UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja
Máster universitario en Seguridad Informática

[METODOLOGÍA PARA LA IMPLEMENTACIÓN DE UN SGSI EN LA FUNDACIÓN UNIVERSITARIA JUAN DE CASTELLANOS, BAJO LA NORMA ISO 27001:2005]

Trabajo Fin de Máster

Presentado por: Alemán Novoa, Helena Clara Isabel

Director/a: Martínez Herráiz, José

Ciudad: Tunja
Fecha: 20 de febrero de 2015

CONTENIDO

Lista de figuras

Lista de Tablas

INTRODUCCIÓN

Las tecnologías de la información y las comunicaciones han dotado al mundo actual de un sin número de posibilidades que le permiten al ser humano gozar de comodidad y rapidez en sus procesos cotidianos; sin embargo, a raíz de estos adelantes tecnológicos también surge la necesidad de proteger y salvaguardar los sistemas informáticos en su conjunto: software, hardware y datos, de amenazas que impidan su correcto funcionamiento y puedan afectar la integridad, disponibilidad y confidencialidad de la información.

Las organizaciones han colocado un sin número de mecanismos y medidas de seguridad para proteger sus activos informáticos, siendo estos insuficientes para llegar a cumplir con sus metas de seguridad, por tanto, la legislación y la comunidad internacional se han unido para generar normas y estándares en cuanto a seguridad informática, estableciendo parámetros para evaluar, medir, prevenir, mitigar y corregir los riesgos que pueden provocar pérdida del negocio, daños en la imagen corporativa, sanciones legales y hasta cierre de una empresa.

Los SGSI (Sistemas de Gestión de Seguridad Informática) son una herramienta corporativa que permiten establecer un plan de acción para la solución de problemas de seguridad a nivel técnico, organizativo y legislativo, mediante el uso de estrategias como el análisis de riesgos, el mejoramiento y mantenimiento de la seguridad de la información, y garantizando la continuidad de negocio.

La implementación de un SGSI se encuentra determinada por la estructura organizacional de las instituciones, lo cual abarca características como: tipo, tamaño, objetivos, servicios, procesos, personal y requerimientos de seguridad que establece la misma, para lo cual se apoya en estándares internacionales tales como ISO/IEC 27001.

Algunos de los tipos de instituciones que requieren la implementación de un SGSI son las Universidades de carácter privado, a fin de medir los niveles de riesgo, identificando amenazas, vulnerabilidades e impactos en sus actividades organizacionales, para lo cual se requiere el diseño de una metodología que les permita identificar su estado actual en cuanto a seguridad informática y realizar el alistamiento para implementar su propio SGSI y a su vez complementar sus procesos de certificación de calidad ISO 91001.

1.1 Justificación

Las instituciones universitarias de carácter privado, al igual que cualquier organización, manejan información sensible de gran importancia para el cumplimiento de sus metas y objetivos misionales, tal es el caso del proceso y almacenamiento de datos de estudiantes, docentes y administrativos, al igual que instalaciones, aplicaciones y equipos tecnológicos que requieren ser protegidos para permitir la integridad disponibilidad y autenticidad de la información.

Los cambios tecnológicos a los que están expuestas las instituciones universitarias también hacen necesaria la aplicación de un SGSI, que facilite su adaptabilidad dentro de un contexto de mercado competitivo, lo cual solo se puede aplicar mediante la identificación, valoración y evaluación de sus activos, riegos y vulnerabilidades a los que se encuentran expuestas dentro de sus pilares de actuación: academia, docencia y extensión.

Actualmente, la Fundación Universitaria Juan de Castellanos no posee una metodología que permita integrar y organizar de manera cíclica los requisitos para la implementación de un SGSI, lo cual se podrá integrar con los procesos de aplicación del Sistema de Gestión de Calidad bajo la norma ISO 9001: 2008 y certificación Institucional en la que se encuentra.

La importancia de la metodología planteada radica en que se establecerán los pasos a seguir para la implementación de un SGSI en la Fundación Universitaria Juan de Castellanos que servirá como base para otras Universidades de carácter privado, que permita dar a conocer los requisitos y estrategias para su acople y mejora continua, estableciendo un marco de gestión de la seguridad basado en del estándar ISO 27001 internacionalmente reconocido.

1.2 Objetivos

1.2.1 Objetivo general

Establecer una metodología para la implementación de un SGSI en la Fundación Universitaria Juan de Castellanos, teniendo como base el estándar ISO 27001.

1.2.2 Objetivos específicos

- ✓ Determinar los parámetros y lineamientos que se deben tener en cuenta para la implementación de un SGSI, basado en la norma ISO 27001:2005 en una organización.
- ✓ Analizar la estructura organizacional y características principales de la Fundación Universitaria Juan de Castellanos, para posteriormente proponer una metodología que permita gestionar la seguridad informática.
- ✓ Diseñar una metodología para la implementación y mantenimiento de un SGSI, norma ISO 27001, en la Fundación Universitaria Juan de Castellanos, teniendo en cuenta las fases de planificación, implementación, revisión, mantenimiento y mejora.
- ✓ Recomendar algunas herramientas que faciliten la implementación del SGSI en cada una de las etapas propuestas por la norma ISO 27001:2005.

2 MARCO TEÓRICO

La seguridad informática se encuentra regulada por un compendio de normas que permiten implementar mecanismos de seguridad para salvaguardar los activos que tienen que ver con los sistemas informáticos, una de ellas es el estándar ISO 27001, donde se describen los lineamientos de seguridad que deben tener las organizaciones para garantizar la confidencialidad, autenticidad e integridad de la información.

2.1 SGSI

Según la norma UNE – ISO/IEC 27001, es una parte del sistema de gestión general, basada en un enfoque de riego empresarial, que se establece para crear, implementar, operar, supervisar, mantener y mejorar la seguridad de la información, permitiendo el control sobre los sistemas de información y la información que se maneja en la organización.

Algunos de los beneficios que aporta un SGSI son:

- ✓ Conocimiento profundo a cerca de la organización, cómo funciona y a su vez proporciona un plan de mejoramiento continuo para solucionar las posibles inconsistencias de seguridad informática presentadas.
- ✓ Analizar los riesgos, identificando amenazas, vulnerabilidades y su impacto dentro de las actividades de la organización.
- ✓ Generar y aplicar planes de mejoramiento continuo en la gestión de la seguridad informática.
- ✓ Garantizar la continuidad y disponibilidad del negocio.
- ✓ Reducir los costos vinculados a los incidentes presentados.
- ✓ Incrementar los niveles de confianza de los clientes y usuarios de los sistemas informáticos.
- ✓ Aumentar el valor comercial de los productos ofrecidos y mejorar la imagen corporativa de la empresa.
- ✓ Cumplir con la legislación nacional e internacional establecida en cuanto a protección de datos sensibles, comercio electrónico, propiedad intelectual, entre otras, relacionadas con la seguridad de la información.

2.1.1 Proceso de implementación de un SGSI

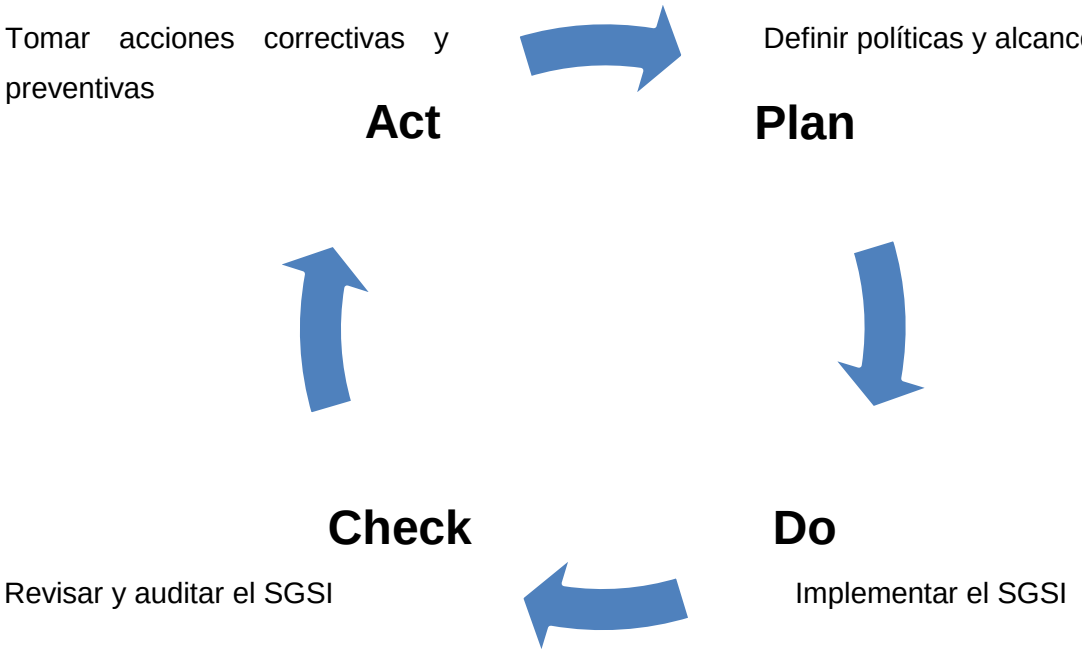
Para establecer y gestionar un SGSI se utiliza el ciclo PDCA (Plan, Do, Check, Act), en español planear, hacer, chequear y actuar, esta metodología se puede aplicar a todos los procesos del SGSI y permite establecer una mejora continua en toda clase de organizaciones.

