Plan Director de Seguridad para una universidad colombiana

Trabajo Final del Máster - Memoria

Desarrollado por:

Ana Rocío León Lugo

Consultor:

Msc. Antonio José Segovia Henares

Profesor responsable:
PhD. Carles Garrigues Olivella

MÁSTER INTERUNIVERSITARIO EN SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES – MISTIC

7 de Junio de 2017

AGRADECIMIENTOS:

A mi familia por ser mi soporte y la razón para vivir y darme motivos para ser feliz.

A L. por creer, confiar en mí, darme alegría, cariño y motivación para trabajar.

A mi consultor Antonio, por su paciencia y por ser siempre el faro que me lleva a buen puerto.

A mi tutor Juan José por su orientación y consejos.

Al Ingeniero Fernando y compañeros de la universidad, por permitirme trabajar y atender mis sugerencias.

A mis queridos amigos, por estar siempre presentes, incluso ante la distancia.

Que Dios los bendiga.

RESUMEN

El presente proyecto tiene como objetivo desarrollar el Plan Director de Seguridad de la Información para una universidad colombiana, orientado a reducir los riesgos a los que está expuesta la información hasta unos niveles aceptables a partir del análisis del inventario de activos, aplicando la metodología de Análisis y Gestión de riesgos MAGERIT, la norma ISO/IEC 27001:2013 y 27002, como base para la implementación del Sistema de Gestión de Seguridad de la Información, basado en el concepto de mejora continua.

Dicho Plan Director tomará como insumos el análisis diferencial en materia de seguridad de la información de la Universidad y los resultados del análisis de riesgos para plantear un conjunto de proyectos, que permitan generar la base del Sistema de Gestión de Seguridad de la Información. Adicionalmente se entrega el modelo de madurez en materia de seguridad de la información de la Universidad, usando los controles ISO/IEC 27002:2013.

ABSTRACT

The present project aims to develop the Information Security Master Plan for a colombian University, it is aimed at reducing the risks to which the information is exposed until reaching acceptable levels from the analysis of the inventory of assets, it is aimed at reducing the risks, to which the information is exposed starting from the analysis of the inventory of assets until achieving acceptable levels of security, This will be achieved by applying the MAGERIT Risk Analysis and Management methodology, ISO/IEC 27001: 2013 and 27002, as the basis for the implementation of the Information Security Management System, based on the concept of continuous improvement.

This Master Plan will take as input the differential analysis in the field of information security of the University and the results of the risk analysis in order to propose a set of projects, which will generate the basis of the Information Security Management System. Additionally, the university's data security maturity model is delivered using the ISO / IEC 27002: 2013 controls.

Contenido

LISTA DE FIGURAS

LISTA DE TABLAS

1. INTRODUCCIÓN

Las tecnologías de la información y las comunicaciones vienen dando un gran soporte a los procesos organizativos de las entidades educativas, tanto en el apoyo al funcionamiento como para la toma decisiones estratégicas que propendan para el cumplimiento de sus metas. La mayoría de los procesos son soportados, gestionados y automatizados por sistemas informáticos. En una universidad colombiana, dichos sistemas de información cuentan con interfaces que permiten a los miembros de la Comunidad universitaria ubicados dentro y fuera del campus, realizar consultas y modificación de información desde cualquier lugar del mundo.

En dicho escenario de alta conectividad, que la mayoría de los procesos organizativos en las Universidades se soportan en su infraestructura tecnológica, se cuenca con innumerables ventajas, pero a la vez, conlleva un conjunto de riesgos en el manejo de datos confidenciales y en la disponibilidad de los servicios que presta la Universidad y hace que la seguridad de la información sea uno de los puntos fundamentales a tener en cuenta para la continuidad de los procesos relacionados con su misión crítica y la operatividad en los niveles acordados a pesar de dichos riesgos.

Organizaciones del tamaño de una universidad colombiana deben manejar el tema de la seguridad de la información de forma metodológica, planificada, con enfoque de continuidad del negocio y de mejora continua. Además es fundamental tener en cuenta su participación en el entorno en la que se deben obedecer regulaciones, garantizar la protección de los datos de carácter personal de los miembros de la comunidad universitaria y de empresas con las que se tiene relación de carácter contractual.

El desafío de la Universidad en seguridad de la información es por tanto, encontrar e implementar una metodología que conduzca al desarrollo de su Sistema de Gestión de Seguridad de la Información, que provea los niveles de seguridad requeridos, y que sustenten la confianza necesaria a la misma entidad, a sus socios de negocios y a sus usuarios (alumnado, cuerpo docente y administrativo y directivos), teniendo en cuenta:

- Las necesidades de los procesos del negocio con respecto a la información, aplicaciones y servicios telemáticos.
- El uso eficaz y eficiente de los recursos tecnológicos como soporte a dichos procesos de negocio.

- El desarrollo de un enfoque estratégico, racional económicamente y proactivo para la evaluación y tratamiento de riesgos, con criterios amplios y basados en costo-beneficio.

1.1. Planteamiento del problema

Debido al tamaño de la Universidad, a la cantidad de procesos soportados por la tecnologías de información, a la legislación actual colombiana, la cual obliga a la Universidad a velar por la protección de los datos personales de los miembros de la Comunidad Universitaria y a los nuevos problemas que está enfrentando la Universidad en materia de TICS, se hace fundamental el planteamiento de una estrategia en materia de la seguridad de la información.

La norma internacional ISO/IEC 27001 en su versión 2013 se adecúa de forma coherente al sistema de calidad de la Universidad, debido a los cambios que se realizaron respecto a la versión anterior y además es certificable, por lo que la Universidad, por lo que la alta dirección se encuentra interesada en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).

Pero dicha implementación debe ser realizada en el marco de un diagnóstico del estado actual en el que se encuentra la Universidad y de la mano de una metodología adecuada para realizar dicha implementación, la cual será implantada a través de un conjunto de proyectos de seguridad de la información. El objetivo de dichos proyectos será encaminado a reducir los riesgos a los que se expone la organización a unos niveles aceptables.

1.2. Alcance del Plan Director

El alcance que tiene el Plan Director para esta organización viene determinado en la importancia que la Universidad plantea para la implementación del Sistema de Gestión de Seguridad de la Información y la posterior certificación en la norma ISO 27001, ajustando los procesos al ya implementado Sistema de Gestión de la Calidad de la Universidad. Con la implementación del Plan Director se persigue la identificación de riesgos que corren los activos de la organización, los cuales deben ser identificados, cuantificado su impacto y con la propuesta de un plan de acción para hacer frente, evaluando el impacto residual que la implantación de dicho plan lleva consigo.

La Universidad tiene diferenciado el componente de Tecnologías de la Información y Comunicaciones en dos partes, donde la Vicerrectoría de Virtualidad maneja procesos independientes de la Dirección de TICs central, con presupuesto distinto. El proyecto abSISTENOTASrá la infraestructura, los sistemas de información y los procesos desarrollados por la Dirección de TICs, la cual es una dependencia de la Vicerrectoría Administrativa. La Universidad no tiene un SGSI implantado y no se han realizado estudios previos en el área de seguridad para tomar de base y por tanto el análisis respecto a los activos, sus amenazas y los planes de acción se desarrollarán en el presente proyecto.

No hace parte del presente proyecto la certificación 27001:2013 por medio de una entidad certificadora, pero si se entregará un diagnóstico del estado actual en materia de seguridad de la información, así como la propuesta de planes a implementar en esta materia, con el objetivo de cumplir con dicha norma, basados en la guía de buenas prácticas que nos provee ISO 27002:2013.

1.3. Alcance del SGSI

La propuesta de alcance para el SGSI, para el desarrollo del plan director de seguridad y como propuesta para la futura certificación ISO/IEC 27001:2013 es la siguiente:

"*Los sistemas de información que dan soporte a la infraestructura de red LAN y WLAN, los servicios web, correo y herramientas colaborativas y a las actividades académicas de la Universidad con sede en Bogotá, según la declaración de aplicabilidad 001*".

1.4. Objetivos del Plan Director de Seguridad

OBJETIVO GENERAL

Plantear el Plan Director para la Universidad orientado a reducir los riesgos a los que está expuesta la información hasta unos niveles aceptables a partir del análisis del inventario de activos, aplicando la metodología de Análisis y Gestión de riesgos MAGERIT, la norma ISO/IEC 27001:2013 y 27002, como base para la implementación del Sistema de Gestión de Seguridad de la Información, basado en el concepto de mejora continua.

OBJETIVOS ESPECÍFICOS

- Revisar el estado actual de la Universidad respecto a la seguridad de la información, con base a la norma ISO/IEC 27001 y 27002 versión 2013.
- Proponer la política de seguridad para la Universidad.
- Revisar la correcta implementación de las herramientas de seguridad de la información implementadas actualmente.
- Revisar el cumplimiento de la regulación y la normatividad en materia de seguridad de la información por parte de la universidad.
- Realizar el inventario de activos de la Universidad en materia de seguridad de la información.
- Proponer mejoras al sistema de gestión de incidentes.
- Definir roles y responsabilidades de propietarios de activos.
- Analizar las amenazas a los que están dispuestos dichos activos.
- Definir el impacto potencial de dichas amenazas en los activos.
- Proponer un plan de acción para luchar contra dicha amenazas.
- Desarrollar la auditoría de cumplimiento de acuerdo al modelo de madurez resultado de la revisión de los controles ISO 27001:2013

1.5. Metodología utilizada para el desarrollo del proyecto

El Plan Director de Seguridad resultado del presente proyecto, pretende ser una hoja de ruta para que la Universidad inicie su proceso de implementación del Sistema de Gestión de la Seguridad de la Información, objetivo que la misma se ha fijado como parte de los planes de Acreditación de Alta Calidad para garantizar la calidad de sus procesos, basándose en los estándares de Alta Calidad propuestos por el Ministerio de Educación de la República de Colombia. La Universidad se encuentra en mora de articular los esfuerzos que se vienen realizando en materia de seguridad de la información que han sido atomizados y reactivos y es por ello que el Plan Director servirá como modelo para la gestión adecuada de la seguridad de la información, articulado al ya existente Sistema de Gestión de la Calidad y en el marco regulatorio y legal colombiano en materia de seguridad de la información.

El desarrollo del proyecto se abordó por medio de un esquema metodológico de implementación por fases, y cada una de las cuales

busca abordar un objetivo específico, las cuales se sintetizan en el siguiente diagrama:

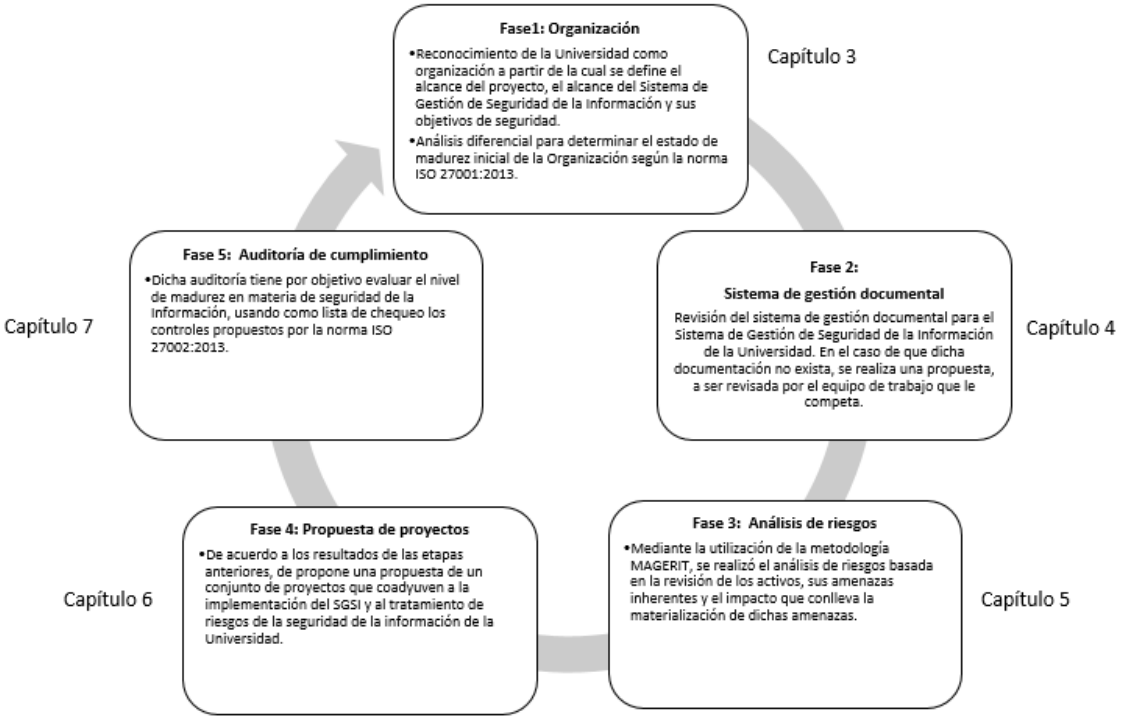


Figura 1. Metodología usada para el Plan Director de una universidad colombiana

En el capítulo 2 se expondrá una breve descripción de los estándares ISO/IEC 27001:2013 e ISO/IEC 27002:2013. En el capítulo 3, se sintetiza el trabajo realizado en la fase1 acerca de la organización. El esquema documental se encuentra propuesto en el capítulo 4. El capítulo 5 se centra en el análisis de riesgos de seguridad de la información de la Universidad, para el SGSI de la Universidad. La fase 4, acerca de la propuesta de proyectos, es expuesta en el capítulo 6 y la auditoría de cumplimiento se desarrolla en el capítulo 7. El capítulo 8 cierra la memoria con las conclusiones y recomendaciones, resultados del desarrollo del presente proyecto.

2. MARCO NORMATIVO: ISO 27000

Las normas ISO/IEC 27000 es un conjunto de estándares que han sido publicados por la Organización Internacional de Estandarización –ISO y la Comisión Internacional Electrotécnica –IEC que contiene las mejores prácticas para la seguridad de la información recomendadas para desarrollar, implementar y mantener Sistemas de Gestión de la Seguridad de la Información (Wikipedia, s.f.).

Las normas de la familia ISO/IEC 27000 incluyen:

ISO/IEC 27000	Definiciones y vocabulario.
ISO/IEC 27001	Requerimientos para un SGSI[1].
ISO/IEC 27002	Técnicas de seguridad. Código de práctica para controles de la seguridad de la información.
ISO/IEC 27003	Guía de implementación de un SGSI.
ISO/IEC 27004	Métricas para la gestión de seguridad de la información.
ISO/IEC 27005	Gestión de riesgos en seguridad de la información.
ISO/IEC 27006	Requisitos para la acreditación de las organizaciones que certifican las empresas con sistemas de gestión de seguridad de la información
ISO/IEC 27007	Guía para realizar la auditoría del SGSI.
ISO/IEC 27016	Norma para el análisis financiero y económico de equipos y procedimientos de seguridad de la información.
ISO/IEC 27017	Guía de seguridad para Cloud Computing.
ISO/IEC 27035	Gestión de incidentes de seguridad de la información.

Tabla 1. Familia ISO/IEC 27000.

Para el presente proyecto, se trabajaron los estándares ISO/IEC 27001:2013 e ISO/IEC 27002:2013. El estándar 27001 en su primera versión, la 2005 fue publicada en octubre del dicho año, como resultado de la evolución de otros estándares, como son:

La Norma BS 1901, fue publicada por la British Standars y de ella surgen BS 17799-1:1995 que desarrolla las mejores prácticas para administración de la seguridad de la información, la BS-7799-2:1999 que establecía los requisitos para implementar un SGSI y certificarse por ello.

En 2005: la Organización Internacional de Estandarización ISO se basó en BS 7799-2:2002 para desarrollar la ISO 17799, que fue la base para el estándar

[1] SGSI: Sistema de Gestión de Seguridad de la información

ISO/IEC 27002. En el mismo año también aparece la norma ISO/IEC 27001:2005 como norma internacional certificable.

Estas dos normas evolucionaron por la necesidad de unificar los distintos sistemas de gestión que se desarrollan en las empresas basadas en los estándares ISO y de allí surge el anexo SL. Dicho anexo es una directriz de la ISO para la redacción de normas de sistemas de gestión que se basan en dos pilares:

- Títulos idénticos para los capítulos, para que todas las normas estén organizadas de la misma manera y cuenten con los mismos capítulos y secciones básicas y para que en cada norma en particular, de acuerdo a sus necesidades, se adicionen subcapítulos y subcláusulas en las áreas de interés.
- Se manejan texto y términos comunes idénticos, llamados textos estándar que tengan la misma significación en todas las normas; y
- En todas las normas se usará el mismo vocabulario básico y para cada norma en particular, se agregarán definiciones adicionales para los términos técnicos propios de su especialidad.

La otra novedad de las versiones 2013 respecto a las 2005 surge de la necesidad de alinear dichas normas con los principios trabajados en la norma de gestión de los riesgos, ISO 31000, para permitir la integración de los sistemas, aplicando metodologías similares de evaluación del riesgo.

2.1. Norma 27001:2013

"Esta norma ha sido elaborada para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información". (Instituto Colombiano de Normas Técnicas y Certificación. ICONTEC., 2013, pág. i). El desarrollo de un SGSI en una organización será producto de las necesidades y objetivos de la misma, de los requerimientos de seguridad de sus activos, de los procesos organizacionales implantados y del tamaño y estructura de dicha organización. La seguridad de la información basada en esta norma se definirá en base de preservar la confidencialidad, integridad y disponibilidad de la información para sus usuarios.

La norma ISO 27001:2013 promueve la adopción de un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el SGSI de una organización. Para que dicho sistema funcione de forma eficaz, la organización debe gestionar actividades que usan recursos o procesos. La aplicación de un sistema de procesos dentro de una organización,

junto con la identificación e interacciones entre estos procesos y su gestión, por lo que las organizaciones desarrollan un enfoque basado en procesos.

La norma ISO 27001:2103 cuenta con 10 capítulos, en los cuales se aplica el método PHVA, también conocido como ciclo de Deming, de mejora continua, estrategia de calidad en la cual se basan los sistemas de gestión desarrollados bajo las normas ISO.

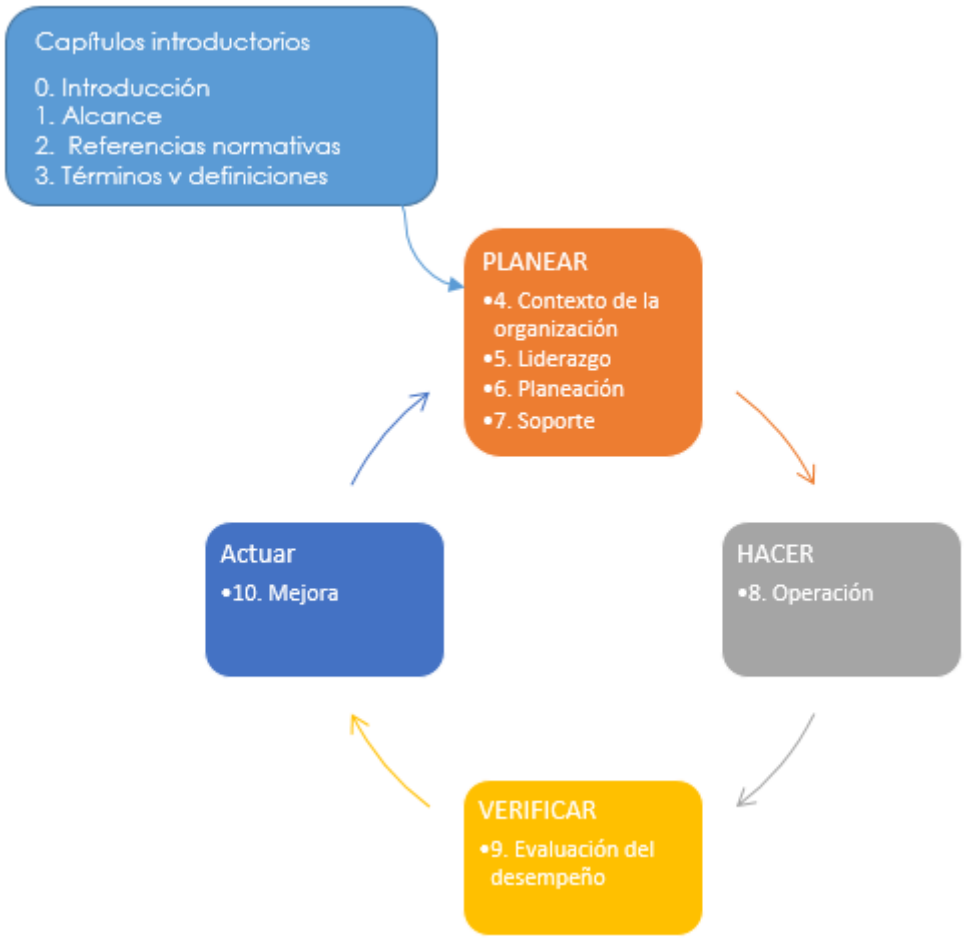


Figura 2. Contenido de ISO 27001:2003 de acuerdo al ciclo Deming. Construcción propia.

La adopción del modelo PHVA refleja los principios establecidos en las Directrices OCDE (2002) que controlan la seguridad de sistemas y redes de información. Esta norma brinda un modelo robusto para implementar los principios en aquellas directrices que controlan la evaluación de riesgos, diseño e implementación de la seguridad, gestión y reevaluación de la seguridad. (Instituto Colombiano de Normas Técnicas y Certificación. ICONTEC., 2015)

La norma en su anexo A cuenta con objetivos de control, obtenidos de la norma ISO/IEC 2002:2013 de los numerales de 5 al 18 y están alineados con ella. A continuación nos referimos a dicha norma.

2.2. Norma 27002:2013

La ISO/IEC 27002 fue preparada por el comité técnico conjunto ISO/IEC JT1: Tecnologías de información, subcomité SC 27: Técnicas de seguridad de T.I. La segunda edición de la norma es la versión 2013 y fue diseñada para el usarse como referencia para la selección de controles al momento de implementar Sistemas de Gestión de Seguridad de la Información, con base a la norma técnica ISO 27001. También puede ser usado como documento guía para la implementación de controles de seguridad comúnmente aceptados, por parte de organizaciones que quieren salvaguardar la confidencialidad, integridad y disponibilidad de su información.

Los controles referidos por la norma están clasificados en 14 dominios de seguridad, que agrupan 35 objetivos de control, para un total de 114 controles. El anexo 1 sintetiza los controles, de acuerdo al objetivo de control que abSISTENOTASn y al dominio de seguridad al cual pertenecen.

3. EMPRESA OBJETO DE ESTUDIO: UNIVERSIDAD COLOMBIANA

El desarrollo de este proyecto se enfoca sobre una universidad colombiana, entidad de carácter privado con una población estudiantil de aproximadamente 20.000 estudiantes, 800 docentes y aproximadamente 200 empleados administrativos. La Universidad cuenta con 35 años de experiencia, como institución carácter tecnológico de carreras intermedias para la población bogotana y sus objetivos fueron avanzando hasta que obtuvo su categoría de Universidad.

La Universidad cuenta con certificación ISO 9001:2008 recientemente para el **diseño y desarrollo de programas académicos y prestación de servicios de educación**, por lo que cuenta con un Sistema de Gestión de Calidad, el cual está avalado por las directivas de la Universidad, basado en los siguientes principios:

1. El principio de la evaluación permanente y el mejoramiento continuo, con el cual se cimienta el compromiso de definir, mantener y mejorar los diferentes componentes del Sistema Integrado de Calidad, a través del conocimiento permanente de las necesidades y expectativas del estudiante y su familia, del egresado, de los profesores, de los colaboradores, de la familia, de los empleados y el entorno empresarial y de los requerimientos de los entes de regulación.

2. El principio del desarrollo del talento humano, orientado a la formación y capacitación permanente de nuestro personal, en procura de la autorrealización de la persona y de la generación de un mayor sentido de pertenencia con la Institución, fortaleciendo así el nivel de servicio para la satisfacción de nuestros estudiantes y las partes interesadas.

3. El principio del respeto, orientado a fomentar espacios para que todos los miembros de la comunidad generen un clima organizacional que fomente la cultura del BUEN SERVICIO.

4. El principio de la gestión racional de los recursos, el cual busca asegurar la disponibilidad de los recursos para el cumplimiento de la

misión Institucional y la política de calidad, a través de una adecuada planeación de todos los procesos.

5. El principio de la información clara, establece una estructura organizacional adecuada y formal, acompañada de procesos definidos, simplificados y revisados continuamente y soportados en sistemas de información adecuados a las necesidades de dichos procesos.

6. El principio de la pertinencia, con el cual nos comprometemos a mejorar la pertinencia de los programas académicos a través de la definición y aplicación de la metodología e instrumentos orientados para este fin, como mecanismo de realimentación para realizar adecuadamente los procesos misionales.

7. El principio del buen vecino, se encamina por definir y tomar las medidas adecuadas que logren una sana convivencia con nuestro entorno más cercano. (Manual del Sistema de Gestión de la Calidad. Diseño y Desarrollo de programas académicos y Prestación del Servicio de Educación Superior., págs. 18-19)

Actualmente la Universidad está comprometida en adquirir la Acreditación de alta calidad a nivel institucional, a través de la Acreditación de sus programas. Dentro de este proyecto a 7 años, uno de los objetivos los cuales apuntan es la implementación de un Sistema de Gestión de Seguridad de la Información y la correspondiente certificación ISO27001, integrando dicho sistema con el Sistema de Gestión de la Calidad de la Universidad.

3.1. Infraestructura de la Universidad

La Universidad cuenta con 2 sedes en el país. La sede de Bogotá, que es la sede principal, cuenta con dos ubicaciones zonales en la ciudad, una es el campus, recientemente inaugurado, donde funcionarán las nuevas carreras de gastronomía y es la zona para prácticas deportivas y académicas extracurriculares y la principal que es un conglomerado de 6 edificios, por lo que estudiantes, administrativos y docentes se mueven por un área de varios cientos de metros no resguardados, aunque se cuenta con la adecuada vigilancia por edificio.

3.2. Composición organizativa

El organismo principal de la Universidad es el Consejo Superior Universitario[2] que toma las decisiones primordiales de la institución. El Rector es la primera autoridad ejecutora de las decisiones tomadas en dicho ente y cuenta con cuatro vicerrectorías, cada una especializada en su área: la Vicerrectoría Administrativa, la Vicerrectoría Académica, la Vicerrectoría de aseguramiento de la calidad, la Vicerrectoría de Educación Abierta y a distancia y la Vicerrectoría de Investigación.

La Dirección de Informática y TICs es una dependencia de la Vicerrectoría Administrativa y está estructurada de la siguiente manera:

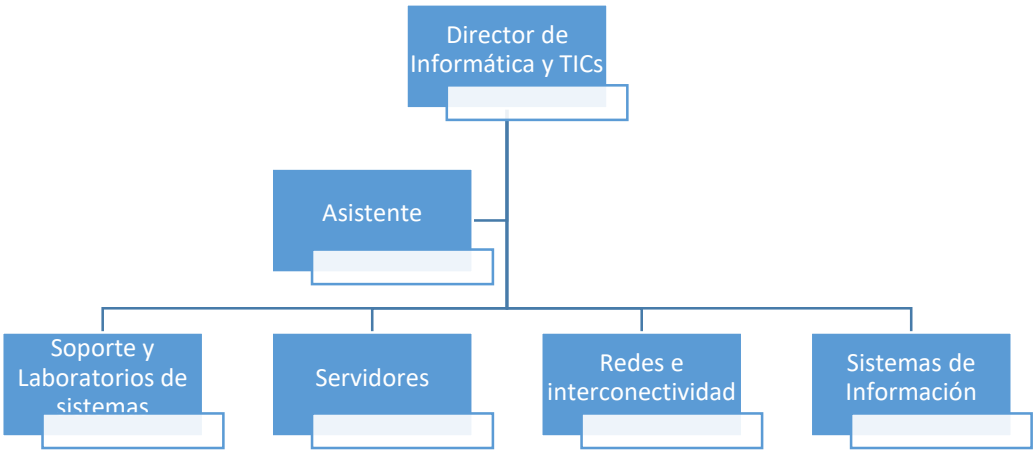


Figura 3. Organigrama funcional del Dirección TIC. Elaboración propia.

