Acuerdos de intercambio de información
		[I.11]	Emanaciones electromagnéticas	Ausencia de monitoreo de señales externas	**A**	Art. 44	Mantenimiento de los equipos
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	**A**	Art. 46	Documentación de procedimientos de los operación
		[E.9]	Errores de re encaminamiento	Configuraciones erróneas, Ausencia de monitoreo	**A**	Art. 64	Políticas y procedimientos de intercambio de información
		[E.10]	Errores de secuencia	Ausencia de sincronización	**MA**	Art. 63	Segregación en redes
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	**MA**	Art. 30	Gestión de privilegios de acceso
[Media] Soportes de información:							
[disk]	Discos	[I.1]	Fuego	Ausencia de capacitación sobre extintores	**A**	Art. 41	Emplazamiento y protección de equipos
	Discos	[I.3]	Contaminación mecánica	Ausencia de mantenimiento preventivo	**A**	Art. 44	Mantenimiento de los equipos
[vdisk]	virtuales	[I.5]	Avería de origen físico o lógico	Fallo en los equipos informáticos	**A**	Art. 44	Mantenimiento de los equipos
		[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	**A**	Art. 67	Acuerdos de confidencialidad o no revelación
	Almacenamie						
[san]	nto en red	[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	**A**	Art. 30	Gestión de privilegios de acceso

		[A.7]	Uso no previsto	Ausencia de registro de eventos de control de accesos	**A**	Art. 30	Gestión de privilegios de acceso

Fuente: Elaborado por el autor, en referencia a la Metodología MAGERIT, Libro II "Catálogo de Elementos" (2012)

[P] Personal

Tabla 35

Selección de las salvaguardas con respecto al personal relacionado con el sistema Ignug

Activo: [P] Personal		**Amenaza**		**Vulnerabilidad**	**Riesgo**	**Controles ISO/27002_2017**	
[ue] Usuarios externos							
[ue]	Empresas formadoras	[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles, sin protección	A	Art. 26	"Política de Control de Acceso"
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	A	Art. 30	Gestión de privilegios de acceso
[ui] Usuarios internos							
[uest]	Estudiantes	[E.1]	Errores de los usuarios	Ausencia de manuales de usuario	A	Art. 47	Documentación de procedimientos de operación
[ud]	Docentes	[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	A	Art. 67	Acuerdos de confidencialidad o no revelación
[ua]	Autoridades	[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles, sin protección	MA	Art. 26	"Política de Control de Acceso"
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	MA	Art. 30	Gestión de privilegios de acceso
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	MA	Art. 30	Gestión de privilegios de acceso
		[A.19]	Divulgación de información	Ausencia de control en las cuentas dadas de baja de los usuarios	A	Art.32	Retirada o reasignación de los derechos de acceso
[adm] Administradores de sistemas; [dba] Administradores de base de datos: [com] administrador de comunicaciones							
[adm]	Admin. sistema	[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	Art. 47	Documentación de procedimientos de operación
[adma]	Ignug	[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	Art. 67	Acuerdos de confidencialidad o no revelación

Activo: [P] Personal			Amenaza	Vulnerabilidad	Riesgo	Controles ISO/27002_2017	
[adba] [adbap]	Apoyo de admin.	[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles, sin protección	MA	Art. 26	"Política de Control de Acceso"
[adcom]	Ignug Admin.BDD Apoyo de admin. BDD Admin. data center	[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	MA	Art. 30	Gestión de privilegios de acceso
		[A.19]	Divulgación de información	Ausencia de acuerdos de confidencialidad	**MA**	Art.32	Retirada o reasignación de los derechos de acceso
[des] Equipo de desarrollo							
[desd]	desarrolladores docentes	[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	MA	Art. 47	Documentación de procedimientos de operación
[dese]	desarrolladores estudiantes	[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	MA	Art. 67	Acuerdos de confidencialidad o no revelación
		[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles, sin protección	MA	Art. 26	"Política de Control de Acceso"
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	MA	Art. 30	Gestión de privilegios de acceso
		[A.19]	Divulgación de información	Ausencia de acuerdos de confidencialidad	**A**	Art.32	Retirada o reasignación de los derechos de acceso
[prov] Proveedores							
[provi]	proveedores de internet	[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	**A**	Art. 67	Acuerdos de confidencialidad o no revelación
		[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles, sin protección	MA	Art. 26	"Política de Control de Acceso"
[provhv]	proveedores de hosting virtual	[E.19]	Fugas de información	Ausencia de acuerdos de confidencialidad	MA	Art. 67	Acuerdos de confidencialidad o no revelación
		[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles, sin protección	MA	Art. 26	"Política de Control de Acceso"
		[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	MA	Art. 30	Gestión de privilegios de acceso
		[A.19]	Divulgación de información	Ausencia de acuerdos de confidencialidad	MA	Art.32	Retirada o reasignación de los derechos de acceso

Fuente: Elaborado por el autor, en referencia a la Metodología MAGERIT, Libro II "Catálogo de Elementos" (2012)

CAPÍTULO V

DISEÑO DEL MODELO DE CIBERSEGURIDAD

5.1 Introducción

El trabajo realizado en el capítulo 4 sobre el "Análisis y Situación Actual", aportó con el reconocimiento de las amenazas y vulnerabilidades a los que se pueden exponer los activos de información y de servicios del Sistema de Gestión Académica Ignug; para solventarlos, se propone crear un modelo de Ciberseguridad, en referencia a la Norma ISO/IEC 27002:2017, código de buenas prácticas para los controles de seguridad de la información (ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015), que permitirá la selección de los controles adecuados, mediante directrices como: acceso y derechos de uso; realizar evaluaciones periódicas de riesgos con el fin de verificar nuevas vulnerabilidades y controlarlas para garantizar las características y principios fundamentales de la ciberseguridad.

5.2 Estructura de la Norma ISO/IEC 27002:2017

La norma, consta de 14 capítulos de controles, conteniendo 35 categorías principales de seguridad y 114 controles. Sirven para organizar la información a alto nivel dentro del ámbito de la conectividad. Ver Anexo 1 "Controles ISO/IEC 27002:2017".

5.3 Abreviaturas

- COIP: Código Orgánico Integral Penal del Ecuador
- DA: Directorio activo
- DBA: Administrador de bases de datos

- CISO: Gerente de Ciberseguridad (*Chief Information Security Officer*)
- ID: identificador
- ISTY: Instituto Superior Tecnológico Yavirac
- HTTPS: Protocolo de transferencia de hipertexto seguro
- SDLC: Ciclo de vida de desarrollo de software
- SENESCYT: Secretaría de Educación Superior, Ciencia, Tecnología e Innovación
- SGA: Sistema de Gestión Académica
- SOC: Líder del Centro de Operaciones de Seguridad y el equipo de seguridad de ISTY
- S-SDLC: Ciclo de vida de desarrollo de software seguro
- TIC: Tecnologías de la Información y Comunicación

5.4 Diseño de la Política de Ciberseguridad

Artículo 1.- Ámbito. - La presente Política aplica a los activos de información, servicios y personal relacionados con el SGA Ignug del Instituto Superior Tecnológico Yavirac.

Artículo 2.- Objeto. - El presente instrumento establecerá directrices considerando el entorno de riesgos de seguridad, para la protección de la información y servicios proporcionados por el Sistema de Gestión Académico Ignug, incluyendo buenas prácticas, principios de diseño, selección y gestión de los controles de la Norma ISO/IEC 27002:2017.

Artículo 3.- Estructura Organizacional de la Ciberseguridad. - La estructura organizacional que se recomienda, será la encargada de la actualización de la política, la redacción de nuevas políticas y procedimientos de seguridad; además de la implementación del modelo de seguridad propuesto y la auditoría con respecto al cumplimiento. Ver la Figura Nº 12.

Figura 12: Estructura organizacional de seguridad del ISTY
Fuente: Elaborado por el autor

Auditoría. – Controlará la implementación de los controles de seguridad de la política y verificará el cumplimiento del objetivo. Estará integrado por los siguientes miembros:

- CISO
- Equipo de seguridad de SENESCYT

Comité de Dirección. – Estratégico, encargado de aprobar, actualizar y socializar la política y procedimientos de seguridad. Se conformará por las siguientes autoridades:

- CISO
- Rector del ISTY
- Vicerrector del ISTY

Dirección Ejecutiva. - Táctico operacional, encargado de implementar los controles de la política. Estará integrado por los siguientes miembros:

- SOC
- Unidad de TIC

Capítulo 1: Política de Seguridad de la Información

Categoría: Directrices de gestión de la seguridad de la información

Artículo 4.- Política para la seguridad de la información. - El Comité de Dirección tendrá la misión de aprobar la presente Política de seguridad, la socializará a la Dirección Ejecutiva y a toda la comunidad educativa.

Artículo 5.- Revisión de la política. - La presente política, será revisada por el Comité de Dirección de forma anual y cuando se integren desarrollos nuevos al Sistema Ignug; para conservar su idoneidad, ajuste y eficacia.

Capítulo 2: Organización de la Seguridad de la Información

Categoría: Organización interna

Artículo 6.- Roles y responsabilidades. - Los responsables de la seguridad de la información son: el Comité de Dirección y la Dirección Ejecutiva conforme el Artículo 3 de la Estructura Organizacional de la Ciberseguridad. El Área de Auditoría deberá verificar el cumplimiento de la aplicación de la presente política y las que se creen.

Artículo 7.- Segregación de tareas. – El SOC, segregará las tareas de acuerdo a las responsabilidades asignadas a los integrantes de la Unidad de TIC y otorgará las credenciales de acceso a las diferentes aplicaciones y servicios que el SGA Ignug provee.

Artículo 8.- Contacto con las autoridades. - La Dirección Ejecutiva, deberá comunicar al CISO, sobre posibles incidentes suscitados interna o externamente. El CISO, al ser la máxima autoridad jerárquica de la seguridad del ISTY, deberá comunicar de los sucesos efectuados, a los miembros del Comité de Dirección, a los responsables de los servicios contratados como internet y *hosting virtual*, con el fin de emprender acciones de recuperación, acordes al tipo de ataque sufrido.

Artículo 9.- Seguridad de la información en la gestión de proyectos. - Para la gestión de proyectos informáticos, se deberán incluir medidas de seguridad en el SDLC, así como, el análisis de riesgos de seguridad, con el fin de minimizar las vulnerabilidades de los nuevos desarrollos a integrarse con el Sistema Ignug. Para la generación del proceso de creación de sistemas informáticos de gobierno y el mantenimiento de un proyecto, se recomienda hacer uso de la Norma IEEE 1074-2006; de igual manera, la Norma ISO/IEC 27034-1, ayuda a integrar seguridad en el SDLC del software.

Se recomienda aplicar el uso de principios y buenas prácticas en las actividades de todas las fases del SDLC.

Categoría: Los dispositivos móviles y el teletrabajo

Artículo 10.- Política de dispositivos móviles. - Los dispositivos móviles del instituto, deberán ser registrados en un inventario de activos, para resguardarlos se deberá considerar la protección de los equipos informáticos y tomar en cuenta los siguiente:

- Restricción de instalación de software
- Requisitos para aplicar parches y actualizaciones del software
- Limitaciones de conexión a servicios de información
- Registros y validaciones de acceso
- Cifrado
- Salvaguarda anti *malware*
- Aseguramiento de la disponibilidad
- Reproducción de documentos
- Copias de respaldo
- Protocolos de seguridad inalámbrica

Artículo 11.- Teletrabajo. - En determinadas ocasiones, el personal de la institución podrá realizar teletrabajo con el fin de dar continuidad a los procesos académicos; para asegurar las actividades de teletrabajo, se podrán considerar los siguientes aspectos:

- El entorno físico donde se realice el teletrabajo, deberá contemplar el ambiente adecuado.
- Las comunicaciones y el acceso remoto a la red, deberán efectuarse mediante controles y validaciones de acceso y protocoles de encriptación.
- Usar redes virtuales, mediante canales de cifrado
- Mantener acuerdos de licencias de herramientas
- Auditoría y monitoreo de la seguridad
- Cancelación de los permisos y autorizaciones

La institución, mediante la gestión del Comité de Dirección, Dirección Ejecutiva y Comité de la Seguridad de la información, deberá implementar la presente política con las medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.

Capítulo 3: Seguridad relativa a los recursos humanos

Categoría: Antes del empleo

Artículo 12.- Términos y condiciones del empleo. - Para contratar al personal docente y administrativo del ISTY, se deberán establecer términos y condiciones de seguridad de la información y buen uso de los servicios proporcionados por el SGA Ignug, dentro del contrato de trabajo. De igual manera, los docentes asignados a la Unidad de TIC, se comprometerá en firmar un acuerdo de confidencialidad, con el objetivo de resguardar las características de la seguridad.

Categoría: Durante del empleo

Artículo 13.- Responsabilidades de gestión. - El Comité de Dirección, deberá dar seguimiento, concienciar y exigir a la comunidad académica y los proveedores de internet y *hosting virtual*, el cumplimiento de la Política de seguridad y los procedimientos establecidos por el ISTY.

Como buena práctica, se registrarán los datos de los usuarios de la comunidad educativa y del personal nuevo, en el Sistema de Gestión de Usuarios, con el fin de mantener centralizados los procesos de acceso para el uso de los diferentes módulos que forman parte de la plataforma Ignug.