Las fases del modelo PDCA corresponden con una serie de acciones que permiten establecer un modelo de indicadores y métricas evaluables en un periodo de tiempo específico de tal manera que se pueda valorar el avance de los planes de mejoramiento propuestos por la organización.

Según Gómez Fernández (2012, p.14) en su libro Guía de Aplicación de la Norma UNE-ISO/IEC 27001, las fases del modelo PDCA incluirían las siguientes actividades:

- ✓ **PLAN:** En esta fase se planifica, diseña y establece el SGSI, sistematizando las políticas que se van a aplicar en la organización, se establecen los fines a alcanzar y su correspondencia con los objetivos de negocio, los medios que se utilizarán para ello, los procesos de negocio y los activos que lo soportan, cómo se orientará el análisis de riesgos y los criterios que se seguirán para gestionar las contingencias de modo coherente con las políticas y objetivos de seguridad.
- ✓ **Do:** Es la fase en el que se implementa y pone en funcionamiento el SGSI. Las políticas y los controles escogidos para cumplirlas se implementan mediante recursos técnicos, procedimientos o ambas cosas a la vez, y se asignan responsables a cada tarea para comenzarlas según las instrucciones.
- ✓ **Check:** esta fase es la de monitorización y revisión del SGSI. Hay que controlar que los procesos se ejecutan como se ha establecido, de manera eficaz y eficiente, alcanzando los objetivos definidos para ello. Además, hay que verificar el grado de cumplimiento de las políticas y procedimientos, identificando los fallos que pudieran existir y su origen, mediante revisiones y auditorías.
- ✓ **Act:** Es la fase en la que se mantiene y mejora el SGSI, decidiendo y efectuando las acciones preventivas y correctivas necesarias para rectificar los fallos, detectados en las auditorías internas y revisión del SGSI, o cualquier otra información relevante para permitir la mejora permanente del SGSI.

Figura 1. Ciclo PDCA ISO 27001:2005



Fuente: Norma ISO 27001: 2005

2.2 ISO

International Organization for Standardization (Organización Internacional de Normalización).

2.3 ISO 27001

Norma publicada el 15 de octubre de 2005, con algunas actualizaciones realizadas en 2013, Es la primera del estándar ISO 27000 y la norma principal de la familia, ya contiene los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI) y su auditoría, además de un compendio de recomendaciones y buenas prácticas descritas en la ISO 27002. Por su naturaleza es un estándar internacional que abarca todas las organizaciones y es la única que tiene certificación por parte de los auditores externos de los SGSI. Este estándar se basa en el mencionado modelo PDCA (Plan-Do-Check-Act), ciclo de mejora continua que consiste en planificar, desarrollar, comprobar y actuar en relación con lo detectado al efectuar las comprobaciones.

2.3.1 Dominios de la Norma ISO 27001

2.3.1.1 Política de seguridad

Estipular las políticas con respecto a la seguridad de la información siguiendo los lineamientos dados por ISO 27001/17799.

2.3.1.2 Organización de la seguridad

Gestionar la seguridad de la información teniendo en cuenta roles, compromisos, autorizaciones, acuerdos, manejo con terceros, etc.

2.3.1.3 Gestión de activos

Se relaciona con el mantenimiento y protección apropiados de todos los activos de información.

2.3.1.4 Seguridad del Recurso Humano

Busca asegurar que empleados, contratistas y terceros entiendan sus responsabilidades y sean adecuados de acuerdo con el rol de desempeño, permitiendo minimizar los riesgos relacionados con personal.

2.3.1.5 Seguridad Física y del entorno

Prevenir accesos físicos no autorizados dentro del contexto de actuación de la organización, daños o interferencias a las instalaciones y a su información.

2.3.1.6 Gestión de comunicaciones y operaciones

Garantizar la correcta y segura operación de las áreas de procesamiento de información, dentro de las cuales están las actividades operativas y concernientes a la plataforma tecnológica de los sistemas informáticos.

2.3.1.7 Control de acceso

Realizar el control físico o lógico de los accesos a los activos de la información.

2.3.1.8 Adquisición, desarrollo y mantenimiento de sistemas de información:

Asegurar la inclusión de todos los controles de seguridad en los sistemas de información nuevos o en funcionamiento, dentro de los cuales está la infraestructura, aplicaciones, servicios, etc. También regula la adquisición de software para la organización y los contratos de soporte y mantenimiento asociados a ellos.

2.3.1.9 Gestión de incidentes de seguridad

Permitir que los eventos de seguridad de la información y las debilidades asociadas con los sistemas de información, sean comunicados de tal manera que se tome una acción correctiva adecuada y en el momento indicado.

2.3.1.10 Gestión de la continuidad del negocio

Enfocado en reaccionar en contra de interrupciones a las actividades de la función misional de la empresa y en proteger los procesos críticos contra fallas mayores en los sistemas de información o desastres y, por otro lado, asegurar que se recuperen a tiempo.

2.3.1.11 Cumplimiento

Busca prevenir el incumplimiento total o parcial de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.

2.4 ISO 27002

Corresponde a una serie de recomendaciones y guías de buenas prácticas para el mejoramiento de la seguridad de las organizaciones, define una serie de objetivos de control y gestión, los cuales se encuentran incluidos dentro de los mismos dominios descritos en la ISO 27001. La diferencia entre estas dos normas es que la única certificable es la ISO 27001.

Los objetivos de control y los controles de la norma ISO 27002 sirven de guía para el desarrollo de políticas de seguridad internas y la implementación de prácticas efectivas de gestión de la seguridad en las organizaciones. Estos objetivos de control están sujetos a un análisis de riesgos previo y los niveles de control se determinarán de acuerdo con los requisitos de seguridad identificados y a los recursos dispuestos para tal fin por parte de la administración.

2.5 ISO 27005

Según Moreno (2009, p. 28), esta norma establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Esta norma apoya el desarrollo de uno de los requisitos base para la implementación de la ISO 27001:2005 y el cumplimiento de otros como es la “valoración de los riesgos” que incluye la identificación, análisis, evaluación y tratamiento de los riesgos en la seguridad de la información.

Adicionalmente, brinda soporte y conceptos generales que se especifican en la norma ISO 27001, y está diseñada con el objetivo de facilitar la implementación de la seguridad de la información, con base en el enfoque de gestión de riesgo.

2.6 Seguridad de la información

(Information Security) Se refiere a la confidencialidad, integridad y disponibilidad de la información, independientemente del medio en que se almacenen o procesen los datos, además, también puede involucrar otras propiedades como autenticación, responsabilidad y el no repudio.

- ✓ **Integridad:** según la norma ISO/IEC 13335, es la propiedad de salvaguardar la exactitud y completitud de los activos.
- ✓ **Confidencialidad:** se refiere según la norma ISO/IEC 13335 a la propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados.
- ✓ **Disponibilidad:** propiedad de la información de ser accesible y utilizable por una entidad autorizada (ISO/IEC 13335).

De manera general, en una Institución Universitaria o en cualquier tipo de organización se pueden presentar amenazas tales como:

- ✓ Internas
- ✓ Externas
- ✓ Naturales

2.7 Información institucional Fundación Universitaria Juan de Castellanos

2.7.1 Misión

La Fundación Universitaria Juan de Castellanos se compromete con la investigación científica y la transmisión pedagógica del conocimiento en la búsqueda de la verdad; se desempeña en la formación integral del hombre, de acuerdo con los ideales cristianos expresados en los siguientes valores: Vida y Amor, Fe y Esperanza, Verdad y Belleza, Responsabilidad y Libertad, Justicia y Trabajo; emplea metodologías pedagógicas apropiadas a los beneficiarios de sus programas extensión, formación técnica, tecnológica, profesional y posgraduada, para que por la "Civilización del Amor", todos sus miembros participen en la pastoral católica e investiguen en ciencias básicas, aplicadas, sociales y humanas al servicio del bien común. (Fundación Universitaria Juan de Castellanos, 2012, Horizonte Institucional).