3.3. Sistemas de Información de una universidad colombiana

Esta universidad colombiana cuenta con varios sistemas de información que sirven de soporte a los distintos procesos tanto misionales como de apoyo. El sistema de información académica antiguo y el sistema de información académica *que por motivos de confidencialidad llamaremos SISTENOTAS* basado en PeopleSoft, el cual fue comprado y parametrizado por un proveedor externo, pero que es administrado por personal de la Universidad. El sistema de información financiera también fue realizado por terceros, que brindan en mantenimiento y actualización. Los servicios de red tales como los portales web

[2] Ver Anexo 1: Organigrama de la Universidad Colombiana

de la universidad, han sido desarrollados por el Departamento de TICs y los servidores se encuentran localizados en el edificio principal de la Universidad. Estos servidores prestan servicios a las dos sedes regionales.

3.4. Infraestructura Tecnológica de una universidad colombiana

Respecto a la infraestructura de red, la universidad cuenta con enlaces VPN entre las dos ciudades: Bogotá y Medellín. A nivel Bogotá, las diferentes sedes cuentan con conexiones de fibra óptica y la red está dividida en VLANs segmentadas de acuerdo a la funcionalidad de los Hosts.

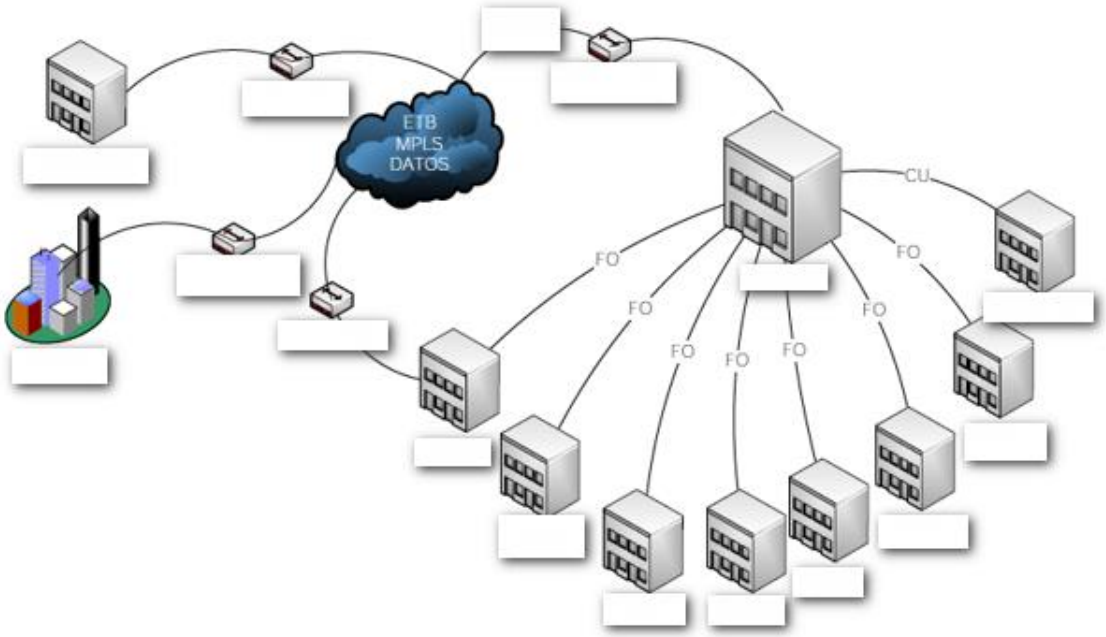


Figura 4 Mapa de enlaces de red de una universidad colombiana.
Fuente: Dirección TIC Universidad Colombiana
Por motivos de seguridad, se elimina la información confidencial

Cada sede cuenta con un firewall, el cual soporta todas las políticas que son generales a cada una de las VLAN de la universidad. El sistema antivirus es centralizado y no se cuenta con un sistema de protección y detección de intrusos.

La Universidad no cuenta con un documento Política de Seguridad de la Información, ni procedimientos en el Sistema de Gestión de Calidad correspondientes al tema. El Director de TICs de la Universidad proyecta el inicio

las actividades conducentes a la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) a partir del 2017, por lo cual le parece fundamental el desarrollo del Proyecto en la Universidad, para que en base a sus resultados, se empiece con la implementación del SGSI.

3.5 Análisis diferencial de una universidad colombiana con respecto a ISO/IEC 27001: 2013 + ISO/IEC 27002

La norma ISO/IEC 27001 es un estándar para la implementación de un Sistema de Gestión de Seguridad de la Información, la cual especifica los requisitos para establecer, implementar, mantener y mejorar de forma continua dicho sistema dentro del contexto de la organización. (Instituto Colombiano de Normas Técnicas y Certificación. ICONTEC., 2013). La versión que se usa en el presente proyecto es la 2013, debido al cambio de enfoque realizado por la ISO para que en el caso de organizaciones que cuentan con sistemas de gestión, puedan integrar los requisitos y se pueda cumplir con todos los que sean implementados en base a los estándares de dicha organización.

La norma ISO/IEC 27002 fue desarrollada como elemento de referencia para la selección de controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de Información(SGSI) con base en la ISO/IEC 27001 o bien como un manual de buenas prácticas que sirva de guía para organizaciones que implementan controles de seguridad comúnmente aceptados. (Instituto Colombiano de Normas Técnicas y Certificación. ICONTEC., 2015).

De forma preliminar, se necesita conocer de manera global el estado actual de la Universidad en relación de la Seguridad de la Información, por lo que es necesario realizar el análisis diferencial de la Universidad basados en las normas ISO/IEC 27001:2013 y 27012:2013.

Para ello se han realizado un conjunto de entrevistas con el Vicerrector General de la Universidad, el Director de Tecnologías de Información, los ingenieros de soporte técnico, una Coordinadora de programa, la Jefe de calidad de la Universidad y el Ingeniero técnico de la Vicerrectoría de Virtualidad, la cual nos dio los resultados del estado preliminar de la Seguridad de Información de acuerdo a las normas anteriormente citadas y el estado de madurez del sistema al momento de iniciar el proyecto de Plan Director.

Los resultados del análisis diferencial de la norma ISO 27001:2013, se pueden apreciar en el Anexo1, de los cuales se realizó una evaluación cuantitativa con los siguientes resultados:

Numeral	Dominio	Cumplimiento
4	**Contexto de la organización**	0%
5	**Liderazgo**	8%
6	**Planificación**	0%
7	**Soporte**	5%
8	**Operación**	0%
9	**Evaluación de Rendimiento**	0%
10	**Proceso de mejora**	15%

Tabla 2: Evaluación de la norma ISO27001:2013 en una universidad colombiana

Por el hecho de no contar con un Sistema de Gestión de Seguridad de la Información, el porcentaje de cumplimiento es mínimo, con solo algunos numerales que tienen relación con el Sistema de Gestión de la Calidad implementados, como en el numeral de procesos de mejora, liderazgo y soporte.

Figura 5. Gráfico de radar. Cumplimiento de la norma SGSI anterior al Plan Director

Respecto a los objetivos de control y controles que se presentan como anexo en la norma ISO/IEC 27001:2013 y que cuenta se desarrolla en la norma ISO/IEC 27002:2013, se obtuvieron los resultados expuestos en el Anexo 1 en la sección de controles, los cuales podemos resumir, asociando una valoración cuantitativa, según el nivel de implementación, en la siguiente tabla:

DOMINIO	CONTRO-LES	SIN IMPLEMENTAR	PARCIALMENTE IMPLEMENTADO	IMPLEMENTADO	PORCENTAJE DE IMPLEMENTACIÓN
5. POLÍTICAS DE SEGURIDAD	**2**	2			0%
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	**7**	7			0%
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	**6**	5	1		3,3%
8. GESTIÓN DE ACTIVOS	**10**	7	2	1	19,85%
9. CONTROL DE ACCESO	**14**	6	6	2	45,83%
10.CIFRADO	**2**	1	1	0	5%
11. SEGURIDAD FÍSICA Y AMBIENTAL	**15**	4	7	4	41.53%
12. SEGURIDAD EN LA OPERATIVA	**14**	2	6	6	53.75%

Tabla 2: Evaluación de los controles ISO27002:2013 en una universidad colombiana

Se puede inferir de la tabla, que ya existen algunos controles asociados a la norma, pero que aún falta cerca de la mitad de controles por implementar, como se puede apreciar en la figura:

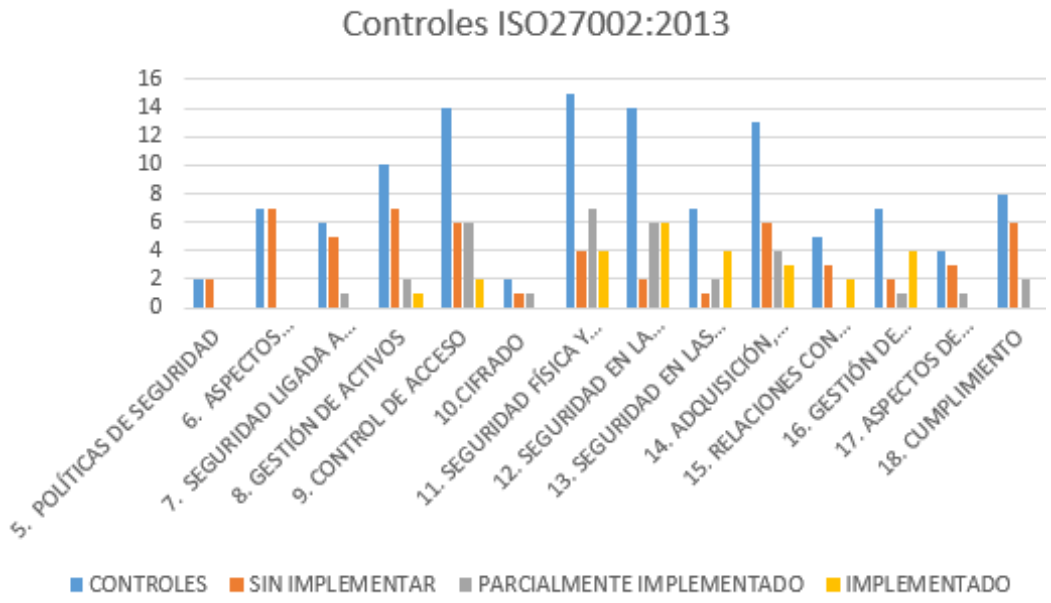


Figura 6 Estado de los controles de ISO 27002:2013 en una universidad colombiana

Con el gráfico de radar, se puede inferir que algunos dominios tienen controles implementados en gran porcentaje, como en el caso de seguridad en las telecomunicaciones y gestión de incidentes. Por esta razón hay que enfocar las propuestas producto del presente proyecto en la implementación de controles en los dominios que no cuentan con ninguno y que hagan parte del alcance del SGSI planteado por la entidad.

Figura 7 Gráfico de radar de estado de los controles del Anexo 1 de ISO27001:2013

4. SISTEMA DE GESTIÓN DOCUMENTAL

4.1. Esquema documental del SGSI

Toda organización que piense en certificarse en ISO/IEC 27001:2013 debe contar con un esquema documental que soporte el Sistema de Gestión de la Seguridad de la Información. Los documentos que soportan dicho sistema son:

- Definición del Alcance del Sistema de Gestión de la Seguridad de la Información (definida en el capítulo anterior).
- Política General de Seguridad de la Información.
- Procedimientos para:
  - Control de documentación
  - Auditorías internas
  - Medidas preventivas y correctivas
- Metodologías de evaluación de riesgos
- Declaración de Aplicabilidad
- Plan de tratamiento de riesgos
- Registros

En este capítulo revisaremos el estado de dicha documentación para una universidad colombiana.

4.1.1 Política de Seguridad de la Información

Actualmente, la universidad no cuenta con Política de Seguridad de la Información escrita y aprobada por la Alta Dirección. Las políticas implementadas en sus sistemas no cuentan con un soporte escrito de las mismas, por lo que en este proyecto se realizar una propuesta de Política General de Seguridad de la Información para la Universidad.

La política propuesta en el presente proyecto, fue discutida con el Director de Tecnologías de la Información de la Universidad y se ha presentado al Rector a la Universidad para su aprobación por parte del Consejo Superior Universitario. Esta política se soporta en los requisitos que como institución debe cumplir la Universidad, su estrategia de negocio, la reglamentación, legislación contratos actuales y en el entorno de amenazas a la seguridad de la información en los que una institución como una universidad colombiana debe manejar en su operación.

Para el diseño de las políticas de seguridad de la información, se tiene en cuenta que la política de una universidad colombiana está consignada en su lema "Humanismo y Tecnología para el tercer milenio", la cual concreta la aspiración institucional de la simbiosis de lo humano y tecnológico. Para garantizar las funciones sustantivas que conllevan su misión social, el Sistema Integrado de calidad interactúa con el Modelo de autoevaluación institucional, el cual permite ganar una visión global y unificada sobre el estado de los procesos de la ECCI, a través del análisis de sus indicadores, el seguimiento de los proyectos de mejora, la percepción de los actores del proceso, los resultados emanados de las auditorías y la implementación de las acciones correctivas y preventivas. (Comité de Planeación. Universidad ECCI, 2011, págs. 8-9)

El documento de Política General de Seguridad de la Información, propuesto en el presente proyecto y presentado a la alta dirección de la Universidad se encuentra en el ANEXO 4. PROPUESTA DE POLÍTICA DE SEGURIDAD DE UNA UNIVERSIDAD COLOMBIANA.

4.1.2 Procedimiento de auditorías internas

De acuerdo con la definición de auditoría de la norma ISO 19011: "La auditoría es un proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios de auditoría" (Instituto Colombiano de Normas Técnicas, ICONTEC, 2011, pág. 1).

Para el caso de los Sistemas de Gestión de Seguridad de la Información, la Universidad debe llevar a cabo auditorías internas de forma programada y planificada para verificar si el SGSI cumple con los requisitos de la organización respecto al sistema y a los requisitos de la norma ISO 27001:2013 y para verificar si el sistema está implementado y es mantenido de forma eficaz (Instituto Colombiano de Normas Técnicas y Certificación. ICONTEC., 2013, pág. 10).

Al momento de realizar el proyecto, este procedimiento no se encuentra definido en el sistema de gestión de la Universidad, por lo que se realiza una propuesta de procedimiento acorde a las necesidades de la Universidad para los procesos involucrados. Este procedimiento se encuentra descrito en el **¡Error! No se encuentra el origen de la referencia.**.

Para el diseño del procedimiento, se utilizaron las definiciones de la norma ISO 19011:2011 anteriormente mencionada y el procedimiento de auditorías internas del Sistema de Gestión de la Calidad de la Universidad (PR-SIC-003).

4.1.3 Gestión de indicadores

Un indicador de seguridad es "un valor que se obtiene comparando datos (o atributos según ISO 27004) lógicamente relacionados, referentes al comportamiento de una actividad, proceso o control dentro de un tiempo específico" (Alejandro Corletti, 2008)

Una universidad colombiana cuenta con indicadores para su sistema de gestión de calidad, pero no cuenta con indicadores para la gestión de la seguridad de la información, por lo que en este proyecto se realiza la propuesta de indicadores de seguridad a ser utilizados en el SGSI de una universidad colombiana.

El Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, también conocido como MinTIC ha desarrollado un estudio de sobre indicadores para la gestión de la seguridad de la información (MInisterio de Tecnologías de la Información y Comunicación - MINTIC, 2015) que pueden ser de utilizados por empresas del estado y demás organizaciones.

Se ha tomado de base dicho documento para generar algunos indicadores para el Sistema de Gestión de Seguridad de la Información de la entidad, así como indicadores basados en controles de la norma ISO27002:2013.

La matriz de indicadores de gestión para el SGSI de una universidad colombiana se presenta en el ANEXO 6. INDICADORES DE GESTIÓN PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE UNA UNIVERSIDAD COLOMBIANA.

4.1.1 Gestión de roles y responsabilidades

La gestión de roles y responsabilidades en el ámbito de seguridad de la información debe estar basada en distintos criterios tales como las políticas de seguridad de la empresa, los activos a los cuales tiene permisos, las

responsabilidades de protección de dichos activos, las actividades de gestión del riesgo aceptables y residuales entre otras cosas.

La estructura organizativa de la seguridad de la información en una universidad colombiana s, junto a las responsabilidades de cada rol se encuentra expuesta en el ANEXO 7. GESTIÓN DE ROLES Y RESPONSABILIDADES.

4.1.2 Metodología de análisis de riesgos

Para el Plan Director de Seguridad de una universidad colombiana se utilizará como metodología de análisis de riesgos, MAGERIT[3]. La versión más reciente es la 3.0. Esta metodología ofrece un método sistemático para el análisis de riesgos y para la implementación de medidas de control adecuadas para mitigar los riesgos analizados. Magerit ha sido usada por el Ministerio de las TIC colombiano como base para los estudios de evaluación del riesgo en las entidades públicas colombianas (Ministerio de Tecnologías de la Información y Comunicación - MINTIC, 2016).

La metodología está publicada en tres libros: en el primer libro se plantea el método o estructura del modelo de gestión de riesgo. El libro II resume el catálogo de elementos o inventario de activos y sus características. El libro III ofrece una guía de técnicas frecuentemente utilizadas para de riesgos.

MAGERIT identifica la gestión del riesgo en dos grandes actividades: el análisis y el tratamiento del riesgo. El análisis del riesgo permite determinar qué tiene al información (activos) y estimar qué podría pasar (amenazas) y a partir de ello calcular el impacto y el riesgo. El tratamiento de los riesgos permite organizar las medidas de protección de los activos del riesgo a través de salvaguardas. (Consejo Superior de Administración Electrónica de España, 2012, pág. 20).

El método de análisis de riesgos se desarrolla en un conjunto de pasos:

[3] Magerit es una metodología de análisis y gestión de riesgos de los Sistemas de Información, diseñada por el Consejo Superior de Administración Electrónica para la minimización de los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas de España y base para la metodología de gestión del riesgo usada por MinTIC en Colombia.

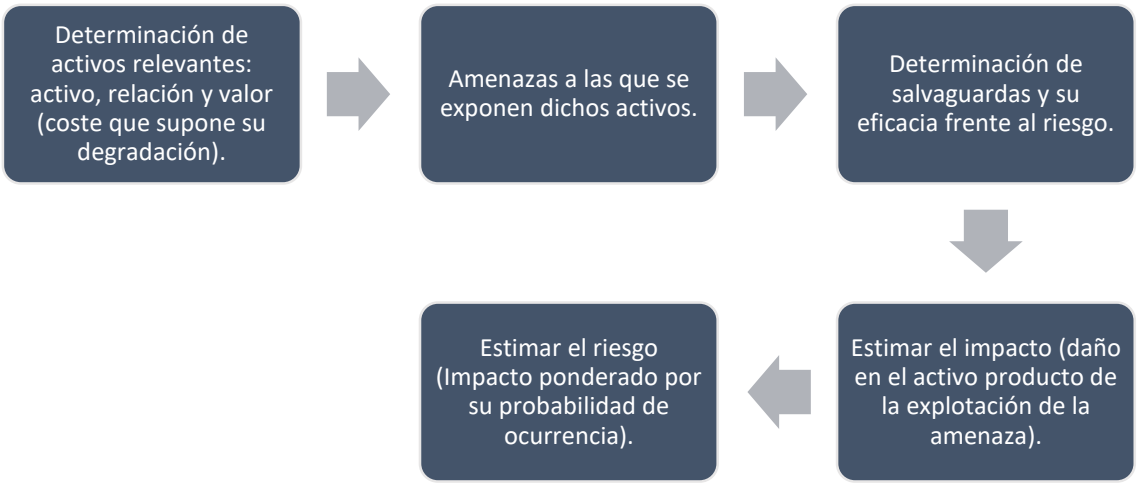


Figura 8. Metodología de análisis del riesgo - Fuente: Magerit v3.0

Paso 1: Determinación y caracterización de los activos: levantamiento de un modelo de valor

Los activos esenciales en un sistema de información son la información que manejan y los servicios que se prestan. A partir de allí se definen los activos relevantes: datos, servicios, software, hardware, soportes de información, equipamiento auxiliar, redes de comunicaciones, instalaciones y personas.

Las actividades a realizar para la determinación y caracterización de los activos son:

Figura 9. Paso 1: Identificación y caracterización de los activos.

Paso 2: Identificación de las amenazas: Levantamiento del mapa de riesgos

Una vez definidos y caracterizados los activos, se realiza la identificación de las amenazas que pueden afectar a cada activo. Las actividades a realizar en esta fase son:

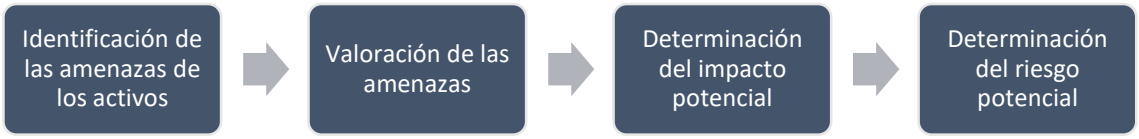


Figura 10. Paso 2: Identificación de las amenazas.

Paso 3: Caracterización de las salvaguardas

En este paso se definen las contramedidas o salvaguardas, que son los mecanismos tecnológicos de reducen el riesgo. Las actividades a realizar para ello son:

Figura 11. Paso 3: Caracterización de las salvaguardas

Paso 4: Impacto residual

Una vez definidas las salvaguardas a implementar, siempre quedará un riesgo residual que conlleva un impacto residual. Por tanto, una vez realizado el paso 3, se realiza un recálculo de impacto con el nuevo nivel de degradación posterior la implementación de las salvaguardas.

Paso 5: Riesgo residual

Así como se realiza un recálculo del impacto, una vez seleccionadas las salvaguardas y teniendo en cuenta su eficacia, el riesgo residual es producto de un recálculo de riesgo usando el impacto residual y su probabilidad de ocurrencia.

En el capítulo 5 se aplicará la metodología del análisis del riesgo MAGERIT 3.0, haciendo uso de la guía de técnicas para la caracterización y valoración de los activos, amenazas, riesgos de cada una de las fases expuestas por dicho modelo.

4.1.3 Declaración de aplicabilidad

La declaración de aplicabilidad es el documento donde se especifican los controles de la norma ISO/IEC 27002:2013 que serán utilizados en el sistema de gestión de seguridad de la información. La declaración de aplicabilidad para

el SGSI de una universidad colombiana se encuentra en el ANEXO 8. DECLARACIÓN DE APLICABILIDAD DEL SGSI.

5. ANÁLISIS DEL RIESGO

Como requisito para la certificación del Sistema de Gestión de Seguridad de la Información por ISO 27001:2013, es necesario realizar el plan de gestión del riesgo. Como fue mencionado en el capítulo anterior, la metodología que se trabaja en el presente proyecto es la metodología MAGERIT en su versión 3.0. Para ellos se levantarán los siguientes documentos:

- Levantamiento de un modelo del valor del sistema, mediante el cual se identifican los activos relevantes para el SGSI.
- Levantamiento de un mapa de riesgos del sistema, mediante el cual se identifican las amenazas que aquejan dichos activos y se les dá una valoración.
- Levantamiento de la información actual de las salvaguardas implementadas.
- Evaluación del impacto potencial y residual del SGSI en estudio.
- Evaluación del riesgo potencial y residual de dicho sistema.
- Información de las áreas de mayor impacto y mayor riesgo para tomar decisiones sobre el tratamiento del riesgo

La metodología MAGERIT propone que las actividades del análisis de riesgos se realicen a través de las siguientes tareas:

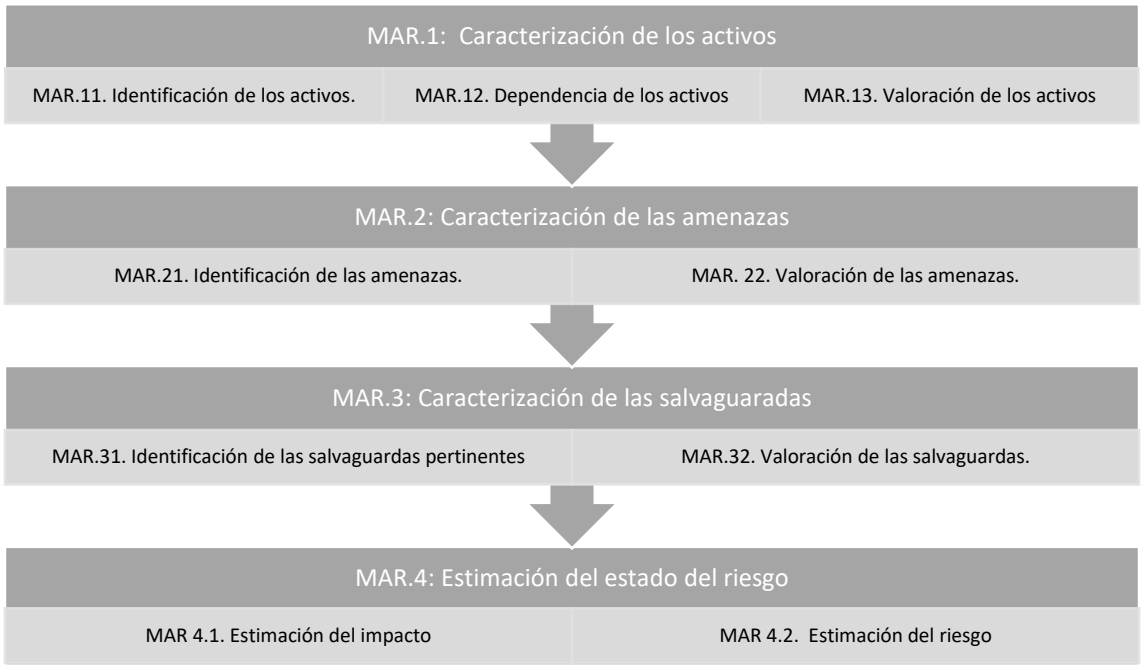


Figura 12. Método de análisis del riesgo. Tomado de MAGERIT (Consejo Superior de Administración Electrónica de España, 2012, pág. 36)

5.1 Caracterización de los activos

La primera actividad de la metodología es la caracterización de los activos relacionados con los sistemas de información de una universidad colombiana. Los activos cubren no solamente la información a proteger y que es manejada por dichos sistemas de información, también están los servicios que se prestan, los datos, servicios auxiliares de soporte, software y hardware, dispositivos de almacenamiento de datos, equipamiento auxiliar, redes de comunicaciones, instalaciones y las personas que interactúan con la información.

La información se puede relacionar por medio de las dependencias, las cuales generan una jerarquización de los activos, para lo cual la metodología permite la organización de los activos por capas, donde las capas inferiores dependerán de las superiores.

