

# **Implementación de sistema de gestión de la seguridad de la información para el aseguramiento del proceso de ingreso de notas en un portal web universitario**

Jilmar Chaverra Barco

Trabajo de Grado presentado para optar al título de Especialista en Seguridad Informática

Asesor: Carlos Andres Arboleda Suaza, Magíster (MSc) en Arquitectura de Software.



UNIVERSIDAD DE  
SAN BUENAVENTURA  
COLOMBIA

Universidad de San Buenaventura  
Facultad de Ingenierías (Medellín)  
Especialización en Seguridad Informática  
Medellín, Colombia

2021

---

Citar/How to cite Chaverra Barco. [1]

Referencia/Reference [1] Chaverra Barco, J., “Implementación de Sistema de Gestión de la Seguridad de la Información para el aseguramiento del proceso de ingreso de notas en un portal web Universitario”, Trabajo de grado especialización, Especialización en Seguridad Informática, Universidad de San Buenaventura Medellín (Antioquia), 2021.

Estilo/Style:  
IEEE (2020)



Especialización en Seguridad Informática, Cohorte II.



Biblioteca Digital (Repositorio)  
[www.bibliotecadigital.usb.edu.co](http://www.bibliotecadigital.usb.edu.co)

### **Bibliotecas Universidad de San Buenaventura**

Biblioteca Fray Alberto Montealegre O.F.M. - Bogotá.

Biblioteca Fray Arturo Calle Restrepo O.F.M. - Medellín, Bello, Armenia, Ibagué.

Departamento de Biblioteca - Cali.

Biblioteca Central Fray Antonio de Marchena – Cartagena.

**Universidad de San Buenaventura Colombia** - [www.usb.edu.co](http://www.usb.edu.co)

Bogotá - [www.usbbog.edu.co](http://www.usbbog.edu.co)

Medellín - [www.usbmed.edu.co](http://www.usbmed.edu.co)

Cali - [www.usbcali.edu.co](http://www.usbcali.edu.co)

Cartagena - [www.usbctg.edu.co](http://www.usbctg.edu.co)

Editorial Bonaventuriana - [www.editorialbonaventuriana.usb.edu.co](http://www.editorialbonaventuriana.usb.edu.co)

Revistas científicas – [www.revistas.usb.edu.co](http://www.revistas.usb.edu.co)

## **Dedicatoria**

Primero a DIOS por esta Bendición tan grande que me ha regalado al mostrarme esta elección de especialización.

A mis padres Juan Manuel Chaverra(QEPD), y Ana Rosa Barco de Chaverra(QEPD), quienes desde el cielo me acompañan y en vida me enseñaron que cada día hay que superarse como persona y así servir mejor a quienes nos necesitan.

A mis Hijas y a mi compañera de lucha que son el motor y por quienes me esfuerzo cada día de mi vida

A mis Hermanos Januar, Yudi, Yency, Jhonny y Yamil Chaverra barco, por el apoyo incondicional para este logro

.

## TABLA DE CONTENIDO

RESUMEN.....	7
ABSTRACT .....	8
I. INTRODUCCIÓN .....	9
II. PLANTEAMIENTO DEL PROBLEMA .....	11
III. JUSTIFICACIÓN.....	14
IV. OBJETIVOS.....	15
A. Objetivo general .....	15
V. PROBLEMA DE INVESTIGACIÓN.....	16
VI. MARCO TEÓRICO.....	17
A. Sistemas de Gestión de la Seguridad de la Información SGSI.....	17
B. Contenido .....	18
C. Seguridad de la información.....	19
D. Controles De Seguridad Según Norma ISO 27002 .....	20
VII. METODOLOGÍA .....	22
VIII. RESULTADOS.....	24
A. Controles de seguridad basados en la norma iso 27001 .....	24
B. Políticas de seguridad de la información A.5.....	25
2) Revisión de las políticas de seguridad de la información: .....	25
C. Organización de la seguridad de la información A.6.....	25
3) Controles de acceso:.....	26
4) Criptografía – Cifrado y gestión de claves A.10:.....	26
5) Seguridad de las comunicaciones A.13:.....	27
6) Adquisición, desarrollo y mantenimiento del sistema A.14: .....	27

7)	Gestión de incidentes de seguridad de la información A.16: .....	28
IX.	ANÁLISIS DE RIESGO.....	29
A.	Identificación de activos.....	29
B.	Plataforma Academusoft.....	30
C.	Gestión colaborativa.....	30
D.	Gestión Extensión .....	30
E.	Gestión académica.....	30
F.	Gestión administrativa y financiera.....	31
G.	Gestión docencia .....	31
H.	Gestión investigación .....	31
I.	Gestión Administrativa y Financiera – Gestasoft .....	31
J.	APP UTCH Móvil.....	32
K.	Bibliotecas.....	32
L.	Riesgos y amenazas .....	33
X.	PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL PORTAL DE NOTAS DE LA UTCH .....	38
A.	Plan de mejora para el portal web de notas en la UTCH .....	38
1)	Hoja de ruta: .....	39
B.	Pautas en la política de seguridad del manejo de la información.....	41
XI.	CONCLUSIONES .....	42
	REFERENCIAS .....	43

## LISTA DE TABLAS

TABLA I ANALISIS DE LAS DEFICIENCIAS.....	35
---	----

## RESUMEN

Este informe se desarrolló con el fin de ofrecer una significativa contribución, sobre la forma de llevar a cabo la elaboración e implementación de un protocolo de seguridad informático digital, orientado hacia los servidores web vulnerables de la Universidad Tecnológica del Chocó, permitiendo hacer una detección de los riesgos posibles, amenazas o vulnerabilidades que se suelen encontrar diariamente en estos portales. Así pues, mediante un plan de contingencia basado en un sistema de gestión de la seguridad de la información, se busca solventar una problemática que afecta a toda una institución, desde la parte administrativa hasta el cuerpo estudiantil y el profesorado.

Este plan de apoyo contó con un método investigativo basado en la Norma ISO-27001, que busca garantizar la confidencialidad, integridad y disponibilidad de la información que almacena esta institución universitaria.

***Palabras clave* — Servidores web, vulnerabilidades, seguridad, información, informático, norma.**

## ABSTRACT

El This report was developed in order to offer a significant contribution on how to carry out the development and implementation of a digital computer security protocol, oriented towards the vulnerable web servers of the Technological University of Chocó, allowing the detection of possible risks, threats or vulnerabilities that are usually found daily in these portals. Thus, through a contingency plan based on an information security management system, it seeks to solve a problem that affects an entire institution, from the administrative part to the student body and faculty.

This support plan had an investigative method based on the ISO-27001 Standard, which seeks to guarantee the confidentiality, integrity and availability of the information stored by this university institution.

***Keywords*** — **Web servers, vulnerabilities, security, information, information technology, rule.**

## I. INTRODUCCIÓN

Los servidores que almacenan gran cantidad de información en la web son sumamente vulnerables y están expuestos a un gran número de amenazas y malversaciones informáticas por parte de ciertos grupos (llámense hackers o piratas informáticos).

En el momento dado el aumento del uso de la internet, el avance de la tecnología y la carencia de conocimiento para disminuir los riesgos de asaltos o vulneraciones en todo sentido, ha producido inmensas amenazas en las empresas para materializar riesgos y generar un impacto negativo en las instituciones, generando dificultades para mantener las facultades propenden por proteger la información: oportunidad, probidad y reserva de la misma [15, p.334].

Para evitar que este tipo de situaciones se presenten, existen algunas medidas de contingencia, como lo son las Técnicas utilizados en gestionar y asegurar de la Información, como son técnicas o métodos de criptación de datos, bloqueadores de malware, etc., los cuales son frecuentemente utilizados por empresas, instituciones, organizaciones y grandes plataformas con el fin de proteger su información; de esta manera, se logra minimizar el riesgo de robos o fraudes informáticos.

Ahora bien, la Universidad Tecnológica del Chocó Diego Luis Córdoba, que se encuentra ubicada en la capital del departamento del Chocó, Quibdó, cuenta con 40 programas académicos de pregrado y 11 de postgrado [14], es una de las principales Instituciones Públicas de Educación Superior ubicadas en el territorio del pacífico colombiano; por ende, cuenta con una amplia cantidad de información almacenada en sus servidores. Sin embargo, esta institución no posee un sistema dedicado a la protección de sus bases de datos y, por consiguiente, es sumamente vulnerable a los males mencionados anteriormente.

