Artículo de Investigación

# Diseño del Modelo de Ciberseguridad IADI para el Sistema de Gestión Académica Ignug del Instituto Superior Tecnológico Yavirac

# Design of the IADI Cybersecurity Model for the Ignug Academic Management System of the Yavirac Higher Technological Institute

Chulde, Lorena; Défaz, Hugo

**Lorena Chulde**
lchulde@yavirac.edu.ec
Instituto Superior Tecnológico Yavirac, Ecuador
**Hugo Défaz**
americo3.defaz@gmail.com
Universidad Central del Ecuador, Ecuador

**Ecuadorian Science Journal**
GDEON, Ecuador
ISSN-e: 2602-8077
Periodicidad: Semestral
vol. 5, núm. Esp.3, 2021
esj@gdeon.org

Recepción: 31 Agosto 2021
Aprobación: 24 Octubre 2021

**URL:** http://portal.amelica.org/ameli/jatsRepo/606/6062738023/index.html

**DOI:** https://doi.org/10.46480/esj.5.3.160



**Como citar :** Chulde, L., & Défaz, H. (2021). Diseño del Modelo de Ciberseguridad IADI para el Sistema de Gestión Académica Ignug del Instituto Superior Tecnológico Yavirac. Ecuadorian Science Journal, 5(3), 272-292. DOI: https://doi.org/10.46480/esj.5.3.160

**Resumen:** En el presente artículo, se da a conocer el procedimiento de la gestión de riesgos, mediante el análisis y tratamiento de los riesgos, identificando los activos, las amenazas, el impacto y las salvaguardas, aplicando la metodología Magerit con el fin de diseñar el Modelo de Ciberseguridad IADI 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.

**Palabras clave:** Análisis de Riesgos, Ciberseguridad, Gestión de Riesgos, Metodología Mágerit, Modelo de Ciberseguridad, Norma ISO, IEC 27002:2017, Seguridad de Software.

**Abstract:** In this article, the risk management procedure is disclosed, through the analysis and treatment of risks, identifying assets, threats, impact and safeguards, applying the Magerit methodology in order to design the Model of IADI Cybersecurity through the controls chosen from the ISO / IEC 27002: 2017 security standard that allows the personnel of the Software Development Area of the Yavirac Higher Technological Institute, the mitigation of the risks found on the platform and in this way guarantees the normal operation of the Ignug Academic Management System.

**Keywords:** Cybersecurity, Cybersecurity Model, ISO , IEC 27002: 2017 Standard, Magerit Methodology, Risk Analysis, Risk Management, Software Security.

## Introducción

Las organizaciones desarrollan las actividades cotidianas mediante el uso de la tecnología desde cualquier sitio y en cualquier momento; usan herramientas que permiten ejecutar transacciones de grandes cantidades de datos y acceder a ellos en tiempo real, mediante sistemas de información, servicios electrónicos y redes de comunicaciones.

La información es el recurso estratégico más importante de las entidades, constituye un factor decisivo al momento de tomar decisiones en las organizaciones; sin embargo, se pueden presentar problemas de vulnerabilidad y amenazas para su seguridad, está expuesta a sufrir modificaciones, a ser eliminada, hurtada y divulgada.

El Instituto Superior Tecnológico Yavirac, implementó el Sistema de Gestión Académica Ignug, que agiliza los procesos y facilita el acceso a los datos relevantes de la institución en tiempo real; sin embargo, carece de protección por lo que, es de vital importancia resguardar la información, los sistemas por los cuales se procesa y los dispositivos electrónicos que la transfieren. En ausencia de seguridad, el SGA Ignug corre el riesgo de sufrir daños, 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, pudiendo quedar inoperativo, lo que puede ocasionar retrasos en la gestión académica; por tal razón, es indispensable protegerlo contra amenazas intencionales o accidentales.