5.1.1. Identificación de los activos

Para el caso de estudio, se han identificado 71 tipos de activos organizados de la siguiente manera y etiquetados de acuerdo a la propuesta de Magerit (MAGERIT - versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información. Libro II. Catálogo de elementos., 2012), lo cual se desarrolla en el siguiente cuadro.

Inventario de activos
[I] Información
[I_esencial] Datos esenciales [I_estudiante]Información académica de estudiantes de la universidad [I_PEI] Plan educativo institucional [I_PEP] Plan Educativo de Programa [I_notas] Notas de los estudiantes [I_aspirante] Listado de los aspirantes [I_desercion] Listado de estudiantes desertados [I_micros] Contenidos curriculares de cada curso [I_personal] Datos de carácter personal [I_docente] Información personal de los docentes [I_adm] Información personal de los empleados administrativos [I_estudiante]Datos personales de los estudiantes
[S] Servicios

Los servicios que presta una universidad colombiana a su comunidad tanto en el perfil de usuario interno como externo, son los siguientes:
Servicios internos:
[SI_internet] Servicio de acceso a internet en el campus.
[SI_www_aulas] Sitio web de las aulas virtuales
[SI_www_atenea] Sitio web de la Biblioteca
[SI_correo] Correo electrónico de la Universidad

Servicios externos o al público en general
[SI_www_] Sitio web de la universidad

El canal de internet es redundante de 100 Mbps con la empresa proveedora de servicios ETB.

[D] Datos

[D_config] Archivos de configuración
[D_backups] Copias de seguridad
[D_pass] Contraseñas
[D_acl] Datos de control de acceso
[D_log] Archivos de registro de actividad

[Soft]Software

[Soft_SISTENOTAS] Sistema de gestión Académica
[Soft_Moodle] Sistema de aulas virtuales
[Soft_people] Sistema crm de la universidad
[Soft_glpi] Sistema de gestión de soporte técnico
[Soft_nomina] Sistema de nómina
[Soft_antivirus] Software antivirus
[Soft_pm] Software de biblioteca
[Soft_so] Sistemas operativos
[Soft_office] Herramientas ofimáticas
[Soft_navegador] Navegador web
[Soft_correo] Cliente de correo electrónico
[Soft_autocad] Software en aulas de sistemas

El sistema de gestión académica de la Universidad se denomina SISTENOTAS.
La plataforma de aulas virtuales utiliza moodle.
Los servidores utilizan Linux CentOS7
La universidad cuenta con un contrato de campus agreement con Microsoft para el uso de sistema operativo Windows (7, 8,10) y Office.
Se cuenta con 125 licencias de autocad para uso académico.

[Hard] Hardware

[Hard_ap] Access Points
[Hard_firewall] Firewall de la red
[Hard_impresora] Impresoras
[Hard_pbx] PBX
[Hard_pc] Equipos de escritorio
[Hard_portatil] Equipos portátiles
[Hard_router] Enrutadores
[Hard_scanner] Escáneres
[Hard_servidor] Servidores
[Hard_switch] Switches (encaminadores)

Se cuenta con un total de 7 puntos de acceso inalámbrico en las distintas sedes.
Hay un firewall perimetral conectado al router de borde.
Se cuenta con 47 impresoras en las distintas dependencias administrativas.
Se tiene un equipo PBX que administra las extensiones telefónicas de la universidad.
Se cuenta con un total de 1257 equipos entre equipos de escritorio y de las salas de cómputo.
En total se tienen 35 equipos portátiles para actividades administrativas.
Hay 5 enrutadores uno en cada sede.
Se cuenta con un total de 20 escáneres en dependencias administativas.
En el datacenter se cuenta con 5 servidores para los servicios principales que se prestan en la universidad.
Hay en total 42 switches con capacidades de VLAN en la Universidad.

[Alm] Dispositivos de almacenamiento de información

[Alm_cinta]Cinta magnética
[Alm_discos] Discos duros
[Alm_usb] Dispositivos USB

La cinta magnética se usa para las copias de seguridad de los sistemas de información académica y financiera, los cuales se entregan en custodia para la empresa que presta el servicio de backups.
Los discos duros de soporte se encuentran en un arreglo RAID en un equipo espejo.
Los dispositivos de USB contienen material de respaldo para el sistema de información SISTENOTAS.

[Aux] Equipamiento auxiliar

[Aux_cableado] Cableado estructurado de las sedes [Aux_gabinete] Gabinetes de telecomunicaciones [Aux_ups] Sistemas de información ininterrumpida [Aux_ventilación] Equipos de ventilación de cuartos de comunicaciones [Aux_cableado] Cableado estructurado de las sedes [Aux_gabinete] Gabinetes de telecomunicaciones Se cuenta con 5 cuartos de comunicaciones en la sede principal, 5 en la sede J, 3 en la sede G y 3 en la sede J. Se cuenta con una UPS regulada para los equipos del datacenter de la sede principal, 4 UPS en la sede P y 1 UPS en la Biblioteca de la sede G. Se cuenta con equipos de ventilación en el datacenter.
[Com] Redes de comunicaciones
[Com_inalámbrica] Red inalámbrica [Com_internet] internet [Com_LAN] Red LAN interna [Com_telefónica] Red telefónica Existen 4 redes inalámbricas con cubrimiento en las sedes principal, J, G y P. La red LAN conecta todas las dependencias administrativas y académicas de la Universidad. Para la conexión entre las sedes, se usa la fibra óptica provista por el Proveedor de servicios de internet. La red telefónica interna se maneja mediante PBX.
[Inst] Instalaciones
[Inst_oficina] Oficinas administrativas [Inst_edificio] Edificios En la sede Bogotá se cuentan 4 edificios con oficinas de rlas distintas dependencias administrativas en cada una de las sedes.
[P] Personas
[P_uinterno] Usuario interno [P_admred] Administrador de red [P_admserv] Administrador de servidores [P_admapl] Administrador de aplicaciones [P_softw] Ingenieros de desarrollo [P_soporte] Ingenieros de soporte [P_vicerrector]Vicerrector [P_coord] Coordinador de proceso

[P_asistente] Asistente administrativo [P_gestionh] Directora de Gestión humana [P_docente] Docente [P_uexterno] Usuario externo

Tabla 3. Inventario de activos del sistema basado en Magerit 3.0

5.1.2. Dependencia entre activos

La dependencia entre activos permite identificar las relaciones de dependencia entre los mismos, categorizarlos y reconocer cómo un activo de orden superior se puede ver perjudicado por una amenaza explotada para afectar un activo de orden inferior.

Debido a la gran cantidad de activos a considerar en el sistema, se ha generado un diagrama de dependencias con las categorizaciones principales activos identificados en el inventario de activos.

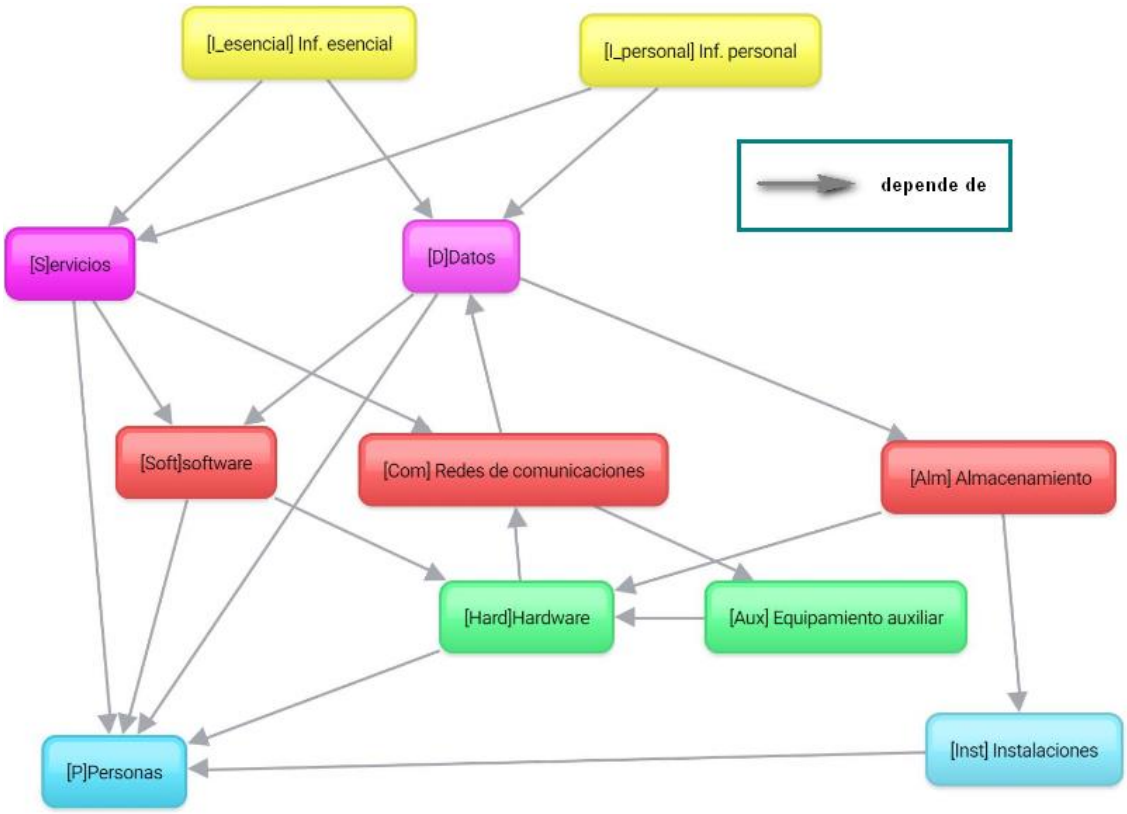


Figura 13. Grafo de dependencia entre categorías de activos del SGSI de la Universidad

5.1.3. Valoración de los activos

Para realizar la valoración de los activos se toma en consideración tanto las dimensiones en que el activo es relevante, como su estimación de la valoración de cada dimensión.

Las dimensiones a considerar según la metodología Magerit son:

- [C]onfidencialidad de los datos
- [I]ntegridad de los datos
- [D]isponibilidad de los servicios
- [A]utenticidad de la información y los usuarios
- [T]razabilidad del uso del servicio y los datos

Los criterios de la valoración se realizaron de forma cuantitativa con la siguiente escala:

NIVEL	0	1-2	3-5	6-8	9	10
CRITERIO	Despreciable[4]	Bajo[5]	Medio[6]	Alto[7]	Muy alto[8]	Extremo[9]

El resultado de dicha valoración se resume en la siguiente tabla:

CAT.	ID. ACTIVO	ACTIVO	VALOR	CRITICIDAD				
				C	I	D	A	T
[I] Información	**[I_estudiante]**	Información académica de estudiantes de la universidad.	Alto	9	9	7	10	9
	[I_PEI]	Plan educativo institucional.	Medio	1	4	9		
	[I_PEP]	25 Planes Educativo de Programa.	Medio	1	4	9		
	[I_notas]	17500 registros de Notas de los estudiantes.	Muy alto	10	9	7	10	10
	[I_aspirante]	1 Listado de los aspirantes por semestre.	Alto	8	7	7		4

[4] Irrelevante para la organización.
[5] Daño menor para la organización.
[6] Daño importante para la organización.
[7] Daño importante para la organización.
[8] Daño grave para la organización.
[9] Daño muy grave para la organización.

	[I_desercion]	1 Listado de estudiantes desertados por semestre.	Medio	6	4	8	4	4
	[I_micros]	25 Contenidos curriculares de cada programa.	Medio	2	6	9		
	[I_personal]	Datos de carácter personal	Muy alto	9	9	10	9	9
	[I_docente]	Información personal de 435 docentes	Muy alto	9	9	10	9	9
	[I_adm]	Información personal de 123 empleados administrativos	Muy alto	9	9	10	9	9
	[I_estudiante]	Datos personales de 17500 estudiantes aproximadamente.	Muy alto	9	9	10	9	9
[S] Servicios	**[SI_internet]**	Servicio de acceso a internet en el campus por un canal de 100Mbps.	Alto	7	8	10	5	7
	[SI_www_aulas]	Sitio web de las aulas virtuales para 5800 estudiantes por semestre, aproximadamente.	Alto	7	8	7	5	8
	[SI_www_atenea]	Sitio web de la Biblioteca Wolmar Casadiego.	Alto	7	8	7	5	8
	[SI_correo]	Correo electrónico de la Universidad con cuentas para estudiantes, docentes y administrativos.	Muy alto	10	9	10	9	10
	[SI_www_]	Sitio web de la universidad	Alto	7	8	10	9	9
[D] Datos	**[D_config]**	Archivos de configuración	Muy alto	9	9	9	9	9
	[D_backups]	Copias de seguridad de la información a respaldar (servidores)	Alto	3	8	6	8	8
	[D_pass]	Contraseñas en el sistema de información SISTENOTAS, GMAIL de 17500 estudiantes.	Alto	10	10	10	2	9
	[D_acl]	Datos de control de acceso por cada VLAN (son 3)	Medio	5	4	4	5	4
	[D_log]	Archivos de registro de actividad de los sistemas.	Medio	5	2	5	1	8

[Soft] Software	[Soft_SISTENOTAS]	Sistema de gestión Académica	Muy alto	10	10	10	9	10
	[Soft_Moodle]	Sistema de aulas virtuales	Alto	8	8	9	8	8
	[Soft_people]	Sistema crm de la universidad	Muy alto	9	7	10	9	10
	[Soft_glpi]	Sistema de gestión de soporte técnico	Alto	5	2	8	9	9
	[Soft_nomina]	Sistema de nómina	Muy alto	10	8	10	9	9
	[Soft_antivirus]	Software antivirus	Muy alto	9	9	9	9	9
	[Soft_pm]	Software de biblioteca	Alto	6	5	10	5	5
	[Soft_so]	Sistemas operativos	Muy alto	9	9	10	9	10
	[Soft_office]	Herramientas ofimáticas para 1257 equipos	Medio	5	5	4	5	5
	[Soft_navegador]	Navegador web	Medio	4	4	4	4	4
	[Soft_correo]	Cliente de correo electrónico	Medio	9	2	5	4	4
	[Soft_autocad]	125 licencias de Software en aulas de sistemas	Medio	4	5	5	5	5
[Hard] Hardware	[Hard_ap]	7 Access Points	Alto			8	5	6
	[Hard_firewall]	Firewall de la red	Alto			8	5	8
	[Hard_impresora]	47 Impresoras	Medio			3	5	5
	[Hard_pbx]	1 PBX	Medio			9	2	2
	[Hard_pc]	1257 Equipos de escritorio	Alto			7	5	6
	[Hard_portatil]	38 Equipos portátiles	Medio			6	5	6
	[Hard_router]	5 Enrutadores	Alto			9	5	8
	[Hard_scanner]	20 Escáneres	Medio			5	3	3
	[Hard_servidor]	5 Servidores	Muy alto			10	9	9
	[Hard_switch]	42 Switches	Medio			4	5	5
[Alm] Disp. de alm.	[Alm_cinta]	8 Cintas magnéticas	Alto			8		
	[Alm_discos]	20 Discos duros	Alto			8		
	[Alm_usb]	350 Dispositivos USB	Alto			8		

[Aux] Equipamiento auxiliar	**[Aux_cableado]**	Cableado estructurado de las 5 sedes	Muy alto			9		
	[Aux_gabinete]	5 Gabinetes de telecomunicaciones	Muy alto			9		
	[Aux_ups]	5 Sistemas de información ininterrumpida	Alto			8		
	[Aux_ventilación]	1 Equipos de ventilación de cuartos de comunicaciones	Muy alto			9		
[Com] Redes de comunicaciones	**[Com_inalámbrica]**	4 Redes inalámbricas	Alto	7	9	7	7	7
	[Com_internet]	1 conexión a Internet	Muy alto	9	9	9	9	9
	[Com_LAN]	1 Red LAN interna	Alto	10	8	10	5	8
	[Com_telefónica]	1 Red telefónica	Medio	3	1	6	5	2
[Inst] Instala	**[Inst_oficina]**	Oficinas administrativas	Medio	7	0	9		
	[Inst_edificio]	Edificios	Medio	4	0	7		3
[P] Personas	**[P_uinterno]**	Usuario interno	Medio			5		
	[P_admred]	1 Administrador de red	Ext alto			10		
	[P_admserv]	1 Administrador de servidores	Ext alto			10		
	[P_admapl]	1 Administrador de aplicaciones	Muy alto			9		
	[P_softw]	2 Ingenieros de desarrollo	Medio			4		
	[P_soporte]	4 Ingenieros de soporte	Alto			6		
	[P_vicerrector]	3 Vicerrectores	Medio			4		
	[P_coord]	21 Coordinadores de proceso	Medio			4		
	[P_asistente]	25 Asistentes administrativos	Medio			3		
	[P_gestionh]	1 Directora de Gestión humana	Alto			6		
	[P_docente]	435 Docentes	Medio			5		
	[P_uexterno]	Usuario externo	Medio			4		

Tabla 4. Valoración de los activos

5.2 Caracterización de las amenazas

Con los activos ya identificados y valorados en el numeral anterior, el siguiente paso consiste en determinar las amenazas que puede afectar a cada activo. Magerit identifica las amenazas que pueden afectar a los activos de acuerdo con las siguientes categorías:

1. Desastres naturales [N]
2. De origen industrial [I]
3. Errores y fallos no intencionados [E]
4. Ataques intencionados [A]

Las amenazas pueden centrarse en un activo en particular y por una reacción en cadena afectar el resto de activos de acuerdo a sus relaciones de dependencia.

La actividad de caracterización de amenazas se puede diferenciar en dos tareas: la identificación de las amenazas que afectan a los activos y la valoración de las mismas.

5.2.1. Identificación de las amenazas

Para la identificación de las amenazas se ha usado el capítulo 5 del libro II de la metodología (MAGERIT - versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información. Libro II. Catálogo de elementos., 2012, págs. 25-47), de las cuales se obtiene la tabla de identificación de amenazas para una universidad colombiana:

N. Desastres naturales			
COD.	**AMENAZA**	**ACTIVOS AFECTADOS**	**DIM. AFECTADAS**
N.1	Fuego	[Hard_ap] [Hard_firewall] [Hard_impresora] [Hard_pbx] [Hard_pc] [Hard_portatil] [Hard_router] [Hard_scanner] [Hard_servidor] [Hard_switch] [Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica] [Inst_oficina] [Inst_edificio] [Aux_cableado] [Aux_gabinete] [Aux_ups] [Aux_ventilación] [Alm_cinta] [Alm_discos] [Alm_usb]	[D]
N.2	Daños por agua	[Hard_ap] [Hard_firewall] [Hard_impresora] [Hard_pbx] [Hard_pc] [Hard_portatil] [Hard_router] [Hard_scanner] [Hard_servidor] [Hard_switch]	[D]

N. Desastres naturales			
		[Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica] [Inst_oficina] [Inst_edificio] [Aux_cableado] [Aux_gabinete] [Aux_ups] [Aux_ventilación] [Alm_cinta] [Alm_discos] [Alm_usb]	
N.*	Desastres naturales	[Hard_ap] [Hard_firewall] [Hard_impresora] [Hard_pbx] [Hard_pc] [Hard_portatil] [Hard_router] [Hard_scanner] [Hard_servidor] [Hard_switch] [Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica] [Inst_oficina] [Inst_edificio] [Aux_cableado] [Aux_gabinete] [Aux_ups] [Aux_ventilación] [Alm_cinta] [Alm_discos] [Alm_usb]	[D]

I. De origen industrial			
COD.	**AMENAZA**	**ACTIVOS AFECTADOS**	**DIM. AFECTADAS**
I1	Fuego	[Hard_ap] [Hard_firewall] [Hard_impresora] [Hard_pbx] [Hard_pc] [Hard_portatil] [Hard_router] [Hard_scanner] [Hard_servidor] [Hard_switch] [Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica] [Inst_oficina] [Inst_edificio] [Aux_cableado] [Aux_gabinete] [Aux_ups] [Aux_ventilación] [Alm_cinta] [Alm_discos] [Alm_usb]	[D]
I.2	Daños por agua	[Hard_ap] [Hard_firewall] [Hard_impresora] [Hard_pbx] [Hard_pc] [Hard_portatil] [Hard_router] [Hard_scanner] [Hard_servidor] [Hard_switch] [Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica] [Inst_oficina] [Inst_edificio] [Aux_cableado] [Aux_gabinete] [Aux_ups] [Aux_ventilación] [Alm_cinta] [Alm_discos] [Alm_usb]	[D]
I.*	Desastres industriales	[Hard_ap] [Hard_firewall] [Hard_impresora] [Hard_pbx] [Hard_pc] [Hard_portatil] [Hard_router] [Hard_scanner] [Hard_servidor] [Hard_switch] [Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica] [Inst_oficina] [Inst_edificio] [Aux_cableado] [Aux_gabinete] [Aux_ups] [Aux_ventilación] [Alm_cinta] [Alm_discos] [Alm_usb]	[D]

I. De origen industrial			
I.5	Averías de origen físico o lógico	[Soft_SISTENOTAS] [Soft_Moodle] [Soft_people] [Soft_glpi] [Soft_nomina] [Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad] [Hard_ap] [Hard_firewall] [Hard_impresora] [Hard_pbx] [Hard_pc] [Hard_portatil] [Hard_router] [Hard_scanner] [Hard_servidor] [Hard_switch] [Aux_cableado] [Aux_gabinete] [Aux_ups] [Aux_ventilación] [Alm_cinta] [Alm_discos] [Alm_usb]	[D]
I.6	Corte del suministro eléctrico	[Hard_ap] [Hard_firewall] [Hard_impresora] [Hard_pbx] [Hard_pc] [Hard_portatil] [Hard_router] [Hard_scanner] [Hard_servidor] [Hard_switch] [Aux_cableado] [Aux_gabinete] [Aux_ups] [Aux_ventilación]	[D]
I.8	Fallos del servicio de comunicaciones	[Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica]	[D]
I.10	Degradación de los soportes de almacenamiento de información	[Alm_cinta] [Alm_discos] [Alm_usb]	[D]

E. Errores y fallos no intencionados			
COD.	**AMENAZA**	**ACTIVOS AFECTADOS**	**DIM. AFECTADAS**
E.1	Errores de usuarios	[D_pass] [SI_internet] [SI_www_aulas] [SI_www_atenea] [SI_correo] [SI_www_] Soft_SISTENOTAS] [Soft_Moodle] [Soft_people] [Soft_glpi] [Soft_nomina] [Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad] [I_estudiante] [I_PEP] [I_notas] [I_aspirante] [I_desercion] [I_micros] [I_personal] [I_docente] [I_adm] [I_estudiante]	[D], [I], [C]
E.2	Errores del administrador	[I_estudiante] [I_notas] [I_aspirante] [I_desercion] [I_personal] [I_docente] [I_adm] [I_estudiante] [D_config] [D_backups] [D_pass] [D_acl] [D_log] [SI_internet] [SI_www_aulas] [SI_www_atenea] [SI_correo] [SI_www_] [Soft_SISTENOTAS]	[D], [I], [C]

E. Errores y fallos no intencionados			
		[Soft_Moodle] [Soft_people] [Soft_glpi] [Soft_nomina] [Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad] [Hard_ap] [Hard_firewall] [Hard_impresora] [Hard_pbx] [Hard_pc] [Hard_portatil] [Hard_router] [Hard_scanner] [Hard_servidor] [Hard_switch] [Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica]	
E,3	Errores de monitorización	[D_log]	[I], [T]
E.4	Errores de configuración	[D_config]	[I]
E.7	Deficiencias en la organización	[P_uinterno] [P_admred] [P_admserv] [P_admapl] [P_softw] [P_soporte] [P_vicerrector] [P_coord] [P_asistente] [P_gestionh] [P_docente]	[D]
E.8	Difusión de software dañino	[Soft_SISTENOTAS] [Soft_Moodle] [Soft_people] [Soft_glpi] [Soft_nomina] [Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad]	[D], [I], [C]
E.9	Errores de re-encaminamiento	[Soft_nomina] [Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [SI_internet] [SI_www_aulas] [SI_www_atenea] [SI_correo] [SI_www_] [Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica]	[C]
E.10	Errores de secuencia	[Soft_SISTENOTAS] [Soft_Moodle] [Soft_people] [Soft_glpi] [Soft_nomina] [Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad] [SI_internet] [SI_www_aulas] [SI_www_atenea] [SI_correo] [SI_www_] [Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica]	[I]
E.15	Alteración accidental de información	[D_config] [D_backups] [D_acl] [D_log] [I_estudiante] [I_notas] [I_aspirante] [I_desercion] [I_personal] [I_docente] [I_adm] [I_estudiante] [Soft_SISTENOTAS] [Soft_Moodle] [Soft_people] [Soft_glpi] [Soft_nomina] [Soft_antivirus] [Soft_pm] [Soft_so]	[I]

E. Errores y fallos no intencionados			
		[Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad] [Alm_cinta] [Alm_discos] [Alm_usb]	
E.18	Destrucción de la información	[D_config] [D_backups] [D_acl] [D_log] [I_estudiante] [I_notas] [I_aspirante] [I_desercion] [I_micros] [I_personal] [I_docente] [I_adm] [I_estudiante] [Soft_SISTENOTAS] [Soft_Moodle] [Soft_people] [Soft_glpi] [Soft_nomina] [Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad] [Alm_cinta] [Alm_discos] [Alm_usb]	[D]
E.19	Fugas de información	[D_config] [D_backups] [D_pass] [D_acl] [D_log] [I_estudiante] [I_notas] [I_aspirante] [I_desercion] [I_micros] [I_personal] [I_docente] [I_adm] [I_estudiante] [Soft_SISTENOTAS] [Soft_Moodle] [Soft_people] [Soft_glpi] [Soft_nomina] [Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad] [Alm_cinta] [Alm_discos] [Alm_usb] [Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica] [P_uinterno] [P_admred] [P_admserv] [P_admapl] [P_softw] [P_soporte] [P_vicerrector] [P_coord] [P_asistente] [P_gestionh] [P_docente] [P_uexterno]	[C]
E.20	Vulnerabilidades de los programas	[Soft_SISTENOTAS] [Soft_Moodle] [Soft_people] [Soft_glpi] [Soft_nomina] [Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad]	[D], [I], [C]
E.21	Errores de mantenimiento/ actualización de los programas (software).	[Soft_SISTENOTAS] [Soft_Moodle] [Soft_people] [Soft_glpi] [Soft_nomina] [Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad]	[D], [I]
E.23	Errores de mantenimiento/ actualización de los programas (hardware).	[Hard_ap] [Hard_firewall] [Hard_impresora] [Hard_pbx] [Hard_pc] [Hard_portatil] [Hard_router] [Hard_scanner] [Hard_servidor] [Hard_switch] [Aux_cableado] [Aux_gabinete]	[D]

E. Errores y fallos no intencionados			
		[Aux_ups] [Aux_ventilación] [Alm_cinta] [Alm_discos] [Alm_usb]	
E.24	Caída del sistema por agotamiento de recursos	[Hard_ap] [Hard_firewall] [Hard_impresora] [Hard_pbx] [Hard_pc] [Hard_portatil] [Hard_router] [Hard_scanner] [Hard_servidor] [Hard_switch] [Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad] [Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica]	[D]
E.25	Pérdida de equipos	[Hard_ap] [Hard_firewall] [Hard_impresora] [Hard_pbx] [Hard_pc] [Hard_portatil] [Hard_router] [Hard_scanner] [Hard_servidor] [Hard_switch] [Alm_cinta] [Alm_discos] [Alm_usb] [Aux_cableado] [Aux_gabinete] [Aux_ups] [Aux_ventilación]	[D], [C]
E.28	Indisponibilidad de personal	[P_uinterno] [P_admred] [P_admserv] [P_admapl] [P_softw] [P_soporte] [P_vicerrector] [P_coord] [P_asistente] [P_gestionh] [P_docente]	[D]