En ese sentido, Para y para mitigar estas amenazas, las instituciones deben realizar acciones programáticas para ello. Estas acciones son conocidas como Sistema de Gestión de Seguridad de la Información (SGSI) y contienen los pasos que debe seguir la organización, el personal calificado o indicado y la documentación necesaria para garantizar que el SGSI

pueda implementarse y produzca la respectiva retroalimentación. El concepto de SGSI aparece de forma clara en la pauta o norma ISO 27001, donde aparecen inmersos las recomendaciones en cuanto al tema de cuidado integral de la información [15, 2011, p.334].

En el presente trabajo se buscará desarrollar una propuesta de SGSI aplicable al portal web de la Universidad Tecnológica del Chocó, para minimizar los riesgos de ataques en los datos que sustentan información correspondiente al proceso de ingreso de notas en su Banco de datos web respectivo.

## II. PLANTEAMIENTO DEL PROBLEMA

La Universidad tecnológica del chocó, no tiene un sistema de seguridad de la información acorde a las exigencias de hoy, con el que pueda gestionar la detección de elementos que la vulneran, los peligros y la amenaza a las que periódicamente se ve expuesta la información en dicha organización; no se tienen ajustados o parametrizados controles que permitan disminuir ataques o delitos informáticos que colocan en riesgo la integridad, reserva y disposición de este vital tesoro en las organizaciones.

Se tienen procesos establecidos por iniciativa propia de los miembros del equipo de la oficina de Gestión Informática; como muestra, no se tiene una parametrización clara sobre el manejo de las credenciales de usuario, no se tienen registros de control y depuración de claves tanto para su creación como para la composición de las mismas.

La organización tiene muchos datos el crecimiento paulatino en sus diferentes áreas y en sus diferentes roles, producto de la apertura de nuevos programas, paralelo a ello se evidencia la carencia de adopción de procesos que permiten analizar sus riesgos de pérdida de información teniendo en cuenta los activos que directa o indirectamente son ligados al tema de salvaguardar este preciado Bien como está plasmado en la Metodología Magerit en la cual nos apoyamos para esta propuesta.

Si no se implementan buenas prácticas en el tema de aseguramiento de la información, luego de un meticuloso análisis de riesgos, se determina que muy seguramente la institución se verá en constante riesgo y en peligro del bien más preciado de las mismas alterando el funcionamiento Cohesionado en pro de evitar, ataques en las diferentes modalidades existentes que pueden ser intromisiones, alteración o raptos de información, alteración en los servicios además de otras consecuencias con estos ataques[1].

Este planteamiento muestra lo que cotidianamente sucede en casi todas las instituciones estatales en el tema de amenazas hacia el tesoro que para este caso es la Información que se produce desde y hacia las instituciones y aún más en las universidades del estado.

### *A. Antecedentes*

Un primer trabajo corresponde a Villena (2006) que realiza el trabajo de tesis de Gestión De Seguridad en organizaciones Financieras, que su finalidad es crear los lineamientos primordiales y de esta manera establecer, un buen modelo de o proceso de seguridad de información (SGSI) en una organización financiera del Perú, lo que se busca es tener un nivel adecuado, aplicando las estrategias que dan valor y con el cuidado a frente a los riesgos latentes que siempre aparecen para en cuanto al cuidado de la información y es donde la mejor alternativa es la implementación del SGSI.

EL autor en su investigación muestra cierta preocupación frente a la mirada que desde las instituciones financiera o en su efecto en todas miran al SGSI como una entidad que es complicada para ser implementada, dado los rigurosos procedimientos y exigencias para los usuarios y a los sistemas como tal, pero no obstante este sistema deben verlo como un objetivo que da valor a la empresa como tal y empoderar dicho sistema como, como herramienta de apoyo para la obtención de dichos objetivos.

(Rayme, 2007), presenta la aplicabilidad en términos de seguridad de información en las empresas o instituciones, dándole la misma importancia que en sus sistemas de Calidad o las líneas de producción que la caracterizan, lo que se quiere demostrar aquí como la aplicabilidad o implementación de políticas que para el tema de salvaguardar la información se requieren, tendrá los mejores resultados cuando se aplique a cabalidad en las instituciones que para este caso serían las universidades, especialmente en sus procesos más críticos como lo son Matricula, Admisiones, Grados entre otros, pues en estos servicios se recopila información trascendental y confidencial como lo es la información de Aspirantes, los que ya hacen parte de la institución, certificados para cualquier actor de la comunidad universitaria, los documentos se grados, Bases de datos del sistema financiero institucional, además de los correos institucionales, etc. Basados en esto se realizó un estudio en terceto de instituciones del orden superior de la capital de Perú en su zona metropolitana: la Universidad de San Marcos (UNMSM), la Nacional Federico Villarreal (UNFV) y la San Juan Bautista (UPSJB), y de esta manera hacer las respectivas propuestas que tienen como objetivo implementar políticas eficientes a través de la implementación de un adecuado Sistema de gestión para la seguridad de la información.

Ampuero (2011), en su proyecto o tesis en la cual propone principalmente un sistema de gestión para la seguridad de la información para una compañía de seguros cuyo objetivo principal es además de mostrar y recomendar las etapas correspondientes para la implementación de dicho sistema(SGSI), y que este a su vez debe adaptarse a cualquier tipo de organización sin importar que sea pública o privada, aunque la intención inicial sea para ser implementada en compañía de seguros, asumiendo de que la información es el activo máspreciado para toda organización, y es allí donde se ven obligadas a protegerla de la mejor manera, este proyecto, deja como insumo, el cómo desarrollar el diseño, dejando claro cómo se aplica el sistema de seguridad.

### III. JUSTIFICACIÓN

Actualmente, uno de los efectos colaterales post-pandemia (Covid 19) en las instituciones de formación académica, es el cierre total o parcial de sus aulas; es decir, los campus de estos organismos, se encuentran restringidos para el estudiantado (medida impuesta por el Ministerio Nacional de Salud). En consecuencia, la metodología que forzosamente han debido adoptar los colegios, institutos, academias, universidades y demás, ha sido la muy polémica “Virtualidad”. Pero, ¿qué relación puede tener esto con el tema en cuestión?, es muy simple, pues a día de hoy, la Universidad tecnológica del Chocó no cuenta con un sistema de seguridad de la información que le permita protegerse de manera óptima, de las posibles amenazas o riesgos informáticos a los que sitios así están expuestos normalmente. Por ende, existen muchos inconvenientes que giran en torno a la ausencia de algo que en la situación actual del sistema educativo (modalidad virtual), se hace sumamente indispensable, más aún cuando la institución en mención, ha ido creciendo significativamente, expandiendo su base de datos y sobre cargándose de información que no tiene cómo administrar o cómo controlar internamente.

No contar con una medida de seguridad en un sitio web o en servidores propios, es altamente peligroso en la actualidad, pues existe la abundancia de malware, el robo y la manipulación de datos, los espías informáticos, los fraudes de suplantación, el desfalco de cuentas institucionales, estafas virtuales a nombre de entidades de educación superior, entre otros. Estos inconvenientes, básicamente son la principal razón por la cual se debe implementar y/o desarrollar un sistema de gestión de seguridad de la información en la Universidad tecnológica del Chocó, para que esta logre una reestructuración y organización eficaz de sus bases de datos, con el fin de subsanar una evidente falencia y así, dar solución a una problemática que aplica para corto, mediano y largo plazo.

## IV. OBJETIVOS

### *A. Objetivo general*

Implementar un Sistema de Gestión de la Seguridad de la Información (SGSI) para el aseguramiento del proceso de ingreso de notas en un portal web universitario.

### *B. Objetivos específicos*

- Identificar los controles recomendados en la Norma ISO- 27001 para garantizar la confidencialidad, integridad, disponibilidad y no repudio de la información, para la protección de la información en Instituciones Universitarias.
- Realizar un análisis de riesgo para identificar los principales daños de los activos de información para el proceso de ingreso de notas de una universidad.
- Proponer un Sistema de Gestión de Seguridad de la Información (SGSI), enfocado en el aseguramiento de los riesgos identificados para el proceso de ingreso de notas.
- Verificar el Sistema de Gestión de Seguridad de la información propuesto en el portal web Universidad Tecnológica del Chocó.