Artículo 14.- Concienciación, educación y capacitación en seguridad de la información. - El Comité de Dirección, se encargará de socializar, capacitar y concienciar al personal que se incorpora por primera vez al ISTY, de igual manera, cuando la Política sea actualizada, se deberá hacer conocer a toda la comunidad educativa y a los miembros de la Dirección Ejecutiva para que la ejecuten.

Para efectos de la capacitación, se podrán usar medios físicos y digitales con el contenido de la Política de seguridad, la misma que será diseñada por el Departamento de Diseño y Comunicación y aprobada por el Comité de Dirección. Se llevarán a cabo, mediante campañas publicitarias por mensajería electrónica, redes sociales, portal web institucional, *webinars* y exposiciones presenciales.

Es obligación de toda la familia del Yavirac, asistir a los eventos de capacitación y socialización.

Artículo 15.- Proceso disciplinario. - Se ejecutarán las acciones disciplinarias plasmadas en el Reglamento de Disciplina del ISTY, hacia las personas que incumplan con los

artículos de la presente Política y que atenten voluntaria e involuntariamente contra la seguridad de los activos del Sistema Ignug.

Se contemplará el siguiente proceso:

- La Dirección Ejecutiva, emitirá un informe con la falta o brecha de seguridad producida al Comité de Dirección, con el fin, de que se realice la respectiva investigación.
- El Comité de Dirección, investigará detalladamente sobre la violación de seguridad, en el caso de ser positiva, propondrá las acciones disciplinarias, conforme al Reglamento Disciplinario del ISTY; además, reportará a la Policía Judicial PJ, para que se le aplique el Código Orgánico Integral Penal del Ecuador COIP.

Categoría: Finalización del empleo o cambio en el puesto de trabajo

Artículo 16.- Responsabilidades ante la finalización o cambio. – El CISO definirá un proceso de fin de actividades reflejado en un informe final en el cual se incluyan los requisitos de seguridad y responsabilidades legales que conlleven a acuerdos de confidencialidad de cese de funciones; lo aprobará el Comité de Dirección, con el fin de dar de baja al personal que se excluya de la institución. Se desactivarán los permisos desde el Sistema de Gestión de Usuarios, para bloquear el acceso a los módulos del Ignug; además, se inhabilitarán los permisos de ingreso al correo electrónico institucional desde el administrador de correos *Google.*

El Comité de Dirección, deberá informar a la Dirección Ejecutiva sobre la desvinculación del personal, para que se ejecute el procedimiento de dada de baja del empleado del Sistema de Gestión de Usuarios.

Capítulo 4: Gestión de activos

Categoría: Responsabilidad sobre los activos. -

Artículo 17.- Inventario de activos. – La Dirección Ejecutiva, deberá implementar herramientas informáticas y establecer un mecanismo apropiado, para levantar la información y otros activos referentes al tratamiento de los datos y servicios que proporciona Ignug, con el fin de elaborar un inventario y mantenerlo actualizado.

Se deberán identificar los activos relevantes, clasificarlos, valorarlos y documentarlos, con el objetivo de darles un adecuado tratamiento, almacenamiento, transmisión.

El Área de Auditoría, deberá auditar cada semestre el catálogo de activos; el mismo que deberá ser íntegro, consistente y estar actualizado.

Para la implementación se recomienda:

- Inventariar los activos del SGA Ignug
- Inventariar los activos de Hardware
- Inventariar los activos de soporte de Software

Artículo 18.- Propiedad de los activos. – El Comité de Dirección asignará un propietario a cada uno de los activos, tomando en cuenta las funciones designadas al personal, mediante actas de entrega-recepción y la documentación de uso del bien; si no hubiera usuarios designados, la Dirección Ejecutiva, será el custodio de dichos activos; de igual manera, se responsabilizará de los activos nuevos recibidos por parte de la entidad rectora SENESCYT o de empresas donantes.

La Dirección Ejecutiva registrará los activos nuevos en el inventario, los clasificará debidamente, les asignará un custodio y dará seguimiento al manejo adecuado de los mismos, tomando en cuenta los controles de acceso.

Artículo 19.- Uso aceptable de los activos.- El Comité de Dirección, documentará las reglas de uso de los activos, de acuerdo a la categorización de ellos; socializará y facilitará el acceso a dichos documentos y manuales de uso, para que los usuarios se mantengan enterados sobre el buen tratamiento de la información, servicios e infraestructura tecnológica en el cual se encuentra implementada la plataforma Ignug, de esta manera, se logrará reducir las amenazas y posibles ataque sobre los activos del ISTY.

Artículo 20.- Devolución de activos. - Dado el caso, de que se le haya asignado un equipo o dispositivo informático al personal saliente, la Dirección Ejecutiva revisará el estado del activo; si éste se encontrara en mal estado, el funcionario deberá arreglarlo o reconocer el coste del bien; posterior, lo entregará al Departamento Administrativo del ISTY.

Categoría: Clasificación de la información

Artículo 21.- Clasificación de la información. - La Dirección Ejecutiva, recopilará toda la información y la clasificará según el grado de valor, sensibilidad y confidencialidad que ésta tenga. Se elaborará un catálogo de clasificación considerando la siguiente escala:

- [D.pub] Información de carácter pública
- [D.C] Información de difusión limitada
- [D.R] Información de nivel confidencial

  El nivel de protección dependerá de la valoración del activo.

Artículo 22.- Etiquetado de la información. - La Dirección Ejecutiva, etiquetará los activos mediante abreviaturas y números secuenciales, tomando en cuenta la clasificación, valoración y usabilidad; el código de cada activo, se lo registrará en el inventario.

Artículo 23.- Manipulado de la información. - El Comité de Dirección, redactará el procedimiento para el uso adecuado de la información, de acuerdo a la clasificación

detallada en el Artículo Nº 21. En el documento, se considerarán los siguientes principios de seguridad:

- Mínimo privilegio: se deberá conceder un conjunto restrictivo de actividades
- Separación de privilegios: se deberá permitir el acceso a los datos necesarios para realizar las actividades diarias.
- Conservar de los registros de los usuarios autorizados
- Backups: se mantendrán protegidas las copias de seguridad con accesos restringidos
- Almacenamiento: se almacenarán los activos, conforme las especificaciones de los fabricantes.

Categoría: Manipulación de los soportes

Artículo 24.- Gestión de soportes extraíbles. - El Comité de Dirección, elaborará la manera de proceder con la gestión de soportes extraíbles, se tomarán en cuenta algunas de las características secundarias y principios de la seguridad:

- Autenticación: se deberán proteger contra acceso no autorizados a los soportes que contengan la información limitada, mediante credenciales de usuario.
- Criptografía: se implementarán técnicas de criptografía para proteger la información confidencial de los dispositivos extraíbles.
- Separación de la información: se deberán usar varios soportes extraíbles con el propósito de proteger a la data de acuerdo a la clasificación.
- Disponibilidad: se remplazarán los soportes cuando éstos hayan cumplido su vida útil, la transferencia de la información, se gestionará con la matriz RACI.

Artículo 25.- Soportes físicos en tránsito. - El Comité de Dirección, elaborará el procedimiento para la autorización de extraer los soportes físicos del ISTY, en tránsito, en

el caso de ser necesario, se solicitará autorización para extraer soportes del ISTY y se mantendrá trazabilidad de los registros de las salidas de los medios extraíbles.

Capítulo 5: Control de acceso

Categoría: Requisitos de negocio para el control de acceso

Artículo 26.- Política de Control de Acceso. - El Comité de Dirección, elaborará una "Política de Control de Acceso", la misma que será ejecutada por la Dirección Ejecutiva; para la elaboración de la política se considerarán las características complementarias de la seguridad, principios y buenas prácticas:

- Autenticación. - se deberán otorgar credenciales de acceso de usuario y contraseña y permitir el cambio del *password* en la primera oportunidad de ingreso a los servicios.
- Multifactor de autenticación. - para todos los accesos administrativos, incluido el acceso administrativo de dominio, la autenticación puede incluir varias técnicas, que incluyen el uso de tarjetas inteligentes, certificados, tokens de contraseña de un solo uso (OTP), datos biométricos u otros métodos de autenticación similares.
- Mínimo privilegio. - se concederá a cada usuario el acceso únicamente al conjunto restrictivo de tareas con las que desempeñará sus actividades
- Separación de privilegios. - se asignarán roles a los usuarios para que accedan únicamente a las funcionalidades con las ejecutan sus laborales.
- Formatos. - los usuarios que necesiten permisos de acceso a cualquier servicio del Ignug, deberán solicitar mediante un documento formal las peticiones de acceso.
- Fin de derechos de acceso. - cuando los usuarios sean separados de la institución, se deberán revisar los permisos otorgados para darle de baja mediante el Sistema de Gestión de Usuarios.

Artículo 27.- Acceso a las redes y a los servicios de red. - Se proporcionarán permisos para usar las redes *Fast Ethernet*, *Wifi* y servicios, a los usuarios que realicen tareas administrativas y de docencia, no se otorgarán permisos a los estudiantes, puesto que usan los equipos de los laboratorios.

Categoría: Gestión de acceso de usuario

Artículo 28.- Registro y baja de usuarios. - El CISO, elaborará formatos de solicitudes con el fin de que los usuarios pidan permisos de acceso a los módulos y datos del sistema Ignug. El Comité de Dirección, analizará dichas solicitudes y aprobará los permisos hasta dos semestres, luego se los analizará y renovará nuevamente en caso de ser necesario.

Para dar de baja a los usuarios se deberá inactivarlos desde el Sistema de Gestión de Usuarios, con la revocación del ID.

Artículo 29.- Provisión de acceso de usuario. - El Comité de Dirección, realizará el procedimiento legal para conceder y derogar permisos de accesos a los módulos y servicios del Ignug a toda la comunidad educativa; se aplicará los controles de la "Política de Control de Acceso".

Artículo 30.- Gestión de privilegios de acceso. - Se controlará el acceso a los diferentes servicios del SGA Ignug, mediante la aplicación de la "Política de Control de Acceso", que deberá tomar en cuenta siguiente:

- Mínimo privilegio. - para evitar que varios usuarios tengan derechos de administrador, y que los usen para instalaran aplicaciones y servicios no autorizados, privilegio indefinido.
- Separación de privilegios. - implicará la asignación únicamente de un subconjunto de funcionalidades y datos que ofrece todo el sistema Ignug.

- Separación de dominios. - reflejar el uso de técnicas de compartimentación de los usuarios, datos y servicios con la finalidad de realizar las tareas asignadas a ellos, con los datos autorizados, utilizando los recursos tecnológicos como memoria, disco duro, etc. asignados para la ejecución de los servicios
- Para otorgar los derechos de privilegios se deberá asignar un ID por usuario, previo a la aprobación de permisos mediante solicitud.

Artículo 31.- Gestión de la información secreta de autenticación de los usuarios. - La "Política de Control de Acceso", contendrá la gestión de la entrega de las credenciales de autenticación, de acuerdo a las siguientes indicaciones:

- Las credenciales se entregarán en sobre cerrado en las manos del destinario, previo a la aceptación del acuerdo de confidencialidad si se trata de manejo de información sensible.
- Se deberá solicitar cambio de contraseña al primer uso del *password.*
- La información de autenticación, debería ser generado por una herramienta de generación de códigos, con la finalidad de que sea difícil de acordarse.

Artículo 32.- Retirada o reasignación de los derechos de acceso. - Al finalizar el contrato laboral de los usuarios y administradores del SGA Ignug o, si los estudiantes finalizan sus estudios en el instituto, se eliminarán los permisos de ingreso a los diferentes servicios que proporciona la plataforma.

Categoría: Responsabilidades del usuario

Artículo 33.- Uso de la información secreta de autenticación. - El Comité de Dirección, realizará campañas recordando a los usuarios sobre el buen uso de las credenciales de autenticación, advertirá lo siguiente:

- No se divulgará de ninguna forma verbal o por escrito los datos de autenticación.
- Se cambiará el *password* cada dos meses, o cuando se tengan sospechas de fuga de información.
- Cuando se cambien las contraseñas, no se deberán usar datos personales como fechas de cumpleaños, nombres de familiares, debido a que pueden ser fáciles de adivinar mediante un ataque de fuerza bruta; se recomienda leer el Artículo 31 de la presente Política.
- Se asegurará que la información secreta esté asegurada, se puede usar herramientas de encriptado para cifrarla.

Categoría: Control de acceso a sistemas y aplicaciones

Artículo 34.- Restricción del acceso a la información. - Se deberá restringir el acceso a la información, para ello, se considerarán los principios del Artículo 30 sobre la Gestión de privilegios de acceso.

Artículo 35.- Procedimientos seguros de inicio de sesión. - Se controlarán los inicios de sesión, mediante validaciones de acceso que permitirán comparar las credenciales ingresadas con las credenciales existentes en la base de datos del Ignug. Se considerarán principios de diseño, mismos que deberían constar en la "Política de Control de Acceso".

- Mostrar un mensaje que indique que el uso al servicio es permitido únicamente para usuarios autorizados.
- No facilitar ayudas como recordatorios y funciones que permitan ver la clave.
- Se permitirán hasta 3 intentos de ingreso de las credenciales de autenticación, si al tercer intento falla, automáticamente la cuenta de usuario deberá bloquearse.

- Registros de eventos de seguridad. - se registran los intentos en un archivo de registro de eventos *log*, con el fin de contabilizar el número de intentos realizados al sistema Ignug.
- Entorno de producción inseguro. - se deberá asegurar que la validación de la entrada no pueda ser evitada, confiar en listas blancas válidas, rechazar los ejecutables de fuentes no autorizadas.