A. Ataques intencionados			
COD.	**AMENAZA**	**ACTIVOS AFECTADOS**	**DIM. AFECTADAS**
A.3	Manipulación de los registros de actividad (log)	[D_log]	[I], [T]
A.4	Manipulación de la configuración.	[D_config]	[D], [I], [C]
A.5	Suplantación de la identidad del usuario	[I_estudiante] [I_notas] [I_aspirante] [I_desercion] [I_personal] [I_docente] [I_adm] [I_estudiante] [D_config] [D_backups] [D_pass] [D_acl] [D_log] [SI_internet] [SI_www_aulas] [SI_www_atenea] [SI_correo] [SI_www_] [Soft_SISTENOTAS] [Soft_Moodle] [Soft_people] [Soft_glpi] [Soft_nomina] [Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad] [Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica]	[D], [I], [C]
A.6	Abuso de privilegios de acceso.	[I_estudiante] [I_notas] [I_aspirante] [I_desercion] [I_personal] [I_docente] [I_adm] [I_estudiante] [D_config] [D_backups] [D_pass] [D_acl] [D_log]	[D], [I], [C]

A. Ataques intencionados			
		[SI_internet] [SI_www_aulas] [SI_www_atenea] [SI_correo] [SI_www_] [Soft_SISTENOTAS] [Soft_Moodle] [Soft_people] [Soft_glpi] [Soft_nomina] [Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad] [Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica]	
A.7	Uso no previsto	[I_estudiante] [I_PEP] [I_notas] [I_aspirante] [I_desercion] [I_micros] [I_personal] [I_docente] [I_adm] [I_estudiante] [D_pass] [SI_internet] [SI_www_aulas] [SI_www_atenea] [SI_correo] [SI_www_] [Soft_SISTENOTAS] [Soft_Moodle] [Soft_people] [Soft_glpi] [Soft_nomina] [Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad] [Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica] [Hard_ap] [Hard_firewall] [Hard_impresora] [Hard_pbx] [Hard_pc] [Hard_portatil] [Hard_router] [Hard_scanner] [Hard_servidor] [Hard_switch] [Aux_cableado] [Aux_gabinete] [Aux_ups] [Aux_ventilación] [Alm_cinta] [Alm_discos] [Alm_usb] [Inst_oficina] [Inst_edificio]	[D], [I], [C]
A.8	Difusión de software dañino	[Soft_SISTENOTAS] [Soft_Moodle] [Soft_people] [Soft_glpi] [Soft_nomina] [Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad]	[D], [I], [C]
A.9	Re-encaminamiento de paquetes	[SI_internet] [SI_www_aulas] [SI_www_atenea] [SI_correo] [SI_www_] [Soft_SISTENOTAS] [Soft_Moodle] [Soft_people] [Soft_glpi] [Soft_nomina] [Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad] [Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica]	[C]
A.10	Alteración de la secuencia	[SI_internet] [SI_www_aulas] [SI_www_atenea] [SI_correo] [SI_www_] [Soft_SISTENOTAS] [Soft_Moodle] [Soft_people] [Soft_glpi] [Soft_nomina] [Soft_antivirus] [Soft_pm] [Soft_so]	[I]

A. Ataques intencionados			
		[Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad] [Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica]	
A.11	Acceso no autorizado	[I_estudiante] [I_PEI] [I_PEP] [I_notas] [I_aspirante] [I_desercion] [I_micros] [I_personal] [I_docente] [I_adm] [I_estudiante] [D_config] [D_backups] [D_pass] [D_acl] [D_log] [SI_internet] [SI_www_aulas] [SI_www_atenea] [SI_correo] [SI_www_] [Soft_SISTENOTAS] [Soft_Moodle] [Soft_people] [Soft_glpi] [Soft_nomina] [Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad] [Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica] [Hard_ap] [Hard_firewall] [Hard_impresora] [Hard_pbx] [Hard_pc] [Hard_portatil] [Hard_router] [Hard_scanner] [Hard_servidor] [Hard_switch] [Aux_cableado] [Aux_gabinete] [Aux_ups] [Aux_ventilación] [Alm_cinta] [Alm_discos] [Alm_usb] [Inst_oficina] [Inst_edificio]	[I], [C]
A.12	Análisis de tráfico	[Com_inalámbrica] [Com_internet] [Com_LAN]	[C]
A.13	Repudio	[SI_internet] [SI_www_aulas] [SI_www_atenea] [SI_correo] [SI_www_] [D_log]	[C]
A.14	Interceptación de información (escucha)	[Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica]	[C]
A.15	Modificación deliberada de información	[I_estudiante] [I_PEI] [I_PEP] [I_notas] [I_aspirante] [I_desercion] [I_micros] [I_personal] [I_docente] [I_adm] [I_estudiante] [D_config] [D_backups] [D_acl] [D_log] [SI_internet] [SI_www_aulas] [SI_www_atenea] [SI_correo] [SI_www_] [Soft_SISTENOTAS] [Soft_Moodle] [Soft_people] [Soft_glpi] [Soft_nomina] [Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad] [Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica] [Inst_oficina] [Inst_edificio]	[I]
A.18	Destrucción de información	[D_config] [D_backups] [D_acl] [D_log] [I_estudiante] [I_PEP] [I_notas] [I_aspirante]	[D]

A. Ataques intencionados			
		[I_desercion] [I_micros] [I_personal] [I_docente] [I_adm] [I_estudiante] [SI_www_aulas] [SI_www_atenea] [SI_correo] [SI_www_] [Soft_SISTENOTAS] [Soft_Moodle] [Soft_people] [Soft_glpi] [Soft_nomina] [Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad] [Alm_cinta] [Alm_discos] [Alm_usb] [Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica]	
A.19	Divulgación de información	[I_estudiante] [I_PEI] [I_PEP] [I_notas] [I_aspirante] [I_desercion] [I_micros] [I_personal] [I_docente] [I_adm] [I_estudiante] [D_config] [D_backups] [D_acl] [D_log] [SI_internet] [SI_www_aulas] [SI_www_atenea] [SI_correo] [SI_www_] [Soft_SISTENOTAS] [Soft_Moodle] [Soft_people] [Soft_glpi] [Soft_nomina] [Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad] [Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica] [Hard_pc] [Hard_portatil] [Hard_scanner] [Hard_servidor] [Alm_cinta] [Alm_discos] [Alm_usb] [Inst_oficina] [Inst_edificio]	[C]
A.22	Manipulación de programas	[Soft_SISTENOTAS] [Soft_Moodle] [Soft_people] [Soft_glpi] [Soft_nomina] [Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad]	[D], [I], [C]
A.23	Manipulación de los equipos.	[Hard_ap] [Hard_firewall] [Hard_impresora] [Hard_pbx] [Hard_pc] [Hard_portatil] [Hard_router] [Hard_scanner] [Hard_servidor] [Hard_switch] [Alm_cinta] [Alm_discos] [Alm_usb] [Aux_cableado] [Aux_gabinete] [Aux_ups] [Aux_ventilación]	[D], [I], [C]
A.24	Denegación de servicio.	[Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad] [Hard_ap] [Hard_firewall] [Hard_impresora] [Hard_pbx] [Hard_pc] [Hard_portatil] [Hard_router] [Hard_scanner] [Hard_servidor] [Hard_switch]	[D]

A. Ataques intencionados			
		[Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica]	
A.25	Robo	[Hard_ap] [Hard_firewall] [Hard_impresora] [Hard_pbx] [Hard_pc] [Hard_portatil] [Hard_router] [Hard_scanner] [Hard_servidor] [Hard_switch] [Alm_cinta] [Alm_discos] [Alm_usb] [Aux_cableado] [Aux_gabinete] [Aux_ups] [Aux_ventilación]	[D], [C]
A.26	Ataque destructivo	[Hard_ap] [Hard_firewall] [Hard_impresora] [Hard_pbx] [Hard_pc] [Hard_portatil] [Hard_router] [Hard_scanner] [Hard_servidor] [Hard_switch] [Alm_cinta] [Alm_discos] [Alm_usb] [Aux_cableado] [Aux_gabinete] [Aux_ups] [Aux_ventilación] [Inst_oficina] [Inst_edificio]	[D]
A.26	Ocupación enemiga	[Inst_oficina] [Inst_edificio]	[D], [C]
A.28	Indisponibilidad de personal.	[P_uinterno] [P_admred] [P_admserv] [P_admapl] [P_softw] [P_soporte] [P_vicerrector] [P_coord] [P_asistente] [P_gestionh] [P_docente]	[D]
A.29	Extorsión	[P_uinterno] [P_admred] [P_admserv] [P_admapl] [P_softw] [P_soporte] [P_vicerrector] [P_coord] [P_asistente] [P_gestionh] [P_docente]	[D], [I], [C]
A.30	Ingeniería social	[P_uinterno] [P_admred] [P_admserv] [P_admapl] [P_softw] [P_soporte] [P_vicerrector] [P_coord] [P_asistente] [P_gestionh] [P_docente]	[D], [I], [C]

5.2.2. Valoración de las amenazas

Una vez identificadas las amenazas que afectan al sistema, es fundamental valorar su influencia en el valor del activo teniendo en cuenta dos parámetros:

- El impacto, es decir, cuán perjudicado resultaría el valor del activo en el caso de materializarse la amenaza.
- La probabilidad que se materialice la amenaza.

En el caso del plan desarrollado para el sistema en estudio, se tomará la siguiente tabla de probabilidad de ocurrencia, de carácter cuantitativo:

Probabilidad	Valor		Periodicidad
MB (Muy baja)	1/100	Muy poco frecuente	Siglos
B (Baja)	1/10	Poco frecuente	Cada varios años
M (Media)	1	Normal	Una vez al año
A (Alta)	10	Frecuente	Mensualmente
MA (Muy alta)	100	Muy frecuente	A diario

Tabla 5: Tabla de probabilidad[10]

Para medir el impacto se toma un porcentaje del valor del activo que se pierde en caso de que se presente una incidencia, por lo cual se puede tomar de referencia la siguiente tabla:

Impacto	Valor
Muy bajo	10%
Bajo	20%
Medio	50%
Alto	75%
Muy alto	100%

Tabla 6. Tabla de valoración del impacto

Aplicando estas métricas a cada una de las amenazas que pueden afectar a los activos se obtienen las siguientes tablas para cada categoría de activo:

[I] Información/datos esenciales

Id. Activo	Id. Amenaza	Frecuencia	Dimensiones				
			C	I	D	A	T
[I_estudiante], [I_notas], [I_personal], [I_docente], [I_adm]	E.1 Errores de usuarios	10	10%	10%	10%		
	E.2 Errores del administrador	1	10%	10%	20%		
	E.15 Alteración accidental de información	10		10%			

[10] (Consejo Superior de Administración Electrónica de España, 2012, pág. 28)

Id. Activo	Id. Amenaza	Frecuencia	Dimensiones				
			C	I	D	A	T
	E.18 Destrucción de la información	1			50%		
	E.19 Fugas de información	1	50%				
	A.5 Suplantación de la identidad del usuario	0,1	75%	100%			
	A.6 Abuso de privilegios de acceso.	1	10%	10%	10%		
	A.7 Uso no previsto	0,1	20%	10%	10%		
	A.11 Acceso no autorizado	1	50%	50%			
	A.15 Modificación deliberada de información	0,1		75%			
	A.18 Destrucción de información	0,01			50%		
	A.19 Divulgación de información	0,01	75%				
[I_PEI] [I_PEP] [I_micros]	A.7 Uso no previsto	0,1	10%	10%	10%		
	A.11 Acceso no autorizado	0,1	10%	10%			
	A.15 Modificación deliberada de información	0,01		50%			
	A.19 Divulgación de información	1	25%				
[I_aspirante], [I_desercion]	E.1 Errores de usuarios	10	50%	10%	50%		
	E.2 Errores del administrador	1	50%	10%	50%		
	E.15 Alteración accidental de información	10		50%			
	E.18 Destrucción de la información	1			50%		
	E.19 Fugas de información	1	50%				
	A.5 Suplantación de la identidad del usuario	0,1	75%	100%			
	A.6 Abuso de privilegios de acceso.	1	10%	10%	10%		

Id. Activo	Id. Amenaza	Frecuencia	Dimensiones				
			C	I	D	A	T
	A.7 Uso no previsto	0,1	20%	10%	10%		
	A.11 Acceso no autorizado	1	50%	50%			
	A.15 Modificación deliberada de información	0,1		75%			
	A.18 Destrucción de información	0,01			50%		
	A.19 Divulgación de información	0,01	75%				

[S] Servicios

Id. Activo	Id. Amenaza	Frecuencia	Dimensiones				
			C	I	D	A	T
[SI_internet]	I.5 Averías de origen físico o lógico	0,1			100%		
	E.1 Errores de usuarios	0,01			50%		
	E.2 Errores del administrador	0,1	20%	10%	50%		
	E.9 Errores de re-encaminamiento	0,01	10%				
	E.10 Errores de secuencia	0,01		10%			
	A.5 Suplantación de la identidad del usuario	0,01				100%	
	A.6 Abuso de privilegios de acceso.	0,01	50%	10%	50%		
	A.7 Uso no previsto	0,1	10%	10%	20%		
	A.9 Re-encaminamiento de paquetes	0,01	10%				
	A.10 Alteración de la secuencia	0,01		10%			
	A.11 Acceso no autorizado	0,1	50%	10%			
	A.13 Repudio	0,01				100%	

Id. Activo	Id. Amenaza	Frecuencia	Dimensiones				
			C	I	D	A	T
	A.15 Modificación deliberada de información	0,01		20%			
[SI_www_aulas] [SI_www_atenea] [SI_correo] [SI_www_]	I.5 Averías de origen físico o lógico	0,01			100%		
	E.1 Errores de usuarios	0,1	20%	20%			
	E.2 Errores del administrador	0,01	20%	20%			
	E.8 Difusión de software dañino	0,01	20%	20%	50%		
	E.10 Errores de secuencia	0,01	20%		20%		
	E.15 Alteración accidental de información	0,1		20%			
	E.18 Destrucción de la información	0,01			20%		
	E.19 Fugas de información	0,1	20%				
	E.20 Vulnerabilidades de los programas	0,1	20%	10%	50%		
	E.21 Errores de mantenimiento/ actualización de los programas (software).	0,1	20%	10%	20%		
	E.24 Caída del sistema por agotamiento de recursos	1			50%		
	A.5 Suplantación de la identidad del usuario	1				50%	
	A.6 Abuso de privilegios de acceso.	0,1				50%	
	A.7 Uso no previsto	0,1	20%				
	A.8 Difusión de software dañino	0,01			20%		
	A.9 Re-encaminamiento de paquetes	0,01	10%				
	A.10 Alteración de la secuencia	0,01	10%				

[D] Datos

Id. Activo	Id. Amenaza	Frecuencia	Impacto por dimensión				
			C	I	D	A	T
[D_config] [D_backups] [D_acl] [D_log]	E.2 Errores del administrador	1	20%	20%	20%		
	E.4 Errores de configuración	0,1		50%			
	E.15 Alteración accidental de información	10		20%			
	E.18 Destrucción de la información	0,1			20%		
	E.19 Fugas de información	0,01	20%				
	A.4 Manipulación de la configuración.	0,1		50%			
	A.5 Suplantación de la identidad del usuario	0,1	50%	20%		100%	
	A.6 Abuso de privilegios de acceso.	0,1	100%	20%			
	A.11 Acceso no autorizado	0,1	100%	50%		100%	
	A.15 Modificación deliberada de información	0,01		50%			
	A.18 Destrucción de información	0,01			50%		
	A.19 Divulgación de información	0,1	100%				
[D_pass]	E.1 Errores de usuarios	1	50%				
	E.2 Errores del administrador	0,01	20%				
	E.19 Fugas de información	0,1	20%				
	A.5 Suplantación de la identidad del usuario	1				100%	
	A.6 Abuso de privilegios de acceso.	0,1				100%	
	A.11 Acceso no autorizado	0,1				100%	

[Soft] Software

Id. Activo	Id. Amenaza	Frecuencia	Impacto por dimensión				
			C	I	D	A	T
[Soft_SISTENOTAS] [Soft_Moodle] [Soft_people] [Soft_glpi] [Soft_nomina]	I.5 Averías de origen físico o lógico	0,1			70%		
	E.1 Errores de usuarios	10	10%	10%	10%		
	E.2 Errores del administrador	1	10%	20%	20%		
	E.8 Difusión de software dañino	0,1	10%	20%	20%		
	E.9 Errores de re-encaminamiento	0,01	10%	10%	10%		
	E.10 Errores de secuencia	0,01		20%			
	E.15 Alteración accidental de información	1		20%			
	E.18 Destrucción de la información	0,1			50%		
	E.19 Fugas de información	10	50%				
	E.20 Vulnerabilidades de los programas	0,1	20%	20%	20%		
	E.21 Errores de mantenimiento/ actualización de los programas (software).	0,1		20%	20%		
	A.5 Suplantación de la identidad del usuario	0,1	50%	10%		100%	
	A.6 Abuso de privilegios de acceso.	0,1	50%	20%	20%		
	A.7 Uso no previsto	0,1	20%	20%	100%		
	A.8 Difusión de software dañino	0,1	75%	75%	100%		
	A.9 Re-encaminamiento de paquetes	0,01	50%				
	A.10 Alteración de la secuencia	0,01		50%			
	A.11 Acceso no autorizado	0,1	50%	20%			

Id. Activo	Id. Amenaza	Frecuencia	Impacto por dimensión				
			C	I	D	A	T
	A.15 Modificación deliberada de información	0,1		50%			
	A.18 Destrucción de información	0,1			50%		
	A.19 Divulgación de información	1	50%				
	A.22 Manipulación de programas	0,1	100%	100%	100%		
[Soft_antivirus] [Soft_pm] [Soft_so] [Soft_office] [Soft_navegador] [Soft_correo] [Soft_autocad]	I.5 Averías de origen físico o lógico	10			50%		
	E.1 Errores de usuarios	0,1	10%	10%	10%		
	E.2 Errores del administrador	0,1	10%	10%	10%		
	E.8 Difusión de software dañino	0,1	10%	20%	20%		
	E.9 Errores de re-encaminamiento	0,01	10%	10%	10%		
	E.10 Errores de secuencia	0,01		20%			
	E.15 Alteración accidental de información	0,01		10%			
	E.18 Destrucción de la información	0,01			50%		
	E.19 Fugas de información	0,01	50%				
	E.20 Vulnerabilidades de los programas	0,01	20%	20%	20%		
	E.21 Errores de mantenimiento/ actualización de los programas (software).	0,1		20%	20%		
	A.5 Suplantación de la identidad del usuario	0,01	50%	50%		100%	
	A.6 Abuso de privilegios de acceso.	0,1	50%	20%	20%		
	A.7 Uso no previsto	0,1	10%	10%	100%		

Id. Activo	Id. Amenaza	Frecuencia	Impacto por dimensión				
			C	I	D	A	T
	A.8 Difusión de software dañino	1	75%	75%	100%		
	A.9 Re-encaminamiento de paquetes	0,1	50%				
	A.10 Alteración de la secuencia	0,1		50%			
	A.11 Acceso no autorizado	0,1	50%	20%			
	A.15 Modificación deliberada de información	0,1		50%			
	A.18 Destrucción de información	0,1			50%		
	A.19 Divulgación de información	1	50%				
	A.22 Manipulación de programas	1	100%	100%	100%		

[Hard] Hardware

Id. Activo	Id. Amenaza	Frecuencia	Impacto por dimensión				
			C	I	D	A	C
[Hard_ap] [Hard_firewall] [Hard_pbx] [Hard_router] [Hard_switch]	N.1 Fuego	0,01			100%		
	N.2 Daños por agua	0,01			100%		
	N.* Desastres naturales	0,01			100%		
	I1 Fuego	0,01			100%		
	I.2 Daños por agua	0,01			100%		
	I.* Desastres industriales	0,01			100%		
	I.5 Averías de origen físico o lógico	0,1			100%		
	I.6 Corte del suministro eléctrico	0,01			75%		
	E.2 Errores del administrador	0,1	50%	50%	50%		

Id. Activo	Id. Amenaza	Frecuencia	Impacto por dimensión				
			C	I	D	A	C
	E.23 Errores de mantenimiento/ actualización de los programas (hardware).	0,1			100%		
	E.24 Caída del sistema por agotamiento de recursos	0,01			50%		
	E.25 Pérdida de equipos	0,01	100%		100%		
	A.7 Uso no previsto	0,1	100%	50%	100%		
	A.11 Acceso no autorizado	0,01	50%	50%			
	A.23 Manipulación de los equipos.	0,01	50%		50%		
	A.24 Denegación de servicio.	0,01			100%		
	A.25 Robo	0,01	100%		100%		
	A.26 Ataque destructivo	0,1			100%		
[Hard_servidor]	N.1 Fuego	0,01			100%		
	N.2 Daños por agua	0,01			100%		
	N.* Desastres naturales	0,01			100%		
	I1 Fuego	0,01			100%		
	I.2 Daños por agua	0,01			100%		
	I.* Desastres industriales	0,01			100%		
	I.5 Averías de origen físico o lógico	0,1			100%		
	I.6 Corte del suministro eléctrico	0,1			100%		
	E.2 Errores del administrador	0,1			25%		
	E.23 Errores de mantenimiento/ actualización de los programas (hardware).	0,1			75%		

Id. Activo	Id. Amenaza	Frecuencia	Impacto por dimensión				
			C	I	D	A	C
	E.24 Caída del sistema por agotamiento de recursos	0,01			50%		
	E.25 Pérdida de equipos	0,01	100%		100%		
	A.7 Uso no previsto	0,1	100%	50%	100%		
	A.11 Acceso no autorizado	0,01	50%	50%			
	A.23 Manipulación de los equipos.	0,01	50%		50%		
	A.24 Denegación de servicio.	0,01			100%		
	A.25 Robo	0,01	100%		100%		
	A.26 Ataque destructivo	0,1			100%		
[Hard_pc] [Hard_portatil] [Hard_scanner] [Hard_impresora]	N.1 Fuego	0,01			100%		
	N.2 Daños por agua	0,01			100%		
	N.* Desastres naturales	0,01			100%		
	I1 Fuego	0,01			100%		
	I.2 Daños por agua	0,01			100%		
	I.* Desastres industriales	0,01			100%		
	I.5 Averías de origen físico o lógico	1			100%		
	I.6 Corte del suministro eléctrico	0,01			50%		
	E.2 Errores del administrador	0,1	20%	20%	50%		
	E.23 Errores de mantenimiento/ actualización de los programas (hardware).	0,1			100%		
	E.24 Caída del sistema por agotamiento de recursos	0,01			50%		
	E.25 Pérdida de equipos	0,01	100%		100%		
	A.7 Uso no previsto	1	100%	10%	100%		

Id. Activo	Id. Amenaza	Frecuencia	Impacto por dimensión				
			C	I	D	A	C
	A.11 Acceso no autorizado	0,01	20%	10%			
	A.23 Manipulación de los equipos.	0,01	20%		20%		
	A.24 Denegación de servicio.	0,01			100%		
	A.25 Robo	0,01	100%		100%		
	A.26 Ataque destructivo	0,1			100%		

[Alm] Disp.

Id. Activo	Id. Amenaza	Frecuencia	Impacto por dimensión				
			C	I	D	A	C
[Alm_cinta] [Alm_discos] [Alm_usb]	N.1 Fuego	0,01			100%		
	N.2 Daños por agua	0,01			100%		
	N.* Desastres naturales	0,01			100%		
	I1 Fuego	0,01			100%		
	I.2 Daños por agua	0,01			100%		
	I.* Desastres industriales	0,01			100%		
	I.5 Averías de origen físico o lógico	0,1			100%		
	I.10 Degradación de los soportes de almacenamiento de información	0,01			100%		
	E.15 Alteración accidental de información	0,1	50%				

Id. Activo	Id. Amenaza	Frecuencia	Impacto por dimensión				
			C	I	D	A	C
	E.18 Destrucción de la información	0,1	50%				
	E.19 Fugas de información	0,1	100%				
	E.23 Errores de mantenimiento/ actualización de los programas (hardware).	0,1			100%		
	E.25 Pérdida de equipos	0,1			100%		
	A.7 Uso no previsto	1	10%				
	A.11 Acceso no autorizado	0,1	10%				
	A.15 Modificación deliberada de información	0,01		20%			
	A.18 Destrucción de información	0,1		50%			
	A.19 Divulgación de información	0,1	100%				
	A.23 Manipulación de los equipos.	0,1		20%			
	A.25 Robo	0,1			100%		
	A.26 Ataque destructivo	0,01	50%		100%		

[Aux] Equipamiento auxiliar

Id. Activo	Id. Amenaza	Frecuencia	Impacto por dimensión				
			C	I	D	A	T
[Aux_cableado] [Aux_gabinete] [Aux_ups]	N.1 Fuego	0,01			100%		
	N.2 Daños por agua	0,01			100%		

Id. Activo	Id. Amenaza	Frecuencia	Impacto por dimensión				
			C	I	D	A	T
[Aux_ventilación]	N.* Desastres naturales	0,01			100%		
	I1 Fuego	0,01			100%		
	I.2 Daños por agua	0,01			100%		
	I.* Desastres industriales	0,01			100%		
	I.5 Averías de origen físico o lógico	1			100%		
	I.6 Corte del suministro eléctrico	0,1			100%		
	E.23 Errores de mantenimiento/ actualización de los programas (hardware).	1			50%		
	E.25 Pérdida de equipos	0,1			100%		
	A.7 Uso no previsto	0,01	10%	10%			
	A.11 Acceso no autorizado	0,01	50%	50%			
	A.23 Manipulación de los equipos.	0,01			100%		
	A.25 Robo	0,01			100%		
	A.26 Ataque destructivo	0,01			100%		

[Com] Redes de comunicaciones

Id. Activo	Id. Amenaza	Frecuencia	Impacto por dimensión				
			C	I	D	A	T
[Com_inalámbrica] [Com_internet] [Com_LAN] [Com_telefónica]	N.1 Fuego	0,01			100%		

Id. Activo	Id. Amenaza	Frecuencia	Impacto por dimensión				
			C	I	D	A	T
	N.2 Daños por agua	0,01			100%		
	N.* Desastres naturales	0,01			100%		
	I1 Fuego	0,01			100%		
	I.2 Daños por agua	0,01			100%		
	I.* Desastres industriales	0,01			100%		
	I.8 Fallos del servicio de comunicaciones	0,01			100%		
	E.2 Errores del administrador	0,1	10%	10%	50%		
	E.9 Errores de re-encaminamiento	0,1	10%				
	E.10 Errores de secuencia	0,01		10%			
	E.19 Fugas de información	0,01		20%			
	E.24 Caída del sistema por agotamiento de recursos	0,01			50%		
	A.5 Suplantación de la identidad del usuario	0,01				100%	
	A.6 Abuso de privilegios de acceso.	0,1	50%	10%	50%		
	A.7 Uso no previsto	1	10%	10%	10%		
	A.9 Re-encaminamiento de paquetes	0,01	10%				
	A.10 Alteración de la secuencia	0,01		10%			
	A.11 Acceso no autorizado	0,01	50%	10%			
	A.12 Análisis de tráfico	0,01	20%				

Id. Activo	Id. Amenaza	Frecuencia	Impacto por dimensión				
			C	I	D	A	T
	A.14 Interceptación de información (escucha)	0,01	20%				
	A.15 Modificación deliberada de información	0,01		20%			
	A.19 Divulgación de información	0,01	50%				
	A.24 Denegación de servicio.	0,1			50%		

[Inst] Instalaciones

Id. Activo	Id. Amenaza	Frecuencia	Impacto por dimensión				
			C	I	D	A	T
[Inst_oficina] [Inst_edificio]	N.1 Fuego	0,01			100%		
	N.2 Daños por agua	0,01			100%		
	N.* Desastres naturales	0,01			100%		
	I1 Fuego	0,01			100%		
	I.2 Daños por agua	0,01			100%		
	I.* Desastres industriales	0,01			100%		
	A.7 Uso no previsto	1	50%	50%	50%		
	A.11 Acceso no autorizado	0,1	50%	50%			
	A.15 Modificación deliberada de información	0,01		50%			
	A.19 Divulgación de información	0,01	50%				
	A.26 Ataque destructivo	0,01			100%		

Id. Activo	Id. Amenaza	Frecuencia	Impacto por dimensión				
			C	I	D	A	T
	A.27 Ocupación enemiga	0,01	50%		100%		

[P] Personas

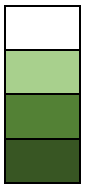
Id. Activo	Id. Amenaza	Frecuencia	Impacto por dimensión				
			C	I	D	A	T
[P_admred] [P_admserv] [P_admapl]	E.7 Deficiencias en la organización	0,01			20%		
	E.19 Fugas de información	0,01	20%				
	E.28 Indisponibilidad de personal	0,01			100%		
	A.28 Indisponibilidad de personal.	0,01			100%		
	A.29 Extorsión	0,01	20%	20%	20%		
	A.30 Ingeniería social	0,01	20%	20%	20%		
[P_softw] [P_soporte]	E.7 Deficiencias en la organización	0,01			20%		
	E.19 Fugas de información	0,01	20%				
	E.28 Indisponibilidad de personal	0,01			100%		
	A.28 Indisponibilidad de personal.	0,01			100%		
	A.29 Extorsión	0,01	20%	20%	20%		
	A.30 Ingeniería social	0,01	20%	20%	20%		
[P_vicerrector] [P_coord] [P_gestionh]	E.7 Deficiencias en la organización	0,1			20%		

Id. Activo	Id. Amenaza	Frecuencia	Impacto por dimensión				
			C	I	D	A	T
	E.19 Fugas de información	0,01	20%				
	E.28 Indisponibilidad de personal	0,01			100%		
	A.28 Indisponibilidad de personal.	0,01			100%		
	A.29 Extorsión	0,01	50%	20%	20%		
	A.30 Ingeniería social	0,1	20%	20%	20%		
[P_asistente] [P_docente]	E.7 Deficiencias en la organización	0,1			50%		
	E.19 Fugas de información	0,01	50%				
	E.28 Indisponibilidad de personal	0,01			100%		
	A.28 Indisponibilidad de personal.	0,01			100%		
	A.29 Extorsión	0,01	10%	10%	10%		
	A.30 Ingeniería social	0,1	10%	10%	10%		

5.4 Estimación del impacto potencial

De acuerdo con el análisis de riesgo desarrollado en el punto anterior, se necesita realizar el cálculo del impacto potencial de las amenazas sobre los activos. Para ello se utiliza el producto de la valoración del activo de acuerdo a cada dimensión de seguridad y el valor del impacto promedio de acuerdo a cada una de las amenazas. El resultado de este cálculo nos permite visualizar el valor de referencia para cada activo y a partir de allí calcular el riesgo aceptable y residual. El resultado detallado de este punto lo podemos encontrar en el ANEXO 9: CÁLCULO DEL IMPACTO POTENCIAL.