## V. PROBLEMA DE INVESTIGACIÓN

¿De qué manera la implementación de un Sistema de Gestión de Seguridad de la Información puede minimizar los riesgos de ataques en los activos de información correspondientes al proceso de ingreso de notas en un portal web universitario?

## VI. MARCO TEÓRICO

Las bases de datos son básicamente el pilar de toda organización, pues en ellas reposa una cantidad significativamente importante de información de todo tipo; información cuyo fin es ser consultada, procesada, modificada y utilizada después por el mecanismo que la almacene o gestione. Esta especie de banco de información es la herramienta que más utilizan para la estructura de datos, es aquí bajo el concepto de Bases de datos donde se facilita la labor de integridad, oportunidad de la información tanto de los diseñadores de software, como de los usuarios finales [16]. A continuación, se señalan algunos puntos que se desprenden de este segmento; los cuales son: Sistemas de gestión de la seguridad de la información, seguridad de la información y controles de seguridad de la información, además de los referentes teóricos de cada uno de estos apartados.

### *A. Sistemas de Gestión de la Seguridad de la Información SGSI*

El SGSI (en inglés: information security management system, ISMS) es, un conjunto de pasos lógicos que utilizamos para administrar información este concepto es utilizado por la ISO/IEC 27001, que, aunque no es la única que existe se enmarca bajo este concepto.

Este conjunto de políticas, de procesos y de reglas que se plasman en el busca principalmente, asegurar la información, hacerla oportuna y confiable minimizando los riesgos, el SGSI debe propender por la efectividad y adaptación en la organización tanto internamente como en el entorno de la organización [1].

De esta manera estas reglas organizadas para la protección de la información en la medida que sean implementadas bajo la oportunidad, efectividad y óptima ejecución, se convierten en una herramienta poderosa de protección del activo informático.

También podemos describir este sistema en general como un trozo importante del sistema, que se apoya en dirección a la detección en primera medida a los riesgos que tienen o amenazan a la empresa, estableciendo creación, implementación, operatividad, supervisión, revisión mantenimiento y mejora en el nivel del aseguramiento de la información. Como resultado todo ello implica una operatividad en la organización en donde lo intuitivo pasara a segundo plano y se actuara tomando el control real sobre todo lo que tiene que ver con los sistemas automatizados que

sobre información en la organización se refiere. Esto permite conocer el funcionamiento de la organización, su funcionamiento y saber que hacer para mejorar.

La Norma expresa que como todo sistema de gestión plasma en su metodología, políticas, el planificarlas, los respectivos responsables, los procesos que se deben hacer y el recurso humano y económico. Es decir, la información documentada bajo las reglas de los sistemas de gestión ISO, las cuales siempre vienen documentadas siendo la manera adecuada de formalizar normas, y de esta manera hacerlas de fácil entendimiento en su transmisión o comunicación, y de otra manera comunicarla sería ambigua o de poca confianza transmitirla de forma verbal por ejemplo verbal, pues existiría una informalidad lo cual no es la finalidad de esta norma [2].

Es gracias a estas normas que las diferentes organizaciones estatales y privadas como el faro o referente guía para una adecuada implementación y formalización de las políticas logran un nuevo viraje que se le da a cualquier institución para salvaguardar la información mitigando al máximo el riesgo de pérdida, permitiendo el sostenimiento a través de la protección de los sistemas informáticos y la consecución de los objetivos que se han trazado las diferentes instituciones.

Es intrínseco afirmar que hoy en día las organizaciones sostienen sus negocios en sistemas informáticos que apoyan su continuidad, por ende, la consecución de sus objetivos trazados a corto, mediano y largo plazo. En base a ello, el concepto de Seguridad de la Información toma un sentido de vital importancia para el correcto resguardo y manipulación de la información. Por ello, ISO e ISACA, dos grandes entidades relacionadas a Sistemas de Información, la conceptualizan como la preservación de la confidencialidad, integridad y disponibilidad de la información de una organización, independiente del formato que tenga o se asocie, ya sea: físico, digital, electrónico, o de otras formas.

En la edición 27001:2007 (Ampliada con el Esquema Nacional de Seguridad):

Esta edición trata también de los requisitos del Esquema Nacional de Seguridad, reglamento de obligado cumplimiento para las Administraciones Públicas.

### *B. Contenido*

- Introducción a los Sistemas de Gestión de Seguridad de la Información (SGSI)
- Comprender la Norma UNE-ISO/IEC 27001
- Comprender la Norma UNE-ISO/IEC 27002

- Definición e implementación de un SGSI
- Proceso de certificación
- Relación entre los apartados de la norma y la documentación del sistema
- Correspondencia entre las Normas UNE-EN ISO 9001:2008, UNE-EN ISO 14001:2004 y UNE-ISO/IEC 27001:2007
- Caso práctico: modelo de SGSI
- Texto completo de la Norma UNE-ISO/IEC 27001:2007 "Tecnología de la información. Técnicas de seguridad. - Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos".

Nuevos apartados de esta segunda edición:

- Comprender el Esquema Nacional de Seguridad (ENS)
- Implementación del ENS
- Ejemplo práctico: plan de adecuación [3].

### *C. Seguridad de la información*

El concepto de seguridad de la información significa proteger la información y los sistemas de información de un acceso, uso, divulgación, alteración, modificación, lectura, inspección, registro o destrucción no autorizados.

La seguridad informática es el nombre genérico para el conjunto de herramientas diseñadas con el fin de proteger los datos almacenados en un equipo y evitar ataques de piratas informáticos. Seguridad en la red es el nombre genérico para el conjunto de herramientas diseñadas para proteger los datos durante su transmisión a través de una red de telecomunicación [5], lógicamente esta protección siempre debe estar acompañada del personal idóneo, que vigila la aplicación y el uso de las herramientas tecnológicas implementadas para ello.

Un SGSI tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada de la misma. La correcta gestión de la seguridad de la información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información [6], estos tres aspectos de conservación de la información son el pilar de todo SGSI en cualquier institución que busca calidad en el tratamiento ideal de su información.

El activo más importante que tiene una organización es la información y, por lo tanto, deben existir lineamientos claros que permitan su aseguramiento sin dejar de lado la seguridad física aplicada a los equipos donde se encuentra almacenada. Dichos lineamientos o técnicas están dadas por la seguridad lógica y aspectos de la seguridad física que permite la creación de barreras y procedimientos que resguardan la información y permiten el acceso a ella única y exclusivamente a personal autorizado [7], lo cual se garantiza con una optimización de recursos en todos los aspectos de la organización, permitiendo la adquisición de herramientas vanguardistas que permitan la exclusividad de acceso al personal autorizado.

La seguridad de la información está relacionada con las medidas preventivas, aplicadas con el fin de salvaguardar y proteger la información bajo la confidencialidad, disponibilidad e integridad. La información puede presentarse en diversos formatos y medios tanto físicos, como electrónicos. Por lo tanto, las organizaciones deben adoptar y adaptar metodologías para proteger los archivos y registros, mantener en funcionamiento una infraestructura tecnológica adecuada que sirva para la custodia y salvaguarda de la información [8], en este sentido se requiere la adquisición de sistemas compatibles para asegurar el correcto funcionamiento de la institución o empresa partiendo de que siempre la información es el recurso Vital de las mismas.

#### *D. Controles De Seguridad Según Norma ISO 27002*

En esta fase se hace el estudio de las causas que originan los hallazgos. Una vez confirmados, se definen los controles apropiados de acuerdo a la norma ISO/IEC 27002 se establece su tratamiento, y finalmente, se diseñan las políticas y procedimientos dentro de las cuales se incluyen los controles, y que finalmente irán en el diseño del SGSI.

Confirmados los hallazgos, se establecen los controles de seguridad como políticas y procedimientos de acuerdo a la norma ISO/IEC 27002, se definen los más apropiados para mitigar los riesgos y se adaptan para la organización. Luego se determina el tratamiento de los riesgos para aceptarlos, transferirlos a terceros o aplicar los controles y posteriormente éstos se integran a las políticas y a los procedimientos institucionales si existen.