Artículo 36.- Sistema de gestión de contraseñas. - El Sistema de Gestión de usuarios del Ignug, deberá integrar una funcionalidad para establecer contraseñas seguras y robustas, o a su vez se deberá hacer uso de una herramienta que genere contraseñas con las características antes indicadas. Se considerarán los siguientes aspectos:

- Se identificará al usuario mediante un código (ID).
- Los usuarios deberán cambiar la contraseña, al iniciar por primera vez la sesión de cualquiera de los módulos del SGSA Ignug.
- La contraseña deberá contener mínimo 12 caracteres, letras mayúsculas y minúsculas, números y caracteres especiales.
- Se ocultarán a través de puntos para no verlas.
- Cifrar las contraseñas y luego almacenarlas de forma separada de los datos de información del Sistema Ignug.

Artículo 37.- Control de acceso al código fuente de los programas. - Se restringirá el acceso al código fuente, mediante la aplicación de principios y buenas prácticas.

- Seguridad por oscuridad. - se deberá guardar la información de forma cifrada, en carpetas ocultas en el servidor.

- Separación de dominios. - se usarán técnicas de separación de código ejecutable, código fuente y procesos en el servidor de producción o, se almacenará el código fuente en otros equipos que nos sean el de producción; el usuario deberá ejecutar las tareas necesarias con los datos necesarios.
- Registro de sucesos de seguridad. - se deberán *logs* en los cuales se registren datos como: usuario, fecha, hora, acción realizada, con el fin de auditar si personas extrañas al instituto han ingresado a los módulos del Ignug.

Capítulo 6: Criptografía

Categoría: Controles criptográficos

Artículo 38.- Política de uso de los controles criptográficos. - El Comité de Dirección, deberá elaborar una política para usar las técnicas criptográficas, la misma que alcanzar los objetivos de seguridad como la confidencialidad. Integridad, no repudio y autenticación; contemplarán los siguientes factores influyentes:

- Seguridad por oscuridad. - se deberán encriptar las claves utilizando diferentes técnicas de criptografía.
- Herramientas. - se usarán herramientas adecuadas para la conversión de texto legible en texto cifrado.
- Algoritmos de encriptación. - se deberán usar los algoritmos de encriptación integrados en un *framework* o, a su vez desarrollados por los programadores.
- Será responsable de la gestión de claves, el coordinador de TIC del ISTY.

Artículo 39.- Gestión de claves. - En la Política del Artículo 38, se deberá considerar el uso, la protección y la duración de la clave de cifrado.

- Se deberán utilizar diferentes técnicas de generación de claves, con el fin de crear *keys* seguras para acceder a la información del Sistema Ignug.
- Mediante herramientas y proveedores confiables, se generarán y obtendrán certificados de clave pública.
- Se almacenarán las claves en un dispositivo físico y también virtual, de forma encriptada, de esa manera si algún atacante logra acceder a ellas, no las podrá descifrar.
- Se realizarán *backups* de las claves cada semana.

Capítulo 7: Seguridad física y del entorno

Categoría: Áreas seguras

Artículo 40.- Controles físicos de entrada. - El acceso a la Unidad de TIC, deberá ser restringida, se considerarán las siguientes indicaciones:

- Únicamente el personal que labora en el área, tendrá acceso a la misma.
- Si una persona externa a TIC tuviera la necesidad de ingresar al departamento, deberá portar un permiso otorgado por el SOC.
- Se llevará una bitácora con el registro de los usuarios externos que ingresan a TIC.

Categoría: Seguridad de los equipos

Artículo 41.- Emplazamiento y protección de equipos. - Se deberá reducir el riesgo de las amenazas ambientales de los equipos asignados a la administración del Sistema Ignug, de las bases de datos, equipos de desarrollo, etc. mediante las siguientes prácticas:

- Se medirán las condiciones adecuadas del ambiente con aparatos dedicados.
- Queda terminantemente prohibido el consumo de alimentos en la Unidad de TIC.

- Se contará con respaldos en la nube, en el caso de que un equipo físico se dañe, no se perderá la información.
- Se dará mayor grado de protección a los equipos que contienen data sensible.
- Se deberá controlar que el personal de mantenimiento ingrese con maletas y otros objetos en el cual quepan los equipos.

Artículo 42.- Instalaciones de suministro. - Se protegerán a los equipos contra fallos de alimentación eléctrica, mediante la adquisición de UPS que permita apagar los equipos hasta 15 minutos después de haberse interrumpido el servicio eléctrico.

Artículo 43.- Seguridad del cableado. - Se deberá proteger al cableado de la red *Fast Ethernet*, contra interferencias o daños; se considerarán los siguientes aspectos:

- Se deberán aislar los cables de red de los cables de energía eléctrica, para minimizar la interferencia.
- Los cables deberán ser implementados por el techo, para evitar manipulación de los mismos.
- Se controlará el acceso al data center y se llevará una bitácora del personal que ingresa al área.

Artículo 44.- Mantenimiento de los equipos. - Se realizará un mantenimiento previo y uno correctivo de los equipos de TICs de forma adecuada tomando en cuenta las siguientes directrices:

- Únicamente el personal autorizado brindará soporte a los equipos de TICs y de otras áreas.
- Se registrarán todos los fallos reales en un formato realizado por la Dirección Ejecutiva.

- Se deberán mantener bitácoras de los mantenimientos realizados a las Pcs. de TICs y de otras áreas.
- Se deberá programar y enviar un cronograma a las autoridades y a los custodios de los equipos.

Artículo 45.- Retirada de materiales propiedad de la empresa. - Los equipos, la información o los sistemas, no deberán salir de las instalaciones del ISTY, sin autorización previa; si fuese necesario la extracción de los activos indicados, se deberá registrar en una bitácora las características del bien retirado.

Artículo 46.- Seguridad de los equipos fuera de las instalaciones. - Se deberá asegurar que el equipo extraído no se deje en cualquier lugar desatendido, o se exponga a robo. Si el quipo en mención llegara a sufrir daños o pérdidas, el personal responsable deberá correo con los gastos de reparación o reposición.

Capítulo 8: Seguridad de las operaciones

Categoría: Procedimientos y responsabilidades operacionales

Artículo 47.- Documentación de los procedimientos de operación. - El Comité de Dirección, redactará la documentación de los procedimientos de operación adecuados y los socializarla al personal encargado para su ejecución.

Los procedimientos deberán especificar lo siguiente:

- Se deberán instalar y configurar los módulos del sistema Ignug, únicamente los responsables delegados mediante memorando por parte de la Dirección Ejecutiva.
- Se tratará y manipulará la información manual y automatizada de forma responsable.
- Se realizarán copias de respaldo de forma periódica y programada, en el momento que se tenga menor usabilidad de la data y los servicios.

- En el caso de que se necesite reiniciar los sistemas o recuperarlos de alguna falla, se deberá comunicar a la comunidad educativa sobre la baja del servicio; para ello se aplicará el Plan de Recuperación y Continuidad.
- Se realizará monitorización tanto a los equipos como a los servicios que proporciona el Ignug.

Artículo 48.- Gestión de cambios. - Para la gestión de cambios de los módulos de SGA Ignug, o migración de data, se deberá trabajar con la matriz RACI, previa aprobación de del Comité de Dirección, para dar seguimiento y ejecución secuencial a las tareas por cumplirse, se tomará en cuenta los siguientes puntos:

- Mediante un formato elaborado por el CISO, se registrarán los cambios significativos tanto de las aplicaciones como de las bases de datos y la información.
- Se planificará y se levantará un cronograma para la implementación de los cambios.
- Se comunicará a todo el personal, sobre el tiempo que estará fuera de servicio el Sistema Ignug.
- Una vez implementados los cambios, se realizarán pruebas de validación del correcto funcionamiento de la aplicación en cuestión.
- Se aplicarán procedimientos de *rollback,* en el caso de que la aplicación Ignug haya sido perjudicada involuntaria o deliberadamente.

Artículo 49.- Gestión de capacidades. - Se deberá hacer un estudio sobre el crecimiento poblacional del ISTY, con la finalidad de adquirir los recursos tecnológicos necesarios para que la plataforma Ignug funcione óptimamente.

Artículo 50.- Separación de los recursos de desarrollo, prueba y operación. - Se deberán independizar los entornos de desarrollo, preproducción y producción del Sistema Ignug y la base de datos, para minimizar riesgos de cambios al momento de desarrollar o

ejecutar las pruebas funcionales, no funcionales y de seguridad, se considerará los siguientes puntos:

- Se definirán y documentarán las reglas y configuraciones operativas y de seguridad en todos los servidores.
- Los cambios y actualizaciones deberán realizarse en el servidor de desarrollo, posteriormente subirlos al ambiente de pruebas para la ejecución de pruebas funcionales, no funcionales y de seguridad, previa la puesta en producción.
- Las pruebas no se realizarán en producción.
- Los usuarios utilizarán diferentes credenciales de autenticación para cada entorno.
- La información sensible no se reproducirá en el entorno de pruebas.

Categoría: Protección contra el software malicioso (malware)

Artículo 51.- Controles contra el código malicioso. - Se deberá implementar antivirus que permitan la detección y prevención de código malicioso, se considerarán las siguientes directrices:

- Se prohibirá el uso de software no autorizado
- Se registrarán URLs de sitios web sospechosos en el firewall, con el fin de bloquear las páginas web de dudosa procedencia.
- Se revisarán los ficheros de los datos y de las aplicaciones del Ignug, para encontrar posibles archivos que no pertenezcan a los activos del sistema.
- Se deberá mantener actualizado el sistema operativo de los servidores de desarrollo, pruebas y producción.
- Implementar anti spam en el servidor de correo electrónico de google.
- En el caso de ejecutarse el código malicioso en el servidor de producción, se aplicará el Plan de Continuidad para recuperar los servicios en el menor tiempo posible.

Categoría: Copias de seguridad

Artículo 52.- Copias de seguridad de la información. - El Comité de Dirección, deberá establecer el procedimiento para realizar copias de respaldo de datos, servicios, archivos de configuraciones, código fuente; se considerarán los siguientes aspectos:

- El procedimiento de respaldo definirá la conservación y protección de los activos en mención.
- Se deberán asignar los recursos necesarios para garantizar que los respaldos almacenados sean precisos y completos para ello, se verificará que la data fuente y la de respaldo tengan el mismo tamaño y el mismo hash.
- Los dispositivos en los que se almacenan los respaldos, deberán tener un adecuado tratamiento.
- Se realizarán respaldos manuales cada semana y respaldos automatizados todos los días en horas de bajo tránsito.

Categoría: Registros y supervisión

Artículo 53.- Registro de eventos. - Se deberán registrar eventos de seguridad (*logs*) para garantizar las acciones efectuadas por los usuarios y posibles ciberatacantes.

- Se revisarán los eventos *logs* cada semana y cuando se produzcan eventos de actividades sospechosas, excepciones, incidencias y sucesos de seguridad, se deberán revisar los registros de eventos.
- Los registros deberán contener información como: identificadores del usuario, localización de los dispositivos, actividades ejecutadas en el sistema, fecha y hora, número de intentos de acceso a los recursos de servidores, direcciones y protocolos de red, alarmas mediante la revisión de accesos, habilitación y deshabilitación de los sistemas de protección.

- Se deberán generar eventos de seguridad para redes, servidores, aplicaciones, bases de datos, diferenciándolos por la información capturada.

Artículo 54.- Protección de la información del registro. - Se protegerán los dispositivos y los registros de eventos de seguridad, se tomará en cuenta lo siguiente:

- Los registros de eventos deberán resguardarse contra manipulaciones indebidas, alteraciones del contenido de los *logs*, borrado de la información, accesos no autorizados.
- Se almacenarán en dispositivos físico y virtuales durante 4 años; pasado este tiempo, si no se registraron anomalías en estos logs, se podrán eliminar, caso contrario permanecerán en archivo hasta 7 años.

Artículo 55.- Registros de administración y operación. - Se deberán generar registros de eventos de las tareas realizadas por los responsables de administrar y operar el sistema Ignug y las bases de datos, protegerlos y revisarlos.

Artículo 56.- Sincronización del reloj. - Se deberán sincronizar los relojes de los servidores que alojan a las aplicaciones y la información del SGA Ignug, para que los registros de eventos y generación de reportes reflejen el tiempo real en el que sucedieron acontecimientos.

Categoría: Control del software en explotación

Artículo 57.- Instalación del software en explotación. - El Comité de Dirección, deberá crear procedimientos e implementarlos con el apoyo del UTIC, para controlar los cambios de software.

Se tomarán en cuenta las siguientes directrices:

- Se mantendrán actualizados el sistema operativo y los servidores de alojamiento de la plataforma Ignug, bases de datos, servidores de respaldo.
- Se deberán subir a producción ejecutables y actualizaciones revisadas, luego de haber superado exhaustivas pruebas de funcionalidad, técnicas y de seguridad.
- Se conservarán versiones anteriores, para realizar *rollback,* en el caso de que en la implementación del software algo saliese incorrecto.
- Se mantendrán registros de auditorías de las actualizaciones de las bibliotecas y dependencias.

Categoría: Gestión de la vulnerabilidad técnica

Artículo 58.- Gestión de las vulnerabilidades técnicas. - Se deberá realizar análisis de debilidades de los módulos del Ignug implementados y en desarrollo, con el fin de evaluar el grado de vulnerabilidad de los sistemas y adoptar las salvaguardas respectivas de acuerdo al nivel de amenaza.