Se usarán los siguientes distintivos para visualizar la valoración de cada activo:



Bajo
Medio
Alto
Muy alto

Tabla 7. Valoración del riesgo

Los resultados por activo son los siguientes:

CAT.	ID. ACTIVO	VALOR	IMPACTO POTENCIAL (ImpC + ImpI + ImpD + ImpA + ImpD)
[I] Información	[I_estudiante]	Alto	19
	[I_PEI]	Medio	3
	[I_PEP]	Medio	3
	[I_notas]	Muy alto	20
	[I_aspirante]	Alto	17
	[I_desercion]	Medio	13
	[I_micros]	Medio	4
	[I_personal]	Muy alto	21
	[I_docente]	Muy alto	21
	[I_adm]	Muy alto	21
	[I_estudianteper]	Muy alto	21
[S] Servicios	[SI_internet]	Alto	20
	[SI_www_aulas]	Alto	13
	[SI_www_atenea]	Alto	13
	[SI_correo]	Muy alto	18
	[SI_www_]	Alto	18
[D] Datos	[D_config]	Muy alto	27

CAT.	ID. ACTIVO	VALOR	IMPACTO POTENCIAL (ImpC + ImpI + ImpD + ImpA + ImpD)
	[D_backups]	Alto	18
	[D_pass]	Alto	7
	[D_acl]	Medio	14
	[D_log]	Medio	10
[Soft] Software	[Soft_SISTENOTAS]	Muy alto	39
	[Soft_Moodle]	Alto	33
	[Soft_people]	Muy alto	35
	[Soft_glpi]	Alto	24
	[Soft_nomina]	Muy alto	37
	[Soft_antivirus]	Muy alto	36
	[Soft_pm]	Alto	26
	[Soft_so]	Muy alto	37
	[Soft_office]	Medio	19
	[Soft_navegador]	Medio	16
	[Soft_correo]	Medio	20
	[Soft_autocad]	Medio	19
[Hard] Hardware	[Hard_ap]	Alto	8
	[Hard_firewall]	Alto	8
	[Hard_impresora]	Medio	3
	[Hard_pbx]	Medio	9
	[Hard_pc]	Alto	7
	[Hard_portatil]	Medio	6
	[Hard_router]	Alto	9
	[Hard_scanner]	Medio	5
	[Hard_servidor]	Muy alto	10
	[Hard_switch]	Medio	4
[Alm] Disp. de alm.	[Alm_cinta]	Alto	8

CAT.	ID. ACTIVO	VALOR	IMPACTO POTENCIAL (ImpC + ImpI + ImpD + ImpA + ImpD)
	[Alm_discos]	Alto	8
	[Alm_usb]	Alto	8
[Aux] Equipamiento auxiliar	[Aux_cableado]	Muy alto	9
	[Aux_gabinete]	Muy alto	9
	[Aux_ups]	Alto	8
	[Aux_ventilación]	Muy alto	9
[Com] Redes de comunicaciones	[Com_inalámbrica]	Alto	19
	[Com_internet]	Muy alto	24
	[Com_LAN]	Alto	22
	[Com_telefónica] Red telefónica	Medio	13
[Inst] Instalaciones	[Inst_oficina]	Medio	13
	[Inst_edificio]	Medio	9
[P] Personas	[P_admred]	Ext alto	10
	[P_admserv]	Ext alto	10
	[P_admapl]	Muy alto	9
	[P_softw]	Medio	4
	[P_soporte]	Alto	6
	[P_vicerrector]	Medio	4
	[P_coord]	Medio	4
	[P_asistente]	Medio	3
	[P_gestionh]	Alto	6
	[P_docente]	Medio	5

Tabla 8. Impacto potencial total por activo

El resultado de la tabla de impacto potencial será tomado en cuenta para decidir las acciones a plantear y de manera priorizada, decidir su ejecución.

5.5 Nivel de riesgo aceptable y residual

Para finalizar esta fase, se hace necesario realizar los cálculos referentes al riesgo aceptable y riesgo residual. El riesgo será tomado como el producto de la frecuencia calculada en el numeral *[5.2.2. Valoración de las amenazas*] con el impacto potencial calculado en el numeral anterior.

Los valores de riesgo a consideran se resaltarán de acuerdo a la siguiente tabla:

		RANGO	RIESGO POTENCIAL
		<10	Riesgo aceptable
		10-50	Riesgo moderado
		>50	Riesgo a importante e intolerable

Tabla 9. Nivel de riesgo potencial

Los resultados se han sintetizado en la siguiente tabla:

CAT.	ID. ACTIVO	VALOR	IMPACTO POTENCIAL					FRECUENCIA	RIESGO				
			C	I	D	A	T		C	I	D	A	T
[I] Información	[I_estudiante]	Alto	6,8	9	3,5	0	0	10	68	90	35	0	0
	[I_PEI]	Medio	0,3	2	0,9	0	0	1	0,3	2	0,9	0	0
	[I_PEP]	Medio	0,3	2	0,9	0	0	1	0,3	2	0,9	0	0
	[I_notas]	Muy alto	7,5	9	3,5	0	0	10	75	90	35	0	0
	[I_aspirante]	Alto	6	7	3,5	0	0	10	60	70	35	0	0
	[I_desercion]	Medio	4,5	4	4	0	0	10	45	40	40	0	0
	[I_micros]	Medio	0,5	3	0,9	0	0	1	0,5	3	0,9	0	0
	[I_personal]	Muy alto	6,8	9	5	0	0	10	68	90	50	0	0
	[I_docente]	Muy alto	6,8	9	5	0	0	10	68	90	50	0	0
	[I_adm]	Muy alto	6,8	9	5	0	0	10	68	90	50	0	0
	[I_estudianteper]	Muy alto	6,8	9	5	0	0	10	68	90	50	0	0

CAT.	ID. ACTIVO	VALOR	IMPACTO POTENCIAL					FRECUENCIA	RIESGO				
			C	I	D	A	T		C	I	D	A	T
[S] Servicios	[SI_internet]	Alto	3,5	1,6	10	5	0	0,1	0,4	0,2	1	0,5	0
	[SI_www_aulas]	Alto	1,4	1,6	7	2,5	0	1	1,4	1,6	7	2,5	0
	[SI_www_atenea]	Alto	1,4	1,6	7	2,5	0	1	1,4	1,6	7	2,5	0
	[SI_correo]	Muy alto	2	1,8	10	4,5	0	1	2	1,8	10	4,5	0
	[SI_www_]	Alto	1,4	1,6	10	4,5	0	1	1,4	1,6	10	4,5	0
[D] Datos	[D_config]	Muy alto	9	4,5	4,5	9	0	10	90	45	45	90	0
	[D_backups]	Alto	3	4	3	8	0	10	30	40	30	80	0
	[D_pass]	Alto	5	0	0	2	0	10	50	0	0	20	0
	[D_acl]	Medio	5	2	2	5	0	10	50	20	20	50	0
	[D_log]	Medio	5	1	2,5	1	0	10	50	10	25	10	0
[Soft] Software	[Soft_SISTENOTAS]	Muy alto	10	10	10	9	0	10	100	100	100	90	0
	[Soft_Moodle]	Alto	8	8	9	8	0	10	80	80	90	80	0
	[Soft_people]	Muy alto	9	7	10	9	0	10	90	70	100	90	0
	[Soft_glpi]	Alto	5	2	8	9	0	10	50	20	80	90	0
	[Soft_nomina]	Muy alto	10	8	10	9	0	10	100	80	100	90	0
	[Soft_antivirus]	Muy alto	9	9	9	9	0	10	90	90	90	90	0
	[Soft_pm]	Alto	6	5	10	5	0	10	60	50	100	50	0
	[Soft_so]	Muy alto	9	9	10	9	0	10	90	90	100	90	0
	[Soft_office]	Medio	5	5	4	5	0	10	50	50	40	50	0
	[Soft_navegador]	Medio	4	4	4	4	0	10	40	40	40	40	0
	[Soft_correo]	Medio	9	2	5	4	0	10	90	20	50	40	0
	[Soft_autocad]	Medio	4	5	5	5	0	10	40	50	50	50	0

CAT.	ID. ACTIVO	VALOR	IMPACTO POTENCIAL					FRECUENCIA	RIESGO				
			C	I	D	A	T		C	I	D	A	T
[Hard] Hardware	[Hard_ap]	Alto	0	0	8	0	0	0,1	0	0	0,8	0	0
	[Hard_firewall]	Alto	0	0	8	0	0	0,1	0	0	0,8	0	0
	[Hard_impresora]	Medio	0	0	3	0	0	0,1	0	0	0,3	0	0
	[Hard_pbx]	Medio	0	0	9	0	0	0,1	0	0	0,9	0	0
	[Hard_pc]	Alto	0	0	7	0	0	0,1	0	0	0,7	0	0
	[Hard_portatil]	Medio	0	0	6	0	0	0,1	0	0	0,6	0	0
	[Hard_router]	Alto	0	0	9	0	0	0,1	0	0	0,9	0	0
	[Hard_scanner]	Medio	0	0	5	0	0	0,1	0	0	0,5	0	0
	[Hard_servidor]	Muy alto	0	0	10	0	0	0,1	0	0	1	0	0
	[Hard_switch]	Medio	0	0	4	0	0	0,1	0	0	0,4	0	0
[Alm] Disp. de alm.	[Alm_cinta]	Alto	0	0	8	0	0	1	0	0	8	0	0
	[Alm_discos]	Alto	0	0	8	0	0	1	0	0	8	0	0
	[Alm_usb]	Alto	0	0	8	0	0	1	0	0	8	0	0
[Aux] Equipamiento auxiliar	[Aux_cableado]	Muy alto	0	0	9	0	0	1	0	0	9	0	0
	[Aux_gabinete]	Muy alto	0	0	9	0	0	1	0	0	9	0	0
	[Aux_ups]	Alto	0	0	8	0	0	1	0	0	8	0	0
	[Aux_ventilación]	Muy alto	0	0	9	0	0	1	0	0	9	0	0
[Com] Redes de comunicacion	[Com_inalámbrica]	Alto	3,5	1,8	7	7	0	1	3,5	1,8	7	7	0
	[Com_internet]	Muy alto	4,5	1,8	9	9	0	1	4,5	1,8	9	9	0
	[Com_LAN]	Alto	5	1,6	10	5	0	1	5	1,6	10	5	0
	[Com_telefónica] Red telefónica	Medio	1,5	0,2	6	5	0	1	1,5	0,2	6	5	0
[Inst] Instala	[Inst_oficina]	Medio	3,5	0	9	0	0	1	3,5	0	9	0	0
	[Inst_edificio]	Medio	2	0	7	0	0	1	2	0	7	0	0
[P] Personas	[P_admred]	Ext alto	0	0	10	0	0	0,01	0	0	0,1	0	0
	[P_admserv]	Ext alto	0	0	10	0	0	0,01	0	0	0,1	0	0
	[P_admapl]	Muy alto	0	0	9	0	0	0,01	0	0	0,1	0	0
	[P_softw]	Medio	0	0	4	0	0	0,01	0	0	0	0	0

CAT.	ID. ACTIVO	VALOR	IMPACTO POTENCIAL					FRECUENCIA	RIESGO				
			C	I	D	A	T		C	I	D	A	T
	[P_soporte]	Alto	0	0	6	0	0	0,01	0	0	0,1	0	0
	[P_vicerrector]	Medio	0	0	4	0	0	0,1	0	0	0,4	0	0
	[P_coord]	Medio	0	0	4	0	0	0,1	0	0	0,4	0	0
	[P_asistente]	Medio	0	0	3	0	0	0,1	0	0	0,3	0	0
	[P_gestionh]	Alto	0	0	6	0	0	0,1	0	0	0,6	0	0
	[P_docente]	Medio	0	0	5	0	0	0,1	0	0	0,5	0	0

Tabla 10. Valoración del riesgo para los activos del sistema.

5.6 Riesgo aceptable y residual

El Comité de Seguridad de la información de la Universidad, ha decidido que el riesgo aceptado pertenezca al rango [0,50], es decir, que cualquier valoración que sea mayor o igual a 50 en cualquiera de las dimensiones de seguridad, será evaluado para considerar acciones de mitigación del riesgo, a corto plazo y un riesgo inferior a esa cifra será aceptado.

Cuando el riesgo esté entre 10 y 50, se revisará la posibilidad de integrar entre las acciones de mitigación del riesgo y puesta en marcha de controles, a mediano plazo.

De acuerdo a los resultados obtenidos de la tabla 9, se puede deducir que las dos categorías de activos con mayor riesgo corresponden a la Información esencial y al software (sistemas de información) y a partir de estas dos categorías se orientarán la fase siguiente: mejoras propuestas para mitigación del riesgo.

6. PROPUESTA DE PROYECTOS

De acuerdo a los resultados del análisis diferencial realizado en el capítulo 2 y los resultados del plan de tratamiento de riesgos del capítulo 5, en este capítulo se proponen un conjunto de proyectos para poder mejorar el estado de seguridad de la información en una universidad colombiana.

Por otra parte es necesario, además de contar con la aprobación por parte del Consejo Superior Universitario de la Política General de Seguridad de la Información, de la nueva estructuración de roles y responsabilidades en materia de seguridad de la información y la contratación del Responsable de Seguridad de la información y la adopción de los indicadores propuestos, la creación y aprobación de nuevos procedimientos y actividades que también se proponen en este capítulo.

6.1 Proyectos propuestos

En la siguiente tabla se enumeran las propuestas de proyectos a ejecutar, así como el control al cual soportan y su impacto en la mitigación de los riesgos contemplados en el capítulo anterior:

	PROYECTO	DOMINIO / CONTROL SGSI	RIESGO A MITIGAR
6.1.1	Plan de capacitación sobre SGSI a distintos estamentos que tratan la información.	7.2, A.9.2, A11.2.8, A11.2.9, A43.2.4, A16.1.2, A16.1.3, A16.1.6, A18.1.4, A18.2.2	E.1, E.7, E.19, A.15, A.30
6.1.2	Organización de la Dirección de TICS.	5.3, 7.2, A6.1.1, A6.1.2, A7.2.2	E.2, E.7, E.28
6.1.3	Cifrado de discos duros de dispositivos móviles (portátiles, tablets y móviles) de personal que maneje información sensible.	8.3, A6.2.1, A11.2.6	E18, E.19, A4, A.19, A.29

	PROYECTO	DOMINIO / CONTROL SGSI	RIESGO A MITIGAR
6.1.4	Plan de Continuidad del Negocio y Recuperación de desastres	A12.3, A.17.1.1, A17.1.2, A17.1.3	N.1, N.2, N.*, I.2, I.*, I.8, I.10
6.1.5	Selección adquisición e implementación de un sistema gestor de eventos y seguridad de la información (SIEM)	A16.1	E.2, E.3, E.4, E.20, A.3, A.5, A.6, A.7, A.8, A.11, A.12, A.14, A.24
6.1.6	Selección adquisición e implementación de un software de gestión de inventarios.	A8.1, A8.3, A11.2.5, A11.2.6 A11.2.7	A.18, A.19, E.25
6.1.7	Selección adquisición e implementación de un sistema de prevención y detección de intrusos (IDS e IPS) para la red de datos de la Universidad sede Bogotá.	A16.1, A12.2.1	A.3, A.5, A.6, A.7, A.8, A.11, A.12, A.14, A.24
6.1.8	Selección adquisición e implementación de un sistema de detección de vulnerabilidades.	A16.1	E.20
6.1.9	Parametrización del sistema de helpdesk para que incluya la gestión de incidentes.	A16.1	
6.1.10	Selección adquisición e implementación de un DLP (Data Loss Prevention).	A18.1.2, A18.1.3, A18.1.4	A.18, A.19, A.30
6.1.11	Plan de auditorías al SGSI de la Universidad.	9.2, A18.1.2, A18.2.2, A18.2.3	
6.1.12	Compra de memorias USB cifradas para uso en datacenters y dependencias que manejan información sensible.	8.3, A6.2.1, A11.2.6	A.18, A.19, A.30
6.1.13	Implementación de un mecanismo de autenticación	A11.1	A.11

	PROYECTO	DOMINIO / CONTROL SGSI	RIESGO A MITIGAR
	de dos factores para el ingreso al Datacenter de la Universidad.		
6.1.14	Hardening de servidores de una universidad colombiana.	A11.5	A.18, A.19

Tabla 11. Proyectos propuestos y su impacto en ISO 27001:2013 y Matriz de riesgos a mitigar

Para desarrollar los proyectos relacionados con sistemas de información o software nuevo, se trabajará una metodología con las siguientes fases:

1. Investigación del mercado y selección de soluciones para el proyecto
2. Pruebas de concepto de cada una de las selecciones consideradas.
3. Selección de unas métricas para la toma de decisión de la mejor solución o herramienta de software más ajustada a las necesidades del SGSI de la Universidad.
4. Selección de la solución de acuerdo a la valoración, de acuerdo a cada una de las métricas.
5. Adquisición de la solución, con las condiciones evaluadas.
6. Implementación de la solución
7. Pruebas de la solución
8. Puesta en producción

Adicionalmente a las soluciones resultado de los proyectos mencionados, es necesario el estudio, aprobación y puesta en marcha de los siguientes procedimientos:

	PROCEDIMIENTO	DOMINIO / CONTROL SGSI
6.2.1	Procedimiento de borrado seguro para equipos que son cambiados de dependencia y/o son dados de baja	A11.2.7
6.2.2	Procedimiento para el manejo de controles criptográficos	10.1.1
6.2.3	Procedimiento de gestión de incidentes de seguridad de la información	6.1.3, A16.1
6.2.5	Procedimiento para la ubicación y configuración de alarmas para gestión	A12.1.3

	PROCEDIMIENTO	DOMINIO / CONTROL SGSI
	de la capacidad de los equipos servidores y de comunicaciones de la Universidad.	
6.2.6	Procedimiento de revisión de políticas de seguridad	9.3, A18.2, A18.2.3
6.2.7	Procedimiento de tratamiento de no conformidades en materia de seguridad de la información.	10.1
6.2.8	Procedimiento de revisión del estado del SGSI.	10.2, A18.2.2

Tabla 12. Procedimientos nuevos a elaborar para soportar el SGSI de la Universidad

Por otra parte, es necesario realizar cambios en las normativas vigentes para incluir numerales correspondientes a la seguridad de la información, tales como inclusión de funciones en materia de seguridad de la información, procesos disciplinarios y sanciones para los distintos estamentos:

NORMATIVA A MODIFICAR/CREAR	DOMINIIO / CONTROL SGSI
Reglamento de trabajo	5.3, 7.2, 7.3
Manual de convivencia de los estudiantes.	
Estatuto docente	

Tabla 13. Reglamentos a modificar para cumplimiento del SGSI.

6.1.1 Plan de capacitación sobre SGSI a distintos estamentos que tratan la información

OBJETIVO	
- Mejorar las competencias de los responsables de tratamiento de la información en una universidad colombiana, respecto a la confidencialidad, integridad y disponibilidad de la misma y los riesgos que corre dicha información.	
ALCANCE	
Empleados administrativos, docentes y estudiantes de una universidad colombiana, sede Bogotá.	
RESPONSABLE	**ÁREAS INVOLUCRADAS**
Oficial de seguridad de la información	Todos los estamentos
COSTO APROXIMADO	$20'000.000

PLAZO DE CONSECUCIÓN	Corto plazo
TIEMPO ESTIMADO DE EJECUCIÓN	6 meses
ACTIVIDADES	
- Elaboración de un plan de capacitación. - Estudio de hojas de vida de capacitadores - Aprobación de recursos y actividades de formación - Ejecución del plan de formación - Evaluación de las actividades de capacitación por parte de los participantes.	

6.1.2 Reorganización de la Dirección de TICS.

OBJETIVO	
Gestionar de una forma adecuada la seguridad de la información según el cargo y de acuerdo a los roles caracterizados y a las nuevas funciones resultantes de los nuevos proyectos y la puesta en marcha del SGSI.	
ALCANCE	
La reorganización abSISTENOTAS únicamente la Dirección de TICS.	
RESPONSABLE	**ÁREAS INVOLUCRADAS**
Director de TICs	Dirección de TICS
COSTO APROXIMADO	$100.000.000 anuales
PLAZO DE CONSECUCIÓN	Corto plazo
TIEMPO ESTIMADO DE EJECUCIÓN	3 meses
ACTIVIDADES	
- Revisión del manual de funciones de cada uno de los profesionales contratados actualmente. - Revisión de las nuevas funciones de seguridad de la información para la dirección y los nuevos roles de acuerdo al desarrollo de los proyectos propuestos. - Identificación de los nuevos cargos a cubrir, para solicitud al Consejo Superior Universitario. - Caracterización de los cargos nuevos y actuales y reestructuración del manual de funciones. - Contratación del personal nuevo. - Entrenamiento del personal nuevo.	

6.1.3 Cifrado de discos duros de dispositivos móviles (portátiles, tablets y móviles) de personal que maneje información sensible.

OBJETIVO	
Proteger la información almacenada en dispositivos móviles de ataques contra la confidencialidad e integridad y secuestro de información.	
ALCANCE	
Equipos móviles (portátiles, tables, celulares) de los miembros del Consejo Superior Universitario, Vicerrectores y Jefes de área que manejen información sensible.	
RESPONSABLE	**ÁREAS INVOLUCRADAS**
Director de TIC	Dirección de TICS
COSTO APROXIMADO	$5.000.000
PLAZO DE CONSECUCIÓN	Mediano plazo
TIEMPO ESTIMADO DE EJECUCIÓN	2 meses
ACTIVIDADES	
- Evaluación de los dispositivos móviles cuyo dispositivo de almacenamiento amerita ser cifrado. - Realización del proceso de cifrado. - Capacitación al personal que usará dichos equipos.	

6.1.4 Plan de Continuidad del Negocio y Recuperación de desastres.

OBJETIVO	
Evitar la interrupción de los servicios de misión crítica y restablecer el pleno funcionamiento en el menor tiempo posible	
ALCANCE	
Sistemas de información: SISTENOTAS y financiero	
RESPONSABLE	**ÁREAS INVOLUCRADAS**
Vicerrector Administrativo	Todas
COSTO APROXIMADO	$50.000.000
PLAZO DE CONSECUCIÓN	Mediano plazo
TIEMPO ESTIMADO DE EJECUCIÓN	Un año
FASES	
- Identificación y priorización de las amenazas. - Análisis de impacto en la Universidad.	

- Creación del plan de respuesta y recuperación. - Adecuación de la solución. - Pruebas. - Refinamiento del plan de continuidad.

6.1.5 Selección adquisición e implementación de un sistema gestor de eventos y seguridad de la información (SIEM).

OBJETIVO	
Soportar el proceso de gestión de incidentes de seguridad para una universidad colombiana, sede Bogotá.	
ALCANCE	
Sede Bogotá	
RESPONSABLE	**ÁREAS INVOLUCRADAS**
Director de TICS	Dirección de TICS Vicerrectoría Administrativa
COSTO APROXIMADO	$20.000.000
PLAZO DE CONSECUCIÓN	Mediano plazo
TIEMPO ESTIMADO DE EJECUCIÓN	6 meses
FASES	
- Investigación del mercado y selección de soluciones para el proyecto - Pruebas de concepto de cada una de las selecciones consideradas. - Selección de unas métricas para la toma de decisión de la mejor solución o herramienta de software más ajustada a las necesidades del SGSI de la Universidad. - Selección de la solución de acuerdo a la valoración, de acuerdo a cada una de las métricas. - Adquisición de la solución, con las condiciones evaluadas. - Implementación de la solución - Pruebas de la solución - Puesta en producción	

6.1.6 Selección adquisición e implementación de un software de gestión de inventarios.

OBJETIVO	
Soportar las actividades de gestión de activos físicos en la Universidad ECCI.	
ALCANCE	
Sede Bogotá	
RESPONSABLE	**ÁREAS INVOLUCRADAS**
Vicerrector Administrativo	Inventarios
COSTO APROXIMADO	$35.000.000
PLAZO DE CONSECUCIÓN	Corto plazo
TIEMPO ESTIMADO DE EJECUCIÓN	6 meses
FASES	
- Investigación del mercado y selección de soluciones para el proyecto - Pruebas de concepto de cada una de las selecciones consideradas. - Selección de unas métricas para la toma de decisión de la mejor solución o herramienta de software más ajustada a las necesidades del SGSI de la Universidad. - Selección de la solución de acuerdo a la valoración, de acuerdo a cada una de las métricas. - Adquisición de la solución, con las condiciones evaluadas. - Implementación de la solución - Pruebas de la solución - Puesta en producción	

6.1.7 Selección adquisición e implementación de un sistema de prevención y detección de intrusos (IDS e IPS) para la red de datos de la Universidad sede Bogotá.