2.7.2 Visión

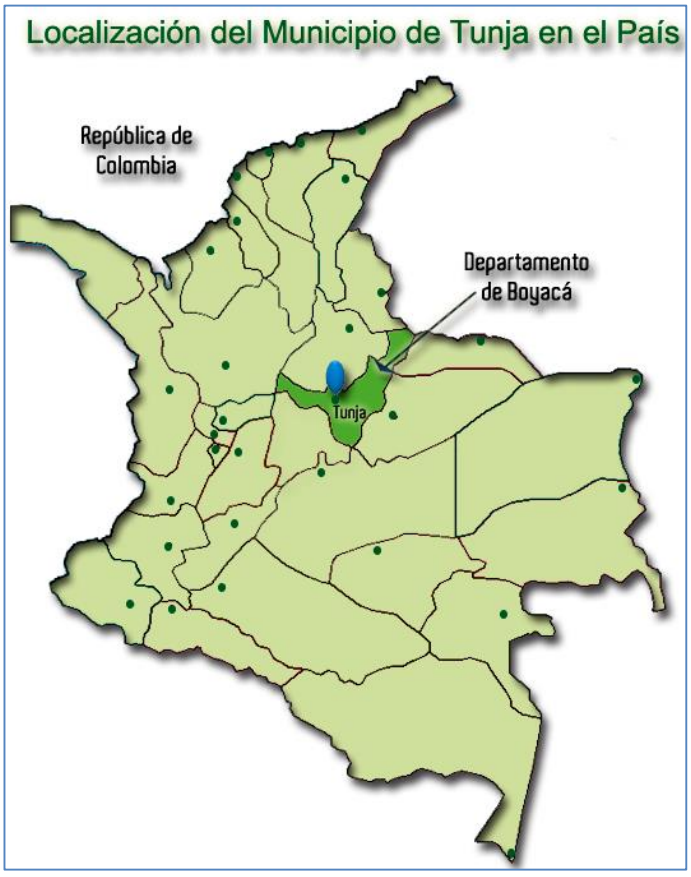
La FUJC, en el año 2019, se consolidará como una Institución de excelencia académica e investigativa, de liderazgo y calidad por la amplia cobertura de sus programas, aportando soluciones a la región y al país, con programas acreditados de Alta Calidad y estudios

avanzados en Maestrías. Abrirá la posibilidad del intercambio nacional e internacional, con fin de estimular el espíritu emprendedor e innovador a partir de las iniciativas de los estudiantes. Detectará las potencialidades para la creación de empresas de base tecnológica que permitan el crecimiento y la consolidación de propuestas competitivas que contribuyan al crecimiento y desarrollo socioeconómico de la Región y el País. (Fundación Universitaria Juan de Castellanos, 2012, Horizonte Institucional).

2.7.3 Descripción general

La Fundación Universitaria Juan de Castellanos se encuentra ubicada en la ciudad de Tunja, departamento de Boyacá – Colombia.

Figura 2. Mapa ubicación Fundación Universitaria Juan de Castellanos



Fuente: www.tunja-boyaca.gov.co

2.7.4 Facultades

La Fundación Universitaria Juan de Castellanos es una institución de Educación Superior de carácter privado, actualmente ofrece los siguientes programas de pregrado y posgrado en sus diferentes Facultades:

- ✓ **Facultad de Ingeniería:** Ingeniería Electrónica, Ingeniería de Sistemas, Ingeniería de Telecomunicaciones.
- ✓ **Facultad de Ciencias de la Educación**: Licenciatura en Educación Física, Recreación y Deporte, Licenciatura en Ciencias Religiosas y Ética. Programas de Posgrado: Especialización en Informática Educativa, Especialización en Ética y Pedagogía, Especialización en Lúdica Educativa, Especialización en Planeación Educativa, Especialización en Educación e Intervención para la Primera Infancia.
- ✓ **Facultad de Ciencias Agrarias:** Medicina Veterinaria, Ingeniería Agropecuaria, Zootecnia.
- ✓ **Facultad de Ciencias Jurídicas y Políticas Internacionales:** Derecho.
- ✓ **Facultad de Ciencias Sociales y Económicas:** Trabajo Social, Contaduría Pública, Administración Turística y Hotelera.

Igualmente se encuentra compuesta por las siguientes Unidades de apoyo académico:

2.7.5 Unidades de apoyo académico

- ✓ Unidad de Bienestar universitario
- ✓ Biblioteca e información científica
- ✓ Instituto de Investigaciones
- ✓ Registro y control académico
- ✓ Extensión Universitaria
- ✓ Instituto de Lenguas
- ✓ Unidad y Asesoría de sostenimiento tecnológico
- ✓ Oficina de Talento Humano
- ✓ Unidad de Comunicaciones
- ✓ Unidad financiera
- ✓ Recursos educativos
- ✓ Oficina de Tesorería y cartera
- ✓ Pastoral Universitaria
- ✓ Almacén
- ✓ Laboratorios
- ✓ Unidad Editorial

La Fundación Universitaria en su estructura física cuenta con tres sedes y un campus universitario dotado de infraestructura tecnológica para el desarrollo de sus actividades misionales:

- ✓ Sede Álvaro Castillo
- ✓ Sede Crisanto Luque
- ✓ Sede Soracá
- ✓ Campus Universitario

2.8 Estructura organizacional**:**

La Fundación Universitaria Juan de Castellanos está liderada por el Consejo Superior y Rectoría y tiene dos áreas de control operacional: Vicerrectoría Académica y Vicerrectoría Administrativa y, estás a su vez, están conformadas por diferentes unidades administrativas y Facultades que trabajan en equipo para "la formación integral de futuros profesionales y el desarrollo del conocimiento y la investigación en bien de la sociedad".

Figura 3. Organigrama General Fundación Universitaria Juan de Castellanos.

Fuente: Fundación Universitaria Juan de Castellanos, (2012), Estructura Organizacional.

2.8.1 Mapa de procesos de la fundación universitaria Juan de Castellanos

El mapa de procesos se encuentra estructurado según el ciclo de Deming: Planear-Hacer-Verificar-Actuar PHVA, respondiendo a los principios de calidad definidos en las Normas ISO 9001 del Sistema de Gestión de Calidad es el resultado de la integración coherente de los procesos Estratégicos, Procesos Misionales, Procesos de Apoyo y Procesos de Evaluación y Control.

2.8.1.1 Procesos Estratégicos

Son aquellos que direcciona el Sistema de Gestión de la Calidad, permitiendo hacer control sobre los procesos del mismo. Entre estos procesos se encuentran:

- ✓ Direccionamiento Estratégico
- ✓ Gestión Tecnológica y Comunicaciones
- ✓ Relaciones Internacionales
- ✓ Gestión de la Calidad

*2.8.1.2 **Procesos Misionales**:*

Son aquellos que apuntan al cumplimento de la misión y visión de la Universidad, por lo cual son parte fundamental de la institución de educación superior como los son:

- ✓ Docencia
- ✓ Investigación
- ✓ Proyección social
- ✓ Bienestar Universitario

2.8.1.3 Procesos de Apoyo

Son los procesos necesarios para gestionar los recursos institucionales y que soportan el desarrollo de la institución, deben apoyar la gestión de los demás procesos del sistema para que la Gestión Universitaria cumpla con la política, la misión y la visión de la Universidad, entres estos procesos están:

- ✓ Gestión Documental
- ✓ Gestión de Bienes, Suministros y Servicios
- ✓ Gestión Financiera
- ✓ Gestión Jurídica
- ✓ Gestión del Talento Humano
- ✓ Gestión de Infraestructura
- ✓ Gestión de Matriculas

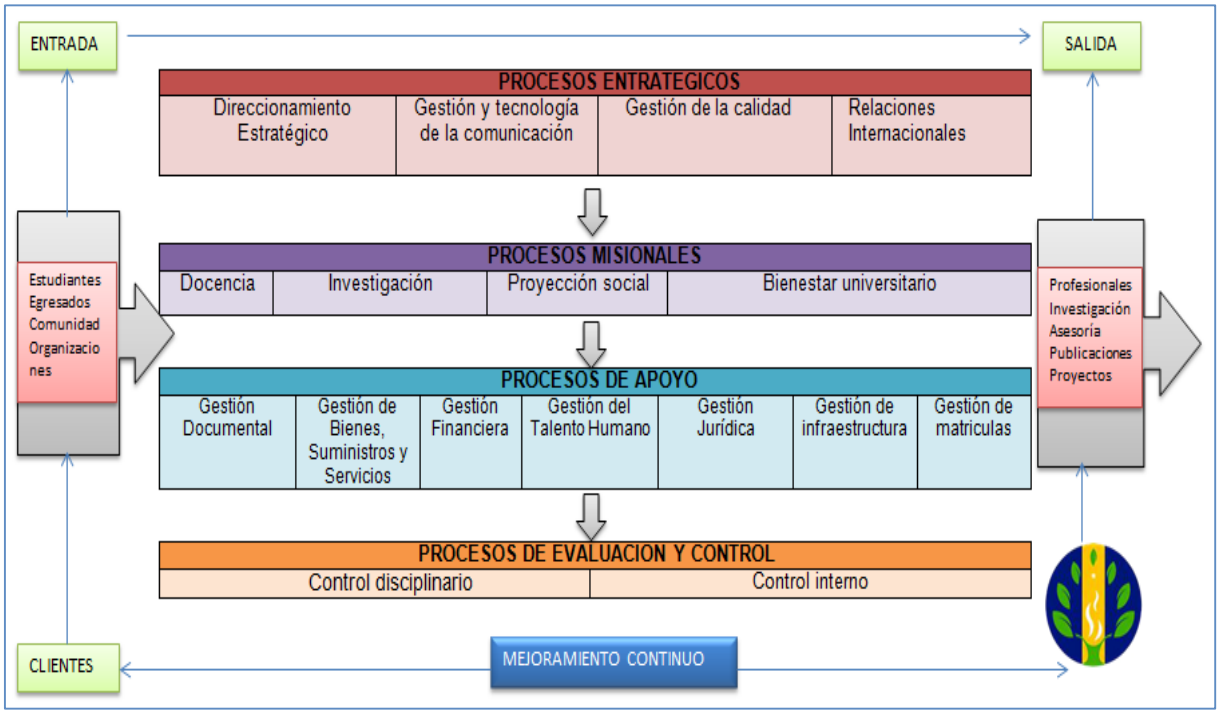
2.8.1.4 ***Procesos de Evaluación y Control***