Se tomará en cuenta un proceso adecuado tanto para el análisis como para implementar las protecciones:

- Para desarrollos nuevos, el análisis de vulnerabilidades deberá realizarse en la fase de despliegue, para controlar las vulnerabilidades reportadas en el informe según el nivel de criticidad de las mismas:

  Nivel alto. - Las vulnerabilidades de grado alto, deberán ser controlas de forma inmediata, puesto que, si llegara a materializarse una amenaza por medio de dichas vulnerabilidades, el grado de afectación a los activos del Sistema Ignug y por ende al ISTY, serían muy alta.

  Nivel medio. - Las vulnerabilidades de grado medio, deberán ser controlas a corto plazo, es decir en el lapso de una semana.

Nivel bajo. - Las vulnerabilidades de grado alto, deberán ser controlas a largo plazo o se podrán considerar como riesgos residuales, debido a que la afectación del activo es muy baja.

- Para desarrollos nuevos, el análisis de vulnerabilidades deberá realizarse en las fases de operación, con el fin de verificar que las salvaguardas implementadas a los módulos que se integrarán a la plataforma Ignug sean resistentes ante cualquier ataque.
- Se deberán realizar pruebas de penetración a los módulos de producción del Ignug, previo a la realización de respaldos y puesta en servidor de pruebas, una vez que se solventen las vulnerabilidades en el ambiente de preproducción, se deberán solucionar en producción.
- Las salvaguardas se deberán implementar tanto en los sistemas y bases de datos del Ignug, como en los servidores de desarrollo, pruebas y producción donde se los aloja.

Artículo 59.- Restricción en la instalación de software. - Se deberá restringir la instalación de herramientas informáticas a usuarios que no sean administradores, para evitar fallas de instalación y la contaminación de código malicioso; el principio que se implementará es el de separación de privilegios.

Categoría: Consideraciones sobre la auditoria de sistemas de información

Artículo 60.- Controles de auditoría de sistemas de información. - El Comité de Dirección deberá establecer un proceso para la realización de auditorías internas, con el fin de verificar el cumplimiento de las actividades de la presente Política y encontrar falencias y superarlas. Las auditorías internas, aportarán con el éxito de las externas.

Se deberá cumplir las siguientes directrices:

- Las actividades del procedimiento de auditoría serán debidamente planificadas y socializadas con dos semanas de anticipación a la Dirección Ejecutiva, con el propósito de tener todo lo solicitado en el momento de la auditoría.
- Las partes deberán acordar el alcance de la auditoría.
- Al momento de la auditoría, deberán estar presentes las dos partes que intervienen en el procedimiento.
- Las comprobaciones serán realizadas por los usuarios responsables de la información y los servicios que brinda el SGA Ignug, los miembros de la Dirección Ejecutiva, serán observadores o podrán intervenir en presencia y bajo supervisión del custodio del activo.
- Al finalizar la auditoría, el Comité de Dirección emitirá un informe con las respectivas observaciones de mejora de la aplicación de la Política.
- La Dirección Ejecutiva, deberá remediar las observaciones emitidas en el informe.
- Finalmente, la Dirección Ejecutiva hará conocer al Comité de Dirección sobre las remediaciones realizadas.

Capítulo 9: Seguridad de las comunicaciones

Categoría: Gestión de la seguridad de redes

Artículo 61.- Controles de red. - El Comité de Dirección establecerá el procedimiento de seguridad para la protección de las redes *Fast Ethernet* y *Wifi* del ISTY, con el fin de salvaguardar la información y los módulos del SGA Ignug.

Se deberán considerar los siguientes aspectos:

- Se definirá responsabilidades para la administración de los equipos de las redes; sin embargo, se deberá tomar en cuenta que la gestión de redes está a cargo de la SENESCYT, por lo tanto, no realizarán cambios a las configuraciones, pero sí

vigilarán que se proporcione el servicio; las inquietudes serán consultadas con el departamento de TIC del ente rector del ISTY.

- El SOC en conjunto con el administrador de redes de comunicaciones, deberán gestionar la protección de las redes mediante técnicas de monitoreo, registro de eventos (*logs),* bitácoras.

Artículo 62.- Seguridad de los servicios de red. - El administrador de redes de comunicaciones deberá implementar seguridades a los servicios de red considerando lo siguiente:

- Configurará el firewall con el fin de filtrar la información entrante y saliente
- Comunicará a TIC de SENESCYT, si los bloqueos de las herramientas implementadas por ejemplo SOPHOS, son efectivos o existen sitios restringidos en los cuales se pueda navegar.
- Con la ayuda de herramientas de monitoreo, se controlará que los módulos del Ignug alojados en el servidor web, estén activos.
- Si un servicio se cae, la Dirección Ejecutiva comunicará sobre dicha anomalía para que se levante lo más pronto posible la aplicación en problemas.
- Se registrará las direcciones *MAC,* de los equipos cuyos usuarios tengan permisos de acceso a la gestión de servicios.

Artículo 63- Segregación en redes. - El administrador de redes de comunicaciones deberá verificar que la segregación de los grupos de usuarios esté realizada de acuerdo al organigrama institucional, con el fin de proporcionar mayor ancho de banda a los departamentos estratégicos y a la Unidad de TIC, para el desempeño exitoso de las actividades académicas.

Categoría: Intercambio de información

Artículo 64.- Políticas y procedimientos de intercambio de información. - Será responsabilidad de la Dirección Ejecutiva implementar los procedimientos, para que la data procesada y transportada mediante los dispositivos electrónicos y medios de comunicaciones, esté protegida frente a amenazas internas y externas.

Se considerarán los siguientes aspectos:

- Se deberá proteger la información del sistema Ignug, transferida mediante redes WAN, de interferencia, duplicados, alteración, fallas, desvío de enrutamiento y destrucción, mediante la implantación de herramientas de detección de intrusos.
- Se deberán instalar herramientas de prevención de intrusos, con el fin de salvaguardar la información de código malicio *malware.*
- Por lo general, se deberá mantener privada la información sobre las personas que gestionan las aplicaciones, bases de datos de SGA Ignug, para evitar posibles ataques intencionados como: acoso, extorción, suplantación de identidad, ingeniería social, entre otros.
- Se usará técnicas criptográficas para encriptar la información de carácter confidencial.

Artículo 65.- Acuerdos de intercambio de información. - El Comité de Dirección, establecerá acuerdos de intercambio de información, tomando en cuenta las siguientes indicaciones:

- Se registrarán eventos de seguridad (logs) con el fin de rastrear la información de los usuarios que ingresan al módulo “Bolsa de Empleo” de la plataforma Ignug.
- Se garantizará el no repudio, mediante la implementación de firmas digitales.
- Los usuarios externos como Empresas Formadoras, deberán constar en el Sistema de Gestión de Usuarios, con el rol y privilegios asignados para acceder a las

funcionalidades mediante un identificador ID de acuerdo al perfil otorgado por la Dirección Ejecutiva.

- Los datos registrados por parte de las empresas, se consideran datos de difusión limitada, por lo tanto, deberán ser encriptados.

Artículo 66.- Mensajería electrónica. - Se deberán proteger los mensajes intercambiados mediante el correo institucional, redes sociales del ISTY y los servicios que brinda el Sistema Ignug; para la defensa de la información.

- Se deberá asegurar el correcto enrutamiento de los mensajes para garantizar la fiabilidad, característica complementaria de la seguridad.
- Se deberá concientizar a los usuarios que forman parte de la comunidad educativa Yavirac, para que cuiden las credenciales de autenticación, tanto del correo electrónico como de los servicios que proporciona el Sistema Ignug para evitar la suplantación de identidad.

Artículo 67.- Acuerdos de confidencialidad o no revelación. – El CISO deberá elaborar formatos de confidencialidad, los mismos que se aprobarán por el Comité de Dirección; en los cuales constará detalladamente lo siguiente:

- Descripción de la información sensible que contiene el Sistema Ignug, como notas, pases de año, récords académicos.
- El tiempo en el cual se le permitirá el acceso a los servicios y datos del Ignug.
- Responsabilidades del personal que accede a los recursos de la plataforma Ignug.
- Sanciones en diferentes escalas, según sea el caso al cometer delitos de robo, edición, fuga, eliminación de información:

  Si la amenaza no es intencional, la sanción será leve, sin embargo;

  Si la materialización de la amenaza es intencionada la sanción será grave

En los dos casos se ejecutará el procedimiento de sanción correspondiente.

- Si la situación lo amerita, se le auditará tanto el equipo como la usabilidad de la data y los servicios.

Capítulo 10: Adquisiciones, desarrollo y mantenimiento de los sistemas de información

Categoría: Requisitos de seguridad en los sistemas de información

Artículo 68.- Análisis de requisitos y especificaciones de seguridad de la información. – La Dirección Ejecutiva, deberá implementar el uso de buenas prácticas de seguridad durante la fase de análisis de requisitos, con el fin de minimizar las vulnerabilidades de los nuevos desarrollos a integrase con el SGA Ignug.

Constarán las siguientes prácticas de seguridad:

- Casos de abuso. - Los analistas de los módulos del Ignug, deberán analizar funcionalidades que las aplicaciones no deben cumplir; identificarán los objetivos de seguridad, identificarán los puntos susceptibles y las amenazas de seguridad a ser neutralizadas por el Ignug; además, definirán restricciones o requisitos negativos del SGA.
- Ingeniería de requisitos de seguridad. - se distinguirán los requisitos servicios de seguridad que garanticen la confidencialidad, integridad, disponibilidad, autenticación, autorización y trazabilidad; adicional, se identificarán los servicios de gestión de sesiones, gestión de errores, excepciones y recuperación de las características de la seguridad; servicios operacionales como entornos de producción, gestión de configuraciones, interoperabilidad, validaciones y política a cumplir.
- Modelado de ataques. - los analistas de sistemas se orientará en dos perspectivas, del defensor y del atacante, con el objetivo de estudiar el pensamiento de los ciberatacantes

e implementar los controles de seguridad adecuados conforme a los resultados obtenidos a través del uso de patrones de diseño o árboles de ataque.

Artículo 69.- Asegurar los servicios de aplicaciones en redes públicas. - La plataforma Ignug, al encontrarse alojada en un servidor virtual a través de la contratación de servicios en la nube, cuya información es transmitida mediante redes WAN e internet, se la deberá proteger de ataques intencionados o errores involuntarios de personas internas y externas al instituto.

Se considerarán los siguientes principios y buenas prácticas:

- Autenticación. - todos los usuarios de los servicios, se deberán autenticar, con el fin de demostrar que son quienes dicen ser.
- Autorización. - se asignarán roles y perfiles a los usuarios.
- Defensa en profundidad. - se introducirán múltiples capas de seguridad con el fin de reducir la visibilidad externa de los componentes del Sistema Ignug, el acceso a la lógica del negocio, al modelo y a las bases de datos.
- Se deberá analizar el tipo de contratación del servicio en la nube, puesto que, alivianará o cargará de actividades de seguridad a los desarrolladores de la Unidad de TIC.

Artículo 70.- Protección de las transacciones de servicios de aplicaciones. - La Dirección Ejecutiva, deberá velar para que las transacciones realizadas por los módulos del Ignug, se efectúen de forma completa, sin errores de enrutamiento, que no sea alterada o reproducida.

La seguridad de las transacciones de los servicios considerará:

- Se asegurará la usabilidad del protocolo de control de transferencia *TCP* del Modelo de Referencia TCP/IP, con el fin de que las transacciones realizadas por el sistema Ignug lleguen a su destinario final de forma íntegra.
- Se deberá contar con el protocolo *HTTPS* a través de la implementación de un certificado SSL, para que toda la información que se transmita mediante el sitio sea cifrada, para garantizar confidencialidad de la información.
- De ser posible, implementar firmas digitales para encriptar los mensajes y asegurar la confidencialidad de los mismos.

Categoría: Seguridad en el desarrollo y en los procesos de soporte

Artículo 71.- Política de desarrollo seguro. - El Comité de Dirección, deberá realizar una Política para adquirir, desarrollar y dar mantenimiento a los módulos nuevos del Sistema Ignug; hará constar una metodología de desarrollo de software seguro, incluyendo las especificaciones de seguridad en cada una de las etapas del S-SDLC:

Se considerarán las siguientes prácticas de seguridad, en cada fase del ciclo de vida de desarrollo de software:

- Casos de abuso
- Ingeniería de requisitos de seguridad
- Análisis de riesgo arquitectónico
- Patrones de diseño
- Pruebas de seguridad basados en riesgo
- Modelado de ataques
- Revisión de código
- Pruebas de penetración
- Configuraciones seguras

- Operaciones de seguridad
- Revisión externa

Artículo 72.- Procedimiento de control de cambios en sistemas. – El CISO, realizará un formato de cambios, que será aprobado por el Comité de Dirección, con el fin de registrar las actualizaciones de los módulos y la base de datos del Sistema Ignug.

Se deberán tomar en cuenta las siguientes indicaciones:

- El Comité de Dirección, aprobará los cambios de acuerdo a las necesidades del ISTY.
- Se levantarán los requerimientos, mediante un documento de especificación de requerimiento o, a su vez historias de usuarios.
- Para el desarrollo de los cambios, actualizaciones o nuevos módulos del Ignug, se aplicará una metodología tradicional o ágil, de forma rigurosa, siguiendo todos los pasos del ciclo de vida de desarrollo de software.
- Se aplicarán principios de diseño y buenas prácticas de un software seguro.
- Mediante el documento en mención, se solicitará la subida a producción con la especificación de las modificaciones realizadas.