OBJETIVO	
Detectar las actividades anormales, que puedan evidenciar la explotación de alguna vulnerabilidad de la infraestructura de red o la materialización de un riesgo de un activo.	
ALCANCE	
Sede Bogotá	
RESPONSABLE	**ÁREAS INVOLUCRADAS**

Director de TICs	Dirección de TICs
COSTO APROXIMADO	$30.000.000
PLAZO DE CONSECUCIÓN	Largo plazo
TIEMPO ESTIMADO DE EJECUCIÓN	6 meses
FASES	
- Investigación del mercado y selección de soluciones para el proyecto - Pruebas de concepto de cada una de las selecciones consideradas. - Selección de unas métricas para la toma de decisión de la mejor solución o herramienta de software más ajustada a las necesidades del SGSI de la Universidad. - Selección de la solución de acuerdo a la valoración, de acuerdo a cada una de las métricas. - Adquisición de la solución, con las condiciones evaluadas. - Implementación de la solución - Pruebas de la solución - Puesta en producción	

6.1.8 Selección adquisición e implementación de un sistema de detección de vulnerabilidades para la red de datos de la Universidad sede Bogotá.

OBJETIVO	
Detectar las vulnerabilidades de sistemas, software, redes y servicios y realizar actividades de pentesting al momento de implementar soluciones nuevas para el manejo de información.	
ALCANCE	
Sede Bogotá	
RESPONSABLE	**ÁREAS INVOLUCRADAS**
Director de TICs	Dirección de TICs
COSTO APROXIMADO	$15.000.000
PLAZO DE CONSECUCIÓN	Mediano plazo
TIEMPO ESTIMADO DE EJECUCIÓN	6 meses
FASES	
- Investigación del mercado y selección de soluciones para el proyecto - Pruebas de concepto de cada una de las selecciones consideradas.	

- Selección de unas métricas para la toma de decisión de la mejor solución o herramienta de software más ajustada a las necesidades del SGSI de la Universidad.
- Selección de la solución de acuerdo a la valoración, de acuerdo a cada una de las métricas.
- Adquisición de la solución, con las condiciones evaluadas.
- Implementación de la solución
- Pruebas de la solución
- Puesta en producción

6.1.9 Parametrización del sistema de helpdesk para que incluya la gestión de incidentes.

OBJETIVO	
Realizar la gestión de incidentes haciendo uso de la plataforma GLPI implementada para soporte técnico.	
ALCANCE	
Sede Bogotá	
RESPONSABLE	**ÁREAS INVOLUCRADAS**
Director de TICS	Dirección de TICs
COSTO APROXIMADO	$1.000.000
PLAZO DE CONSECUCIÓN	Mediano plazo
TIEMPO ESTIMADO DE EJECUCIÓN	2 meses
ACTIVIDARES	
- Revisión de requerimientos para la gestión de incidentes. - Adecuación de los requerimientos y activación de módulos que soporten dichos requerimientos. - Implementación de la solución - Pruebas de la solución - Puesta en producción	

6.1.10 Selección adquisición e implementación de un DLP (Data Loss Prevention).

OBJETIVO	
Disminuir los riesgos asociados con fuga de información sensible y confidencial de la Universidad.	
ALCANCE	
Sede Bogotá	
RESPONSABLE	**ÁREAS INVOLUCRADAS**
Director de TICs	Dirección de TICs
COSTO APROXIMADO	$15.000.000
PLAZO DE CONSECUCIÓN	Largo plazo
TIEMPO ESTIMADO DE EJECUCIÓN	6 meses
FASES	
- Investigación del mercado y selección de soluciones para el proyecto - Pruebas de concepto de cada una de las selecciones consideradas. - Selección de unas métricas para la toma de decisión de la mejor solución o herramienta de software más ajustada a las necesidades del SGSI de la Universidad. - Selección de la solución de acuerdo a la valoración, de acuerdo a cada una de las métricas. - Adquisición de la solución, con las condiciones evaluadas. - Implementación de la solución - Pruebas de la solución - Puesta en producción	

6.1.11 Plan de auditorías al SGSI de la Universidad.

OBJETIVO	
Realizar el seguimiento al Sistema de Gestión de Seguridad de la Información de una universidad colombiana para garantizar el cumplimiento de la norma ISO27001:2013 y la legislación colombiana vigente aplicable,	
ALCANCE	
Sede Bogotá	
RESPONSABLE	**ÁREAS INVOLUCRADAS**
Comité de la Seguridad de la Información	Todas las áreas de la sede Bogotá

COSTO APROXIMADO	$400.000
PLAZO DE CONSECUCIÓN	Corto plazo
TIEMPO ESTIMADO DE EJECUCIÓN	1 año
ACTIVIDADES	
- Formación de personal auditor interno en la norma ISO 27001:2013 - Planeación del plan de auditorías para 2018. - Realización de la auditoría previa a la visita del certificador - Planteamiento de acciones de mejora - Revisión del cumplimiento de las No conformidades por parte del Consejo Superior Universitario - Selección de la entidad certificadora ISO 27001:2013. - Contratación de la empresa certificadora. - Realización de la auditoría de certificación ISO 27001:2013 - Revisión de no conformidades y Planteamiento de acciones de mejora - Revisión del cumplimiento de las No conformidades por parte del Consejo Superior Universitario	

6.1.12 Compra de memorias USB cifradas para uso en datacenters y dependencias que manejan información sensible.

OBJETIVO	
Mitigar el riesgo de pérdida de dispositivos de almacenamiento externo con información sensible o información de carácter personal, para cumplir con la Ley de Protección de datos personales.	
ALCANCE	
Sede Bogotá	
RESPONSABLE	**ÁREAS INVOLUCRADAS**
Director de TICs	Áreas que manejan información sensible
COSTO APROXIMADO	$2.000.000
PLAZO DE CONSECUCIÓN	Largo plazo
TIEMPO ESTIMADO DE EJECUCIÓN	2 meses
ACTIVIDADES	
- Investigación del mercado y selección de soluciones para el proyecto - Pruebas de concepto de cada una de las selecciones consideradas.	

- Selección de unas métricas para la toma de decisión de la mejor solución o herramienta de software más ajustada a las necesidades del SGSI de la Universidad. - Selección de la solución de acuerdo a la valoración, de acuerdo a cada una de las métricas. - Adquisición de la solución, con las condiciones evaluadas. - Implementación de la solución - Pruebas de la solución - Puesta en producción

6.1.13 Implementación de un mecanismo de autenticación de dos factores para el ingreso al Datacenter de la Universidad.

OBJETIVO	
Mejorar los mecanismos de acceso al Datacenter de la Universidad, para evitar la presencia de personal no autorizado en las instalaciones.	
ALCANCE	
Sede Bogotá	
RESPONSABLE	**ÁREAS INVOLUCRADAS**
Director de TICs	Áreas que manejan información sensible
COSTO APROXIMADO	$20.000.000
PLAZO DE CONSECUCIÓN	Largo plazo
TIEMPO ESTIMADO DE EJECUCIÓN	6 meses
ACTIVIDADES	
- Cotización de las memorias extraíbles. - Selección del mejor proponente. - Compra de las memorias. - Entrega a las áreas seleccionadas. - Capacitación sobre su uso.	

6.1.14 Hardening de servidores de una universidad colombiana.

OBJETIVO	
Mitigar el riesgo relacionado por errores en las configuraciones, instalaciones por defecto, puertos abierto innecesarios, mal uso de mecanismos de autenticación y vulnerables de los sistemas operativos, servicios y protocolos.	
ALCANCE	
Sede Bogotá	
RESPONSABLE	**ÁREAS INVOLUCRADAS**
Director de TICs	Áreas que manejan información sensible
COSTO APROXIMADO	$20.000.000
PLAZO DE CONSECUCIÓN	Mediano plazo
TIEMPO ESTIMADO DE EJECUCIÓN	6 meses
ACTIVIDADES	
- Desarrollar cronograma de actividades de hardening. - Realización de dichas actividades - Pruebas.	

Sintetizando la información, se proponen 3 proyectos a corto plazo, 7 proyectos a mediano plazo y cuatro proyectos a largo plazo, de los cuales se proyectan los siguientes costos de inversión por parte de la Universidad.

	PROYECTO	PLAZO CONSECU-CIÓN	TIEMPO ESTIMA-DO	COSTO (pesos)	
6.1.1	Plan de capacitación sobre SGSI a distintos estamentos que tratan la información.	CORTO	6 meses	$20.000.000	
6.1.2	Organización de la Dirección de TICS.	CORTO	3 meses	$100.000.000	
6.1.11	Plan de auditorías al SGSI de la Universidad.	CORTO	1 año	$400.000	
COSTOS ESTIMADOS CORTO PLAZO					**$120.400.000**
6.1.3	Cifrado de discos duros de dispositivos móviles (portátiles, tablets y móviles) de personal que maneje información sensible.	MEDIANO	2 meses	$5.000.000	

	PROYECTO	PLAZO CONSECU-CIÓN	TIEMPO ESTIMA-DO	COSTO (pesos)	
6.1.4	Plan de Continuidad del Negocio y Recuperación de desastres	MEDIANO	1 año	$50.000.000	
6.1.5	Selección adquisición e implementación de un sistema gestor de eventos y seguridad de la información (SIEM)	MEDIANO	6 meses	$20.000.000	
6.1.6	Selección adquisición e implementación de un software de gestión de inventarios.	MEDIANO	6 meses	$35.000.000	
6.1.8	Selección adquisición e implementación de un sistema de detección de vulnerabilidades.	MEDIANO	6 meses	$15.000.000	
6.1.9	Parametrización del sistema de helpdesk para que incluya la gestión de incidentes.	MEDIANO	2 meses	$1.000.000	
6.1.14	Hardening de servidores de una universidad colombiana.	MEDIANO	4 meses	$20.000.000	
COSTOS ESTIMADOS MEDIANO PLAZO					**$146.000.000**
6.1.7	Selección adquisición e implementación de un sistema de prevención y detección de intrusos (IDS e IPS) para la red de datos de la Universidad sede Bogotá.	LARGO	6 meses	$30.000.000	
6.1.10	Selección adquisición e implementación de un DLP (Data Loss Prevention).	LARGO	6 meses	$15.000.000	
6.1.12	Compra de memorias USB cifradas para uso en datacenters y dependencias que manejan información sensible.	LARGO	2 meses	$2.000.000	
6.1.13	Implementación de un mecanismo de autenticación de dos factores para el ingreso al Datacenter de la Universidad.	LARGO	6 meses	$20.000.000	
COSTOS ESTIMADOS LARGO PLAZO					**$67.000.000**
COSTOS TOTALES ESTIMADOS DE PROYECTOS					**$333.400.000**

Tabla 14. Proyectos propuestos, plazos de consecución, tiempo estimado de ejecución y costos proyectados.

En la siguiente página se visualiza el diagrama de Gannt de los proyectos propuestos:

Nombre de tarea	Duración	Comienzo	Fin	Pre	Nombres de los recursos	Costo
PROYECTOS A CORTO PLAZO	**131 días**	**sáb 01/07/17**	**lun 01/01**			**$ 120.400.000**
6.1.1 Plan de capacitación sobre SGSI a distintos estamentos que tratan la información	6 mss	sáb 01/07/17	jue 14/12/17		Oficial de Seguridad de la información	$ 20.000.000
6.1.2 Reorganización de la Dirección de TICS.	3 mss	sáb 01/07/17	jue 21/09/17		Director TIC	$ 100.000.000
6.1.11 Plan de auditorías al SGSI de la Universidad.	*1 año*	lun 01/01/18			COmité de Seguridad de la Información	$ 400.000
MEDIANO PLAZO	**420 días**	**vie 01/09/17**	**jue 11/04**			**$ 146.000.000**
6.1.3 Cifrado de discos duros de dispositivos móviles (portátiles, tablets y móviles) de personal que maneje información sensible.	2 mss	vie 01/09/17	jue 26/10/17		Director TIC	$ 5.000.000
6.1.4 Plan de Continuidad del Negocio y Recuperación de desastres.	*1 año*	lun 01/01/18			Vicerrector Administrativo	$ 50.000.000
6.1.5 Selección adquisición e implementación de un sistema gestor de eventos y seguridad de la información (SIEM).	6 mss	sáb 27/10/18	jue 11/04/19	6	Director TIC	$ 20.000.000
6.1.6 Selección adquisición e implementación de un software	6 mss	jue 16/08/18	mié 30/01/19	8	Vicerrector Administrativo	$ 35.000.000

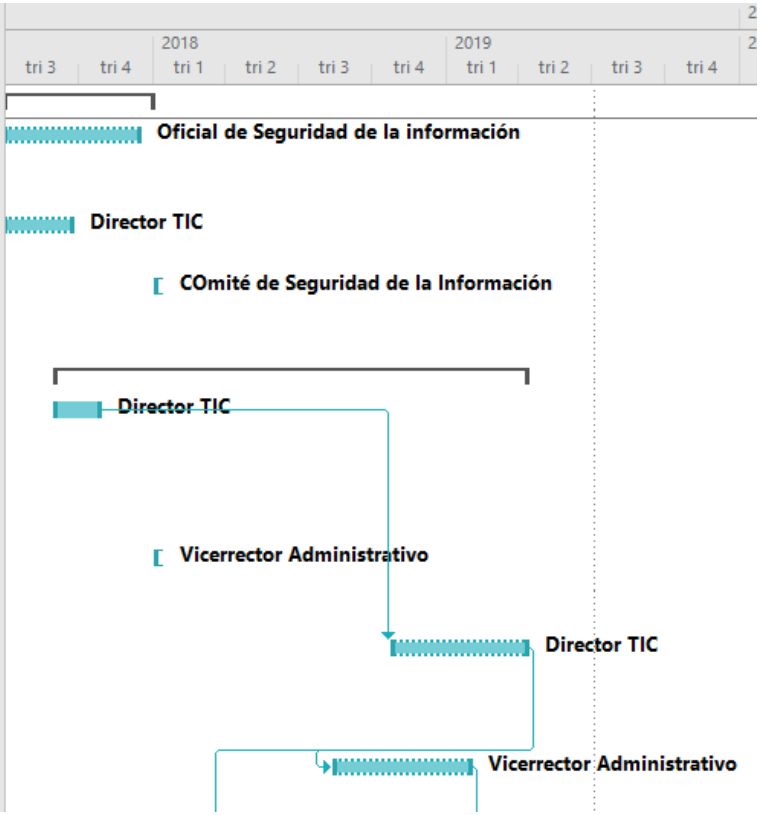


Tabla 15. Diagrama de Gannt Proyectos a corto y mediano plazo

Nombre de tarea	Duración	Comienzo	Fin	Pre	Nombres de los recursos	Costo
6.1.8 Selección adquisición e implementación de un sistema de detección de vulnerabilidades para la red de datos de la Universidad sede Bogotá.	6 mss	vie 13/04/18	jue 27/09/18	8	Director TIC	$ 15.000.000
6.1.9 Parametrización del sistema de helpdesk para que incluya la gestión de incidentes.	2 mss	vie 28/09/18	jue 22/11/18	10	Director TIC	$ 1.000.000
6.1.14 Hardening de servidores de la Universidad	6 mss	mié 31/01/18	mar 17/07/18	10	Director TIC	$ 20.000.000
LARGO PLAZO	**372 días**	**mié 31/01/18**	**jue 04/07/19**			**$ 67.000.000**
6.1.7 Selección adquisición e implementación de un sistema de prevención y detección de intrusos (IDS e IPS) para la red de datos de la Universidad sede Bogotá.	6 mss	mié 31/01/18	mar 17/07/18	9	Director TIC	$ 30.000.000
6.1.10 Selección adquisición e implementación de un DLP (Data Loss Prevention).	6 mss	vie 23/11/18	jue 09/05/19	11	Director TIC	$ 15.000.000
6.1.12 Compra de memorias USB cifradas para uso en datacenters y	2 mss	vie 10/05/19	jue 04/07/19	15	Director TIC	$ 2.000.000

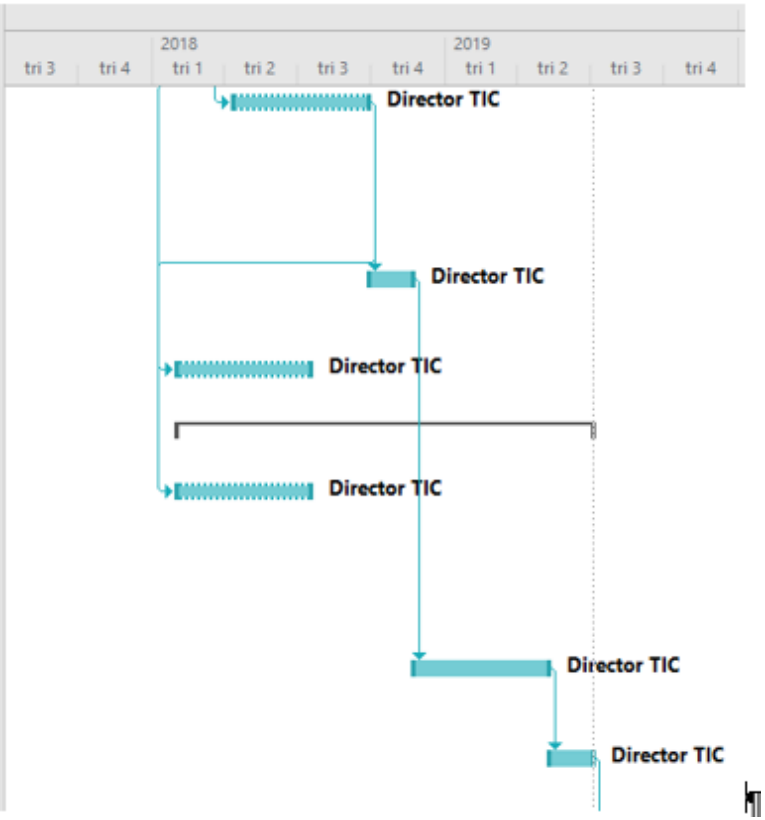


Tabla 16. Diagrama de Gantt de proyectos a largo plazo

7. AUDITORÍA DE CUMPLIMIENTO

7.1. Metodología

En este capítulo se realiza la evaluación del SGSI de la organización, evaluando el grado de madurez alcanzado haciendo uso de ISO 27002:2013. En el numeral 2.2 del presente documento se encuentra ampliamente explicado este manual de buenas prácticas para la gestión de la seguridad de la información, que cuenta con 114 controles, organizados en 14 dominios. Dichos dominios tienen 35 objetivos de control.

El modelo de madurez CMM (Capability Maturity Model) fue creado por el Software Engineer Institute y tiene un conjunto de procedimientos para la evaluación y mejora de los procesos de desarrollo, implementación y mantenimiento de software (Mary Beth Chrissis, 2009). Este modelo puede ser extendido a sistemas de gestión para evaluar el nivel de madurez de dicho sistema.

Los niveles del CMM que se aplicarán para evaluar la madurez del sistema de gestión son los siguientes:

EFECTIVIDAD	CMM	NIVEL	DESCRIPCIÓN
0%	**L0**	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	**L1**	Inicial / Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
			Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea.

EFECTIVIDAD	CMM	NIVEL	DESCRIPCIÓN
50%	**L2**	Reproducible, pero intuitivo	Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	**L3**	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	**L4**	Gestionado y medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para Automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	**L5**	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Tabla 17. Criterios de evaluación del modelo de madurez del SGSI

Las fuentes de información utilizadas para la realización del estado de madurez fueron las siguientes:

- Análisis de la documentación soporte aplicable al SGSI:
  - Política de seguridad propuesta y aprobada.
  - Procedimientos aplicables
  - Política de control de acceso
  - Reglamentos
  - Documentación de gestión de activos
  - Documentación de soporte de los sistemas de información
  - Nuevo organigrama de la Universidad
- Entrevistas
  - Rector de la Universidad

  - Vicerrector General
  - Vicerrectora del VEAD
  - Directora de Gestión Humana
  - Director del centro de documentación
  - Directora de control interno
  - Director de TICS
  - Coordinador de Soporte Técnico.
- Inspección visual en dependencias
- Revisión de registros que soportan los distintos procesos.

El informe de Auditoria al Sistema de Seguridad de la Información se encuentra en el ANEXO 11: INFORME DE AUDITORÍA al final del presente documento.

7.2. Nivel de madurez del SGSI de una universidad colombiana

De acuerdo a la evaluación de los controles de ISO 2700:2012, se sintetizan por medio de tablas las conformidades mayores, menores y observaciones y el estado de madurez de cada uno de los controles. Dicha información se encuentra concentrada en el anexo

Los resultados obtenidos por dominio se resumen en la siguiente tabla:

DOMINIO	NO CONFORMIDADES			MADUREZ	
	MAYORES	MENORES	OBSERVA-CIONES	%	CMM
A5. POLÍTICAS DE SEGURIDAD	2	0	0	20,0%	L1
A.6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA	2	1	0	67,5%	L2
A.7. SEGURIDAD LIGADA A RECURSOS HUMANOS	4	1	0	35,6%	L1
A.8. GESTIÓN DE ACTIVOS	5	1	0	49,2%	L1
A.9. CONTROL DE ACCESOS	3	5	0	90,2%	L3
A.10 CIFRADO	2	0	0	0,0%	L0
A.11. SEGURIDAD FÍSICA Y AMBIENTAL	2	2	0	88,9%	L2
A.12. SEGURIDAD EN LAS OPERACIONES	2	1	2	78,2%	L2
A.13. SEGURIDAD EN LAS TELECOMUNICACIONES	2	1	1	84,4%	L2
A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE	0	0	0	100,0%	L5
A.15. RELACIONES CON PROVEEDORES.	2	1	0	50,8%	L2
A.16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA	4	1	1	48,6%	L1
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA	2	0	0	66,7%	L2
A.18. CUMPLIMIENTO.	5	1	0	29,0%	L1

Tabla 18. Modelo de madurez SGSI de acuerdo con los controles ISO 27002:2013

La información sintetizada en el cuadro anterior puede visualizarse haciendo uso del diagrama de radar para visualizar de forma clara el grado de madurez de cada uno de los dominios de seguridad:

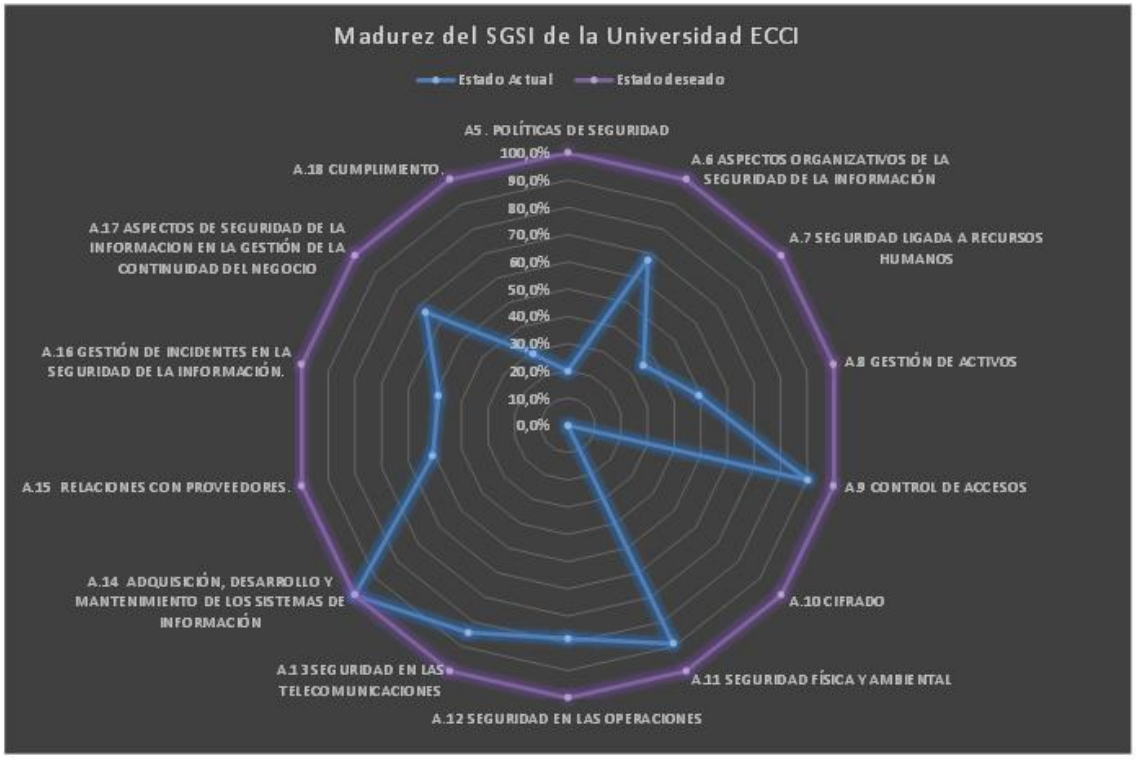


Figura 14. Grado de madurez del SGSI de la ECCI según ISO 27002:2013. Diagrama de radar.

Este formato de visualización permite mostrar que los dominios A10: Cifrado y A5: Políticas de seguridad son los dominios en los que hay que concentrar las actividades de mejoramiento de cada a la Certificación ISO 27001:2013.

Respecto a los controles evaluados (se sacaron 8 controles, debido a que fueron definidos como no aplicables en la Declaración de aplicabilidad) se puede evidenciar que cerca del 40% se encuentran en el nivel de madurez superior (optimizado).