Puesto que la población estudiantil del Yavirac crece cada período lectivo, el uso de la plataforma académica Ignug es indispensable, ya que gestiona información sobre las matrículas, notas de grados, récords académicos, etc. con una gran cantidad de registros que se encuentran en la nube, siendo propenso de sufrir un sinnúmero de ataques informáticos como: destrucción, divulgación, modificación y robo de los datos. Con el fin de minimizar los riesgos de seguridad, es necesario diseñar un modelo de gestión de seguridad, a través de métodos, herramientas y protocolos que permitan defender al sistema, los datos y a 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.

## Conceptos sobre Ciberseguridad

### Ciberseguridad

Se encarga de proteger los recursos informáticos de hardware como servidores, infraestructura, redes de comunicaciones, etc. y software como aplicaciones informáticas, bases de datos e información digital que se trasporta mediante los dispositivos electrónicos; con el fin de reducir los riesgos al mínimo y garantizar la continuidad de los servicios de la organización al tiempo que se administra ese riesgo informático a un cierto costo aceptable.

La ciberseguridad o seguridad cibernética debe cumplir con tres principios fundamentales: confidencialidad, integridad y disponibilidad.

### Características de la ciberseguridad

Confidencialidad. – Asegura que, en el procesamiento de la información privada o sensible, ésta se encuentre protegida contra accesos no autorizados, los cuales pueden derivar en la alteración, divulgación o robo de información confidencial (Baca Urbina, 2019).

Integridad. – Garantiza que la información procesada y transferida mediante dispositivos electrónicos, sea precisa y esté completa, tal y como espera el usuario; es decir que los datos no sean alterados o eliminados por usuarios no autorizados (Roa Buendía, 2013).

Disponibilidad. - Significa que los controles de seguridad y las herramientas de comunicación del sistema deben funcionar correctamente para garantizar que los sistemas trabajen normalmente, la información y los servicios estén siempre disponibles para los usuarios autorizados (Sánchez Cano, 2018).

## Metodología aplicada

Previo a la implementación de los controles de seguridad, se debe realizar un análisis de riegos para una gestión adecuada de los mismos. En el proceso de análisis y gestión de riesgos se usará la guía metodológica de Magerit, estándar enfocado 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.

## Magerit

Magerit es un marco de trabajo que responde e implementa el "Proceso de Gestión de los Riesgos", dentro del "Marco de Gestión de Riesgos", para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información (Magerit, 2012a).

En la Figura Nº 1, se observa que Magerit implementa el proceso de la gestión de riesgos en un marco de trabajo para que las autoridades de las organizaciones tomen decisiones considerando los riesgos existentes del uso de la tecnología.

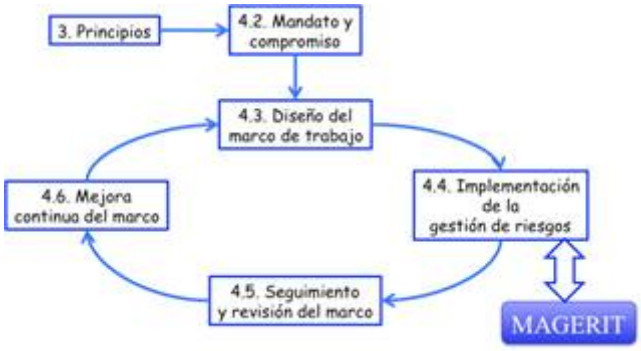


FIGURA 1
ISO 31000 – Marco de trabajo para la gestión de riegos
Metodología de MAGERIT, Libro I –Método- v 3.0 (2012)

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, 2012a).

En la Tabla Nº 1, 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 1.
Actividades de análisis y gestión de riegos

| 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. |
| 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 |

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.

## 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 combinación de dos actividades: análisis y tratamiento de los riesgos.