Estos procesos son aquellos necesarios para medir y recopilar datos destinados a realizar el análisis del desempeño y la mejora de la eficacia y la eficiencia de la Institución y sus funcionarios, dichos procesos se mencionan a continuación:

- ✓ Control Disciplinario
- ✓ Control Interno

El mapa de procesos definido por la Fundación Universitaria Juan de Castellanos, integra sus 15 macro procesos (estratégicos, misionales, de apoyo y evaluación, y control) y su articulación dentro del Sistema de Gestión de Calidad, de acuerdo con los requisitos establecidos por la norma NTC ISO: 2008. En la siguiente figura podemos observar su relación:

Figura 4. Mapa de Procesos Fundación Universitaria Juan de Castellanos



Fuente: Fundación Universitaria Juan de Castellanos, (2012), mapa de procesos.

La Fundación Universitaria Juan de Castellanos tiene una cadena de valor que enmarca sus actividades enfocadas al servicio de los estudiantes, que junto con los procesos mencionados se articulan y serán el marco de referencia para la implementación del SGSI mediante la metodología planteada.

Figura 5. Cadena de Valor Fundación Universitaria Juan de Castellanos

Fuente: Alemán, (2015)

3 METODOLOGÍA PARA LA IMPLEMENTACIÓN DEL SGSI EN LA FUNDACIÓN UNIVERSITARIA JUAN DE CASTELLANOS

La metodología que se propone para la implementación del SGSI en la Fundación Universitaria Juan de Castellanos se basa en el ciclo de mejora continua PDCA (planear, hacer, verificar y actuar) de la norma ISO 27001.El siguiente cuadro relaciona cada una de las fases y sus actividades para la aplicación de la metodología propuesta:

Tabla 1. Fases y Actividades ciclo PDCA - SGSI

FASES CICLO PDCA	ACTIVIDADES
Planear	✓ Definir el alcance del SGSI ✓ Definir la política de seguridad ✓ Metodología para la evaluación de riesgos ✓ Inventario de Activos ✓ Identificar amenazas y vulnerabilidades ✓ Identificar el impacto ✓ Análisis y evaluación de riesgos ✓ Selección de Controles y SOA
Hacer	✓ Definir el plan de tratamiento de riesgos ✓ Implementar el plan de tratamiento de riesgos ✓ Implementar los controles ✓ Formar y concientizar ✓ Aplicar el SGSI
Verificar	✓ Revisar el SGSI ✓ Medir la eficacia de los controles ✓ Revisar los riesgos residuales ✓ Realizar auditorías internas del SGSI ✓ Registrar eventos y acciones
Actuar	✓ Implementar mejoras al SGSI ✓ Aplicar acciones correctivas ✓ Aplicar acciones preventivas ✓ Comprobar la eficacia de las acciones

3.1 Planear

3.1.1 Alcance del SGSI

La Fundación Universitaria Juan de Castellanos tendrá que definir el alcance del SGSI en función de sus características como Institución de Educación Superior, localización, activos y tecnología utilizada, se recomienda inicialmente limitar el alcance a los procesos fundamentales del negocio, donde se tenga la información más relevante de la Universidad, es decir, los que se han identificado en el mapa de procesos como misionales:

- ✓ Docencia
- ✓ Investigación
- ✓ Proyección social
- ✓ Bienestar Universitario

La Fundación Universitaria Juan de Castellanos podrá considerar la inclusión de cualquier otro proceso dentro del SGSI; sin embargo, se recomienda que esta decisión se base en un estudio y análisis que determinen la importancia de incluir dicho proceso para evitar realizar un SGSI fuera de contexto que no sea eficaz y efectivo, al contrario su simplicidad permitirá realizar una buena práctica, teniendo en cuenta que será el primer SGSI que se diseña para la Universidad.

El SGSI de la Fundación Universitaria Juan de Castellanos aplicará para los estudiantes, cuerpo académico, administrativos, contratistas, funcionarios de la Universidad, personal de apoyo y terceros no vinculados directamente a la Institución, que presten sus servicios y utilicen las tecnologías de información y las comunicaciones, los cuales se identificarán como "usuarios" para referirse a cualquiera de estas personas. El SGSI aplica para los activos informáticos, incluidos los equipos propios de la Universidad o arrendados y a los equipos de personas externas que sean conectados a la red de la Fundación Universitaria Juan de Castellanos, información que será contemplada y ampliada en la definición de la política del SGSI.

3.1.2 Política del SGSI

En este ítem se debe realizar la definición de la política del SGSI, la cual debe estar alineada con los objetivos, características, ubicación, activos y tecnología de la Fundación Universitaria Juan de Castellanos, la política debe estar aprobada por el Consejo Superior y se debe realizar su revisión periódicamente cada año. Los objetivos de control que se establecerán posteriormente estarán basados en el marco de referencia de la política del SGSI. Según el

estándar ISO 27001:2005, la política será un súper - conjunto de la política de seguridad de la información.

La política de seguridad es un documento que contiene reglas y principios para el logro de los objetivos de seguridad aplicados a los sistemas informáticos, su organización y buen uso. Estas políticas deben especificar las condiciones, derechos y obligaciones de cada uno de los miembros de la organización con respecto a la utilización de los sistemas informáticos, también deben llevar algunas de las siguientes especificaciones:

- ✓ Deben tener consignados los derechos, responsabilidades y sanciones con base en las normas legales, reglamentos administrativos y técnicos de la Universidad.
- ✓ Servir como soporte y mecanismo de control para definir el buen uso de los recursos institucionales y para dar apoyo a cualquier tipo de procedimiento legal que se pueda presentar.
- ✓ Se deben crear según las características misionales de la institución, recursos, usuarios y medios tecnológicos, entre otros.
- ✓ Deben ser un marco de referencia general de Seguridad Informática institucional.

Las políticas de seguridad generales que se deben tener en cuenta en la Fundación Universitaria Juan de Castellanos para la implementación del SGSI deben tener las siguientes características:

- ✓ **Confiabilidad.** Certificar que los sistemas informáticos brindan información correcta para ser utilizada en los procesos de la Institución.
- ✓ **Eficacia.** Garantizar que la información utilizada es necesaria y útil para el desarrollo de sus procesos y procedimientos.
- ✓ **Disponibilidad.** Garantizar el correcto almacenamiento, recuperación y acceso oportuno de la información, teniendo en cuenta su proceso manual o automático, de tal manera que no interrumpa el cumplimiento de los objetivos misionales y de negocio de la institución.
- ✓ **Eficiencia.** Asegurar que el procesamiento de la información se realice mediante una óptima utilización de los recursos humanos y materiales.
- ✓ **Integridad.** Garantizar que la información procesada es la necesaria y suficiente para el correcto funcionamiento y préstamo de los servicios en cada uno de los sistemas informáticos y procesos.
- ✓ **Exactitud.** Asegurar que la información se encuentra libre de errores y/o alteraciones.

- ✓ **Legalidad.** Certificar legalmente que toda la información y los medios físicos que la contienen, procesan y/o transportan, cumple con las normas locales, nacionales e internacionales vigentes para tal fin.
- ✓ **Confidencialidad.** Garantizar que toda la información se encuentra protegida del uso no autorizado, revelaciones accidentales, espionaje, violación de la privacidad y otras acciones similares de accesos de terceros no permitidos.
- ✓ **Propiedad.** Certificar los derechos de propiedad sobre la información utilizada para el desarrollo de los procesos y servicios ofrecidos por parte de la Institución.
- ✓ **Autorización.** Certificar que los accesos a la información y/o su proceso cumplan con los niveles de autorización correspondientes.
- ✓ **Protección Física.** Garantizar que todos los sistemas informáticos y medios de almacenamiento de la información cuentan con medidas de protección físicas que eviten el acceso y uso indebido por parte de personal no autorizado.