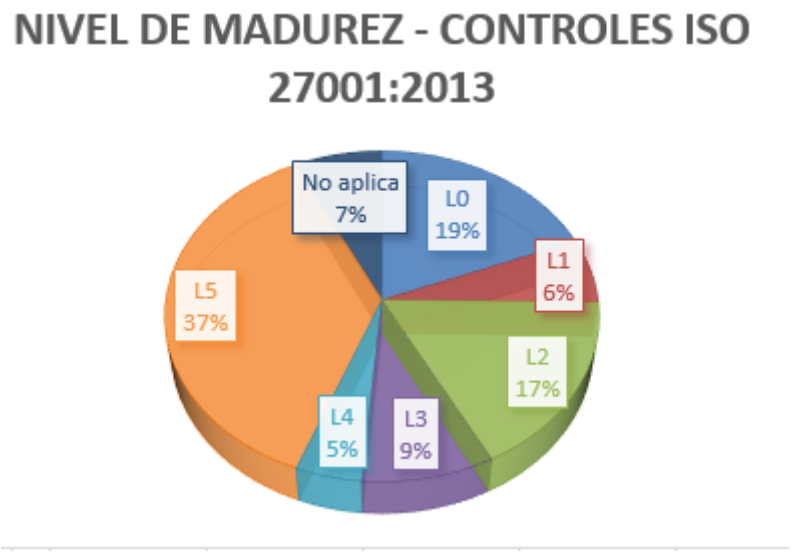


Figura 15. Nivel de madurez de los controles ISO 27001:2013

En la siguiente figura se encuentra el niel de control por dominio:

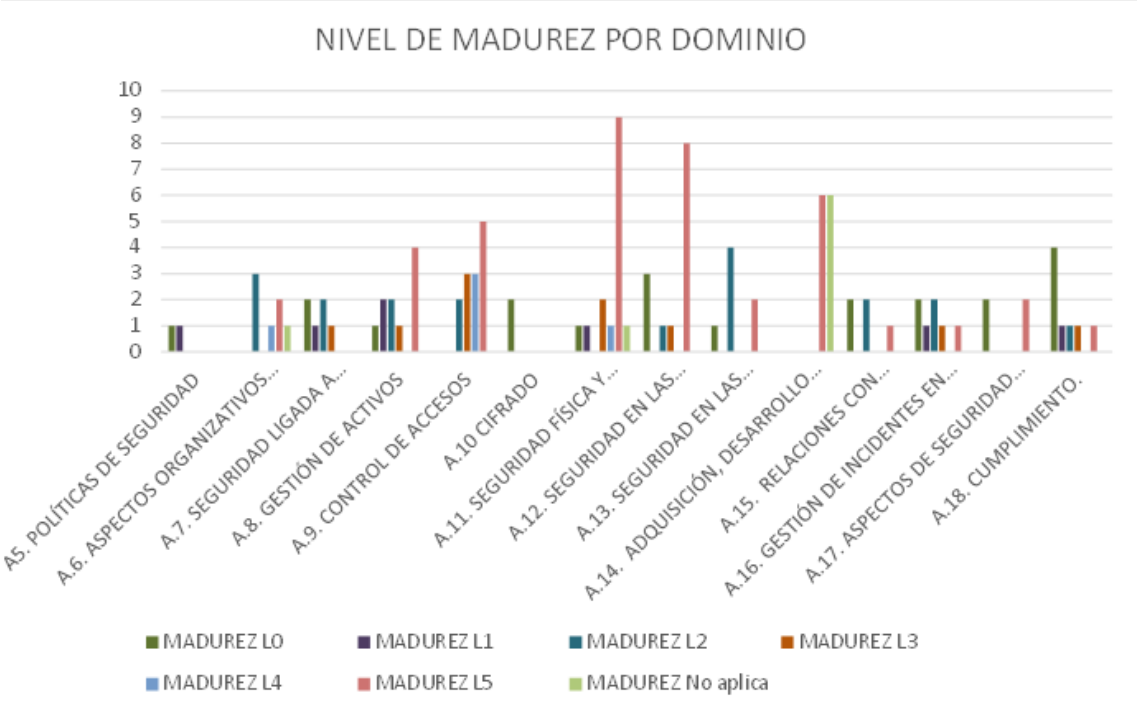


Figura 16. Nivel de madurez por dominio

Respecto a la Auditoría de cumplimiento (anexo), las no conformidades (mayores / menores) y observaciones por cada dominio se encuentran sintetizados en la siguiente figura:

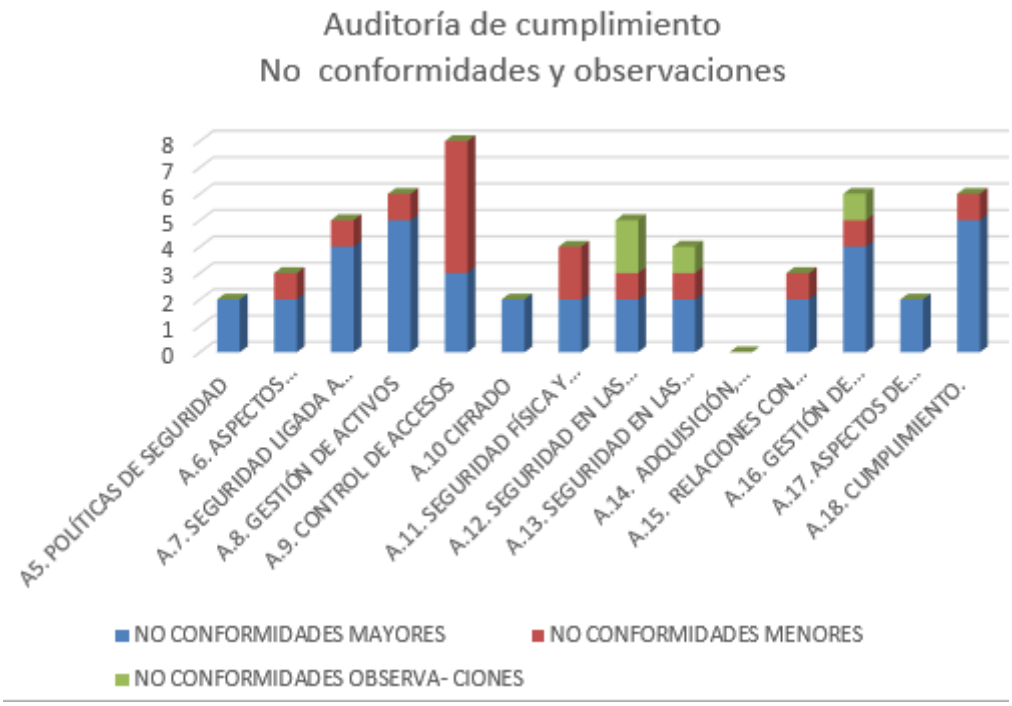


Figura 17: Resultados de la auditoría de cumplimiento

De la figura 17 se puede inferir que las áreas que necesitan orientar sus esfuerzos tienen que ver con los controles asociados con Control de Acceso, Gestión de incidentes de seguridad de la información y gestión de activos y cumplimiento.

Un resultado muy importante es validar desde el punto de vista de los controles y verificar que la pertinencia de las propuesta presentadas en el capítulo anterior, las cuales se soportaron en los resultados de gestión de riesgos apuntan en la misma dirección y lo que ha permitido entregar un diagnóstico coherente y consistente a una universidad colombiana.

8. CONCLUSIONES

El Plan Director de Seguridad de la información para una universidad colombiana, sede Bogotá ha generado en la institución un ambiente de concientización de la importancia de abordar proyectos en materia de seguridad de la información de la información a corto, mediano y largo plazo.

De acuerdo a las reuniones con el señor Rector y el Vicerrector General se identificaron varios proyectos referentes a la seguridad de la información de parte de la Vicerrectoría de Educación a Distancia y de la Vicerrectoría de Investigación, de distinto alcance cada uno, pero que permiten afrontar el tema desde distintas miradas, cada una de las cuales enriquecerá los proyectos que se ejecutarán en este sentido en un futuro próximo.

Como resultado del presente proyecto, se ha entregado a la Universidad la Política General de Seguridad, que viene siendo discutida por las distintas instancias y está pendiente de aprobar por parte del Consejo Superior Universitario. Adicionalmente se presentaron propuestas de procedimientos, cambios organizativos, indicadores y la generación del Comité de seguridad de la información que están también pendientes de ser aprobadas.

El análisis de riesgos de seguridad de la información ya fue entregado a Vicerrectoría general y se encuentra pendiente de ser revisado y aprobado, previo visto bueno de la Dirección TIC y dicha Vicerrectoría.

Los resultados de la fase 4, con la propuesta de proyectos a desarrollar en materia de seguridad de la información, serán estudiados por el Departamento de Planeación, para ser considerado, como parte de los planes de acción con miras a la certificación ISO 27001:2013 que se está proyectando conseguir en un período de 3 años.

Adicionalmente, la Coordinación de Sistemas y la Dirección TIC iniciaron unas campañas de concientización en materia de Seguridad de la Información y se desarrolló una Jornada de Seguridad Informática con presencia de expertos de alto nivel colombianos, la cual se enfocó en temas de ciberseguridad, delitos informáticos y ransomware. Se están desarrollando conversatorios con personal docente y administrativo en temáticas de seguridad de la información, que a futuro hará parte del plan de concienciación en seguridad con miras al cambio de mentalidad del personal académico y administrativo de la Universidad.

Finalmente, de acuerdo a la auditoria de cumplimiento desarrollada en la Fase 5, se obtuvo el nivel de madurez de acuerdo a los controles de ISO 27002:2013, insumo base para el desarrollo de buenas prácticas en materia de seguridad de la información, que complementará el desarrollo de los proyectos y demás iniciativas, que llegando a buen puerto, permitirán que la Universidad gestione la información de una forma segura, con un manejo adecuado del riesgo, en cumplimiento de la normatividad legal colombiana pertinente y orientado a salvaguardar la confidencialidad, integridad y disponibilidad de la información que se genera, almacena, transporta e intercambia con su entorno.

ANEXO 1: CONTROLES ISO 27001:2015

DOMINIOS	OBJETIVOS DE SEGURIDAD	CONTROLES
A.5 Política de seguridad de la información	A.5.1 Orientación de la dirección para la gestión de SI.	A5.1.1 Políticas para la SI
		A.5.1.2 Revisión de políticas para la SI.
A.6. Organización de la SI	A.6.1 Organización interna	A.6.1.1 SI: Roles y responsabilidades
		A.6.1.2 Separación de deberes
		A.6.1.3 Contacto con las autoridades
		A.6.1.4. Contacto con grupos de interés especial
		A.6.1.5. SI en la gestión de proyecto
	A.6.2 Dispositivos móviles y teletrabajo	A.6.2.1 Política para dispositivos móviles
		A.6.2.2 Teletrabajo
A.7 Seguridad de los recursos humanos	A.7.1 Antes de asumir el empleo	A.7.1.1. Selección
		A .7.1.2 Términos y condiciones del empleo
	A.7.2 Durante la ejecución del empleo	A.7.2.1 Responsabilidades de la dirección.
		A.7.2.2 Toma de conciencia, educación y formación en la SI
		A.7.2.3 Proceso disciplinario
A.8. Gestión de activos	A.8.1 Responsabilidad de los activos	A.8.1.1. Inventario de activos
		A.8.1.2 Propiedad de los activos
		A.8.1.3 Uso aceptable de los activos
		A.8.1.4 Devolución de activos
	A.8.2. Clasificación de la información	A.8.2.1 Clasificación de la información
		A.8.2.2 Etiquetado de la información
		A.8.2.3 Manejo de activos
	A.8.3 Manejo de medios de soporte	A.8.3.1 Gestión de medios de soporte removibles
		A.8.3.2 Disposición de medios de soporte
		A.8.3.3 Transferencia de medios de soporte
A.9. Control de acceso	A.9.1 Requisitos de negocio de control de acceso	A.9.1.1 Política de control de acceso

		A.9.1.2 Acceso a redes y servicios en red
	A.9.2. Gestión de acceso a usuarios	A.9.2.1 Registro y cancelación del registro de usuarios
		A.9.2.2 Suministro de acceso de usuarios.
		A.9.2.3 Gestión de derechos de acceso privilegiado.
		A.9.2.4 Gestión de información de autenticación secreta de usuarios.
		A.9.2.5 Revisión de los derechos de acceso de usuarios
		A.9.2.6 Cancelación o ajuste de los derechos de acceso.
	A.9.3 Responsabilidad de usuarios	A.9.3.1 Uso de información secreta
	A.9.4 Control de acceso a sistemas y aplicaciones.	A.9.4.1 Restricción de acceso a información.
		A.9.4.2 Procedimiento de conexión segura.
		A.9.4.3 Sistemas de gestión de contraseñas.
		A.9.4.4 Uso de programas utilitarios privilegiados
		A.9.4.5 Control de acceso a códigos fuentes
A.10 Criptografía	A.10.1 Política de uso de controles criptográficos	A.10.1.1 Políticas sobre el uso de controles criptográficos.
		A.10.1.2 Gestión de claves
A.11 Seguridad física y ambiental	A.11.1 Áreas seguras	A.11.1.1 Perímetro de seguridad física
		A.11.1.2 Controles físicos de entrada
		A.11.1.3 Seguridad de oficinas, salones e instalaciones.
		A.11.1.4 Protección de amenazas externas y ambientales.
		A.11.1.5 Trabajo de áreas seguras.
		A.11.1.1 Áreas de despacho y carga.

	A.11.2. Equipos	A.11.2.1 Ubicación y protección de equipos.
		A.11.2.2 Servicios públicos de soporte
		A.11.2.3 Seguridad del cableado.
		A.11.2.4 Mantenimiento de equipos.
		A.11.2.5 Retiro de activos.
		A.11.2.6 Seguridad de equipos y activos fuera del predio.
		A.11.2.7 Disposición segura o reutilización de equipos.
		A.11.2.8 Equipos sin supervisión de usuarios.
		A.11.2.9 Política de escritorio limpio y pantalla limpia.
A.12 Seguridad de operaciones	A.12.1 Procedimientos operacionales y responsables.	A.12.1.1 Procedimientos de operación documentados.
		A.12.1.2 Gestión de cambios.
		A.12.1.3 Gestión de capacidad
		A.12.1.4 Separación de los ambientes de desarrollo, ensayo y operación.
	A.12.2 Protección contra códigos maliciosos	A.12.2.1 Controles contra códigos maliciosos.
	A.12.3 Copias de respaldo	A.12.3.1 Copias de respaldo de información.
	A.12.4 Registro y seguimiento.	A.12.4.1 Registro de eventos.
		A.12.4.2 Protección de la información de registro.
		A.12.4.3 Registros del administrador y del operador.
		A.12.4.4 Sincronización de relojes
	A.12.5 Control de software operacional	A.12.5.1 Instalación de software de sistemas operativos.
	A.12.6 Gestión de vulnerabilidad técnica.	A.12.6.1 Gestión de las vulnerabilidades técnicas.
		A.12.6.2 Restricciones sobre la instalación de software.

	A.12.7 Consideraciones sobre auditorías de sistemas de información.	A.12.7.1 Controles sobre auditorías de sistemas de información.
A.13 Seguridad de comunicaciones	A.13.1 Gestión de seguridad de redes.	A.13.1.1 Controles de redes.
		A.13.1.2 Seguridad de servicios de red.
		A.13.1.3 Separación en las redes.
	A.13.2. Transferencia de información	A.13.2.1 Políticas y procedimientos de transferencia de información.
		A.13.2.2 Acuerdos sobre transferencia de información.
		A.13.2.3 Mensajes electrónicos.
		A.13.2.4 Acuerdos de confidencialidad.
A.14 Adquisición, desarrollo y mantenimiento de sistemas.	A.14.1 Requisitos de seguridad de los sistemas de información	A.14.1.1 Análisis y especificación de requisitos de seguridad de información.
		A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas.
		A.14.1.3 Protección de transacciones de servicios de aplicaciones.
	A.14.2 Seguridad en los procesos de desarrollo y soporte.	A.14.2.1 Política de desarrollo seguro.
		A.14.2.2 Procedimiento de control de cambios del sistema
		A.14.2.3 Revisión técnica de aplicaciones después de cambios.
		A.14.2.4 Restricciones sobre los cambios de paquetes de software.
		A.14.2.5 Principios de construcción de sistemas seguros.
		A.14.2.6 Ambiente de desarrollo seguro.
		A.14.2.7 Desarrollo contratado externamente.
		A.14.2.8 Pruebas de seguridad de sistemas.
		A.14.2.9 Pruebas de aceptación de sistemas.
	A.14.3 Datos de ensayo	A.14.3.1 Protección de datos de ensayo.

A.15 Relaciones con proveedores		
	A.15.1 Seguridad de la información en las relaciones con proveedores.	A.15.1.1 Política de seguridad de la información para proveedores.
		A.15.1.2 Tratamiento del riesgo dentro de acuerdos de proveedores.
		A.15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
	A.15.2 Gestión de la prestación del servicio por proveedores.	A.15.2.1 Supervisión y revisión de los servicios prestados por terceros.
		A. 15.2.2 Gestión de cambios en los servicios prestados por terceros.
A.16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	A.16.1 Gestión de incidentes de seguridad de la información y mejoras.	A.16.1.1 Responsabilidades y procedimientos.
		A.16.1.2 Notificación de los eventos de seguridad de la información.
		A.16.1.3 Notificación de puntos débiles de la seguridad.
		A.16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
		A.16.1.5 Respuesta a los incidentes de seguridad.
		A.16.1.6 Aprendizaje de los incidentes de seguridad de la información.
		A.16.1.7 Recopilación de evidencias.
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	A.17.1 Continuidad de la seguridad de la información.	A.17.1.1 Planificación de la continuidad de la seguridad de la información.
		A.17.1.2 Implantación de la continuidad de la seguridad de la información.
		A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
	A.17.2 Redundancias.	A.17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

A.18. CUMPLIMIENTO.	A.18.1 Cumplimiento de los requisitos legales y contractuales.	A.18.1.1 Identificación de la legislación aplicable.
		A.18.1.2 Derechos de propiedad intelectual (DPI).
		A.18.1.3 Protección de los registros de la organización.
		A.18.1.4 Protección de datos y privacidad de la información personal.
		A.18.1.5 Regulación de los controles criptográficos.
	A.18.2 Revisiones de la seguridad de la información.	A.18.2.1 Revisión independiente de la seguridad de la información.
		A.18.2.2 Cumplimiento de las políticas y normas de seguridad.
		A.18.2.3 Comprobación del cumplimiento.

Tabla 19. Controles de seguridad ISO/IEC 27002:2013

ANEXO 2. RESULTADOS DE ANÁLISIS DIFERENCIAL

Cumplimiento de la norma ISO 27001:2013

4. CONTEXTO DE LA ORGANIZACIÓN			
	4.1. Conocimiento de la Organización y su contexto.	0%	No existe documento referente al tema.
	4.2 Comprensión de las necesidades y expectativas de las partes interesadas.	0%	No se ha realizado el análisis de necesidades de las partes interesadas para el SGSI.
	4.3 Determinación del alcance del SGSI	0%	No se ha determinado el alcance del SGSI
	4.4 Sistema de Gestión de Seguridad de la Información	0%	No se cuenta con un SGSI
5. LIDERAZGO			
	5.1. Liderazgo y compromiso	50%	La alta dirección se encuentra comprometida con la implantación de un SGSI, así como está comprometida con el sistema de gestión de la calidad..
	5.2 Política	0%	No se cuenta con una política de seguridad de la información.
	5.3 Roles, responsabilidades y autoridades en la organización	0%	No se ha desarrollado aún este tema.
6. PLANIFICACIÓN			
	6.1.Acciones para tratar riesgos y oportunidades	0%	No se ha llevado a cabo el proceso de planificación del SGSI, ni la evaluación de riesgos, ni el tratamiento de los mismos..
	6.2 Objetivos de la seguridad de la información	0%	No se han definido los objetivos de la información.
7. SOPORTE			
	7.1. Recursos.	0%	Se espera que como resultado del presente proyecto, destinar recursos para el SGSI.

4. CONTEXTO DE LA ORGANIZACIÓN			
	7.2 Competencia	0%	De momento nos e cuenta con el manual de competencias.
	7.3 Toma de conciencia	0%	Como no se ha implementado el SGSI, no se cuenta con se han desarrollado campañas de toma de conciencia.
	7.4 Comunicación	0%	Aún no se tiene el SGSI, por lo que no se han desarrollado documentos respecto a este tema.
	7.5 Información documentada	25%	Se maneja información documentada relacionada con la norma, la cual es controlada, pero no la desarrollada en la norma misma.
8. OPERACIÓN			
	8.1. Planificación y control operacional.	0%	No se ha definido qué operaciones deben ser controladas y el plan de tratamiento.
	8.2 Evaluación de riesgos de la seguridad de información.	0%	No se han realizado evaluaciones de riesgos para el SGSI.
	8.3 Tratamiento de riesgos de seguridad de la información	0%	No se cuenta con el plan de tratamiento de riesgos.
9. EVALUACIÓN DEL DESEMPEÑO			
	9.1. Seguimiento, medición, análisis y evaluación.	0%	No se puede realizar evaluación del desempeño porque no se cuenta con SGSI.
	9.2 Auditoría interna.	0%	No se puede realizar auditorías internas porque no se cuenta con SGSI.
	9.3 Revisión por la dirección	0%	No se puede realizar revisiones por la dirección porque no se cuenta con SGSI
10. MEJORA			
	10.1. No conformidades y acciones correctivas.	25%	Aunque no se cuenta con SGSI, se tiene un procedimiento para manejo de no conformidades por el Sistema de Calidad el cual se puede adecuar a nuestro caso..
	10.2 Mejora continua	25%	No se se cuenta aún con el SGSI, pero ya se maneja un modelo de mejora continua en el sistema de calidad..

Dominios, Objetivos de control y controles ISO/IEC 27002:2013

DOMINIO, OBJETIVOS DE CONTROL Y CONTROLES			ESTADO	OBSERVACIONES
5. POLÍTICAS DE SEGURIDAD				
	5.1 Directrices de la Dirección en seguridad de la información.			
		5.1.1. Conjunto de políticas para la seguridad de la información.	0%	No existe documento de Políticas de seguridad de la información.
		5.1.2. Revisión de las políticas para la seguridad de la información	0%	No existe documento de Políticas de seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN				
	6.1. Organización interna			
		6.1.1. Asignación de responsabilidades para la seguridad de la información	0%	No existe en los manuales de funciones, responsabilidades inherentes a la seguridad de la información para ningún trabajador de la Universidad.
		6.1.2. Segregación de tareas	0%	No existe segregación de tareas de seguridad de la información en el Departamento de TICs.
		6.1.3 Contacto con las autoridades.	0%	No se mantienen contactos con las autoridades pertinentes en el área de seguridad de la información en Colombia.
		6.1.4 Contactos con grupos de interés especial	0%	No se tiene contacto por parte de la Universidad, con grupos de interés en el área de seguridad de la información

DOMINIO, OBJETIVOS DE CONTROL Y CONTROLES			ESTADO	OBSERVACIONES
		6.1.5 Seguridad de la información en la gestión de proyectos.	0%	No se tiene en cuenta la seguridad de la información en la gestión de proyectos.
	6.2 Dispositivos para movilidad y teletrabajo.			
		6.2.1 Política de uso de dispositivos para movilidad	0%	No hay establecida una política, ni medidas de seguridad adecuadas para la protección contra riesgos asociados al uso de recursos almacenados en dispositivos móviles.
		6.2.2 Teletrabajo	0%	No hay establecida una política, ni medidas de seguridad adecuadas para la protección contra riesgos asociados al teletrabajo.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS				
	7.1 Antes de la contratación			
		7.1.1 Investigación de antecedentes	0%	En los procesos de contratación, no se realizan revisiones de verificación de antecedentes a candidatos a empleos administrativos y docentes, ni contratistas respecto a la clasificación de la información a la cual va a tener acceso y riesgos percibidos.
		7.1.2 Términos y condiciones de contratación.	0%	No se tienen implementados acuerdos de confidencialidad en los contratos laborales y/o con terceros.
	7.2 Durante la contratación			
		7.2.1 Responsabilidades de gestión	0%	No existen responsabilidades de gestión de la seguridad de la información, asociadas a los manuales de funciones.
		7.2.2 Concienciación, educación y capacitación en seguridad de información.	0%	No se han realizado capacitaciones y campañas de concienciación sobre seguridad de la información en ningún nivel de la organización.

DOMINIO, OBJETIVOS DE CONTROL Y CONTROLES			ESTADO	OBSERVACIONES
		7.2.3 Proceso disciplinario	0%	No existe la figura de proceso disciplinario respecto a seguridad de la información.
	7.3 Cese o cambio de puesto			
		7.3.1 Cese o cambio de puesto de trabajo.	10%	Solo existen mecanismos de seguridad asociados al cierre de cuenta en el caso de cambio de puesto de trabajo en el área de informática.
8. GESTIÓN DE ACTIVOS				
	8.1 Responsabilidad sobre los activos			
		8.1.1 Inventario de activos	0%	No existen levantados inventarios de activos de información en materia de seguridad de la información.
		8.1.2 Propiedad de los activos	10%	Los activos asociados a los recursos se entregan a empleados administrativos que los tengan a su cargo. No se incluyen activos de información.
		8.1.3 Uso aceptable de los activos	0%	No existen políticas asociadas a gestión de activos de información, ni de recursos.
		8.1.4 Devolución de activos	25%	Existen procedimientos asociados a devolución de los activos asociados a recursos por parte de empleados administrativos, pero no de información.
	8.2 Clasificación de la información			
		8.2.1 Directrices de clasificación	0%	No existen directrices de clasificación de la información.
		8.2.2 Etiquetado y manipulación de la información	0%	No existen procedimientos de etiquetado y manipulación de la información.
		8.2.3 Manipulación de activos	0%	No existen políticas asociadas a la manipulación de activos de la información.
	8.3 Manejo de los soportes de almacenamiento			
		8.3.1 Gestión de soportes extraíbles	0%	No existen políticas para la gestión de soportes extraíbles.

DOMINIO, OBJETIVOS DE CONTROL Y CONTROLES			ESTADO	OBSERVACIONES
		8.3.2 Eliminación de soportes	50%	Existe un procedimiento de eliminación de soportes de almacenamiento.
		8.3.3 Soportes físicos en tránsito	100%	Existen procedimientos para el tránsito de soportes físicos extraíbles que contienen copias de seguridad de algunos sistemas de información.
9. CONTROL DE ACCESOS				
	9.1 Requisitos de negocio para el control de acceso			
		9.1.1 Política de control de accesos.	50%	Existe una política de control de acceso por medio de ACLs, pero no está soportada en ningún documento.
		9.1.2 Control de acceso a las redes y servicios asociados.	100%	Se encuentran implementados controles de acceso a las redes y servicios asociados.
	9.2 Gestión de acceso de usuario.			
		9.2.1 Gestión de altas/bajas en el registro de usuarios.	0%	No se gestionan de forma correcta las altas/bajas en el registro de usuario de los sistemas de información.
		9.2.2 Gestión de los derechos de acceso asignados a usuarios.	50%	Se gestionan los derechos de acceso a los usuarios de acuerdo a políticas no soportadas en documentos.
		9.2.3 Gestión de los derechos de acceso con privilegios especiales.	50%	Se gestionan los derechos de acceso a los usuarios de acuerdo a políticas no soportadas en documentos.
		9.2.4 Gestión de la información confidencial de autenticación de usuarios.	0%	No se cuenta con procedimientos para la gestión de la información confidencial de autenticación de usuarios.
		9.2.5 Revisión de los derechos de acceso de los usuarios.	0%	Hay control de autenticación a nivel de sistemas de información y perfiles de usuario, pero no hay procedimientos programados de revisión.
		9.2.6 Cancelación o ajuste de los derechos de acceso.	25%	Se cuenta con actividades de cancelación y ajuste, pero no se lleva un documento que demuestre dichas actividades.
	9.3 Responsabilidades del usuario.			