Al culminar, se elabora el informe final que servirá de insumo para el diseño e implementación del SGSI teniendo en cuenta el ciclo de mejora continua PHVA que permita las

actividades para planear, hacer, verificar y actuar, que intervengan y permeen todos los procesos y servicios dentro de la organización [9], es decir mejoramiento continuo que garantice la calidad de los procesos y la disminución de fallas y la prevención y eliminación de riesgos potenciales.

Si bien el modelo PDCA(ciclo Deming) , es el estándar formal de ISO, éste se construye sobre una base que no necesariamente se aplica a todas las organizaciones, sobre todo cuando éstas no se han involucrado en procesos relacionados con normas ISO, por ello, con una base práctica se presenta, no omite ni restringe las actividades señaladas en el modelo formal, sino que se vale de ellas para sustentar un formato práctico de actividades que deben ser abordadas para lograr un adecuado nivel de seguridad de la información en las áreas de TIC en cualquier tipo de organización. Este modelo que se presenta a continuación reside en su aspecto operativo y práctico, puesto que se considera su estructuración, formación e implementación bajo dos grandes fases:

- Fase de Elaboración
- Fase de Aplicación

Estas fases contemplan el conjunto de actividades que de ellas se desprenden a fin de elaborar y aplicar correctamente el modelo [10], las actividades correspondientes a las fases de este modelo deben ser cíclicas y variarán dependiendo de la empresa u organización en la que se aplique y dependiendo del estado de avance que esta tenga en cuanto a temas de seguridad de información que están posean.

## VII. METODOLOGÍA

Son varias las metodologías desarrolladas para el análisis y gestión del riesgo, y todas, aunque tienen el mismo objetivo, se aplican de diferentes formas en cuanto a la evaluación de riesgos, por ello la selección de la metodología debe ser acorde con las necesidades de la organización para el cumplimiento de sus objetivos [11].

La obtención de una metodología adecuada garantiza en gran medida el éxito del sistema a implementar en la organización cualquiera que sea, pues es la plataforma que soporta el buen funcionamiento de las partes o procesos que conforman el todo para que los procedimientos y controles de seguridad que en últimas se implementaran deben funcionar milimétricamente bien para el éxito del todo que es el sistema de gestión de la seguridad que se ejecute.

Para la aplicación de metodologías de análisis de riesgos en una empresa En la actualidad, uno de los factores más importantes que se debe tener en cuenta en todo tipo de organizaciones es la seguridad de la información, ya que los incidentes relacionados con ésta, comprometen los activos de las empresas y las ponen en riesgo, lo anterior genera la necesidad de implementar sistemas de seguridad a partir de un análisis de riesgos y minimizar así consecuencias no deseada [12], es allí donde la aplicación y puesta en marcha de un Buen Sistema de Gestión de seguridad de la información que involucre a todos los actores de la organización y sensibilizarlos sobre el compromiso y responsabilidad del resguardo de la información que tienen desde el cargo que desempeñan. De allí la utilización de la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es reconocida por ENISA (Agencia Europea de Seguridad de las Redes y de la Información) y promovida por el Consejo Superior de Administración Electrónica con el fin de sistematizar el análisis de los riesgos que pueden presentar los activos de una organización, con base en esta descripción, se determinó que la metodología que brinda un mayor cubrimiento del riesgo, asociado a la seguridad de la información en una empresa es la MAGERIT, en la medida que contempla un análisis de riesgos más detallado, teniendo en cuenta la mayoría de los elementos que forman parte de los objetivos misionales de la organización, protegiendo los datos en los tres principios de seguridad de la información: integridad, confidencialidad y disponibilidad con algunos aspectos adicionales como su confiabilidad y que no permite arbitrariedades del analista, lo que la hace diferente a las otras metodologías mencionadas. Por otra parte, es importante mencionar que esta metodología tiene en cuenta el

riesgo efectivo (inicial), el riesgo residual (después de los controles) y el riesgo intrínseco (probabilidad de materialización de una amenaza) con el fin de asegurar desde todo ángulo los activos de la organización. Una de las principales ventajas que tiene esta metodología para las empresas dentro de sus sistemas de gestión de seguridad es que cuenta con una herramienta propia y permite dar un primer paso para una certificación, ya que se encuentra alineada con los estándares ISO (Organización Internacional para la Estandarización) [13].

Esta metodología a implementar es la más completa y pertinente para el objeto de este proyecto que busca en primera medida detectar y controlar los riesgos de la información a los que se ven abocados los diferentes dependencias de las instituciones educativas desarrollando un programa constante que compromete a todos y cada uno de los actores (Estudiantes, Docentes, Personal Administrativo, egresados, clientes externos...) a adquirir una actitud de detección y prevención de los riesgos permanentes a los que se ve abocada la información que estos administran desde su rol.

## VIII. RESULTADOS

### A. *Controles de seguridad basados en la norma iso 27001*

La norma ISO 27001 es el estándar más conocido en la familia de normas 27000 (Términos y definiciones de un sistema de gestión de la seguridad de la información), proveyendo los requerimientos para implementar un sistema de gestión de la seguridad de la información. Utilizar este grupo de estándares, ayudará a manejar la información corporativa de forma confidencial y segura, desde la información financiera, propiedad intelectual, detalle de los colaboradores o información de partes interesadas.

El número de controles es uno de los cambios importantes que presenta la edición 2013 de la norma en relación con la revisión de 2005. Antes, el anexo A tenía 133 controles. Sin embargo, la edición 2013 del estándar elimina algunos requisitos, tales como acciones preventivas, y el requisito para documentar ciertos procedimientos [17]. Es decir, a partir del año 2013, se sintetizó el anexo A buscando la estandarización de los controles estrictamente necesarios y que, además, proporcionarán en adelante mayor practicidad.

Básicamente, la norma ISO 27001 se compone de 114 controles de seguridad, los cuales están distribuidos dentro del Anexo A de esta norma en 12 grandes grupos:

- Políticas de seguridad de la información: A. 5.
- Organización de la seguridad de la información: A.6.
- Seguridad de los recursos humanos: A. 7.
- Gestión de Activos: A.8.
- Controles de acceso: A.9.
- Criptografía – Cifrado y gestión de claves: A.10.
- Seguridad física y ambiental: A.11.
- Seguridad operacional: A.12.
- Seguridad de las comunicaciones: A.13.
- Adquisición, desarrollo y mantenimiento del sistema: A.14.
- Gestión de incidentes de seguridad de la información A.16.

- Cumplimiento: A.18.

A continuación, se mencionarán las categorías que contienen los controles que pueden ser más aplicables a la finalidad de esta investigación:

#### *B. Políticas de seguridad de la información A.5*

En este grupo, se pretende brindar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones o leyes pertinentes. De esta sección se desprenden los siguientes controles:

##### *1) Políticas para la seguridad de la información:*

Es necesario determinar las políticas de seguridad, que sean aprobadas por medio de la dirección de la entidad a la cual vayan a ser aplicados; también, se deben dar a conocer públicamente y socializarse a los colaboradores, además de algunas partes externas que tengan cierta relevancia. Los siguientes son ejemplos sobre políticas de seguridad: control de acceso, clasificación y manejo de información, seguridad física y ambiental, etc.

##### *2) Revisión de las políticas de seguridad de la información:*

Estos lineamientos requieren acoplarse constantemente a las necesidades, modificaciones o novedades de la entidad pertinente, razón por la cual, se imposibilita que sean estáticos o fijos, y por ende, deben mantenerse en constante actualización.

#### *C. Organización de la seguridad de la información A.6*

En este grupo se debe plantear un cuadro de gestión para comenzar, regular e instaurar el establecimiento operativo de la seguridad interna de la entidad. En este segmento surgen 7 controles con diferentes objetivos.

- Funciones y responsabilidades de la Seguridad de la información
- Separación de funciones
- Contacto con autoridades
- Contacto con grupos de interés especial
- Seguridad de la información en la gestión de proyectos

Los siguientes son los mayormente relacionados con el presente proyecto:

1) *Funciones y responsabilidades de la Seguridad de la información:*

Se deben establecer las obligaciones de cada colaborador o de cada estación de trabajo con respecto al esquema de seguridad establecido.

2) *Separación de funciones:*

Evitar el ingreso inapropiado a las aplicaciones o sistemas que regulan y manipulan la información, a través de la división y asignación de funciones según las áreas pertinentes.