Artículo 73.- Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. – La Dirección de Ejecución, revisará que las aplicaciones no sufran efectos adversos después de actualizar el sistema operativo o instalar herramientas críticas en él, para que los activos de la información y servicios que brinda el SGA Ignug, sean íntegros y estén disponibles.

Artículo 74.- Restricciones a los cambios en los paquetes de software. – EL SOC, supervisará que las actualizaciones de paquetes en el servidor virtual de Contabo, se ejecuten de acuerdo a las herramientas de desarrollo y de implementación del servidor en el que se encuentra alojado el SGA Ignug.

Artículo 75.- Principios de ingeniería de sistemas seguros. - El Comité de Dirección, deberá hacer constar en la Política de Adquisición, Desarrollo y Mantenimiento de las actualizaciones o desarrollo de módulos nuevos del Sistema Ignug, principios de diseño de seguridad de software.

Se aplicarán los siguientes principios de diseño:

- Defender en profundidad
- Diseño simple
- Poco privilegio
- Independencia de privilegios
- Dispersión de dominios
- Aislamiento código, ejecutables, datos, configuración y programa
- Entorno de producción o ejecución inseguro
- Registro de eventos de seguridad
- Fallar de forma segura
- Diseñar un software resistente
- Seguridad por oscuridad es un error
- Seguridad por defecto

Artículo 76.- Entorno de desarrollo seguro. - El Comité de Dirección, registrará en la Política de Adquisición, Desarrollo y Mantenimiento de las actualizaciones o creación de módulos nuevos del Sistema Ignug, la protección adecuada del ambiente de desarrollo seguro; incluirá al personal de desarrollo y manejo de la infraestructura virtual contratado por le ISTY.

Se tomarán en cuenta los siguientes aspectos:

- En primera instancia, se programará en los equipos designados a los desarrolladores.

- Los programadores actualizarán y sincronizarán el código fuente en una rama del repositorio de versiones virtual *GIT HUB*.
- El Coordinador de TIC, revisará la estructura y el código fuente del nuevo desarrollo mediante herramientas automatizadas acorde al framework y lenguaje de programación usados, con el fin de subir a la raíz del repositorio; si hubiese algún error, deberá hacer *rollback* y enviar un mensaje a través de *GIT HUB*, a los programadores para que realicen las correcciones pertinentes.
- El Coordinador de TIC integrará el nuevo producto al entorno de pruebas, con el fin de realizar las pruebas funcionales; la integración la podrá hacer con el uso de herramientas automatizadas.

Artículo 77.- Pruebas funcionales de seguridad de sistemas. - La Dirección Ejecutiva, a través del SOC, llevará a cabo pruebas de seguridad funcionales de las actualizaciones o desarrollo de los módulos del Ignug, para asegurar que el sistema funcione.

Se considerarán las siguientes prácticas:

- Análisis de riesgo arquitectónico. - se identificará el riesgo en los componentes del SGA Ignug para mitigarlo.
- Pruebas de seguridad basados en riesgo. - se contemplarán dos tipos de aproximaciones: evaluaciones de seguridad funcionales y pruebas de seguridad desde la perspectiva del atacante.
- Modelado de ataques. - se orientarán en dos perspectivas, del defensor y del atacante, con el objetivo de estudiar el pensamiento de los ciberatacantes e implementar los controles de seguridad adecuados conforme a los resultados obtenidos en las pruebas.
- Revisión externa. - será considerará la realización de pruebas por parte de personal ajeno al equipo de desarrollo, con el fin de descubrir algún riesgo residual existente.

Artículo 78.- Pruebas de aceptación de sistemas. - La Dirección Ejecutiva, a través del SOC, llevará a cabo pruebas de aceptación de las actualizaciones o desarrollo de los módulos del Ignug, se tomará en cuenta lo siguiente:

- Se verificarán si las actualizaciones o desarrollo de los módulos del Ignug, cumplen con las necesidades de seguridad y con la implementación de las prácticas de desarrollo seguro.
- Se podrán usar herramientas automatizadas para realizar análisis al código fuente, para la implantación de controles de seguridad.
- Se podrán usar herramientas automatizadas para realizar el escaneo de vulnerabilidades, como el *Alient Volt.*
- Las pruebas de aceptación, se realizarán en un ambiente de pruebas seguro para asegurar fiabilidad en los resultados obtenidos.

Categoría: Datos de prueba

Artículo 79.- Protección de los datos de prueba. - La Dirección Ejecutiva, a través del SOC, velará para que las pruebas se realicen con datos de pruebas, puesto que, si se realizan con datos reales descargados de la base de datos de producción, se infringirá con la confidencialidad de la información. Se recomienda lo siguiente:

- Si se necesitara la data de producción, se deberá solicitar permisos al Comité de Dirección, con el objetivo de que la data a descargase en el ambiente de pruebas no sea de carácter sensible.
- Las pruebas se deberán realizar en un ambiente de pruebas.
- Al finalizar las pruebas, los datos de pruebas, se deberán borrar del servidor.

Capítulo 11: Relación de proveedores

Categoría: Seguridad en las relaciones con proveedores

Artículo 80.- Requisitos de seguridad en contratos con terceros. – El Comité de Dirección, establecerá un procedimiento respecto a la seguridad en contratos con terceros, considerando todos los requerimientos de la seguridad de la información de los activos del SGA Ignug.

Se deberá incluir lo siguiente:

- Descripción y clasificación de la información
- Requisitos legales, incluyendo salvaguardas a los datos personales y derechos de autor.
- Obligación contractual de las dos partes, para implementar los controles de seguridad, como: de acceso, evaluación del desempeño,
- Concienciación sobre las indicaciones y requisitos de seguridad; gestión de accidentes informáticos.
- Derechos para auditar a los proveedores y los controles relacionados con el acuerdo.
- Obligaciones del proveedor en cumplimiento de seguridad, estipulado en el contrato y entrega de un informe mensual sobre la certeza de los controles.

Categoría: Gestión de la provisión de servicios del proveedor

Artículo 81.- Control y revisión de la provisión de servicios del proveedor. – El Comité de Dirección, incluirá en el procedimiento a la seguridad en contratos con terceros, los derechos de controlar, revisar y auditar los servicios otorgados por terceros

Se deberán realizar las siguientes tareas:

- Supervisar los niveles de rendimiento del servicio contratado.

- Revisar los informes realizados por el proveedor respecto a los servicios otorgados y los aspectos de seguridad de la información.
- Organizar reuniones periódicas.
- Informar sobre indecentes, resolver y detectar problemas suscitados.
- Asegurar que el proveedor mantenga los recursos suficientes, para avalar la continuidad de los servicios que proporciona el SGA Ignug.

Artículo 82.- Gestión de cambios en la provisión del servicio del proveedor. - El Comité de Dirección, incluirá en el procedimiento a la seguridad en contratos con terceros, el cambio del proveedor del servicio.

Se deberán considerar los siguientes aspectos:

- Modificaciones en los contratos con proveedores
- Cambios a implementarse, por la modificación de procesos del IST Yavirac.
- Cambios en los servicios de los proveedores por la adquisición y actualización de productos, herramientas y servidores.
- El cambio y subcontratación con otros proveedores.

Capítulo 12: Gestión de incidentes de seguridad de la información

Categoría: Gestión de incidentes de seguridad de la información y mejoras

Artículo 83.- Responsabilidades y procedimientos. - El Comité de Dirección, realizará el procedimiento del tratamiento adecuado de los incidentes de la información, asignando responsabilidades mediante las siguientes directrices:

- Se realizarán procedimientos y establecerán responsables para la elaboración del plan y preparación de la respuesta a incidentes; para monitorizar, detectar, analizar y comunicar fallas de seguridad de la información; registrar eventos de incidentes,

manejo de pruebas forenses; evaluación, toma de decisiones y respuesta de recuperación controlada y comunicación al Comité de Dirección.

- Establecer formatos para el registro de eventos de seguridad.
- Crear procedimientos con respecto al proceso disciplinario, el mismo que deberá basarse en el Reglamento Disciplinario del ISTY; además, reportar a la Policía Judicial PJ, para que se le aplique el COIP.
- Establecer procesos de retroalimentación.

Artículo 84.- Notificación de los eventos de seguridad de la información. - El Comité de Dirección, establecerá un procedimiento de notificación de eventos de seguridad de la información, por los canales oficiales del ISTY. El personal responsable, es decir, el Comité de Seguridad de la Información, deberán comunicar cualquier evento de seguridad inmediatamente éste sea detectado.

Se tomarán en cuenta las siguientes situaciones:

- Verificación ineficaz de los controles de seguridad, que afectan a la integridad, disponibilidad y confidencialidad.
- Errores humanos, incumplimientos de políticas o directrices.
- Cambios inesperados del software y violaciones de acceso.
- En el Ecuador, los eventos de seguridad se notifican al Centro de respuesta a incidentes informáticos del Ecuador ECUCERT.

Artículo 85.- Evaluación y decisión sobre los eventos de seguridad de información. - El Comité de Dirección, incluirá en el procedimiento de notificación de eventos, la evaluación de los mismos y si se clasifican como fallas de seguridad, de acuerdo a una escala de clasificación.

Artículo 86.- Respuesta a incidentes de seguridad de la información. - La Dirección Ejecutiva elaborará un informe con la notificación de los eventos de seguridad para su respuesta al Comité de Dirección y al ECUCERT.

Los responsables de dar la respuesta solicitarán lo siguiente:

- Evidencias del incidente, realización de un análisis forense si es posible, escalado del incidente.
- Comunicación del suceso de seguridad, tratamiento de las vulnerabilidades encontradas que pudieran causar un incidente.
- Cuando el incidente se haya controlado, cierre y registro formal del mismo.

Artículo 87.- Aprendizaje de los incidentes de seguridad de la información. - A partir del análisis y resolución de los incidentes de seguridad informática, mediante mecanismos que permitan cuantificar el grado de afectación y el coste de los incidentes, se deberán usar para identificar eventualidades recurrentes e implementar los controles adecuados que reduzcan las amenazas en el futuro.

Artículo 88.- Recopilación de evidencias. - El Comité de Dirección, incluirá en el procedimiento de notificación de eventos de seguridad de la información, el proceso para recopilar evidencias. Se deberá considerar lo siguiente:

- La cadena de custodia
- Que la evidencia sea íntegra
- Responsabilidades de las personas y su competencia
- Documentación y un resumen

Capítulo 13: Aspectos de seguridad de la información para la gestión de la continuidad de negocio

Categoría: Continuidad de la seguridad de la información

Artículo 89.- Planificación de la continuidad de la seguridad de la información. - El Comité de Dirección, elaborará el Plan de Continuidad de la Seguridad de la Información, determinará las necesidades de seguridad de la información y de continuidad en situaciones críticas. Para la construcción del Plan, se deberá basar en las Normas ISO/IEC 27031, ISO 22313 e ISO22301.

Artículo 90.- Implementar la continuidad de la seguridad de la información. - La Dirección Ejecutiva, deberá implementar el plan del Artículo 89, con el apoyo del UTIC.

Artículo 91- Verificación, revisión y evaluación de la continuidad de la seguridad de la información. - El Comité de Dirección verificará, revisará y evaluará que se cumpla con la gestión del Plan de Continuidad.

Categoría: Redundancias

Artículo 92- Disponibilidad de los recursos de tratamiento de la información. - El Comité de Dirección, deberá contemplar en el Plan de Continuidad, redundancia de los servicios críticos que son la razón de ser del ISTY; deberán identificarlos y probar el aseguramiento de la conmutación, para garantizar la disponibilidad del servicio en el caso que el principal no estuviera disponible.

Capítulo 14: Cumplimiento

Categoría: Cumplimiento de los requisitos legales y contractuales

Artículo 93.- Protección de los registros de la organización. - El Comité de Dirección, deberá implementar procedimientos para proteger los registros de los

esquemas de la base de datos del Ignug, contra pérdida, destrucción, falsificación, divulgación, accesos no autorizados.

Artículo 94.- Protección y privacidad de la información de carácter personal. - El Comité de Dirección, deberá incluir en el procedimiento del Artículo 93, la protección y la privacidad de los datos de carácter personal, dicho procedimiento se socializará a las autoridades, coordinadores académicos, coordinadores de carrera y a la Dirección Ejecutiva para su cumplimiento.

Categoría: Revisiones de la seguridad de la información

Artículo 95.- Revisión independiente de la seguridad de la información. - El Comité de Dirección, deberá revisar la Política cada año, con la finalidad de incluir mejoras, de acuerdo a las necesidades de los cambios en el ISTY.

Artículo 96.- Cumplimiento de las políticas y normas de seguridad. - El Comité de Dirección, deberá velar para que la presente Política se implemente a partir de su aprobación; revisará cada año el cumplimiento de procesos y procedimientos a través de la Dirección Ejecutiva.

Artículo 97.- Comprobación del cumplimiento técnico. - El Comité de Dirección, verificará cada semestre que el SGA Ignug, cumpla con la Política presente y normas de seguridad de la información del ISTY; para esto, se apoyará con herramientas de escaneo automáticas y pruebas de penetración que encuentren vulnerabilidades que emitan informes técnicos sobre el estado de la plataforma, los resultados se deberán usar para proteger los puntos críticos de la aplicación.

5.5 Presentación del Modelo

En el Modelo de Ciberseguridad propuesto, se han identificado cuatro pasos a seguir para mejorar la seguridad del problema actual que tiene el SGA Ignug, por lo cual es emergente que se creen las áreas de Seguridad de la Información y Ciberseguridad que se encarguen de ejecutar las fases del estándar indicado, tal como refleja la Figura Nº 13.