DOMINIO, OBJETIVOS DE CONTROL Y CONTROLES			ESTADO	OBSERVACIONES
		9.3.1 Uso de información confidencial para la autenticación.	50%	Los administradores de los sistemas crean contraseñas haciendo uso de buenas prácticas, pero que no han sido socializadas con los usuarios.
	9.4 Control de acceso a sistemas y aplicaciones.			
		9.4.1 Restricción de acceso a la información.	0%	No existe política de control de acceso definida, por lo que las restricciones de acceso que se aplican no se basan en la misma.
		9.4.2 Procedimientos seguros de inicio de sesión.	0%	El jefe de TIC asegura que existe tal procedimiento, pero no se tiene la evidencia.
		9.4.3 Gestión de contraseñas de usuario.	50%	Las contraseñas para acceso a los sistemas de información de la universidad son gestionadas por el departamento de TICs, pero no se cuenta con una herramienta que verifique la calidad de las contraseñas cambiadas por los usuarios.
		9.4.4 Uso de programas utilitarios privilegiados	0%	No se hace seguimiento de dichos programas.
		9.4.5 Control de acceso al código fuente de los programas.	100%	Controlado por el administrador del sistema, certificados por vpn y se manejan logs.
10. CIFRADO				
	10.1 Controles criptográficos			
		10.1.1 Política de uso de los controles criptográficos.	0%	No existe dicha política de uso de controles criptográficos. Se usa cifrado de información de data center y en copias de seguridad.
		10.1.2 Gestión de claves.	10%	Se realizan procedimientos de gestión de claves, pero no se cuenta con la política.
11. SEGURIDAD FÍSICA Y AMBIENTAL				
	11.1 Áreas seguras			

DOMINIO, OBJETIVOS DE CONTROL Y CONTROLES			ESTADO	OBSERVACIONES
		11.1.1 Perímetro de seguridad física.	20%	Solo se aplica el perímetro de seguridad física a una sala de servidores que tiene como acceso exclusivo el personal de TICs.
		11.1.2 Controles físicos de entrada.	20%	Se cuenta con controles de entrada insuficientes para garantizar que solo el personal autorizado dispone de permiso de acceso, que se evidencia en la visita a cuartos de comunicaciones.
		11.1.3 Seguridad de oficinas, despachos y recursos.	25%	Se cuenta con un sistema de seguridad física a oficinas, salas e instalaciones de la organización, pero se tienen muchos problemas con el mismo.
		11.1.4 Protección contra las amenazas externas y ambientales.	25%	Se ha diseñado y aplicado protección física contra desastres naturales, pero no contra ataques maliciosos.
		11.1.5 El trabajo en áreas seguras.	25%	Se cuenta con procedimientos para el desarrollo de trabajos en altura.
		11.1.6 Áreas de despacho, carga y descarga.	100%	Se cuenta con mecanismos de acceso a los edificios que habilitan puertas para dichas actividades y las zonas seguras no tienen cercanía con dichas zonas.
	11.2 Seguridad de los equipos			
		11.2.1 Emplazamiento y protección de equipos.	75%	Se cuentan con mecanismos de control de acceso y en las oficinas y laboratorios se cuenta con mecanismos antiincendios y los edificios construidos en los últimos años cumplen con la regulación antisísmica. Los equipos cuentan con protección en caso de robo.
		11.2.2 Servicios públicos de soporte.	50%	NO todos los equipos cuentan con reguladores que funcionen correctamente, aunque sí los servidores y cuartos de comunicaciones. Los edificios nuevos cumplen plenamente con este control.

DOMINIO, OBJETIVOS DE CONTROL Y CONTROLES			ESTADO	OBSERVACIONES
		11.2.3 Seguridad del cableado.	0%	Se cuenta con zonas donde los cables de datos son accesibles a ataques a la disponibilidad.
		11.2.4 Mantenimiento de los equipos.	100%	Se cuentan con procedimientos de mantenimiento preventivo y correctivo para los equipos que conforman la infraestructura informática.
		11.2.5 Salida de activos fuera de las dependencias de la empresa.	100%	Se cuenta con los procedimientos para la salida de activos fuera de las dependencias, previa autorización por parte del responsable del activo y del departamento de seguridad física.
		11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	100%	Se cuenta con seguros que cubran posibles robos y daños en los equipos y activos que se trasladan fuera de las instalaciones de la universidad.
		11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	0%	No se cuenta con procedimientos para salvaguardar dichos dispositivos de almacenamiento.
		11.2.8 Equipo informático de usuario desatendido.	0%	No se cuenta con los procedimientos que garanticen la protección adecuada en estos casos.
		11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	0%	Los equipos de usuario no tienen permisos para evitar el bloqueo de pantalla.
12. SEGURIDAD EN LAS OPERACIONES.				
	12.1 Responsabilidades y procedimientos de operación.			
		12.1.1 Documentación de procedimientos de operación.	60%	La documentación con la que se cuenta es insuficiente para algunos procedimientos de operación.
		12.1.2 Gestión de cambios.	0%	No se cuenta con procedimientos de gestión de cambios.
		12.1.3 Gestión de capacidades.	80%	Se hace seguimiento al uso de los recursos y proyecciones de requisitos de capacidad en el futuro para servidores y equipos activos, no para todos.

DOMINIO, OBJETIVOS DE CONTROL Y CONTROLES			ESTADO	OBSERVACIONES
		12.1.4 Separación de entornos de desarrollo, prueba y producción	50%	No se cuenta con entornos separados para todos los entornos de desarrollo.
	12.2 Protección contra código malicioso.			
		12.2.1 Controles contra el código malicioso.	50%	Se cuenta con controles para la detección y prevención de malware, pero no para la recuperación en caso de daños.
	12.3 Copias de seguridad.			
		12.3.1 Copias de seguridad de la información.	100%	Se cuenta con los procedimientos para copias de seguridad.
	12.4 Registro de actividad y supervisión.			
		12.4.1 Registro y gestión de eventos de actividad.	25%	Se realizan actividades periódicas de los registros de eventos de actividad del usuario, excepciones, fallas y de seguridad, a nivel de servidor, pero no a niveles de equipos de trabajo.
		12.4.2 Protección de los registros de información.	25%	Se realiza un borrado mensual sin copias de seguridad.
		12.4.3 Registros de actividad del administrador y operador del sistema.	100%	Se realizan registros de actividades del administrador y los operadores, en los servidores.
		12.4.4 Sincronización de relojes.	100%	Se sincronizan con relojes con una fuente de sincronización única.
	12.5 Control del software en explotación.			
		12.5.1 Instalación del software en sistemas en producción.	100%	Se cuenta con procedimientos de control de software en sistemas en producción.
	12.6 Gestión de la vulnerabilidad técnica.			
		12.6.1 Gestión de las vulnerabilidades técnicas.	100%	Se desarrollan actividades para seguimiento de vulnerabilidades técnicas de los sistemas de información preventivas.

DOMINIO, OBJETIVOS DE CONTROL Y CONTROLES			ESTADO	OBSERVACIONES
		12.6.2 Restricciones en la instalación de software.	100%	Los usuarios tienen restringidos los derechos para instalación de software a través de sus perfiles.
	12.7 Consideraciones de las auditorías de los sistemas de información.			
		12.7.1 Controles de auditoría de los sistemas de información.	0%	No se han planificado los requisitos y actividades de auditorías para la verificación de sistemas de información.
13. SEGURIDAD EN LAS TELECOMUNICACIONES				
	13.1 Gestión de la seguridad en las redes.			
		13.1.1 Controles de red.	80%	Se realiza mediante el uso de firewall y VLANs.
		13.1.2 Seguridad de los servicios de la red.	50%	No se manejan SLA en los servicios de red internos, pero sí en los del proveedor de servicios de Internet.
		13.1.3 Segregación de redes.	100%	Las redes se encuentran segmentadas en VLANs.
	13.2 Intercambio de información con partes externas.			
		13.2.1 Políticas y procedimientos de intercambio de información.	100%	Se utilizan procedimientos y controles para intercambio de información con partes externas para cumplir con normatividad del Ministerio de Educación Nacional, la Superintendencia y entidades de control.
		13.2.2 Acuerdos de intercambio.	100%	Existen acuerdos de intercambio con partes externas.
		13.2.3 Mensajería electrónica.	0%	No existen mecanismos de protección de información compartida por este medio.
		13.2.4 Acuerdos de confidencialidad y secreto.	100%	Se trabajan requisitos en los acuerdos de confidencialidad por parte de la organización para la protección de la información.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN				
	14.1 Requisitos de seguridad de los sistemas de información.			

DOMINIO, OBJETIVOS DE CONTROL Y CONTROLES			ESTADO	OBSERVACIONES
		14.1.1 Análisis y especificación de los requisitos de seguridad.	0%	Cuando se realizan adquisición, desarrollo o mantenimiento de sistemas de información, no se incluyen requisitos relacionados con la seguridad de la información.
		14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	50%	Se utilizan VPN para acceso a servicios.
		14.1.3 Protección de las transacciones por redes telemáticas.	0%	NO se protege la información contra el enrutamiento incorrecto o la duplicación no autorizada de mensajes.
	14.2 Seguridad en los procesos de desarrollo y soporte.			
		14.2.1 Política de desarrollo seguro de software.	0%	No se cuenta con política de desarrollo seguro de software.
		14.2.2 Procedimientos de control de cambios en los sistemas.	0%	No se cuenta con procedimientos claros de control de cambios en los sistemas.
		14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	100%	Se realizan pruebas de impacto en las operaciones o en la seguridad de la organización.
		14.2.4 Restricciones a los cambios en los paquetes de software.	50%	En los servidores se realizan actividades de restricción a los cambios en paquetes, más no en los equipos cliente.
		14.2.5 Uso de principios de ingeniería en protección de sistemas.	50%	No se aplican los principios de seguridad de ingeniería de sistemas en las labores de implementación de los sistemas de información.
		14.2.6 Seguridad en entornos de desarrollo.	100%	Se protegen los entornos de desarrollo e integración de sistemas.
		14.2.7 Externalización del desarrollo de software.	50%	Se realizan labores de supervisión y monitoreo, pero no basados en procedimientos.
		14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	0%	No se realizan pruebas de funcionalidad en seguridad en las etapas de desarrollo.

DOMINIO, OBJETIVOS DE CONTROL Y CONTROLES			ESTADO	OBSERVACIONES
		14.2.9 Pruebas de aceptación.	100%	Se establecen programas de prueba con criterios de aceptación de los sistemas, actualizaciones y/o nuevas versiones.
	14.3 Datos de prueba.			
		14.3.1 Protección de los datos utilizados en pruebas.	0%	No se realiza selección de datos de prueba en las pruebas de las implementaciones.
15. RELACIONES CON SUMINISTRADORES.				
	15.1 Seguridad de la información en las relaciones con suministradores.			
		15.1.1 Política de seguridad de la información para suministradores.	0%	No se cuenta con políticas de seguridad para proveedores y terceras personas.
		15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	100%	Se establecen consideraciones de seguridad de la información con los proveedores.
		15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.	0%	No se cuenta con requisitos para abordar riesgos de seguridad asociadas a cadenas de suministro de los servicios y productos de tecnología de información y comunicaciones.
	15.2 Gestión de la prestación del servicio por suministradores.			
		15.2.1 Supervisión y revisión de los servicios prestados por terceros.	100%	Se realiza monitoreo, revisión y auditaje de algunos servicios provistos por terceros.
		15.2.2 Gestión de cambios en los servicios prestados por terceros.	0%	No se realiza la administración de cambios a a provisión de servicios prestados por terceros.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.				
	16.1 Gestión de incidentes de seguridad de la información y mejoras.			
		16.1.1 Responsabilidades y procedimientos.	100%	Se cuenta con procedimientos de gestión para respuesta a incidentes de seguridad de la información.

DOMINIO, OBJETIVOS DE CONTROL Y CONTROLES			ESTADO	OBSERVACIONES
		16.1.2 Notificación de los eventos de seguridad de la información.	100%	Se cuenta con los canales de comunicación de eventos de seguridad de la información.
		16.1.3 Notificación de puntos débiles de la seguridad.	100%	Se cuenta con canales de comunicación para notificación de vulnerabilidades de seguridad.
		16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	100%	Se clasifican los incidentes de seguridad in situ.
		16.1.5 Respuesta a los incidentes de seguridad.	0%	No se cuenta con procedimientos documentados para respuesta a incidentes de seguridad.
		16.1.6 Aprendizaje de los incidentes de seguridad de la información.	0%	No se documentan las resoluciones de incidentes de seguridad.
		16.1.7 Recopilación de evidencias.	50%	Se identifican, recopilan, adquieren y preservan información que pueda servir de evidencia de un ataque a la seguridad de la información en servidores.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO				
	17.1 Continuidad de la seguridad de la información.			
		17.1.1 Planificación de la continuidad de la seguridad de la información.	0%	No se cuenta con requisitos para la seguridad de la información y su gestión durante situaciones adversas tales como crisis y desastres.
		17.1.2 Implantación de la continuidad de la seguridad de la información.	0%	No se cuenta con un plan de recuperación para el mantenimiento del nivel necesario de seguridad en situaciones adversas.
		17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	0%	No se cuenta con controles a evaluar para la continuidad de la seguridad de la información.
	17.2 Redundancias.			

DOMINIO, OBJETIVOS DE CONTROL Y CONTROLES			ESTADO	OBSERVACIONES
		17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	50%	Se cuenta con redundancia en servidores pero no en instalaciones de procesamiento de información y en correspondencia con los requisitos de disponibilidad.
18. CUMPLIMIENTO.				
	18.1 Cumplimiento de los requisitos legales y contractuales.			
		18.1.1 Identificación de la legislación aplicable.	25%	No se cuenta con la información respecto a la legislación aplicable, ni la normativa acerca de seguridad de la información, solo se trabaja el tema de habeas data.
		18.1.2 Derechos de propiedad intelectual (DPI).	50%	No se cuenta con procedimientos para el cumplimiento de los requisitos de salvaguarda de los derechos de propiedad intelectual, pero se cuenta con políticas en los equipos que no permitan instalar software sin autorización.
		18.1.3 Protección de los registros de la organización.	0%	No se cuanta con actividades para salvaguardar los registros contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados.
		18.1.4 Protección de datos y privacidad de la información personal.	0%	No se cuenta con procedimientos para salvaguardar la información personal de acuerdo a la ley.
		18.1.5 Regulación de los controles criptográficos.	0%	No se regulan los controles criptográficos.
	18.2 Revisiones de la seguridad de la información.			
		18.2.1 Revisión independiente de la seguridad de la información.	0%	La Universidad no realiza revisiones independientes en intervalos planificados o cuando se realicen cambios significativos.
		18.2.2 Cumplimiento de las políticas y normas de seguridad.	0%	No se cuenta con políticas y normas de seguridad a ser revisadas por la gerencia.

DOMINIO, OBJETIVOS DE CONTROL Y CONTROLES			ESTADO	OBSERVACIONES
		18.2.3 Comprobación del cumplimiento.	0%	No se cuenta con políticas y normas de seguridad para garantizar su cumplimiento.

Tabla 20 Dominios, Objetivos de control y controles ISO/IEC 27002:2013

Sintetizando la información obtenida acerca del estado de los controles se obtiene que:

DOMINIO	CONTROLES	SIN IMPLEMENTAR	PARCIALMENTE IMPLEMENTADO	IMPLEMENTADO	PORCENTAJE DE IMPLEMENTACIÓN
5. POLÍTICAS DE SEGURIDAD	**2**	2			0%
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	**7**	7			0%
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	**6**	5	1		3,3%
8. GESTIÓN DE ACTIVOS	**10**	7	2	1	19,85%
9. CONTROL DE ACCESO	**14**	6	6	2	45,83%
10.CIFRADO	**2**	1	1	0	5%
11. SEGURIDAD FÍSICA Y AMBIENTAL	**15**	4	7	4	41.53%
12. SEGURIDAD EN LA OPERATIVA	**14**	2	6	6	53.75%
13. SEGURIDAD EN LAS TELECOMUNICACIONES	**7**	1	2	4	75,8%
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	**13**	6	4	3	22,22%

DOMINIO	CONTROLES	SIN IMPLEMENTAR	PARCIALMENTE IMPLEMENTADO	IMPLEMENTADO	PORCENTAJE DE IMPLEMENTACIÓN
15. RELACIONES CON PROVEEDORES	**5**	3	0	2	41,67%
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	**7**	2	1	4	64,24%
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	**4**	3	1	0	25%
18. CUMPLIMIENTO	**8**	6	2	0	6,25%
TOTAL	**114**	**55**	**33**	**26**	**22,47%**

Tabla 21. Síntesis de cumplimiento de Dominios, Objetivos de control y controles ISO/IEC 27002:2013

ANEXO 3. ORGANIGRAMA DE LA UNIVERSIDAD

Este documento ha sido eliminado por petición de la Universidad

Figura 18. Organigrama de una universidad colombiana

ANEXO 4. PROPUESTA DE POLÍTICA DE SEGURIDAD DE UNA UNIVERSIDAD COLOMBIANA

Este documento fue eliminado por petición de la Universidad

ANEXO 6. INDICADORES DE GESTIÓN PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE UNA UNIVERSIDAD COLOMBIANA

Este documento fue eliminado por petición de la Universidad

ANEXO 7. GESTIÓN DE ROLES Y RESPONSABILIDADES

Este documento fue eliminado por petición de la Universidad

ANEXO 8. DECLARACIÓN DE APLICABILIDAD DEL SGSI

Este documento fue eliminado por petición de la Universidad

ANEXO 9: CÁLCULO DEL IMPACTO POTENCIAL

CAT.	ID. ACTIVO	VALOR	CRITICIDAD					DEGRADACION (%)					IMPACTO POTENCIAL				
			C	I	D	A	T	C	I	D	A	T	C	I	D	A	T
[I] Información	[I_estudiante]	Alto	9	9	7	10	9	0,75	1	0,5	0	0	6,8	9	3,5	0	0
	[I_PEI]	Medio	1	4	9			0,25	0,5	0,1	0	0	0,3	2	0,9	0	0
	[I_PEP]	Medio	1	4	9			0,25	0,5	0,1	0	0	0,3	2	0,9	0	0
	[I_notas]	Muy alto	10	9	7	10	10	0,75	1	0,5	0	0	7,5	9	3,5	0	0
	[I_aspirante]	Alto	8	7	7		4	0,75	1	0,5	0	0	6	7	3,5	0	0
	[I_desercion]	Medio	6	4	8	4	4	0,75	1	0,5	0	0	4,5	4	4	0	0
	[I_micros]	Medio	2	6	9			0,25	0,5	0,1	0	0	0,5	3	0,9	0	0
	[I_personal]	Muy alto	9	9	10	9	9	0,75	1	0,5	0	0	6,8	9	5	0	0
	[I_docente]	Muy alto	9	9	10	9	9	0,75	1	0,5	0	0	6,8	9	5	0	0
	[I_adm]	Muy alto	9	9	10	9	9	0,75	1	0,5	0	0	6,8	9	5	0	0
	[I_estudianteper]	Muy alto	9	9	10	9	9	0,75	1	0,5	0	0	6,8	9	5	0	0

CAT.	ID. ACTIVO	VALOR	CRITICIDAD					DEGRADACION (%)					IMPACTO POTENCIAL				
			C	I	D	A	T	C	I	D	A	T	C	I	D	A	T
[S] Servicios	[SI_internet]	Alto	7	8	10	5	7	0,5	0,2	1	1	0	3,5	1,6	10	5	0
	[SI_www_aulas]	Alto	7	8	7	5	8	0,2	0,2	1	0,5	0	1,4	1,6	7	2,5	0
	[SI_www_atenea]	Alto	7	8	7	5	8	0,2	0,2	1	0,5	0	1,4	1,6	7	2,5	0
	[SI_correo]	Muy alto	10	9	10	9	10	0,2	0,2	1	0,5	0	2	1,8	10	4,5	0
	[SI_www_]	Alto	7	8	10	9	9	0,2	0,2	1	0,5	0	1,4	1,6	10	4,5	0
[D] Datos	[D_config]	Muy alto	9	9	9	9	9	1	0,5	0,5	1	0	9	4,5	4,5	9	0
	[D_backups]	Alto	3	8	6	8	8	1	0,5	0,5	1	0	3	4	3	8	0
	[D_pass]	Alto	10	10	10	2	9	0,5	0	0	1	0	5	0	0	2	0
	[D_acl]	Medio	5	4	4	5	4	1	0,5	0,5	1	0	5	2	2	5	0
	[D_log]	Medio	5	2	5	1	8	1	0,5	0,5	1	0	5	1	2,5	1	0
[Soft] Software	[Soft_SISTENOTAS]	Muy alto	10	10	10	9	10	1	1	1	1	0	10	10	10	9	0

CAT.	ID. ACTIVO	VALOR	CRITICIDAD					DEGRADACION (%)					IMPACTO POTENCIAL				
			C	I	D	A	T	C	I	D	A	T	C	I	D	A	T
	[Soft_Moodle]	Alto	8	8	9	8	8	1	1	1	1	0	8	8	9	8	0
	[Soft_people]	Muy alto	9	7	10	9	10	1	1	1	1	0	9	7	10	9	0
	[Soft_glpi]	Alto	5	2	8	9	9	1	1	1	1	0	5	2	8	9	0
	[Soft_nomina]	Muy alto	10	8	10	9	9	1	1	1	1	0	10	8	10	9	0
	[Soft_antivirus]	Muy alto	9	9	9	9	9	1	1	1	1	0	9	9	9	9	0
	[Soft_pm]	Alto	6	5	10	5	5	1	1	1	1	0	6	5	10	5	0
	[Soft_so]	Muy alto	9	9	10	9	10	1	1	1	1	0	9	9	10	9	0
	[Soft_office]	Medio	5	5	4	5	5	1	1	1	1	0	5	5	4	5	0
	[Soft_navegador]	Medio	4	4	4	4	4	1	1	1	1	0	4	4	4	4	0
	[Soft_correo]	Medio	9	2	5	4	4	1	1	1	1	0	9	2	5	4	0
	[Soft_autocad]	Medio	4	5	5	5	5	1	1	1	1	0	4	5	5	5	0
[Hard] Hardware	[Hard_ap]	Alto			8	5	6	1	0,5	1	0	0	0	0	8	0	0
	[Hard_firewall]	Alto			8	5	8	1	0,5	1	0	0	0	0	8	0	0
	[Hard_impresora]	Medio			3	5	5	1	0,5	1	0	0	0	0	3	0	0
	[Hard_pbx]	Medio			9	2	2	1	0,5	1	0	0	0	0	9	0	0
	[Hard_pc]	Alto			7	5	6	1	0,5	1	0	0	0	0	7	0	0
	[Hard_portatil]	Medio			6	5	6	1	0,5	1	0	0	0	0	6	0	0
	[Hard_router]	Alto			9	5	8	1	0,5	1	0	0	0	0	9	0	0
	[Hard_scanner]	Medio			5	3	3	1	0,5	1	0	0	0	0	5	0	0
	[Hard_servidor]	Muy alto			10	9	9	1	0,5	1	0	0	0	0	10	0	0

CAT.	ID. ACTIVO	VALOR	CRITICIDAD					DEGRADACION (%)					IMPACTO POTENCIAL				
			C	I	D	A	T	C	I	D	A	T	C	I	D	A	T
	[Hard_switch]	Medio			4	5	5	1	0,5	1	0	0	0	0	4	0	0
[Alm] Disp. de alm.	[Alm_cinta]	Alto			8			1	0,5	1	0	0	0	0	8	0	0
	[Alm_discos]	Alto			8			1	0,5	1	0	0	0	0	8	0	0
	[Alm_usb]	Alto			8			1	0,5	1	0	0	0	0	8	0	0
[Aux] Equipamiento auxiliar	[Aux_cableado]	Muy alto			9			0,5	0,5	1	0	0	0	0	9	0	0
	[Aux_gabinete]	Muy alto			9			0,5	0,5	1	0	0	0	0	9	0	0
	[Aux_ups]	Alto			8			0,5	0,5	1	0	0	0	0	8	0	0
	[Aux_ventilación]	Muy alto			9			0,5	0,5	1	0	0	0	0	9	0	0
[Com] Redes de comunicaciones	[Com_inalámbrica]	Alto	7	9	7	7	7	0,5	0,2	1	1	0	3,5	1,8	7	7	0
	[Com_internet]	Muy alto	9	9	9	9	9	0,5	0,2	1	1	0	4,5	1,8	9	9	0
	[Com_LAN]	Alto	10	8	10	5	8	0,5	0,2	1	1	0	5	1,6	10	5	0
	[Com_telefónica] Red telefónica	Medio	3	1	6	5	2	0,5	0,2	1	1	0	1,5	0,2	6	5	0
[Inst] Instalaciones	[Inst_oficina]	Medio	7	0	9			0,5	0,5	1	0	0	3,5	0	9	0	0
	[Inst_edificio]	Medio	4	0	7		3	0,5	0,5	1	0	0	2	0	7	0	0

CAT.	ID. ACTIVO	VALOR	CRITICIDAD					DEGRADACION (%)					IMPACTO POTENCIAL				
			C	I	D	A	T	C	I	D	A	T	C	I	D	A	T
[P] Personas	[P_admred]	Ext alto			10			0,2	0,2	1	0	0	0	0	10	0	0
	[P_admserv]	Ext alto			10			0,2	0,2	1	0	0	0	0	10	0	0
	[P_admapl]	Muy alto			9			0,2	0,2	1	0	0	0	0	9	0	0
	[P_softw]	Medio			4			0,2	0,2	1	0	0	0	0	4	0	0
	[P_soporte]	Alto			6			0,2	0,2	1	0	0	0	0	6	0	0
	[P_vicerrector]	Medio			4			0,5	0,2	1	0	0	0	0	4	0	0
	[P_coord]	Medio			4			0,5	0,2	1	0	0	0	0	4	0	0
	[P_asistente]	Medio			3			0,5	0,1	1	0	0	0	0	3	0	0
	[P_gestionh]	Alto			6			0,5	0,2	1	0	0	0	0	6	0	0
	[P_docente]	Medio			5			0,5	0,1	1	0	0	0	0	5	0	0

Tabla 22. Cálculo del Impacto potencial total por activo

ANEXO 10: NIVELES DE MADUREZ DEL SGSI DE UNA UNIVERSIDAD COLOMBIANA

Este documento fue eliminado por petición de la Universidad

ANEXO 11: INFORME DE AUDITORÍA

Este documento fue eliminado por petición de la Universidad

BIBLIOGRAFÍA

Alejandro Corletti, C. A. (2008). Métricas de seguridad, indicadores y cuadros de mando. *Normas y Estándares*, 138-141.

Comité de Planeación. Universidad Colombiana. (2011). *PLAN DE DESARROLLO ECCI "Camino a la Universidad que soñamos"*. Bogotá: ECCI.

Consejo Superior de Administración Electrónica de España. (2012). *MAGERIT - versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de hacienda y Administraciones Públicas.

Instituto Colombiano de Normas Técnicas y Certificación. ICONTEC. (2013). *Norma técnica ISO 27001* . Bogotá: ICONTEC.

Instituto Colombiano de Normas Técnicas y Certificación. ICONTEC. (2015). *Guía Técnica Colombiana de GTC-ISO/IEC 27002.* Bogotá: ICONTEC.

Instituto Colombiano de Normas Técnicas, ICONTEC. (2011). *Norma Internacional ISO 19011: 2011. Directrices para la auditoría de Sistemas de Gestión.* Bogotá: ICONTEC.

MAGERIT - versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información. Libro II. Catálogo de elementos. (2012). Madrid: Ministerio de Hacienda y Administración Pública.

Manual del Sistema de Gestión de la Calidad. Diseño y Desarrollo de programas académicos y Prestación del Servicio de Educación Superior. (2013. Versión 5.0). Bogotá.

Mary Beth Chrissis, M. K. (2009). *CMMI: Guía para la integración de procesos y la mejora de productos. 3rd Edición.* Pearson Education.

MInisterio de Tecnologías de la Información y Comunicación - MINTIC. (2015). *Guía de indicadores de gestión de seguridad de la información.* Bogotá: MINTIC.

Ministerio de Tecnologías de la Información y Comunicación - MINTIC. (2016). *Guía de gestión de riesgos.* Bogotá.

Wikipedia. (s.f.). Obtenido de https://es.wikipedia.org/wiki/ISO/IEC_27000-series