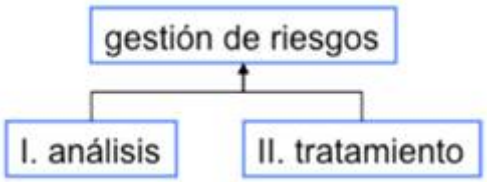


FIGURA 2
Estructura de gestión de riesgos
Metodología de MAGERIT, Libro I –Método- v 3.0 (2012)

En la Figura 3, se observa el esquema formal de la gestión de riesgos propuesto por la ISO 31000.

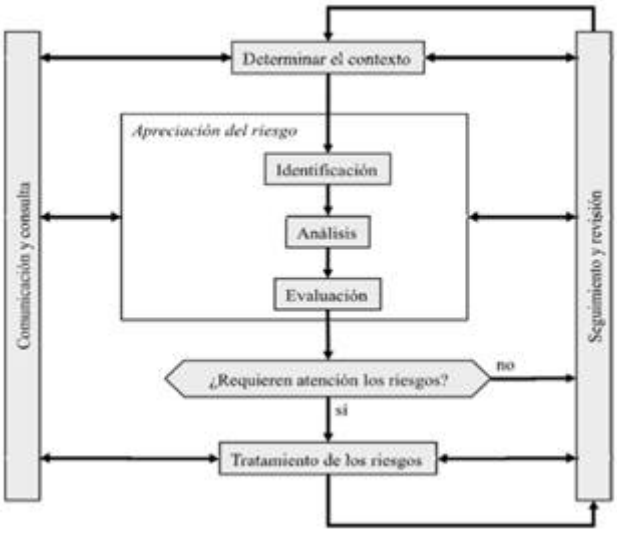


FIGURA 3
ISO 31000 – Proceso de gestión de riesgos
Metodología de MAGERIT, Libro I –Método- v 3.0 (2012)

## Método de análisis de riesgos

Se refiere al proceso sistemático para estimar la magnitud de los riesgos a los que están expuestos los sistemas informáticos. Es fundamental comprender el Análisis de Riesgos y distinguir las actividades y entregables a realizarse en el desarrollo del proyecto, por lo tanto, se deben determinar los activos, amenazas y salvaguardas, con estos elementos se pueden estimar el impacto y el riesgo (Magerit, 2012a).

Previo a la realización del análisis se deben conocer las definiciones de los términos indicados:

Activo. – Es un bien que posee valor para la organización. 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).

Amenaza. - Es todo lo que puede dañar la aplicación, 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.

Algunas de las amenazas más comunes suelen ser: inyección (SQL, OS, XXE y LDAP), irrupción en la autenticación y la sesión, cross site scripting (XSS o scripting de sitio cruzado), irrupción en el control de acceso, cross site request forgery (CSRF o falsificación de peticiones en sitios cruzados), uso de componentes con vulnerabilidades, API con poca protección (OWASP, 2017).

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 Cano, 2018).

Impacto. - Es el peligro relativo (bajo, medio o alto) de una amenaza para los activos de la organización, se puede expresar en términos de dinero o estatus social; se lo cuantifica para poder realizar un adecuado cálculo del riesgo (Sánchez Cano, 2018).

Riesgo. - Es el peligro (impacto × probabilidad) de que realmente se produzca un ataque. El impacto y la probabilidad pueden ser bajos, medios o altos. Puede ser cuantitativa o cualitativa (Magerit, 2012a).

Vulnerabilidad. - Es una debilidad existente en el sistema informático que permite concretar la amenaza, comprometiendo a los activos de la información, dañándolos o robándolos; una aplicación es vulnerable en la medida en que no hay suficiente protección para evitar que llegue a suceder una amenaza (Baca Urbina, 2019).

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. - Es la posibilidad (baja, media, alta) de que ocurra una amenaza.