La política del SGSI para la Fundación Universitaria Juan de Castellanos debe tener en cuenta el marco legal que la define como Institución de Educación Superior y el cual se encuentra establecido mediante las siguientes normas:

- ✓ Ley 30 de 1992
- ✓ Estatuto general
- ✓ Proyecto Educativo Institucional P.E.I
- ✓ Proyecto Formativo del Programa
- ✓ Modelo Pedagógico o Educativo
- ✓ Norma ISO 9001: 2008
- ✓ Lineamientos para la acreditación institucional
- ✓ Lineamientos para la acreditación de programas de pregrado
- ✓ Lineamientos para la acreditación de programas de maestrías y doctorados
- ✓ Guía de procedimiento para la acreditación
- ✓ Plan de desarrollo prospectivo y estratégico
- ✓ Planes de mejoramiento
- ✓ Plan de compras
- ✓ Plan de inversiones
- ✓ Manual de procedimientos bibliotecarios
- ✓ Políticas nacionales de bienestar universitario
- ✓ Reglamento estudiantil
- ✓ Reglamento docente

- ✓ Decreto 3963 parámetros y criterios para la aplicación del Examen de Calidad de la Educación Superior.
- ✓ Decreto 1295 de 2010, Por el cual se reglamenta el registro calificado de que trata la Ley 1188 de 2008 y la oferta y desarrollo de programas académicos de educación superior.
- ✓ Decreto 1781 de 2003
- ✓ Ley 583 de 2000
- ✓ Decreto 2170 de 2005
- ✓ Decreto 2566 de 2003

Adicionalmente para la aplicación del SGSI se deben tener en cuenta las normas legales establecidas para la protección de la información:

- ✓ Ley 1266 del 31 diciembre de 2008, Ley de habeas data y por la cual se regula el manejo de la información contenida en Bases de Datos personales.
- ✓ Ley 594 de 2000 sobre el control de documentos.
- ✓ Legislación específica sobre seguridad de la información, ejemplo ley sobre delitos informáticos.
- ✓ Regulación de la industria de tarjetas de pago -PCI.
- ✓ Ley Estatutaria 1581 de 2012, en donde se dictan disposiciones generales para la protección de datos personales.
- ✓ Decreto 1377 de 2013 por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- ✓ Decreto 2952 de 2010 por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008.
- ✓ Decreto 1727 de 2009 por el cual se determina la forma de presentación de los datos por parte de las entidades que manejan información de terceros o titulares.
- ✓ Resolución 76434 de 2012 por la cual se deroga el contenido del título 15 de la Circular Única de la Superintendencia de Industria y Comercio.
- ✓ Ley de comercio electrónico.
- ✓ Constitución nacional.
- ✓ Ley de propiedad intelectual.
- ✓ Circular 052 de la Superintendencia Financiera,sobre el lavado de activos.
- ✓ Regulación ambiental.

Para que la Política de Seguridad sea un documento de utilidad en la Fundación Universitaria Juan de Castellanos y cumpla con lo establecido en la norma UNE-ISO/IEC 27001 debe cumplir con los siguientes requisitos:

- ✓ Ser redactada de una manera accesible para todo el personal de la Universidad, redactada de forma corta, precisa y de fácil comprensión.
- ✓ Estar aprobada por la Rectoría y publicitada por la misma.
- ✓ Ser de dominio público dentro de la organización, por lo que debe estar disponible para su consulta siempre que sea necesario.
- ✓ Ser la referencia para la resolución de conflictos y otras cuestiones relativas a la seguridad de la Fundación Universitaria Juan de Castellanos.
- ✓ Definir responsabilidades teniendo en cuenta que estas van asociadas a la autoridad dentro de la Universidad. En función de las responsabilidades se decidirá quién está autorizado a acceder a qué tipo de información.
- ✓ Indicar que lo que se protege en la Universidad incluye tanto al personal como a la información, así como su imagen corporativa y continuidad.
- ✓ Ser personalizada y adaptada totalmente para las Institución de Educación Superior.
- ✓ Señalar las normas y reglas que va a adoptar la Fundación Universitaria Juan de Castellanos y las medidas de seguridad que serán necesarias.

En lo que se refiere al contenido, la Política de Seguridad debe incluir de manera general los siguientes apartados:

- ✓ Definición de la seguridad de la información y sus objetivos globales, el alcance de la seguridad y su importancia como mecanismo de control que permite compartir la información.
- ✓ Declaración por parte de la Rectoría apoyando los objetivos y principios de la seguridad de la información.
- ✓ Breve explicación de las políticas
- ✓ Definición de responsabilidades generales y específicas, en las que se incluirán los roles pero nunca a personas concretas dentro de la Universidad.
- ✓ Referencias a documentación que pueda sustentar la política.

La Política de Seguridad debe ser un documento completamente actualizado, por lo que debe ser revisado y modificado anualmente. Además, existen otros tres casos en los que es imprescindible su revisión y actualización, los cuales corresponden a:

- ✓ Después de grandes incidentes de seguridad.
- ✓ Después de una auditoría del sistema sin éxito.
- ✓ Frente a cambios que afectan a la estructura de la Universidad.

Igualmente la política debe considerar los criterios y metodología para la valoración del riesgo, donde se debe tener en cuenta:

- ✓ Definir una metodología para la evaluación y clasificación de los riesgos que impactan la seguridad de la información.
- ✓ Identificar los riesgos.
- ✓ Analizar y evaluar los riesgos encontrados.
- ✓ Definir objetivos de control y Controles para el tratamiento de los riesgos.
- ✓ Proponer opciones para el tratamiento de los riesgos.

Al definir los alcances del SGSI, se realiza la valoración de los riesgos que involucra.

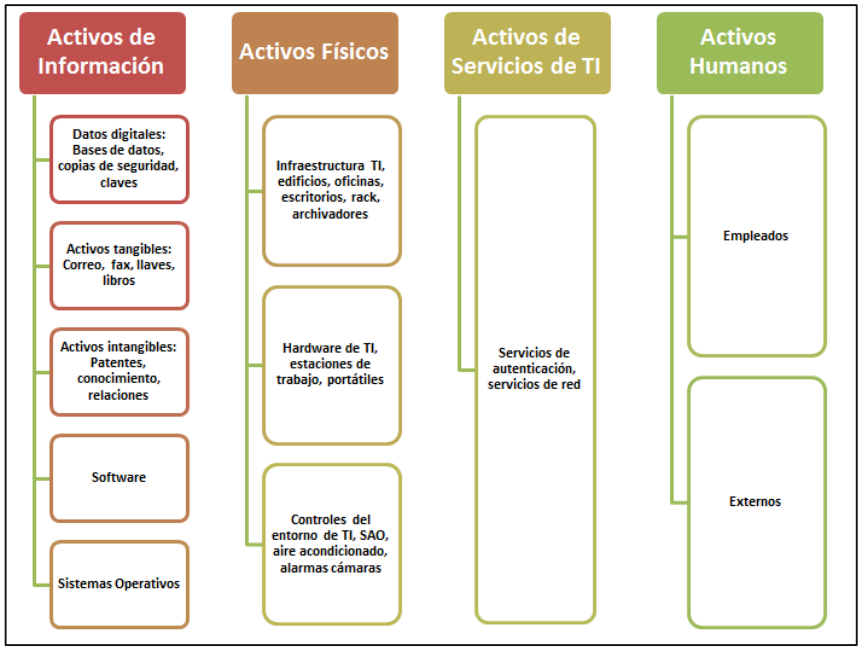
3.1.3 Inventario de Activos

En esta fase se debe realizar un inventario de activos identificando su ubicación, responsable y funciones, lo cual permitirá realizar un análisis y valoración de riesgos para determinar las amenazas, vulnerabilidades e impacto que presentan en la Universidad.

Según la norma ISO 27001:2005, se debe identificar el conjunto de activos de la información, entendiendo un activo como cualquier elemento que represente valor para la Universidad, tal es el caso de activos de información bases de datos, documentación, equipos de laboratorio, instalaciones físicas, manuales, software, hardware, contratos de equipo de comunicaciones, servicios informáticos y de telecomunicaciones, elementos generales como iluminación, energía, aire acondicionado, servicio de internet y las personas, que son quienes generan, transmiten y destruyen información, entre otros, los cuales se encuentran enmarcados dentro de los procesos seleccionados para la definición del alcance (Procesos estratégicos, misionales y de apoyo).