3) *Controles de acceso:*

Los estándares de control de accesos de la norma ISO 270001, están dirigidos a regular y monitorizar los ingresos a los medios de información según las políticas establecidas por la entidad [18].

En esta sección encontramos 8 controles, todos directamente aplicables al objetivo principal de este proyecto.

- Política de control de acceso
- Acceso a las redes y a los servicios de red
- Registro de usuarios y cancelación del registro
- Gestión de acceso a los usuarios
- Gestión de derechos de acceso privilegiados
- Gestión de la información de autenticación secreta de los usuarios
- Revisión de derechos de acceso de usuario

4) *Criptografía – Cifrado y gestión de claves A.10:*

Aquí se evidencian los lineamientos de regulación que permiten una función competente de la criptografía, utilizada con el propósito de salvaguardar la reserva y la entereza de la información, según lo indicado por la norma ISO 27001. En este segmento hay 2 controles.

- Política sobre el empleo de controles criptográficos
- Gestión de claves

5) *Seguridad de las comunicaciones A.13:*

En este componente se pretende consolidar el resguardo de la información en los sistemas adecuados y el resguardo base del soporte; también, se debe mantener un esquema de seguridad en torno a la información conmutada al interior de una organización y también con respecto a otras entidades [18]. En esta agrupación se encuentran 7 controles.

- Controles de Red
- Seguridad de los servicios de red
- Separación en redes
- Políticas y procedimientos de intercambio de información
- Acuerdos de intercambio de información

6) *Adquisición, desarrollo y mantenimiento del sistema A.14:*

Garantizar que la seguridad de la información se mantenga como parte integral de los sistemas de información en todo su ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan servicios a través de Redes públicas [19]. En este apartado se enfatiza en la esencia del sistema, que consiste en mirar constantemente su funcionamiento en las entradas durante el proceso y efectivamente, las salidas que deja verificando el nivel de calidad para lo cual se implementó.

- Análisis y especificación de los requisitos de seguridad
- Aseguramiento de los servicios de aplicación en las redes públicas
- Transacciones en línea
- Política de desarrollo seguro
- Procedimiento de control de cambio del sistema
- Restricciones a los cambios en los paquetes de software
- Principios de la ingeniería de Sistemas Seguros
- Pruebas de seguridad del sistema
- Pruebas de aceptación del sistema

7) *Gestión de incidentes de seguridad de la información A.16:*

Resulta prácticamente imposible que, a día de hoy, no existan ciertos incidentes informáticos en medio de una época sumamente digital. Por ende, se debe optar por modelos de seguridad basados en algunos protocolos o lineamientos, como es el caso de la norma ISO 27001.

Para solventar esta problemática, existen los siguientes controles:

- Responsabilidades y procedimientos
- Reporte de eventos de seguridad de la información
- Reporte de debilidades de seguridad de la información
- Evaluación y decisión sobre los eventos de seguridad de información
- Respuesta a incidentes de seguridad de la información
- Aprendiendo de los incidentes de seguridad de la información

## IX. ANÁLISIS DE RIESGO

Ejecutar un buen y efectivo SGSI es una labor fundamental en la protección de la información, dado que esto permite asegurar la integridad, disponibilidad y confidencialidad de los diferentes activos de información; sin embargo, esta es a su vez, un cometido arduo, pues busca disminuir los diferentes riesgos a los que la información se encuentra expuesta.

Voutssas M., J (2010) en su artículo “Preservación documental digital y seguridad informática” expone que es necesario contar con una base conceptual clara para comprender a cabalidad y de manera integral el concepto de seguridad informática. Entre estos conceptos están, *recursos informáticos*, hace referencia a todo lo que tiene que ver con los recursos o activos informáticos, aparece también el tema de *amenaza* la cual se refiere a la fuente o causa potencial de eventos o incidentes no deseados que pueden resultar en daño a los recursos informáticos, luego aparece el *Impacto*, este apunta a medir el impacto nocivo del evento clasificado como amenaza y en el mismo orden La *vulnerabilidad* o circunstancias de debilidad del recurso informático ,luego el *riesgo* que es la probabilidad de que un evento nocivo ocurra, todo esto ligado, al *principio básico de la seguridad informática* es el de mantener al mínimo los riesgos sobre los recursos informáticos[20].

A continuación, se desarrollará una búsqueda constante de examinar los peligros de los activos informáticos del principal claustro educativo de orden superior del Chocó.

### A. Identificación de activos

Con el fin de realizar un análisis de riesgos efectivo, se requiere identificar los activos de la Universidad Tecnológica del Chocó, la cual cuenta con cuatro salas de cómputo, dotadas con un total de 75 computadores conectados a Internet, además de plataformas, aplicaciones y bibliotecas que ofrecen diferentes servicios de información que serán explicados en los siguientes apartados [23], que además de no ser suficientes para la demanda de estudiantes, Docentes y Personal administrativos, requieren de actualizaciones en Hardware y software y controles de Seguridad.

### *B. Plataforma Academusoft*

Academusoft es una EAS (Enterprise Application Solutions), para las Instituciones de Educación Superior, la cual presenta una opción diferente a las usadas de forma común, hábil y segura para los diferentes procesos académicos y administrativos de la Universidad, buscando generar un mejor impacto en la optimización de la información [21]. Esta plataforma que se encuentra integrada con un número considerable de aplicaciones que le aportan a la institución un manejo más práctico de los diferentes componentes académicos y administrativos de la misma, cuenta con entornos gráficos que optimizan los tiempos de respuesta, este se encuentra sincronizado con los sistemas de información del Ministerio de Educación Nacional (MEN), buscando una mayor seguridad de la información almacenada en ella, como el registro de calificaciones, las clases, horarios de las mismas, liquidación de matrícula, entre otros. La composición de Academusoft se basa en diferentes áreas encargadas de realizar las diferentes gestiones requeridas dentro de la institución [21], que de alguna manera están cumpliendo con los objetivos para los cuales son usados en el momento por la comunidad Universitaria, aunque existen ciertas ambigüedades en su proceso:

### *C. Gestión colaborativa*

Esta área es la encargada de conectar la comunicación necesaria en la organización con sus diferentes apartados, de manera interna y externa, facilitando el trabajo de sus usuarios a partir de una amplia variedad de instrumentos aplicados de manera digital.

### *D. Gestión Extensión*

Esta área es específicamente un software diseñado con el fin de permitir un ingreso, registro, enumeración y seguimiento en los procesos académicos, administrativos y financieros entorno a los cursos que son ofrecidos por la universidad para los programas de "Educación no formal" del área de Extensión de la universidad. Este le permite a la universidad ejercer un control total sobre estos cursos y mejorar el orden de los mismos.

### *E. Gestión académica*

El área de Gestión académica es el encargado de apoyar aquellos procedimientos académicos de la Universidad, tales como la realización de pagos, contrataciones, suministro de

notas en las plataformas, comprendiendo así desde aquel interés en ingresar a la universidad hasta el proceso de grado y profesionalización del estudiante. Este aplicativo es ideal para garantizar claridad en los procesos y le permite también al estudiante tener una relación interactiva con los temas de su interés como su registro y calificaciones.

#### *F. Gestión administrativa y financiera*

Esta gestión es sumamente necesaria para las instituciones, pues ofrece una solución integral en cuanto a administrar cuentas, gestionar información financiera, de proveedores y clientes, ordenar datos de inventarios, distribución y logística de la institución, facilitando el manejo administrativo y financiero. Permite tener claridad en los recursos financieros de la universidad, logrando así evitar errores comunes por fallos en las cuentas, que traen por consiguiente déficit presupuestales gigantes si no son abordados a tiempo.

#### *G. Gestión docencia*

Ahora bien, la docencia forma parte esencial de la entidad Universitaria, puesto que conforma un estamento de trabajadores clave en el quehacer de la institución, por ello este módulo es de gran utilidad, ya que ofrece una variedad de herramientas para garantizar la praxis del docente, tales como bibliotecas, instrumentos digitales y demás.

#### *H. Gestión investigación*

El área investigativa en una institución constituye su aporte a la sociedad, a la nación, a la ciencia y al mundo en general, por tal motivo es necesario contar con herramientas que impulsen y optimicen estos recursos, permitiendo una mejor administración de los proyectos, semilleros, publicación o grupos que giren en torno a ello.