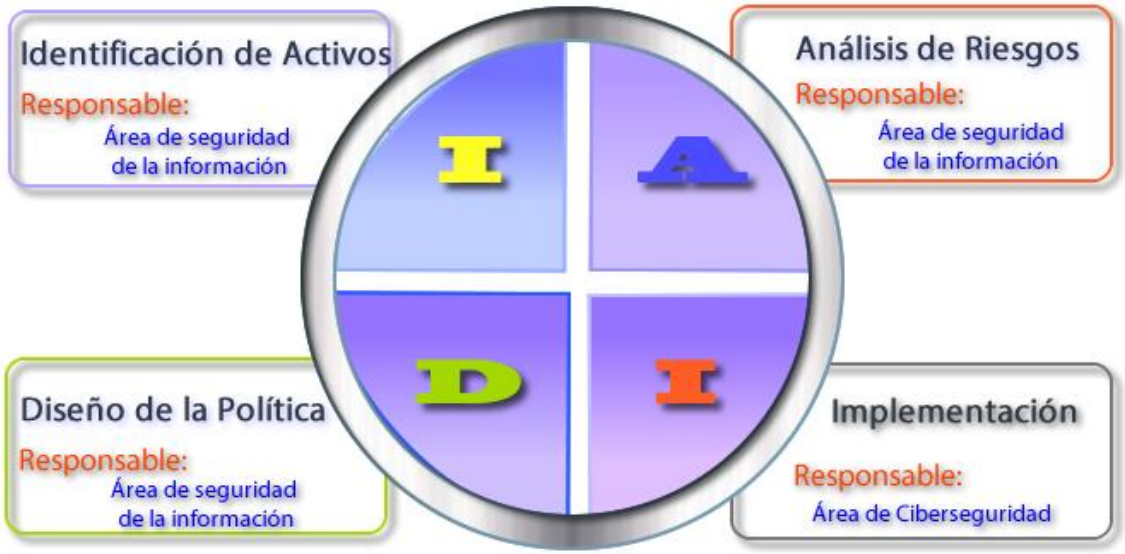

Figura 13: Modelo de Ciberseguridad
Fuente: Creación propia

[I] Identificación de Activos. – El modelo inicia con la identificación de todos los activos de información y de servicios, de acuerdo al análisis y situación actual del Sistema de Gestión Académico Ignug, logrando identificar los siguientes activos: infraestructura, aplicaciones informáticas, datos de información, equipos de informática, soportes de información y el personal relacionado con la administración de la plataforma.

[A] Análisis de Riesgos. – Para el desarrollo del Análisis de Riesgos se aplica la Metodología Magerit, ejecutando siguientes los pasos:

- Activos. - Los activos antes identificados se los clasifica de acuerdo a un esquema de dependencias, valorándolos según las dimensiones de seguridad como son: integridad, confidencialidad, disponibilidad, autenticidad y trazabilidad.

- Amenazas. – Se identifican las amenazas de cada activo y la dimensión comprometida, se las valora de acuerdo a la degradación y a la probabilidad de ocurrencia; se estima el impacto potencial considerando las variables degradación y valor del activo; finalmente, se calcula el riesgo tomando en cuenta la probabilidad de ocurrencia por el impacto.

Se analizan los riesgos de los activos representándolos en el mapa de calor de riesgos, para identificarlos en la zona roja, lo cual significa que estos activos son críticos y necesitan una atención inmediata.

- Salvaguardas. – Se seleccionan las salvaguardas tomando en cuenta el tipo de activo a proteger, la dimensión de seguridad que requiere ser resguardada, las amenazas de las que se debe defender al activo, centrándose en el valor del activo, la probabilidad de que ocurra una amenaza de acuerdo a los riesgos relevante de la zona roja del mapa de calor.

[D] Diseño de la Política. – En la política generada se seleccionaron los controles más apropiados de la Norma ISO/IEC 27002:2017, de acuerdo a la realidad del instituto y en función de los riesgos analizados en el paso anterior. La guía se constituye de 14 capítulos y 97 artículos; considera las directrices de gestión de seguridad de la información del ISTY, toma en cuenta la seguridad respecto a los recursos humanos, la gestión de activos, el acceso a los servicios, cifrado de datos, protección de los equipos en los que se encuentran alojados los datos y aplicaciones, seguridad de las operaciones y comunicaciones, seguridad en el desarrollo y mantenimiento de los sistemas informáticos, la gestión de proveedores y continuidad del negocio; finalmente, contiene artículos sobre

la garantía del cumplimiento de la política para avalar la seguridad de los activos del SGA Ignug del ISTY.

[I] Implementación. - Es responsabilidad del IST Yavirac que adopte el Modelo de Seguridad IADI, para lo cual es emergente crear el Área de Ciberseguridad de TIC que lo implemente. Para ejecutar el estándar, se recomienda seguir procedimientos explicando los trabajos a realizarse mediante ventanas de mantenimiento para no afectar a la libre continuidad de los servicios

Las autoridades del ISTY, deberán crear las siguientes áreas de seguridad con el fin de cumplir el Modelo IADI.

Área de Seguridad de la Información: Integrada por:

Comité de Dirección. - Área estratégica, encargada de aprobar, actualizar y socializar la política, crear otras políticas indicadas en los artículos de la guía propuesta, crear procedimientos de seguridad y socializar a la comunidad educativa.

- **CISO:** Responsable de definir toda la seguridad del instituto, planteará estrategias, programas, políticas y procedimientos para proteger los activos del ISTY.
- **Rector**: Máxima autoridad del ISTY, responsable de aprobar las estrategias, programas, políticas y procedimientos propuestos por el CISO.
- **Vicerrector:** Segunda autoridad del ISTY, responsable de revisar las estrategias, programas, políticas y procedimientos propuestos por el CISO.

Área de Auditoría. - Área estratégica, velará por el cumplimiento de la seguridad de los activos del ISTY; en vista que no se cuenta con personal técnico con los conocimientos de seguridad de la informática, el CISO y el Área de Seguridad Informática de SENESCYT, serán quienes auditen el cumplimiento de los controles.

- **CISO:** Responsable de supervisar el cumplimiento de Modelo completo de seguridad.
- **Área de Seguridad informática de SENESCYT:** Ente rector del ISTY, responsable de supervisar por el cumplimiento de los controles de la política de seguridad de la información.

Área de Ciberseguridad: Integrada por:

Dirección Ejecutiva. - Área táctica operacional, encargada de implementar los controles de la política. Estará integrado por los siguientes miembros:

- **SOC:** Encargado de liderar el Área de Ciberseguridad y el equipo de seguridad de TIC.
- **Unidad de TIC:** Encargado de implementar el Modelo de Ciberseguridad.

En el presente trabajo de titulación, se mencionan términos de Seguridad Informática y Ciberseguridad, refiriéndose a la misma definición, ya que las dos se encargan de la protección de los activos de información y de servicios digitales que son trasmitidos a través de dispositivos de comunicación electrónica.

El Modelo de Ciberseguridad IADI, es una guía a largo plazo que soluciona el tratamiento de los riesgos encontrados en los activos de información y de servicios que provee el SGA Ignug. Puesto que, en el análisis de riesgos, se encontraron muchas amenazas y vulnerabilidades de carácter crítico, siendo necesario mitigarlos inmediatamente, se presenta un Plan a corto plazo, con el fin de mitigar los problemas relacionados a la ciberseguridad.

5.6 Plan a corto plazo

Se plantea el siguiente Plan a corto plazo como complemento al modelo diseñado; puesto que no se cuenta con el personal suficiente para realizar las actividades que ejecuta la Unidad de TIC, con el objetivo que se implemente inmediatamente para mitigar las amenazas y vulnerabilidades de los activos críticos encontrados en el análisis de riesgos.

[D] Datos /[info] Información:

Tabla 36

Selección de salvaguardas para los activos críticos de información del Sistema Ignug

[D] Datos /[info] Información:		**Amenaza**		**Vulnerabilidad**	**Controles ISO/27002:2017**
[per]	Bases de datos con información personal de los estudiantes	[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	Documentación de procedimientos de operación, según el artículo 47, el SOC redactará un manual de instalación y configuración de los pasos a los diferentes entornos de desarrollo.
[C]	**Nivel confidencial:**	[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	Gestión de privilegios de acceso, según el Artículo 30: - Mínimo privilegio: restringir los privilegios necesarios para el desempeño de las tareas autorizadas. - Separación de privilegios: asignar un rol para acceder a un subconjunto de funciones y datos necesarios. - Separación de dominios: minimizar la probabilidad de que los atacantes accedan a los objetos de datos. - Derechos de privilegios mediante un ID por usuario.
[fich]	Archivos	[A.6]	Abuso de privilegio de acceso	Ausencia de control de eventos *logs*	
[backup]	Copias de respaldo	[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	
[int]	Datos de gestión interna				
[paswd]	Credenciales: contraseñas				
[auth]	Datos de validación de credenciales				
[conf]	Datos de configuración del sistema	[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	El CISO elaborará el formato del Acuerdo de Confidencialidad tomando en cuenta las indicaciones del Artículo 67 de la política, para las personas encargadas de administrar los datos y servicios.
[exe]	Código ejecutable	[A.15]	Modificación deliberada de la información	Ausencia de control en la desvinculación del personal	Retirada o reasignación de los derechos de acceso, según el Artículo 32 se eliminarán los permisos de acceso a los datos a los docentes que finalizan el contrato o a los estudiantes que se retiran de la institución, con el fin de que la información no sea corrompida o saboteada.
[R]	**Difusión limitada:** matrices de rendimiento académico, registros de notas, récords académicos, asistencia; datos de las empresas	[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	
		[E.3]	Errores de monitorización (log)	Ausencia de implementación, seguimiento y lectura a los *logs.*	Registro de eventos, según el Artículo 53, se generarán eventos de seguridad para verificar las acciones de los ciberatacantes, el registro contendrá la información indicada en el artículo en mención.
[log]	Registro de actividad	[A.4]	Manipulación de la configuración	Falta de procedimiento formal para la supervisión del registro del SGSI	Gestión de cambios, se trabajará con la matriz RACI, conforme a las indicaciones del Artículo 48 de la política propuesta.

Fuente: Elaborado por el autor, en referencia a los controles del Modelo de Seguridad propuesto

[S] Servicios:

Tabla 37

Selección de salvaguardas de los servicios prestados y subcontratados

[serv] Servicios:		**Amenaza**		**Vulnerabilidad**	**Controles ISO/27002:2017**
[S.ext] Externos / [S.int] Internos					
[ext]	Usuarios externos: empresas formadoras	[A.11]	Acceso no autorizado	Contraseñas inseguras	Gestión de privilegios de acceso, según el Artículo 30: - Mínimo privilegio: restringir los privilegios necesarios para el desempeño de las tareas autorizadas. - Separación de privilegios: asignar un rol para acceder a un subconjunto de funciones y datos necesarios. - Derechos de privilegios mediante un ID por usuario.
[int]	Usuarios Internos: matriculación, gestión de notas, registro	[A.7]	Uso no previsto	Ausencia de registro de control en el acceso a los datos	
[file]	Almacenamiento de archivos				
[gesu]	Gestión usuarios	[A.5]	Suplantación de la identidad del usuario	Contraseñas predecibles o inseguras	Según el Artículo 26, sobre el control de acceso, se utilizará la autenticación multifactor para todos los accesos administrativos, que incluirá varias de técnicas, como certificados, tokens de contraseña, etc.
[idm]	Gestión identidades				
[ipm]	Gestión privilegios				
[ftp]	Transferencia de archivos	[A.19]	Divulgación de información	Falta implementar el certificado SSL	De acuerdo al Artículo 70 sobre la protección de las transacciones de servicios de aplicaciones, se asegurará la conexión mediante cifrado implementando un certificado SSL.
[edi]	Intercambio electrónico de datos				
[S.sub] Subcontratados a terceros					
[vhost]	Hosting virtual de Contabo	[I.5]	Avería de origen físico o lógico	Fallo en los equipos informáticos	Mantenimiento de los equipos, del Artículo 44 de la política propuesta: - Se revisará la parte contractual del servidor virtual con el proveedor, con el fin de que Contabo se encargue de la seguridad del sistema, mientras se implementa el modelo de seguridad propuesto. - Se recomienda contratar PaaS, plataforma como servicio, puesto que el proveedor entrega una plataforma al cliente con hardware, sistema operativo y middleware con las APIS para que el cliente instale la aplicación.
		[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	Documentación de procedimientos de operación del Artículo 47: - El SOC redactará un manual de paso a producción incluyendo los pasos de instalación, configuración y seguridad. - El paso a producción será mediante integración continua, para minimizar la intervención manual, para evitar riesgos en la carga de los módulos.
		[A.6]	Abuso de privilegio de acceso	Ausencia de control de eventos *logs*	Gestionar los privilegios de acceso, según el Artículo 30 de la política propuesta

Fuente: Elaborado por el autor, en referencia a los controles del Modelo de Seguridad propuesto

[SW] Aplicaciones:

Tabla 38

Selección de las salvaguardas de las aplicaciones que integran el Sistema Ignug

[SW] Aplicaciones:		**Amenaza**		**Vulnerabilidad**	**Controles Norma ISO/27002:2017**
[prp] Desarrollo propio / [std] Estándar					
[sgai]	Sistema de gestión académica Ignug	[E.2]	Errores del administrador	Ausencia de manuales de instalación y configuración	Según el Artículo 47, sobre la documentación de procedimientos de operación se realizará lo siguiente: - El SOC redactará un manual de paso a producción incluyendo los pasos de instalación, configuración y seguridad. - Se implementará el paso a producción mediante integración continua, con el fin de minimizar la intervención manual, para evitar riesgos en el paso a producción.
[bddi]	Base de datos "ignug_bdd"				
[backup]	Sistema de backup	[E.19]	Fugas de información	Ausencia de controles en asignar perfiles de usuario	El CISO elaborará el Acuerdo de Confidencialidad tomando en cuenta las indicaciones del Artículo 67 de la política, para las personas encargadas de administrar los datos y servicios.
[app]	Servidor de aplicaciones apache	[E.20]	Vulnerabilidades de los programas (software)	Ausencia de escaneo y actualizaciones	Gestión de las vulnerabilidades técnicas, según el Artículo 58, se realizarán pruebas de penetración que emitan informes técnicos sobre el estado de la plataforma, con el fin de encontrar vulnerabilidades cuyos resultados se deberán usar para proteger los puntos críticos de la aplicación.
[dmbs]	Sistema de gestión de base de Datos Postgres				
[file]	Servidor de archivos	[A.5]	Suplantación de la identidad del usuario	Contraseñas débiles o predecibles	Según el Artículo 26, sobre el control de acceso, se utilizará la autenticación multifactor para los accesos administrativos, que incluirán técnicas, como certificados, tokens de contraseña, etc.
[os]	Sistema Operativo Ubuntu server	[A.6]	Abuso de privilegios de acceso	Ausencia de control de eventos	Gestión de privilegios de acceso, según el Artículo 30: - Mínimo privilegio: restringir los privilegios necesarios para el desempeño de las tareas autorizadas. - Separación de privilegios y dominios. - Derechos de privilegios mediante un ID por usuario.
		[A.11]	Acceso no autorizado	Ausencia de implementación de contraseñas fuertes	
		[E.18]	Destrucción de información	Ausencia de controles de procesos de eliminación	
		[A.15]	Modificación deliberada de la información	Ausencia de procedimientos de desvinculación de los empleados	Retirada o reasignación de los derechos de acceso, según el Artículo 32, se eliminarán los permisos de acceso a los datos a los docentes y estudiantes que cesen sus actividades en el instituto para que la información no sea corrompida o saboteada.
		[A.18]	Destrucción de información	Ausencia de control en las cuentas dadas de baja	

Fuente: Elaborado por el autor, en referencia a los controles del Modelo de Seguridad propuesto

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

El establecimiento de procedimientos y la selección de los controles y principios de seguridad más adecuados de la Norma ISO/IEC 27002:2017, la identificación de los activos y análisis de riesgos a los que están expuestos los activos frente a las amenazas y vulnerabilidades, permitieron el diseño del Modelo de Seguridad IADI, que servirá como guía de prevención de ataques cibernéticos y protección de la información y los servicios proporcionados por el Sistema de Gestión Académica Ignug del Instituto Superior Tecnológico Yavirac.

Los trabajos analizados en el capítulo III sobre diseños de políticas de seguridad con el estándar ISO/IEC 27002:2013, contribuyeron con lineamientos básicos para el desarrollo del modelo, mediante la consideración de los controles adecuados de la Norma ISO/IEC 27002:2017, por lo tanto, se concluye que un modelo de seguridad se lo puede generalizar de acuerdo a los activos y riesgos analizados, con el fin de aplicar a otras entidades en común y que tengan un número igual de usuarios.

La guía metódica, el catálogo de elementos y las técnicas de Magerit, permitieron viabilizar el procedimiento del análisis de vulnerabilidad del SGA Ignug, identificando y clasificando los activos según las dependencias entre ellos, valorándolos de acuerdo a las dimensiones de seguridad, logrando reconocer las amenazas y vulnerabilidades potenciales a los que están expuestos cada uno de los activos para gestionar la seguridad.

La identificación de los activos considerando la dependencia entre ellos, permitió clasificarlos de acuerdo a una estructura jerárquica donde los activos que se encuentran en el nivel más alto dependen de la seguridad de los activos del nivel más bajo, por lo tanto, se deben proteger a los activos iniciando desde por el nivel inferior para que no haya consecuencias en los activos superiores del SGA Ignug.

La priorización de los riesgos estimados de acuerdo a la criticidad reflejada en el mapa de calor, permitió identificar a los activos críticos que deben ser atendidos de forma inmediata, a través de la implementación del Plan a corto plazo y de los controles oportunos mediante las directrices de buenas prácticas y principios de seguridad del Modelo IADI diseñado bajo el estándar ISO /IEC 27002:2017.

La identificación de los activos de información y el análisis de riesgos, permitieron diseñar la Política del Modelo de Seguridad IADI, mediante la selección de los controles pertinentes y principios de la Norma ISO/IEC 27002:2017, de acuerdo a las necesidades del SGA Ignug, lo cual va a permitir que el Área de Ciberseguridad de TIC, gestione los riesgos de la información y proteja a los activos de posibles ataques a los que se encuentra expuesto el sistema.

El Modelo de Seguridad IADI solventa el problema de seguridad a largo plazo, por lo tanto, se realizó un Plan a corto plazo, considerando los activos críticos más relevantes para el IST Yavirac, seleccionándolos del mapa de calor de riesgos y proponiendo los controles más viables de corrección, recuperación, administración, eliminación y concienciación, para que el Área de Ciberseguridad de TIC los implemente sin ningún inconveniente y de forma inmediata.

6.2 Recomendaciones

Se recomienda que las autoridades de la institución, designen de forma inmediata a los miembros de la estructura organizacional de la seguridad planteada en el Artículo 3, con el fin, de que el Comité de Dirección revise y apruebe el Modelo de Ciberseguridad propuesto, para que se lo implemente considerado primeramente el Plan a corto plazo para mejorar la seguridad del problema actual que tienen los activos del IST Yavirac.

Se recomienda que el Comité de Dirección socialice el Modelo IADI, a toda la comunidad educativa del IST Yavirac, con el fin de concientizar sobre el valor de la información, de esa manera prevenir errores involuntarios por parte del personal interno.

Se recomienda que el Comité de Dirección del ISTY revise el Modelo de Seguridad IADI cada dos semestres, debido a que la plataforma informática es actualizada constantemente de esa manera se garantiza la disponibilidad, integridad y confidencialidad de la información y de los servicios que brinda el SGA Ignug.

Se recomienda aplicar los controles de seguridad pertinentes a los nuevos desarrollos de software, para minimizar vulnerabilidades y brechas de seguridad, como acciones preventivas que permitan dar continuidad a los procesos del ISTY.

Se recomienda que el Modelo de Seguridad IADI a implementarse en el IST Yavirac, sea aplicado a otras instituciones educativas con el mismo número de usuarios, ya que es un estándar genérico que considera la mayoría de los controles de la Norma ISO/IEC 27002:2017, con el fin de mitigar los problemas relacionados a la Ciberseguridad.

BIBLIOGRAFÍA

Almeida, J. (2019). Diseño de una política de seguridad de la información para SWEADEN Compañía de Seguros S.A, basado en la norma ISO/IEC 27002:2013 (tesis de maestría). Universidad UISEK, Quito, Ecuador

Ariganello, E. (2014). Redes cisco: Guía de estudio para la certificación CCNA security. Retrieved from http://ebookcentral.proquest.com

Baca, G. (2016). Introducción a la Seguridad Informática. Referido de: http://ebookcentral.proquest.com/lib/biblioseksp/detail.action?docID=4849850.

Barrio, M. (2017). Ciberdelitos: amenazas criminales del ciberespacio: Adaptado reforma Código Penal 2015. Madrid: Reus.

Cárdenas, I. (2020). Diseño de una Política de Seguridad de la Información para la Unidad educativa Borja 3 Canavis, Basado en la Norma ISO/IES 27002:2013 (tesis de maestría). Universidad UISEK, Quito, Ecuador

Cevallos, H. (2019). Diseño de una política de seguridad de la información para el área de TICs del Instituto Tecnológico Superior Central Técnico, basado en la Norma de seguridad ISO/IEC 27002:2013 (tesis de maestría). Universidad UISEK, Quito, Ecuador

Conforme, C. (2018). Diseño de un modelo de gestión de seguridad de la información para el sistema académico de la universidad estatal del sur de Manabí (tesis de maestría). Universidad UISEK, Quito, Ecuador

Contero, W. (2020). Diseño de una política de seguridad de la información basada en la norma ISO 27002:2013, para el Sistema de Botones de Seguridad del Ministerio del Interior (tesis de maestría). Universidad UISEK, Quito, Ecuador

Freire, K. (2017). Estudio y análisis de ciberataques en América Latina, su influencia en las empresas del Ecuador y propuesta de políticas de ciberseguridad (Tesis de pregrado). Guayaquil, Ecuador.

ISACA. (2017). Fundamentos de Ciberseguridad. Segunda Edición.

ISOTools Excellence. (2017) ¿Seguridad informática o seguridad de la información? Recuperado de: http://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

Lara, E. (2019). Diseño de un Modelo de Seguridad de la Información, basado en OSSTMMV3, NIST SP 800-30 E ISO 27001, para centros de Educación: caso de Estudio Universidad Regional Autónoma de los Andes, Extensión Tulcán (tesis de maestría). Universidad UISEK, Quito, Ecuador

Levi S. & Binyaminov N. (2020). Las 10 principales vulnerabilidades del servicio web en 2019. Referido de: https://www.hackers-challenge.com/post/las-10-principales-vulnerabilidades-del-servicio-web-en-2019

https://es.cointelegraph.com/news/ransomware-strikes-three-us-universities

MAGERIT. (2012). Magerit versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I: Método, 127.

MAGERIT. (2012). Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro II: Catálogo de Elementos, 74.

MAGERIT. (2012). Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro III: Guía de Técnicas, 42.

Norma ISO/IEC 27002:2017 (2017). Código de buenas prácticas para los controles de seguridad de la información (ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015). AENOR Internacional S.A. U.

NBR ISO / IEC 27005 (2008) - Tecnología de la información - Técnicas de seguridad - Gestión de riesgos de seguridad de la información. AENOR Internacional S.A. U.

Pacheco, L. (2018). Políticas de seguridad de la información de aprovechamiento estudiantil en la educación general básica en la norma ISO 27002. Universidad Espíritu Santo, Samborondón, Ecuador.

Quevedo, J. (2017). Investigación y Prueba del Ciberdelito (tesis de Programa de Doctorado de Derecho y Ciencia Política, Línea de investigación: Derecho procesal). Universidad de Barcelona, Barcelona, España.

Rodríguez, J. (2016). Diseño y creación de una política de seguridad de la Información (SGSI basado en la normativa ISO 27000 para la Cooperativa Construcción, Comercio y Producción (tesis de maestría). Universidad UISEK, Quito, Ecuador

Romero, M. (Ed.). (2018). Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades. Quito, Ecuador: Área de Innovación y Desarrollo,S.L.

Ross, A. (2da ed.). (2008). *Security Engineering*. Cambridge.

Sánchez, G. (2018). Seguridad Cibernética, Hackeo Ético y Programación Defensiva. México.

Satllings, W. (2017). Cryptography and Network Security: Principles and Practice, 7th Edition.

Torres, E. (2015). Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002:2013. Universidad de Ambato, Ecuador.

Villalba, A. (2015). La Ciberseguridad en España 2011-2015 una propuesta de modelo de organización (Tesis doctoral). Universidad Nacional de Educación a Distancia, Madrid, España.