Los activos se podrían clasificar de manera general, como lo muestra la siguiente figura:

Figura 6. Clasificación de activos



Fuente: http://www.isotools.org/ 2013/12/05/en-inventario-de-activos-en-la-implementacion-de-la-norma-iso-27001/

La información a tener en cuenta para cada activo debe incluir los siguientes elementos:

- ✓ El nombre del activo.
- ✓ La descripción del activo.
- ✓ Tipo o categoría a la que pertenece (Equipo, aplicación, servicio, etc.).
- ✓ Ubicación (Lugar físico en el que se encuentra dentro de la organización).
- ✓ Propietario (Responsable del activo).

Una vez identificados los activos de información se les debe valorar de acuerdo con su importancia dentro de la Universidad, siendo esta apreciación lo más objetiva posible, ya que con ella se determinará sobre qué activos se realizará el análisis de riesgos.

Para el caso de estudio y la aplicación de la metodología propuesta en la Fundación Universitaria Juan de Castellanos tomaremos como ejemplo uno de sus procesos misionales: docencia, estableciendo un inventario de activos como se describe en la siguiente tabla:

Tabla 2. Inventario de Activos de Información Procesos Misionales - Docencia.

	INVENTARIO DE ACTIVOS DE INFORMACIÓN PROCESOS MISIONALES - DOCENCIA			Código: Fecha: No. Pág.
NOMBRE	**DESCRIPCIÓN DEL ACTIVO**	**TIPO DE ACTIVO**	**PROPIETARIO/ RESPONSABLE**	**UBICACIÓN**
Personal	Cuerpo Académico	Empleados – Usuarios	Vicerrector Académico	Salas de profesores
Puestos de Usuarios	Instalaciones Físicas	Físico	Vicerrector Administrativo	Coordenadas de la Universidad.
Puestos de usuario	PC de los usuarios	Físico	Vicerrector Administrativo	Unidad Asesoría y Sostenimiento Tecnológico
Docentes	Información docentes	Información	Vicerrector Administrativo	Servidor / Unidad Asesoría y Sostenimiento Tecnológico
Estudiantes	Información estudiantes	Información	Vicerrector Académico	Servidor / Unidad Asesoría y Sostenimiento Tecnológico / Registro y Control Académico
Calificaciones	Información de resultados del proceso de enseñanza/aprendizaje.	Información	Vicerrector Académico	Servidor / Unidad Asesoría y Sostenimiento Tecnológico /Unidad de Archivo físico
Normatividad	Normas y legislación establecidas	Información	Vicerrector Académico	Servidor / Unidad Asesoría y Sostenimiento Tecnológico/ Unidad de Archivo físico
Informes	Mortalidad académica, deserción académica, inscripciones, registros académicos	Información	Vicerrector Académico	Servidor / Unidad Asesoría y Sostenimiento Tecnológico / Unidad de Archivo físico

Recursos TI	Academisoft SWA Campus virtual Bases de datos digitales, revistas científicas, bibliotecas virtuales	Software	Vicerrector Académico	Servidor / Unidad Asesoría y Sostenimiento Tecnológico
Servidor	Equipo que contiene la información y aplicaciones de software de la Universidad.	Hardware	Vicerrector Administrativo	Unidad Asesoría y Sostenimiento Tecnológico

Elaboró: _____ Revisó_____ Aprobó: _____

Al realizar el inventario de activo es importante tener en cuenta conceptos tales como:

- ✓ **AMENAZA.** Es una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización.
- ✓ **VULNERABILIDAD.** Es la debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

Para realizar el análisis de amenazas y vulnerabilidades es necesario:

- ✓ Realizar una lista de las amenazas que puedan presentarse en forma accidental o
- ✓ intencional en la Fundación Universitaria Juan de Castellanos en relación con los activos de información.
- ✓ Diferenciar estas amenazas de las vulnerabilidades de los activos ya que el análisis debe radicar en las amenazas.
- ✓ Identificar los riesgos internos de los procesos analizando tanto las actividades que se desarrollan como las amenazas identificadas.
- ✓ Identificar los riesgos externos de los procesos. Establecer y analizar los riesgos generados por terceros, subcontratación de servicios o existe personal externo a la organización.

- ✓ Realizar un análisis del entorno en los fenómenos naturales, el ambiente geopolítico, el ambiente tecnológico, el ambiente ecológico y los aspectos socioculturales que rodea la Universidad para definir las amenazas a las que pueden estar expuestos los activos.

A manera de ejemplo en la Fundación Universitaria Juan de Castellanos podríamos revisar algunas amenazas y sus posibles riesgos:

Tabla 3. Amenazas y Riegos (internos – externos).

AMENAZA INTERNA	RIESGO INTERNO
Acceso no autorizado a las aplicaciones de la Fundación Universitaria Juan de Castellanos.	Cambios en la información, posible uso malicioso de la misma y daño a los sistemas informáticos de la Universidad.
Hurto por parte de funcionarios.	Pérdida de información y posible uso de la misma con fines mal intencionados.
Cambio en la información correspondiente a calificaciones del estudiante.	Generación de informes no confiables y fuera de la realidad por alteración de la información.
Uso indebido de la imagen corporativa.	Pérdida de confidencialidad
Fallas en el servidor y los sistemas.	Falta de disponibilidad de la información, pérdidas económicas y de imagen corporativa.
AMENAZA EXTERNA	**RIESGO EXTERNO**
Suplantación de identidad.	Alteración de información e ingreso no autorizado a sistemas informáticos.
Virus informáticos o código malicioso.	Daño a los sistemas informáticos. Pérdida de información.
Robo de información de la Universidad.	Plagio de información confidencial de la Universidad
Hackers – Espionaje.	Ingreso a los sistemas informáticos con fines maliciosos.
Hurto por personal externo.	Pérdida de imagen y uso de información confidencial con fines malintencionados.

3.1.4 Valoración de activos

En esta etapa se valorará para cada activo el impacto o grado en que se puede ver afectado determinado sistema, para el caso de estudio, el proceso, al alterar alguno de sus componentes o activo de información, la escala de puntuación se asigna de acuerdo con sus requisitos propios como lo describe la norma ISO 27001:2005, los cuales están relacionados con los requisitos de Confidencialidad, Integridad y Disponibilidad, para cuantificar el impacto que tienen dentro de su respectivo proceso.

En la siguiente tabla se describen los requisitos de Confidencialidad, Integridad y Disponibilidad que se debe asignar a cada uno de los activos en relación con su nivel de impacto: Alto, Medio y Bajo, según el comportamiento de este dentro del proceso:

Tabla 4. Requisitos de Confidencialidad, Integridad y Disponibilidad por Activo

REQUISITO	NIVEL DE VALORACIÓN		
	BAJO	**MEDIO**	**ALTO**
Confidencialidad	La información es de **carácter público** y no se tiene ningún impacto sobre el resultado del proceso en caso de ser accedido por personas no autorizadas.	La información es de **uso interno exclusivamente o uso restringido solamente** y de ser accedida por personas no autorizadas no afectaría en mayor grado el resultado o pondría en riesgo la empresa.	Confidencial o estrictamente confidencial. La información es de carácter **Secreto** y en caso de ser accedida por personas no autorizadas, el impacto final sobre el proceso o resultado de la empresa sería muy grave.
Integridad	El daño o modificación no autorizada no es crítico para las aplicaciones empresariales y el	El daño o modificación no autorizada no es crítico, pero si es notorio para las	El daño o modificación no autorizada es crítica para la organización y el impacto es

	impacto en la empresa es insignificante o menor.	aplicaciones empresariales y el impacto en la empresa es significativo.	importante y podría conllevar la falta grave o total de la aplicación o sistema empresarial.
Disponibilidad	Se puedes tolerar que el activo no esté disponible por más de un día.	Se puede tolerar que el activo no esté disponible por máximo de medio día a un día.	No se puede tolerar que el activo no esté disponible por más de unas cuantas horas (4), o incluso menos.

Aplicando la tabla anterior a cada uno de los activos relacionados para el proceso de docencia, se podría establecer el valor del activo con respecto a sus requisitos (Confidencialidad-Integridad – Disponibilidad) y sus niveles (1=Bajo, 2=Medio, 3=Alto), siendo la valoración total del activo la suma de los tres valores, tal como se observa a continuación:

Tabla 5. Valor de los Activo con relación a sus requisitos.

Activo	Confidencialidad	Integridad	Disponibilidad	Total
Personal	1	2	3	6
Puestos de Usuarios – PC de los usuarios	1	2	3	6
Puestos de usuario – Instalaciones físicas	3	2	2	7
Docentes	1	2	3	6
Estudiantes	3	3	3	9
Calificaciones	3	3	3	9
Normatividad	2	2	3	7
Informes	2	3	3	8
Recursos TI	3	3	3	9
Servidor	2	3	3	8

El resultado de esta fase será el inventario de activos valorados, para lo cual se sugiere seleccionar un porcentaje de los activos con mayor valor para continuar con la siguiente etapa que es la de Análisis de Riesgos.