#### *I. Gestión Administrativa y Financiera – Gestasoft*

Gestasoft es el encargado de realizar las gestiones administrativas y financieras de la Universidad, apoyando a los trabajadores de estas dependencias en la toma de decisiones de forma acertada y rápida, ya que resume de forma correcta toda la información que se administra en las diferentes áreas y dependencias de la institución [22]. Logrando posicionarse como una excelente solución a las diferentes problemáticas en relación al orden de la información que maneja toda la

organización en general, que, al ser una institución grande, maneja así mismo una gran cantidad de información.

Esta presenta una solución acertada como opción de gran nivel para la gestión de la información producida por la institución; este componente integra a su vez, una gran cantidad de aplicaciones adaptables que potencian las formas de uso con entornos gráficos que facilitan el tiempo de respuesta.

Con la implementación de esta área de Gestasoft, se le posibilita a la universidad realizar el manejo de las cuentas e información financiera con respecto a clientes o proveedores, mejorar la correcta colocación de los datos de inventario, distribución y logística de cualquier organización de carácter público o privado, facilitando el manejo administrativo y financiero. Además de esto, esta área hace uso de una base de datos que permite un mejor flujo de la información toda la institución y está esbozado con el fin de mejorar la visibilidad y el control que tiene la información, dando como resultado la obtención de objetivos como la mejora en el inventario y por ende en los costos, que se ve reflejado en la potencialización de los proyectos cuando estos sean llevados a cabo [22], es en este sentido que las organización de educación superior cualifican sus condiciones para prestar un servicio más seguro y oportuno de sus líneas principales de servicio.

#### *J. APP UTCH Móvil*

La Universidad Tecnológica del Chocó Diego Luis Córdoba a partir de la necesidad que los estudiantes manifestaron, cuenta con una aplicación con una nueva vía de consulta para sus calificaciones, liquidaciones, horarios de clases, entre otras. La comunidad estudiantil puede acceder desde su dispositivo móvil a información de interés, tales como académica o financiera, cuenta con la oportunidad de observar los créditos académicos cursado, aprobados y faltantes, promedios, e información financiera como deudas, liquidaciones y pagos. Esta aplicación está disponible para las operativos IOS y Android, con el nombre Estudiantes UTCH [14], son las posibilidades que en el momento poseen para de alguna manera aumenten el acceso a los servicios como estudiantes pues son lavase de funcionamiento de la Institución.

#### *K. Bibliotecas*

La biblioteca de la Universidad Tecnológica del Chocó cuenta con una biblioteca virtual amplia, con una gran variedad de bases de datos en las diferentes áreas disciplinarias, como cultura

general, matemática, derecho, ciencias de la salud, biología, investigación, ingeniería, ciencias sociales, ciencias de la administración y contabilidad derecho [14], es de anotar que esta área cumple con los requerimientos actuales de Docentes y Estudiantes, dada la posibilidad de interconexión con las Bibliotecas virtuales más grandes del mundo.

#### *L. Riesgos y amenazas*

El análisis de riesgos informáticos es el examen que se le realiza a los diferentes peligros que pueden llegar a afectar el sistema a nivel informático y que además pueden conllevar a situaciones de amenaza de la integridad como robos y producir, a su vez ataques externos que paralicen el funcionamiento del sistema al comprometer los datos y la información. Por esto es necesario realizar el análisis de los riesgos, para determinar cuáles son sus debilidades y así prevenir que estos sucesos se presenten.

Los riesgos que posee la Universidad Tecnológica del Chocó son los siguientes:

- Los servicios de Información queden inhabilitados y estén fuera de operación: La Universidad posee unas plataformas y aplicativos mencionados en el apartado anterior, donde se realizan el registro de calificaciones, de clases, se pueden ver las calificaciones, horarios de clases, liquidación de matrícula, entre otros; existe el riesgo de que estas queden inhabilitadas, a causa del pago inoportuno de los servicios informáticos, errores en el hardware y/o software, bajones y pérdidas de suministro de energía, infraestructura tecnológica obsoleta, y por último, se pueden presentar errores o fallas en el proceso de actualización de la información. En la actualidad, como el control que ejerce la universidad ante este riesgo es una oportuna notificación al proveedor encargado de estas plataformas que es necesario programar un mantenimiento de la misma, además de realizar oportunamente el pago de los servicios informáticos para evitar cortes y fallas en este sentido. Por otra parte, también está la posibilidad de verse amenazados por ciberdelincuentes, que busquen tergiversar o robar información o generar fallos en los servidores por medio de ataques de denegación de servicio DDoS, los cuales inutilizan los sistemas informáticos u otros tipos de ataques.

- Omisión de lineamiento y política sobre el uso de recursos informáticos: La Universidad cuenta con una serie de lineamientos y políticas respecto al uso de los recursos informáticos, sin embargo se presenta un amplio desconocimiento por parte de los funcionarios de la institución, además de que aquellos que tienen conocimiento de los mismos, tienden a omitir, sin embargo el no cumplimiento de los mismos trae como consecuencia el riesgo de ser sancionados por parte de la ley, además de afectar la imagen de la institución. Por parte de la institución han ido promoviendo el cumplimiento de los lineamientos y política sobre el uso de recursos informáticos, a través de boletines informativos a las diferentes dependencias y estamentos universitarios.
- Pérdida de información: Las Instituciones de Educación Superior cuentan una amplia cantidad de información, de sus diferentes estudiantes, programas académicos, docentes, egresados y diferentes dependencias de la misma, toda esta se encuentra almacenada en diferentes servidores y portales web, toda esta información se encuentra en altos niveles de riesgo, puesto que pueden presentarse falencias en la generación de copias de seguridad de los equipos servidores, en los controles de seguridad informática y fallas en la infraestructura tecnológica. Esta pérdida de la información puede ser ocasionada por robos, ataques informáticos, incumplimiento de la gestión institucional, y por mal manejo de la misma. En ese sentido, la institución ha implementado la tercerización del servicio de copias de seguridad de la información de los sistemas de misión crítica, igualmente la implementación del respaldo de la información en la nube mediante el uso de la herramienta OneDrive Institucional.
- Planta o soporte de energía (UPS): La importancia de las UPS está inmersa en lo necesario que resulta contar con un Sistema de Alimentación Ininterrumpida (UPS o SAI), pues este permite que las empresas adquieran tranquilidad al momento de adquirir este tipo de sistemas y proporciona mayor seguridad, concretamente para que, en caso de producirse un problema eléctrico, las infraestructuras de la entidad sigan funcionando con total normalidad. Actualmente el soporte de energía que respalda los equipos del Datacenter no son los adecuados como lo exige la norma, La Ubicación de la oficina debería estar en un segundo piso.

- Infraestructura deficiente: dada la infraestructura física de 15 Bloques, algunos a más de 200 metros de distancia, hay una falta de Segmentación de switches, para tener subredes por bloques o por oficinas (ejemplo haciéndola a través de VLAN).
- Datacenter: este se encuentra ubicado en el primer piso de la Universidad. Se debe reubicar estratégicamente para mayor seguridad, pues no es factible que se encuentre a simple vista y, además, es necesario que su ubicación esté en un espacio con la temperatura adecuada para evitar el sobrecalentamiento de los servidores y prevenir un inconveniente mayor.