## Pasos para determinar el análisis de riesgos

Para realizar el análisis de riesgos, se deben seguir los siguientes pasos:

- Determinación de activos
- Determinación de amenazas
- Determinación del impacto potencial
- Determinación del riesgo potencial
- Determinación de salvaguardas

## Determinación de los activos relevantes

Existen dos activos esenciales la información y los servicios; además, se identifican otros activos de los cuales dependen. En la Tabla Nº 2, se listan los tipos de activos que se deben reconocer en la Seguridad Informática.

TABLA 2.
Actividades de análisis y gestión de riegos

| Activos | Actividades de análisis y gestión de riesgos | Descripción |
|---|---|---|
| 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. |
| | Servicios subcontratados a terceros | |
| Instalaciones físicas | Instalaciones físicas | Sitios físicos que alojan los sistemas informáticos y de comunicación. |
| Personal | Usuarios: externos e internos | Personal relacionado con el uso y administración de los sistemas de informáticos. |
| | Operadores y administradores | de aplicaciones, bases de datos, redes. |
| | Desarrolladores | De los sistemas de información, diseñadores de bases de datos, arquitectura web. |
| 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 | Equipamiento y suministros | Lugar en el que se alojan las aplicaciones para su operación. |
| | Mobiliario | Armarios, etc. |

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

En la Tabla Nº 3, se observa la escala de la degradación del valor del activo de acuerdo a la probabilidad de ocurrencia.

TABLA 3.
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 |

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

## Determinación de las amenazas relevantes

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

En la Tabla Nº 4, se listan las amenazas que afectan a los activos, según el tipo.

TABLA 4.
Tipos de amenazas que se deben reconocer de acuerdo al activo

| Activos | Descripción |
|---|---|
| [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 |

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

En la Tabla Nº 5, se observa la probabilidad de ocurrencia de la amenaza, de manera cuantitativa, tomando como referencia un año.

TABLA 5
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 |

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

## Determinación del impacto potencial

Para determinar del impacto se tomará en cuenta el valor de información y los servicios que prestan los sistemas informáticos 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. Se calcula considerando las variables: valoración y degradación de los activos. Ver Tabla Nº 6.

TABLA 6.
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 |

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

## Determinación del riesgo potencial

Para calcular el riesgo se usa la siguiente fórmula:

Riesgo = Probabilidad de ocurrencia de las amenazas x Impacto

En la Tabla Nº 7, se listan las escalas a considerar para la estimación del impacto.

TABLA 7.
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 |

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

TABLA 8
Estimación del riesgo

| Riesgo | | Probabilidad | | | | |
|---|---|---|---|---|---|---|
| | | 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 |

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

## Tratamiento de los riesgos

Permite organizar la defensa deforma consiente y prudente con el fin de que las funcionalidades de los sistemas no dejen de prestar los servicios al usuario, para que no pase nada malo y estar preparados para atajar las emergencias, sobrevivir a los incidentes y continuar con el negocio; reduciendo al riesgo a un nivel residual que la entidad asume (Magerit, 2012b) .

## Determinación de las salvaguardas

El análisis de riesgos aporta 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 el modelo de Ciberseguridad IADI, 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.

## Norma ISO/IEC 27002

Es un estándar que suministra lineamientos para la implementación de controles de la seguridad informática; con el fin de que la organización 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. Se encuentra vigente a partir de agosto de 2017, anulando a las normas UNE-ISO/IEC 27002:2009 y UNE-ISO/IEC 27002:2015.

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. Se lo plantea para que las empresas desarrollen sus propias directrices de seguridad a ser utilizada (Norma ISO/IEC 27002:2017, 2017).

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. 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 del modelo IADI para preservar la información y los sistemas informáticos, de acuerdo a las necesidades del Sistema de Gestión Académica Ignug.

## Presentación del Modelo de Ciberseguridad IADI

En el Modelo de Ciberseguridad IADI 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 4.


FIGURA 4
Modelo de Ciberseguridad
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.

En las siguientes figuras, se observan los activos identificados.