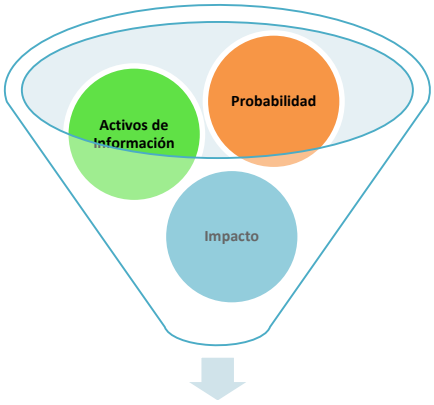
3.1.5 Análisis de Riesgos

El análisis de riesgos tiene como objetivo establecer una priorización de los riesgos de los procesos y activos involucrados en el alcance del SGSI para su tratamiento posterior. En esta etapa se deben identificar las amenazas asociadas a cada uno de los procesos de negocio, activos de información, probabilidad de ocurrencia y vulnerabilidades ante dichas amenazas, lo que permitirá estimar el impacto de la materialización de cualquier falla de seguridad dentro de la organización.

Chavez (2013, p. 4) indica que el análisis de riesgos puede ser cualitativo o cuantitativo, generalmente el análisis de riesgos cualitativo se realiza después del cuantitativo, cuando se quiere profundizar en algún riesgo concreto, en otras ocasiones precede directamente a la planificación de respuesta al riesgo, obviándose el análisis cuantitativo.

Los riesgos serán analizados en términos del activo de información valorado, la probabilidad de ocurrencia de la amenaza y el impacto potencial causado por la pérdida de confidencialidad, integridad y disponibilidad.

Figura 7. Análisis de riesgos



Fuente: Alemán, (2015)

El Análisis de Riesgos le permitirá a la Universidad:

- ✓ Identificar objetivamente los procesos y activos de información críticos que impactan en la continuidad del negocio.
- ✓ Evaluar la eficacia de los controles y procesos de seguridad implantados.
- ✓ Optimizar las futuras inversiones en seguridad.
- ✓ Realizar el seguimiento y control de la evolución de los niveles de riesgo.

Para cada activo se identifican las amenazas que le afectan y se describen las vulnerabilidades asociadas a cada amenaza, por ejemplo para el activo Información de Estudiantes:

Tabla 6. Descripción de amenazas y vulnerabilidades activo Información de estudiantes.

AMENAZA	VULNERABILIDAD
Acceso no autorizado	Sistema de autenticación deficiente. Mala configuración. Sistemas no protegidos contra accesos físicos y lógicos.
Intercepción de la información (escucha)	Ausencia de sistemas de cifrado de información y mensajes. Deficiente definición de políticas de acceso. Ausencia de sanciones y procesos disciplinarios.

Modificación de la Información	Ausencia de protección de la información, almacenamiento y copias de respaldo. Falta de controles de entrada de datos.
Divulgación de la información	Ausencia de medidas de seguridad en el manejo y almacenamiento de la información, carencia de sanciones y procesos disciplinarios.
Información no disponible	Equipos deficientes, proveedores de servicios y sistemas de comunicaciones inadecuados.
Fuego	Carencia o existencia de Sistemas de control de incendios. Ausencia procesos de revisión y mantenimiento.
Robo	Ausencia de controles de acceso físico y lógico. Falta de concienciación y procesos disciplinarios.
Errores de usuario	Ingreso y actualización de datos inadecuados, fallas en controles de entrada de datos, ausencia de procesos disciplinarios.
Fallo de Software	Ausencia de controles de validación de datos, entrada y salida de información. Carencia de controles de autenticación de usuarios.

Una vez definidas las amenazas y vulnerabilidades para cada activo se procederá a valorar el riesgo el cual estará dado por el valor más alto para cada activo teniendo en cuenta:

Nivel de Riesgo = Nivel de Amenaza X Nivel de Vulnerabilidad X Nivel de Impacto

El nivel de la vulnerabilidad como el nivel (o probabilidad) de la amenaza se pueden valorar en una escala de 0 a 3 respectivamente:

- ✓ 0= no aplica
- ✓ 1=Bajo
- ✓ 2=Medio
- ✓ 3=Alto

Teniendo en cuenta estos parámetros, la valoración del riesgo para el caso descrito anteriormente “Información de Estudiantes” estaría determinada de la siguiente forma:

Tabla 7. Valoración de riesgo - Activo Información de estudiantes.

Amenaza	Impacto (Valor del Activo)	Nivel de amenaza	Vulnerabilidad	Nivel de Riesgo
Acceso no autorizado	9	1	1	9
Intercepción de la información (escucha)	9	2	2	36
Modificación de la Información	9	1	1	9
Divulgación de la información	9	2	1	18
Información no disponible	9	3	2	54
Fuego	9	1	0	0
Robo	9	1	2	18
Errores de usuario	9	1	1	9
Fallo de Software	9	2	1	18

Después de realizada la valoración del riesgo para todos los activos del proceso de docencia o procesos involucrados dentro del alcance del SGSI, se debe definir el nivel de riesgo aceptable por la Universidad, este nivel sirve como indicador, definiendo que todos los activos con algún riesgo por encima de este valor deben ser tratados de alguna forma para ser mitigados, eliminados o aceptados.

La evaluación del riesgo se realiza teniendo en cuenta los alcances definidos en el SGSI, para lo cual se realizará una comparación del resultado de la valoración del riesgo de los activos con los criterios y aceptación definidos por la Universidad. En esta etapa también se priorizan los riesgos que deben ser tratados y gestionados de acuerdo con el resultado de la valoración de riesgos.

Existen algunas metodologías específicas para el análisis de riesgos como lo son: Margerit, Coras, NIST SP 800-30 y Octave, dentro de las cuales la Institución podrá elegir investigar y profundizar para realizar su aplicación en este proceso, si es el caso.

Con el establecimiento del plan de tratamiento de riesgos y su aprobación por parte Consejo Superior de la Universidad se daría final a la fase de Planificación del ciclo del PHVA del SGSI.

3.2 Hacer

Teniendo en cuenta lo establecido en el ciclo PHVA, a continuación se realizará la etapa de HACER, lo cual establece según la norma ISO 27001 las siguientes actividades:

- ✓ Definir el plan de tratamiento de riesgos
- ✓ Implementar el plan de tratamiento de riesgos
- ✓ Implementar los controles
- ✓ Formar y concientizar

3.2.1 Plan de tratamiento del riesgo

Una vez analizado y cuantificado los riesgos, así como el impacto que tienen dentro de la Universidad, se deben seleccionar y aplicar las medidas más adecuadas, con el fin de poder modificar el riesgo, para evitar de este modo los daños intrínsecos al factor de riesgo, o bien aprovechar las ventajas que se puedan reportar, verificando el nivel de oportunidad en caso de asumir el riesgo.

El objetivo del Plan de tratamiento del riesgo es definir claramente cómo se implementarán los controles, quién lo hará, cuándo, con qué presupuesto, lo cual permitirá garantizar:

- ✓ Un funcionamiento efectivo y eficiente de la organización.
- ✓ Controles internos efectivos.
- ✓ Conformidad con las leyes y reglamentos vigentes.