TABLA I  
ANÁLISIS DE LAS DEFICIENCIAS

Riesgo	Actividad de Mejora	Instrumentos o recursos.	Responsable
Los servicios de Información queden inhabilitados y estén fuera de operación:	Plataformas queden inhabilitadas: -Pago inoportuno de los servicios informáticos -errores en el hardware y/o software -bajones y pérdidas de suministro de energía, -infraestructura tecnológica obsoleta -errores o fallas en el proceso de actualización de la información	Oportuna notificación al proveedor de estas plataformas: -programar un mantenimiento de la misma -realizar oportunamente el pago de los servicios informáticos para evitar cortes y fallas en este sentido.	Universidad Proveedores de Tecnología.
Omisión de lineamiento y política	-desconocimiento por parte de los	Promoción y Sensibilización del	Alta Gerencia Funcionarios

sobre el uso de recursos informáticos:	funcionarios de la institución -Omisión por parte de aquellos que sí cuentan con conocimiento	cumplimiento de los lineamientos y política sobre el uso de recursos informáticos: -boletines informativos a las diferentes dependencias y estamentos universitarios.	
Pérdida de información:	Falencias en la generación de copias de seguridad de los equipos servidores, en los controles de seguridad informática y fallas en la infraestructura tecnológica, por: -robos -ataques informáticos -incumplimiento de la gestión institucional	-Tercerización del servicio de copias de respaldo o aseguramiento de la información de los sistemas de misión crítica. -la implementación del respaldo de la información en la nube mediante el uso de la herramienta OneDrive Institucional.	Institución Terceros
Planta o soporte de energía	Soporte de energía que respalda los equipos del Datacenter no son los adecuados como lo exige la norma	Sistema de Alimentación Ininterrumpida proporciona mayor seguridad para que en caso de producirse un problema eléctrico, las	Universidad

		infraestructuras de la entidad sigan funcionando con total normalidad.	
Infraestructura Física	Infraestructura física de 15 Bloques, algunos a más de 200 metros de distancia	Hay una falta de Segmentación de switches, para tener subredes por bloques o por oficinas	Universidad Alta gerencia
Ubicación del Datacenter	ubicado en el primer piso de la Universidad	Se debe reubicar estratégicamente para mayor seguridad	Universidad Alta Gerencia  Funcionarios encargados
Gestión del cambio, para la adopción de normas de Seguridad.	La organización en sus diferentes roles no hace el uso adecuado de los recursos informáticos y por desconocimiento de la importancia de la seguridad de la información como el tesoro más preciado de la misma ( <i>no prioriza en la inversión de adquisición de controles</i> ) se hace cada vez más vulnerable	Adquisición de Controles que permitan asegurar la información (Hardware - Software)	-Toda la Comunidad Universitaria en sus diferentes Roles -Alta Gerencia

Nota: Elaboración propia

## X. PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL PORTAL DE NOTAS DE LA UTCH

Asegurar la información, con base en la normativa ISO 27001, se refiere a preservar la confianza, integridad y disposición, igualmente los sistemas comprometidos con su tratamiento, en toda institución cualquiera sea su misión. Lo que nos garantiza que el aseguramiento de la misma es tratado o procesado adecuadamente es identificando principalmente su ciclo de vida y aquellos puntos relevantes implementados para mantener su C-I-D:

- Seguridad (Confidencialidad): Esta no está a disposición de actores a los cuales no se debe mostrar y mucho menos dar disponibilidad de la misma a procesos o instituciones no autorizadas.
- Probidad (Integridad): mantener de la fidelidad y completitud de los datos y la metodología de proceso.
- Oportunidad (Disponibilidad): acceder y utilizar la información y las herramientas tecnológicas de procesamiento de esta a través de los usuarios, entidades autorizadas para procesarla cuando sea requerido. Basados en el empoderamiento y el conocer los ciclos de vida por cada dato o información relevante se debe aplicar el uso de procesos sistemáticos, ordenados, documentados y conocidos por cada usuario de la institución desde una mirada de riesgo organizacional o institucional. Es allí donde constituimos o se implementa u verdadero SGSI.

### A. *Plan de mejora para el portal web de notas en la UTCH*

Si no se cuenta con una buena administración de la seguridad informática en las organizaciones, ya se sabe que el riesgo de daños y pérdidas asociados a la información y los datos se incrementa; por lo tanto, dentro de la estructura interna de la entidad, la Gerencia, según SGSIBlog [23] debe trazar políticas que respalden la seguridad informática en ella, la aplicación de la Norma ISO 27001 y el establecimiento de un Sistema de Gestión que debe abarcar toda la entidad con criterios de colaboración entre dependencias, sus jefes y su personal.

La gestión de la seguridad informática se debe realizar a través de un proceso continuo, complejo y dado a conocer a todos los miembros de la entidad, y a tal proceso se le conoce como su SGSI, que tiene como fundamento para su implementación la Norma NTC ISO 27001:2013. Sólo así se puede tener un cierto (no total) nivel de protección de la información y los datos, porque con un SGSI se logran minimizar los riesgos, conocer los que se mantienen y estar alerta frente a ellos.

Lo que se propone para la implementación de un SGSI dentro de la universidad UTCH y los beneficios que causaría serían, entre otros:

- A partir del análisis de riesgos se pueden identificar las vulnerabilidades y verificar los impactos que se presentan por las actividades realizadas por toda la comunidad universitaria, que puede generar diferentes amenazas y poner en peligro la información como activo primordial.
- Cuando se hace la correcta implementación del SGSI es posible garantizar en su totalidad que la información se encuentre disponible en cualquier momento, que se encuentre segura y que por lo tanto la Universidad puede realizar sus actividades sin tropiezos y tanto con seguridad como con garantía de la disponibilidad y continuidad del negocio.
- Al tener implementado el SGSI se disminuyen en su mayoría las posibilidades de incidentes, lo que se puede traducir en la disminución de costos producidos por ataques informáticos que pueden llevar a pérdidas de información y por lo tanto a pérdida de dinero, entre otros.
- También, ayuda a mejorar la percepción que tiene toda la comunidad universitaria frente a, por ejemplo, la navegación (internet e intranet), ya que de esta manera se asegura la información personal y se evitan problemas a profesores, alumnos y comunidad en general.

*1) Hoja de ruta:*

Las indicaciones pertinentes para llevar a cabo la propuesta del esquema de seguridad, que tienen como objetivo que la universidad estudie, apruebe e implemente estas políticas, para así contar con un correcto uso por parte del plantel de la institución, se desglosan a continuación:

En la hoja de ruta se plantean 6 fases a seguir para garantizar la óptima implementación del SGSI, éstas son:

2) *Desarrollo de las políticas:*

Esta fase hace referencia al proceso de elaboración de las políticas a implementar para la mejora de la seguridad informática, donde la Universidad Tecnológica del Chocó debe delegar responsabilidades a las diferentes áreas con el fin de desarrollar la creación de dichas políticas, escribirlas, estructurarlas y finalmente aprobarlas.

3) *Cumplimiento:*

En esta fase las políticas anteriormente planteadas son llevadas a cabo, deben ser implementadas y enlazadas con los sistemas de seguridad.

4) *Comunicación:*

Fase en la cual se da difusión de dichas políticas implementadas por la Universidad a los diferentes estamentos como los estudiantes, los docentes, funcionarios y demás.

5) *Monitoreo:*

Para esta fase las políticas ya deben estar en funcionamiento y deben ser debidamente monitoreadas, con el fin de establecer la efectividad de las mismas y el cumplimiento de sus funciones.

6) *Mantenimiento:*

Periódicamente es necesario realizar actualizaciones a las políticas implementadas, por ello esta fase hace hincapié en la necesidad de mantener la política actualizada, íntegra, además que se le realicen los ajustes necesarios obtenidos de los monitoreos realizados.

7) *Retiro:*

Esta fase determina la eliminación de una política de seguridad en el momento en que ésta sea insuficiente, haya cumplido su función, o ya no sea necesaria para el portal universitario.

## *B. Pautas en la política de seguridad del manejo de la información*

### *1) Copias de seguridad de la información:*

En este apartado se hace énfasis en la importancia y la pertinencia del establecimiento del respaldo masivo de datos, la ejecución de actividades y el dimensionamiento de algunos mecanismos precisos para un correcto Backup.

### *2) Centros de datos:*

Se hace necesario ubicar la información en Centros de Datos óptimos, que cumplan con los debidos estándares internacionales, donde los elementos tecnológicos que integren las diferentes plataformas se encuentren seguros y libres de vulnerabilidades.

### *3) Cierre de credenciales o cuentas de acceso:*

Aquí se gestiona la suspensión y el retiro de correos institucionales o correos de ingreso de alumnos retirados. Como se indica en el título, tiene que ver con la suspensión de cuentas de correo electrónico y credenciales de acceso a personas que se retiran.

### *4) Control de acceso:*

El acceso a las diferentes plataformas con las que cuenta la universidad es un tema muy delicado, por ende, se hace necesario prevenir y controlar el acceso de los usuarios y sus claves exigiendo cambios periódicos para evitar filtraciones y robos de identidad.

### *5) Resguardo del posible software malicioso:*

Se refiere a la instalación, conformación y reestructuración a nivel de software de los equipos de cómputo; es decir, a la constante revisión, al mantenimiento y a la limpieza frecuente del software contra códigos maliciosos. La actualización del sistema antivirus se debe llevar a cabo desde un servidor dedicado y aplicarlo a las estaciones de trabajo en periodos de tiempo distribuido.