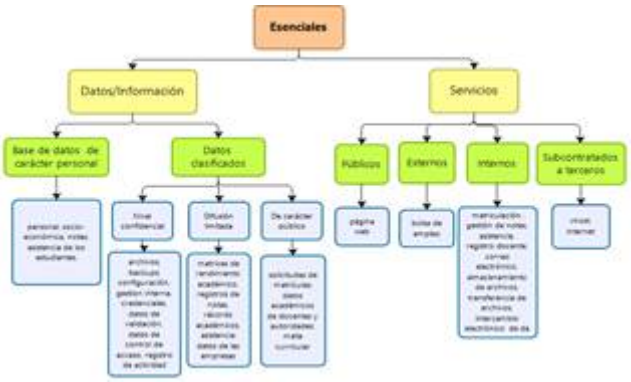


FIGURA 5
Activos esenciales
Elaborado por el autor

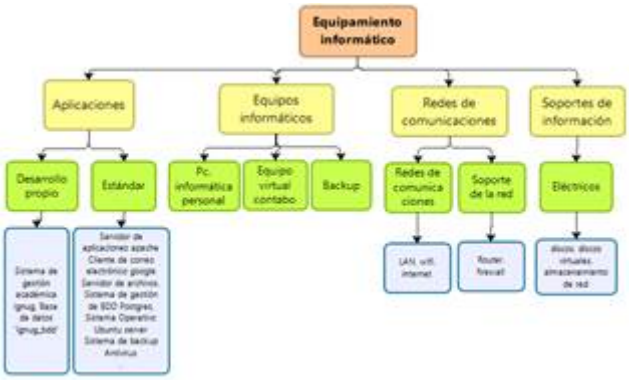


FIGURA 6
Activos equipamiento informático
Elaborado por el autor

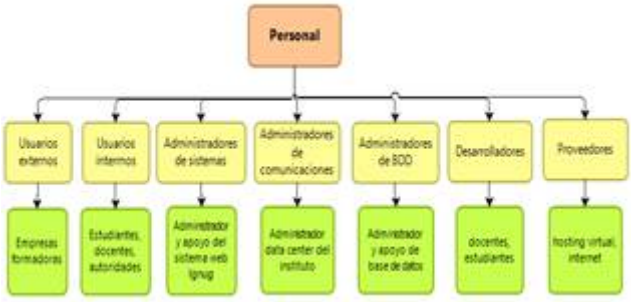


FIGURA 7
Activo Personal
Elaborado por el autor

[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. – Elegir los controles más apropiados de la Política de Seguridad del ISTY, realizada con los controles seleccionados de la Norma ISO/IEC 27002:2017, de acuerdo a la realidad del instituto y en función de los riesgos analizados. La guía se constituye de 14 capítulos y 97 artículos; considera las directrices de gestión de seguridad de la información, 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

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

Ver la Figura Nº 8.


FIGURA 8
Estructura organizacional de seguridad del ISTY
Elaborado por el autor

Auditoría. – Área estratégica que controlará la implementación de los controles de seguridad de la política del ISTY y verificará el cumplimiento del objetivo. Estará integrado por los siguientes miembros:

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

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

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

Dirección Ejecutiva. – Área táctico operacional, encargado 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.

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, el análisis de riesgos completo del SGAI, presenta muchas amenazas y vulnerabilidades de carácter crítico y en vista que la plataforma está completamente desprotegida, es necesario mitigarlas inmediatamente, se presenta el Plan a corto plazo, con el fin de mitigar los problemas relacionados a la ciberseguridad del SGAI del ISTY.

## Modelo a corto plazo

Se plantea el siguiente Plan a corto plazo como complemento al Modelo de Ciberseguridad IADI 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. Ver Anexo 1.