Yavirac. (2019). Inty Yavirac. referido de: http://yavirac.edu.ec/inti-yavirac/

ANEXOS

Anexo 1: Controles ISO/IEC 27002:2017

N°	Capitulos	Categoría	Obejtivo	Código	Artículo política	Control
1	Políticas de Seguridad de la Información	Directrices de gestión de la seguridad de la información	Proporcionar orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normativa pertinentes.	1.1.1	Art. 4	Políticas para la seguridad de la información
				1.1.2	Art. 5	Revisión de las políticas para la seguridad de la información
2	Organización de la Seguridad de la Información	Organización interna	Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información	2.1.1	Art. 6	Roles y responsabilidades en seguridad de la información
				2.1.2	Art. 7	Segregación de tareas
				2.1.3	Art. 8	Contacto con las autoridades
				2.1.4		Contacto con grupos de interés especial
				2.1.5	Art. 9	Seguridad de la información en la gestión de proyectos
		Los dispositivos móviles y el teletrabajo	Garantizar la seguridad e el teletrabajo y en el uso de dispositivos móviles.	2.2.1	Art. 10	Política de dispositivos móviles
				2.2.2	Art. 11	Teletrabajo
3	Seguridad relativa a los recursos humanos	Antes del empleo	Para asegurarse que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran.	3.1.1		Investigación de antecedentes
				3.1.2	Art. 12	Términos y condiciones del empleo
		Durante el empleo	Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades en seguridad de la información	3.2.1	Art. 13	Responsabilidades de gestión
				3.2.2	Art. 14	Concienciación, educación y capacitación en seguridad de la información
				3.2.3	Art. 15	Proceso disciplinario
		Finalización del empleo o cambio en el puesto de trabajo	Proteger los intereses de la organización como parte del proceso de cambio o finalización del empleo.	3.3.1	Art. 16	Responsabilidades ante la finalización o cambio
4	Gestión de activos	Responsabilidad sobre los activos	Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.	4.1.1	Art. 17	Inventario de activos
				4.1.2	Art. 18	Propiedad de los activos
				4.1.3	Art. 19	Uso aceptable de los activos
				4.1.4	Art. 20	Devolución de activos
		Clasificación de la información	Asegurar que la información reciba un nivel adecuado de protección de acuerdo co su importancia para la organización.	4.2.1	Art. 21	Clasificación de la información
				4.2.2	Art. 22	Etiquetado de la información
				4.2.3	Art. 23	Manipulado de la información
		Manipulación de los soportes	Evitar la revelación, modificación, eliminació o destrucción no	4.3.1	Art. 24	Gestión de soportes extraíbles
				4.3.2		Eliminación de soportes
				4.3.3	Art. 25	Soportes físicos en tránsito

Nº	Capitulos	Categoría	Obejtivo	Código	Artículo política	Control
5	Control de acceso	Requisitos de negocio para el control de acceso	Limitar el acceso a los recursos de tratamiento d información y a la información.	5.1.1	Art. 26	Política de control de acceso
				5.1.2	Art. 27	Acceso a las redes y a los servicios de red
		Gestión de acceso de usuario	Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.	5.2.1	Art. 28	Registro y baja de usuario
				5.2.2	Art. 29	Provisión de acceso de usuario
				5.2.3	Art. 30	Gestión de privilegios de acceso
				5.2.4	Art. 31	Gestión de la información secreta de autenticación de los usuarios
				5.2.5		Revisión de los derechos de acceso de usuario
				5.2.6	Art.32	Retirada o reasignación de los derechos de acceso
		Responsabilidades del usuario	Para que los usuarios se hagan responsables de salvaguardar su información de autenticación.	5.3.1	Art. 33	Uso de la información secreta de autenticación
		Control de acceso a sistemas y aplicaciones	Prevenir el acceso no autorizado a los sistemas y aplicaciones.	5.4.1	Art. 34	Restricción del acceso a la información
				5.4.2	Art. 35	Procedimientos seguros de inicio de sesión
				5.4.3	Art. 36	Sistema de gestión de contraseñas
				5.4.4		Uso de utilidades con privilegios del sistema
				5.4.5	Art. 37	Control de acceso al código fuente de los programas
6	Criptografía	Controles criptográficos	Garantizar un uso adecuado y eficaz de la criptografía para protege la confidencialidad, autenticidad y/o integridad de la información.	6.1.1	Art. 38	Política de uso de los controles criptográficos
				6.1.2	Art. 39	Gestión de claves
7	Seguridad física y del entorno	Areas seguras	Prevenir el acceso físico no autorizado, los daños interferencia a la información de la organización y a los recursos de tratamiento de la información.	7.1.1		Perímetro de seguridad física
				7.1.2	Art. 40	Controles físicos de entrada
				7.1.3		Seguridad de oficinas, despacho y recursos
				7.1.4		Protección contra las amenazas externas y ambientales
				7.1.5		El trabajo en áreas seguras
				7.1.6		Areas de carga y descarga
		Seguridad de los equipos	Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.	7.1.7	Art. 41	Emplazamiento y protección de equipos
				7.1.8	Art. 42	Instalaciones de suministro
				7.1.9	Art. 43	Seguridad del cableado
				7.1.10	Art. 44	Mantenimiento de los equipos
				7.1.11	Art. 45	Retirada de materiales propiedad de la empresa

N°	Capitulos	Categoría	Obejtivo	Código	Artículo política	Control
	Seguridad de las operaciones	responsabilidades operacionales	seguro de las instalacione de tratamiento de la información.	8.1.2	Art. 48	Gestión de cambios
				8.1.3	Art. 49	Gestión de capacidades
				8.1.4	Art. 50	Separación de los recursos de desarrollo, prueba y operación
		Protección contra el software malicioso (malware)	Asegurar que los recurso de tratamiento de información y la información están protegidos contra el malware.	8.2.1	Art. 51	Controles contra el código malicioso
		Copias de seguridad	Evitar la pérdida de datos	8.3.1	Art. 52	Copias de seguridad de la información
		Registros y supervisión	Registrar eventos y generar evidencias.	8.4.1	Art. 53	Registro de eventos
				8.4.2	Art. 54	Protección de la información del registro
				8.4.3	Art. 55	Registros de administración y operación
				8.4.4	Art. 56	Sincronización del reloj
		Control del software en explotación	Asegurar la integridad de software en explotación.	8.5.1	Art. 57	Instalación del software en explotación
		Gestión de la vulnerabilidad técnica	Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas	8.6.1	Art. 58	Gestión de las vulnerabilidades técnicas
				8.6.2	Art. 59	Restricción en la instalación de software
		Consideraciones sobre la auditoria de sistemas de información	Minimizar el impacto de las actividades de auditoría en los sistemas operativos.	8.7.1	Art. 60	Controles de auditoría de sistemas de información
9	Seguridad de las comunicaciones	Gestión de la seguridad de redes	Asegurar la protección d la información en las redes y los recursos de tratamiento de la información.	9.1.1	Art. 61	Controles de red
				9.1.2	Art. 62	Seguridad de los servicios de red
				9.1.3	Art. 63	Segregación en redes
		Intercambio de información	Mantener la seguridad en la información que se transfiere dentro de una organización y con cualquier entidad externa	9.2.1	Art. 64	Políticas y procedimientos de intercambio de información
				9.2.2	Art. 65	Acuerdos de intercambio de información
				9.2.3	Art. 66	Mensajería electrónica
				9.2.4	Art. 67	Acuerdos de confidencialidad o no revelación

N°	Capitulos	Categoría	Obejtivo	Código	Artículo política	Control
10	Adquisiciones, desarrollo y mantenimiento de los sistemas de información	Requisitos de seguridad en los sistemas de información	Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.	10.1.1	Art. 68	Análisis de requisitos y especificaciones de seguridad de la información
				10.1.2	Art. 69	Asegurar los servicios de aplicaciones en redes públicas
				10.1.3	Art. 70	Protección de las transacciones de servicios de aplicaciones
		Seguridad en el desarrollo y en los procesos de soporte	Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de los sistemas de información.	10.2.1	Art. 71	Política de desarrollo seguro
				10.2.2	Art. 72	Procedimiento de control de cambios en sistemas
				10.2.3	Art. 73	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
				10.2.4	Art. 74	Restricciones a los cambios en los paquetes de software
				10.2.5	Art. 75	Principios de ingeniería de sistemas seguros
				10.2.6	Art. 76	Entorno de desarrollo seguro
				10.2.7		Externalización del desarrollo de software
				10.2.8	Art. 77	Pruebas funcionales de seguridad de sistemas
				10.2.9	Art. 78	Pruebas de aceptación de sistemas
		Datos de prueba	Asegurar la protección de los datos de prueba.	10.3.1	Art. 79	Protección de los datos de prueba
11	Relación de proveedores	Seguridad en las relaciones con proveedores	Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.	11.1.1		Política de seguridad de la información en las relaciones con los proveedores
				11.1.2	Art. 80	Requisitos de seguridad en contratos con terceros
				11.1.3		Cadena de suministro de tecnología de la información y de las omunicaciones
		Gestión de la provisión de servicios del proveedor	Mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores.	11.2.1	Art. 81	Control y revisión de la provisión de servicios del proveedor
				11.2.2	Art. 82	Gestión de cambios en la provisión del servicio del proveedor

N°	Capitulos	Categoría	Obejtivo	Código	Artículo política	Control
12	Gestión de incidentes de seguridad de la información	Gestión de incidentes de seguridad de la información y mejoras	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.	12.1.1	Art. 83	Responsabilidades y procedimientos
				12.1.2	Art. 84	Notificación de los eventos de seguridad de la información
				12.1.3		Notificación de puntos débiles de la seguridad
				12.1.4	Art. 85	Evaluación y decisión sobre los eventos de seguridad de información
				12.1.5	Art. 86	Respuesta a incidentes de seguridad de la información
				12.1.6	Art. 87	Aprendizaje de los incidentes de seguridad de la información
				12.1.7	Art. 88	Recopilación de evidencias
13	Aspectos de seguridad de la información para la gestión de la continuidad de negocio	Continuidad de la seguridad de la información	La continuidad de la seguridad de la información debería formar parte de los sistemas de gestión de la continuidad de negocio de la organización.	13.1.1	Art. 89	Planificación de la continuidad de la seguridad de la información
				13.1.2	Art. 90	Implementar la continuidad de l seguridad de la información
				13.1.3	Art. 91	Verificación, revisión y evaluación de la continuidad de la seguridad de la información
		Redundancias	Asegurar la disponibilida de los recursos de tratamiento de la información.	13.2.1	Art. 92	Disponibilidad de los recursos d tratamiento de la información
14	Cumplimie nto	Cumplimiento de los requisitos legales y contractuales	Evitar incumplimiento de las bligaciones legales estatutarias, reglamentarias o contractuales relativas a l seguridad de la información o de los requisitos de seguridad.	14.1.1		Identificación de la legislación aplicable y de los requisitos contractuales
				14.1.2		Derechos de propiedad intelectual (DPI)
				14.1.3	Art. 93	Protección de los registros de la organización
				14.1.4	Art. 94	Protección y privacidad de la información de carácter persona
				14.1.5		Regulación de los controles criptográficos
		Revisiones de la seguridad de la información	Garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas procedimientos de la organización.	14.1.6	Art. 95	Revisión independiente de la seguridad de la información
				14.1.7	Art. 96	Cumplimiento de las políticas y normas de seguridad
				14.1.8	Art. 97	Comprobación del cumplimient técnico

Anexo 2: Organigrama Estructural

Anexo 3: Entrevista de Infraestructura

Universidad Internacional SEK

Entrevista

Área:	Unidad de Tecnologías de la Información y Comunicación
Asunto:	Infraestructura
Nombre del entrevistador:	Ing. Lorena E. Chulde O.
Nombre del entrevistado:	Ing. Mauricio Tamayo
Cargo:	Coordinador de la Unidad de Tecnologías de la Información y Comunicación
Fecha:	2020/10/02

Infraestructura en la que se aloja el Sistema de Gestión Académica Ignug

1. En qué tipo de infraestructura se aloja el Sistema de Gestión Académico Ignug?

   El Sistema Ignug se aloja en un servidor virtual.

2. Si el servidor es virtual, cuál es el proveedor del servidor?

   El proveedor del servidor virtual es la empresa Contabo

3. Cuáles son los recursos contratados para el servidor?

   Procesador de10 núcleos de CPU, 60 GB de RAM, 1600 GB de espacio en disco SSD, 100% de espacio en disco SSD, tráfico ilimitado, puerto de 1 Gbit / s, protección DDoS, acceso VNC, dirección IP incluida, / 64 red IPv6 incluida, 4 instantáneas incluidas.

4. Qué sistema operativo tiene instalado?

   Ubuntu Server 20, reinicio y reinstalación del sistema operativo a través de la interfaz web

5. Cuál es el servidor de aplicaciones?
   El servidor de aplicaciones que está instalado es Apache V 2.4.41
6. Cuál es el sistema gestor de base de datos?

   El sistema gestor de base de datos es Postgres V. 12

Ing. César Mauricio Tamayo L.

CESAR MAURICIO TAMAYO LOPEZ

Coordinador de la Unidad de TIC

Anexo 4: Acta de reunión

Universidad Internacional SEK

Acta de reunión

En el Distrito Metropolitano de Quito, provincia de Pichincha, del día 05 de octubre de 2020, luego de verificar el quórum reglamentario, se instala la sesión de recolección de la información y servicios que proporciona el Sistema de Gestión Académica Ignug, la misma que es presidida por la Ingeniera Lorena Chulde.

1. Orden del día

- Datos transaccionados por la plataforma Ignug.
- Módulos del Sistema de Gestión Académica Ignug
- Servicios prestados y contratados
- Personal relacionado con el uso y administración del Sistema Ignug

2. Desarrollo

Nº	Detalle de la información
Datos/Información	Datos personales: Bases de datos con información personal, socio-económica, notas, asistencia de los estudiantes. Datos clasificados: archivos, copias de respaldo, confoiguraicón del sistea, gestión, interna, contraseñas, validación de credenciales, control de acceso, registros de actividad, código fuente, código ejecutable Difusión limitada: matrices de rendimiento académico, registros de notas, récords académicos, asistencia; datos de las empresas De carácter público: solicitudes de matrículas; datos académicos de docentes y autoridades; malla curricular, información del portal
Módulos de la plataforma_	Módulos: Gestión de matriculación, Gestión de Notas y Asistencia, Administración Registro de Asistencia de Docentes, Módulo de Bolsa de Empleo
Servicios prestados:	Públicos: Portal web Externos: Bolsa de empleo Internos: matriculación, gestión de notas, asistencia, registro docente, Correo electrónico, Almacenamiento de archivos, Transferencia de archivos
Servicios contratados:	Internet, infraestructura virtual Usuarios externos: empresas formadoras Usuarios internos: estudiantes, docentes, autoridades
Personal relacionado	Administrador y apoyo la plataforma Ignug Administradores de base de datos de "ignug_bdd" Administradores de comunicaciones Proveedores: internet CNT, equipo virtual Contabo

Se da por finalizada la reunión y para la constancia de esta acta la firman al final los asistentes.

3. ASISTENTES

Firmas	
CESAR MAURICIO TAMAYO LOPEZ	
Ing. César Mauricio Tamayo L. **Coordinador de la Unidad de TIC**	Ing. Lorena Chulde **Docente del IST Benito Juárez**