### *6) Transferencia de información:*

Se deben implementar documentos de aceptación de las políticas de seguridad por parte de los involucrados, junto a firmas de cláusulas previamente definidas de confidencialidad, así mismo

determinar las acciones ante incumplimiento de dichos acuerdos por parte del esclarecimiento de los mecanismos y protocolos a emplear, el empleo de controles criptográficos, entre otros.

7) *Seguridad de software:*

Para mantener una óptima seguridad del software de la Universidad Tecnológica del Chocó, es necesario que las normas de desarrollo se encuentren alineadas a las normas ISO, además de que sean planeadas y desarrolladas capacitaciones y auditorías, acuerdos de licencias, propiedad de código y derechos de propiedad intelectual.

8) *Protección de datos personales:*

Esta política hace referencia al trato de la información personal depositada en las arcas de la Universidad, los derechos de los titulares, la legitimación, las condiciones, las autorizaciones, y la finalidad a la cual serán sometidos, además de los canales habilitados para peticiones, consultas y reclamos, y por último el debido aviso de privacidad en caso de ser necesaria la utilización de sus datos personales en condiciones diferentes a las pactadas.

## XI. CONCLUSIONES

La elaboración de la presente investigación se desarrolló apoyada en la evidente necesidad que tiene la Universidad Tecnológica del Chocó de implementar un Sistema de Gestión de Seguridad de la Información, que le permita administrar de manera correcta y ordenada toda la información de los procesos internos que confieren al almacenamiento y procesamiento de notas en su portal web. Así pues, se llegan a entender los activos de información informáticos como la mejor alternativa en la contemporaneidad, dada su enorme practicidad; sin embargo, se debe contar con un esquema de seguridad que proteja el portal web de los tantos riesgos a los cuales se expone

todo tipo de información en la web. Bajo este espectro, se entiende que las amenazas informáticas presentadas a lo largo de este proyecto, afectan el portal web de la UTCH; estas corresponden a las actividades desarrolladas mediante software, al uso indebido de herramientas y a la manipulación de información, lo que traería consecuencias significativamente negativas en el contenido que la Universidad administra en este espacio, incurriendo de esta forma en fraude y robo de sus bases de datos.

Por tanto, es pertinente seguir los lineamientos de la norma ISO 27001, utilizando este grupo de estándares, que ayudará a manejar la información corporativa de forma confidencial y segura; partiendo desde la información financiera, propiedad intelectual, detalle de los colaboradores o información de partes interesadas. De esta manera, se establece bajo una identificación de riesgos las acciones a seguir para la mejora continua y la solución de necesidades específicas en el control de información y manipulación de la misma.

Gracias a estos datos se puede implementar un nivel de protección seguro a la hora de subir las notas en internet, así los estudiantes no temerán de perder su progreso y se evitaría la suplantación de identidad, pérdidas de datos y ataques informáticos masivos en el campus de UTCH. Por ello, la propuesta presentada en esta investigación es coherente con las necesidades de la institución, toda Universidad o Centro Educativo debe contar con un esquema seguro y eficiente que resguarde las bases de datos internas y evite que esta información se manipule indebidamente, en especial los portales web que se encargan de manipular la información del desempeño académico de los estudiantes, garantizando así su seguridad académica.

## REFERENCIAS

- [1] J. J. Perafán Ruiz and M. Caicedo Cuchimba, “Análisis de riesgos de la seguridad de la información para la institución universitaria Colegio Mayor del Cauca.,” 2014.
- [2] J. P. Rodríguez Guerra, “Diseño de una metodología para la implementación y gestión de un sistema de seguridad para servicios transaccionales en instituciones financieras de la economía popular y solidaria basada en las buenas prácticas de la PCI DSS, caso de estudio Cooperativa de Ahorro y Crédito Construcción Comercio y Producción.,” 2019.
- [3] L. G. Álvarez, “Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información.”

- AENOR, 2012.
- [4] M. R. Torres León, “Diseño de un sistema de gestión de la seguridad de la información (SGSI), basada en la norma ISO/IEC 27001: 2013, para el proceso de servicio post-venta de un integrador de soluciones en Telecomunicaciones.”
- [5] M. Soriano, “Seguridad en redes y seguridad de la información,” *Obtenido [http://improvet.cvut.cz/project/download/C2ES/Seguridad\\_de\\_Red\\_e\\_Informacion.pdf](http://improvet.cvut.cz/project/download/C2ES/Seguridad_de_Red_e_Informacion.pdf)*, 2014.
- [6] E. I. Chilán-Santana and W. F. Pionce-Pico, “Apuntes teóricos introductorios sobre la seguridad de la información,” *Dominio las Ciencias*, vol. 3, no. 4, pp. 284–295, 2017.
- [7] J. J. Perafán Ruiz and M. Caicedo Cuchimba, “Análisis de riesgos de la seguridad de la información para la institución universitaria Colegio Mayor del Cauca.,” 2014.
- [8] F. N. S. Solarte, E. R. E. Rosero, and M. del Carmen Benavides, “Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001,” *Rev. Tecnológica-ESPOL*, vol. 28, no. 5, 2015.
- [9] F. N. S. Solarte, E. R. E. Rosero, and M. del Carmen Benavides, “Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001,” *Rev. Tecnológica-ESPOL*, vol. 28, no. 5, 2015.
- [10] J. B. Salazar and P. G. Campos, “Modelo para Seguridad de la Información en TIC,” *Concepción, Chile Univ. del Bío-Bío*, 2008.
- [11] Octave, Magerit, Mehari, NIST SP 800:30, Coras, Cramm y Ebios
- [12] A. del C. A. Estupiñan, J. A. Pulido, and J. A. B. Jaime, “Análisis de Riesgos en Seguridad de la Información,” *Ciencia, innovación y Tecnol.*, vol. 1, pp. 40–53, 2013.
- [13] A. del C. A. Estupiñan, J. A. Pulido, and J. A. B. Jaime, “Análisis de Riesgos en Seguridad de la Información,” *Ciencia, innovación y Tecnol.*, vol. 1, pp. 40–53, 2013.
- [14] Universidad Tecnológica del Chocó Diego Luis Córdoba. Quibdó. Chocó recuperado de: <https://www.utch.edu.co/nueva/>
- [15] Ladino, M. I., Villa, P. A., & López, A. M. (2011). Fundamentos de iso 27001 y su aplicación en las empresas. *Scientia et technica*, 17(47), 334-339.
- [16] Camps, R. Casillas, L. Costa, D. Ginestà, M. Escofet, C. Mora, O. (2005). “Software libre, bases de datos”. Fundació per a la Universitat Oberta de Catalunya. Barcelona. Recuperado de: <https://www.uoc.edu/pdf/masters/oficiales/img/913.pdf>.

- [17] Escuela Europea de Excelencia, (2019). “El Anexo A y los controles de seguridad en ISO 27001”. Recuperado de: <https://bit.ly/3vtlGar>.
- [18] ISO 27001, (SF). “ISO 27001 AL COMPLETO”. Recuperado de: <https://bit.ly/3xql0UQ>
- [19] Solarte Solarte, F. N., Enriquez Rosero, E. R., & Benavides, M. del C. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica - ESPOL, 28(5). Recuperado a partir de <https://bit.ly/3iEwHW>
- [20] VOUTSSAS M., Juan. 2010. Preservación documental digital y seguridad informática. Investig. bibl 24(50)., pp.127-155. ISSN 2448-8321. Disponible en: <https://bit.ly/3cJZIt8>
- [21] Universidad de Pamplona. (sf). Academusoft. Centro de Investigación Aplicada y Desarrollo en Tecnologías de Información. Recuperado de: <https://bit.ly/3xoEgSG>
- [22] Universidad de Pamplona. (sf). Gestión Administrativa y Financiera - Gestasoft. Centro de Investigación Aplicada y Desarrollo en Tecnologías de Información. Recuperado de: <https://bit.ly/3vrMpnX>
- [23] Control Interno. (2015). Relatoría RENDICIÓN DE CUENTAS. Universidad Tecnológica del Chocó “Diego Luis Córdoba”. Quibdó. Chocó. Disponible en: <https://bit.ly/3zrW1SN>