## Conclusiones

- Las aplicaciones informáticas pueden sufrir ataques internos o externos, siendo susceptibles de amenazas debido a las vulnerabilidades, provocando daños y pérdidas en los activos de las organizaciones, por lo tanto, es urgente que el Instituto Superior Tecnológico Yavirac, implemente el modelo propuesto de ciberseguridad IADI.
- El proceso de análisis y gestión de riesgos es esencial al momento de seleccionar las salvaguardas adecuadas para cada activo y servicio de información con el fin de minimizar los riesgos del SGAI hasta niveles aceptables.
- El Modelo de Seguridad IADI solventa el problema de seguridad a largo plazo, por lo tanto, se presenta 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.

## Referencias Bibliográficas

Baca Urbina, G. (2019). Introducción de la Seguridad Informática. In G. E. Patria (Ed.), Introducción a la Seguridad Informática (p. 54).

Magerit. (2012a). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=es%0Ahttp://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Magerit. (2012b). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Catálogo de Elementos. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=es%0Ahttp://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Magerit. (2012c). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Guía de Técnicas https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=es%0Ahttp://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

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). 1–34. https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0058429

OWASP. (2017). Project Spotlight: OWASP Top 10.

Roa Buendía, F. J. (2013). Seguridad informática (M. D. C. Ariadna Allés, Paloma Sánchez (ed.)). www.mhe.es/cf/informatica

Sánchez Cano, G. (2018). Seguridad cibernética Hackeo etico y programacion defensiva (C. de M. Alfaomega Grupo Editor, S.A. de C.V. – Dr. Isidoro Olvera No. 74, Col. Doctores, C.P. 06720, Cuauhtémoc (ed.); Primera E).

## Datos /[info] Información:

TABLA 9.
Selección de salvaguardas para los activos críticos de información del Sistema Ignug

| [D] Datos /[info] Información: | | Amenaza | | Vulnerabilidad | Controles ISO/27002:2017 |
|---|---|---|---|---|---|
| [per] [C] [fich] [backup] [int] [paswd] [auth] [conf] [exe] [R] [log] | Bases de datos con información personal de los estudiantes Nivel confidencial: Archivos Copias de respaldo Datos de gestión interna Credenciales: contraseñas Datos de validación de credenciales Datos de configuración del sistema Código ejecutable Difusión limitada: matrices de rendimiento académico, registros de notas, récords académicos, asistencia; datos de las empresas Registro de actividad | [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. |
| | | [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. |
| | | [A.6] | Abuso de privilegio de acceso | Ausencia de control de eventos logs | |
| | | [A.11] | Acceso no autorizado | Ausencia de implementación de contraseñas fuertes | |
| | | [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. |
| | | [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. |
| | | [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. |
| | | [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. |

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

## [S] Servicios:

TABLA 10.
Selección de salvaguardas de los servicios prestados y subcontratados

| [serv] Servicios: | | Amenaza | | Vulnerabilidad | Controles ISO/27002:2017 |
|---|---|---|---|---|---|
| [S.ext] Externos / [S.int] Internos | | | | | |
| [ext] [int] [file] [gesu] [idm] [ipm] [ftp] [edi] | Usuarios externos: empresas formadoras Usuarios Internos: matriculación, gestión de notas, registro Almacenamiento de archivos Gestión usuarios Gestión identidades Gestión privilegios Transferencia de archivos Intercambio electrónico de datos | [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. |
| | | [A.7] | Uso no previsto | Ausencia de registro de control en el acceso a los datos | |
| | | [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. |
| | | [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. |
| [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. |

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

## [SW] Aplicaciones:

TABLA 11.
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] [bddi] [backup] [app] [dmbs] [file] [os] | Sistema de gestión académica Ignug Base de datos "ignug_bdd" Sistema de backup Servidor de aplicaciones apache Sistema de gestión de base de Datos Postgres Servidor de archivos Sistema Operativo Ubuntu server | [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. |
| | | [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. |
| | | [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. |
| | | [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. |
| | | [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 | |

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