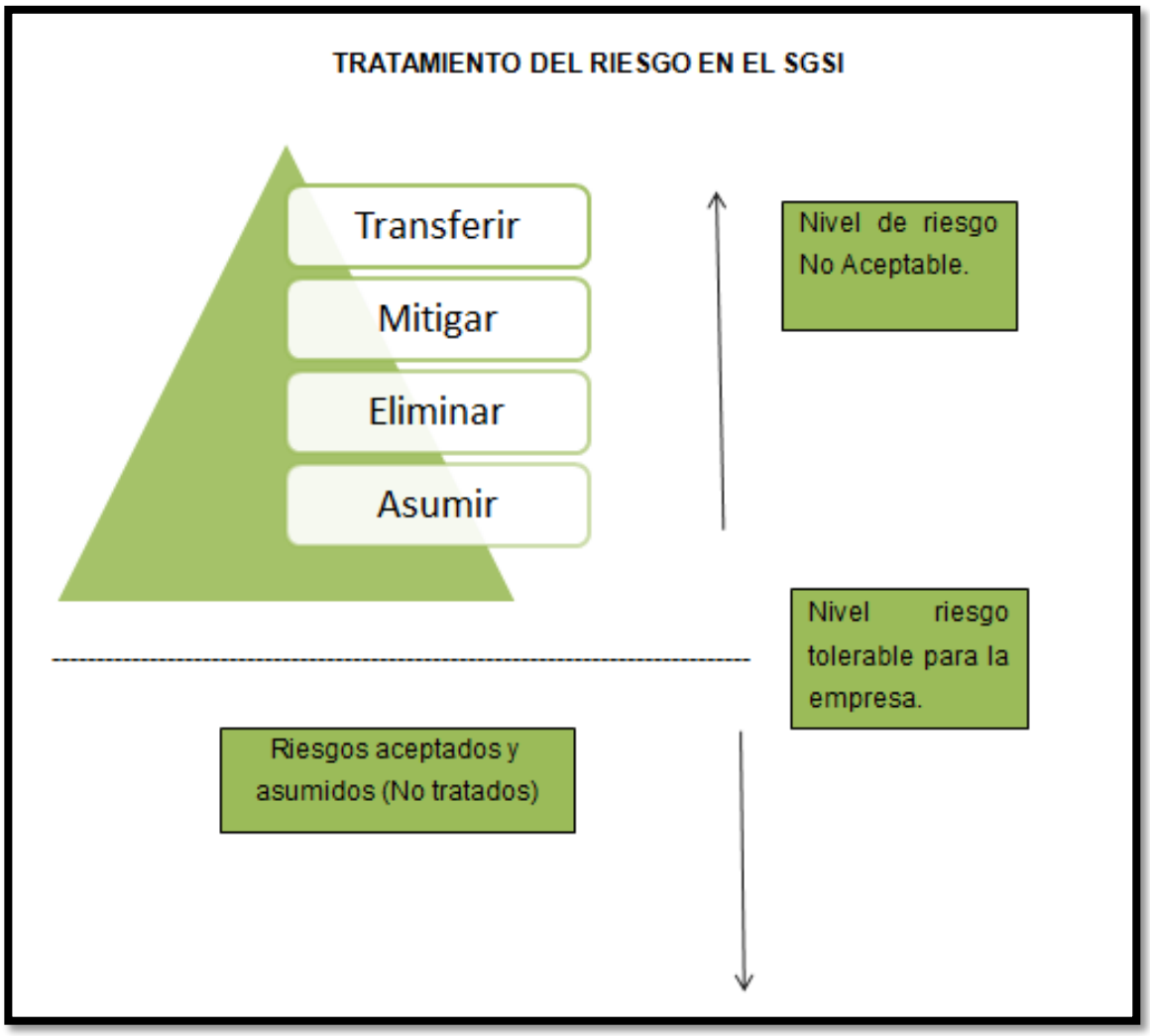
Dentro del plan de tratamiento de riesgos se debe seleccionar para cada riesgo aquella estrategia de respuesta que tenga mayores posibilidades de éxito, se pueden utilizar estrategias tales como:

- ✓ **Eliminación o evitación.** Consiste en eliminar la amenaza eliminando la causa que puede provocarla.
- ✓ **Transferencia.** Esta posibilidad busca trasladar las consecuencias de un riesgo a una tercera parte junto con la responsabilidad de la respuesta.

- ✓ **Mitigación.** Busca reducir la probabilidad o las consecuencias de sucesos adversos a un límite aceptable antes del momento de activación. Es importante que los costos de mitigación sean inferiores a la probabilidad del riesgo y sus consecuencias.

  Para llevar a cabo la mitigación de riesgos es necesario: seleccionar, implantar, y verificar los controles y establecer indicadores. La selección de los controles se podrá realizar utilizando como referencia la Norma ISO 27002 (Guía de buenas prácticas), la cual presenta 133 controles, pero si la Universidad lo desea puede incluir los que crea convenientes.
- ✓ **Aceptación.** Se utiliza cuando se decide no actuar contra el riesgo antes de su activación. La aceptación puede ser activa, cuando se incluye un plan de contingencia que será ejecutado si el riesgo se presenta, o pasiva, cuando no requiere de ninguna acción, únicamente se realiza la gestión del riesgo.

Figura 8. Tratamiento del riesgo en el SGSI.



Fuente: Alemán, (2015)

Se debe nombrar un responsable de implementar la estrategia elegida para cada riesgo según el plan predefinido. Como consecuencia de esta implantación pueden aparecer riesgos residuales, aquellos que permanecen después de implementar las respuestas al riesgo y riesgos secundarios, que pueden aparecer como consecuencia de la implementación de la respuesta a un riesgo.

3.2.2 Selección de Controles

Un control es lo que permite garantizar que cada aspecto del activo, que se valoró con cierto riesgo, quede cubierto y auditable. La selección de controles define el plan de tratamiento de riesgos que estará enmarcada en los 133 controles de la norma ISO/IEC 27002 y el Anexo A de la Norma ISO 27001, Tabla A.1; sin embargo, la Universidad podría considerar adicionar o exceptuar los controles que crea necesarios, es recomendable que para aquellos controles no seleccionados, porque se consideran no aplicables, se indique la razón de su exclusión de manera detallada, lo que servirá como documento de soporte en la fase de certificación y será revisado por los auditores, permitiendo establecer que los controles exceptuados no fueron seleccionados al azar o sin razones de peso.

Los objetivos de control y los controles deben ser seleccionados como parte del proceso de definición y establecimiento del SGSI, teniendo en cuenta los dominios de la norma ISO 27001, los cuales se muestran en la siguiente figura:

Figura 9. Dominios de la ISO 27001.

Fuente: http://www.criptored.upm.es/descarga/GUIA_AUDISEC_GLOBALSGSI.pdf

Para definir los controles la Universidad debe tener en cuenta:

- ✓ El coste del control frente al coste del impacto que supondría que el activo a proteger sufriera un incidente y el valor de dicho activo.
- ✓ La necesidad de disponibilidad del control.
- ✓ Qué controles ya existen.
- ✓ Qué supondría su implantación y mantenimiento, tanto en recursos económicos como en humanos.

Igualmente se debe tener en cuenta la clasificación de los controles, los cuales pueden ser:

- ✓ **Controles Técnicos**. Sistemas de cifrado, copia de seguridad, sistemas de detección de intrusos, actualizaciones de software, antivirus o cortafuegos, etc.
- ✓ **Controles Organizativos**. Política de Seguridad, procedimientos de uso de los sistemas de información para los usuarios, planes de formación, planes de continuidad de negocios, entre otros.

3.2.3 Implementación de los controles

Después de seleccionar los controles que aplicarán para el SGSI de la Universidad y sus activos, se debe realizar la definición del procedimiento a seguir para su implementación, en esta fase se requiere que la Institución disponga de una buena cantidad de tiempo y recursos, por ejemplo en el caso de la implementación de controles y salvaguardas técnicos se requiere de la colaboración del personal que realiza estas funciones y para los controles organizativos será la Vicerrectoría Administrativa quien tendrá que tomar decisiones del caso, así como involucrar en la formación y concienciación a todo el personal.

Se recomienda agrupar diferentes controles para hacer más recursivo el sistema, haciendo de este ejercicio una solución sencilla para aumentar su eficacia y facilitar su implementación y mantenimiento.

3.2.4 Verificación de controles

Los controles implementados deben ser sometidos a revisión para verificar su correcto funcionamiento, estableciendo con anterioridad una serie de objetivos e indicadores que nos

permitan la medición de dicho funcionamiento, esta tarea debe ser realizada por el propietario del activo asignado.

3.2.5 Controles que se deben aplicar en la Fundación Universitaria Juan de Castellanos

A continuación se relacionan los controles a tener en cuenta para el proceso de docencia dentro de la Fundación Universitaria Juan de Castellanos:

En el Anexo No. 1 se relacionan los objetivos de control y controles que se deben aplicar en la Fundación Universitaria Juan de Castellanos, basados en la Norma ISO 27001, Anexo A, los cuales están directamente relacionados con:

3.2.5.1 Controles y objetivos de control relacionados con la Misión Institucional de la Fundación Universitaria Juan de Castellanos:

- ✓ Definición de la política de Seguridad.
- ✓ Clasificación y marcado de la información.
- ✓ Contratos con terceros.
- ✓ Cambios en los contratos de terceros.
- ✓ Comunicaciones de información con terceros.
- ✓ Controles relacionados.

3.2.5.2 Controles y objetivos de control relacionados con el personal:

- ✓ Definición de funciones y responsabilidades.
- ✓ Cláusulas de confidencialidad.
- ✓ Concienciación y educación sobre normas de seguridad.
- ✓ Cambios en los contratos de terceros.
- ✓ Escritorio limpio y seguridad de equipo desatendido.
- ✓ Responsabilidad en el uso de contraseñas.
- ✓ Normas de seguridad en el uso de cuentas de correo electrónico.
- ✓ Formación sobre manejo de incidencias de seguridad.

3.2.5.3 Controles y objetivos de control relacionados con los sistemas de información:

- ✓ Controles de acceso (Físico y lógico).
- ✓ Control contra amenazas externas y ambientales.

- ✓ Control de etiquetado de soportes.
- ✓ Control para la entrega y recepción de soportes con información (interna y externa).
- ✓ Controles de reutilización y eliminación de soportes.
- ✓ Normas de uso de dispositivos móviles y comunicaciones.
- ✓ Normas de uso de soportes de almacenamiento de información y dispositivos extraíbles.
- ✓ Controles para el mantenimiento de equipos.
- ✓ Protección contra fallos en los servicios (internet, electricidad).
- ✓ Protección contra código malicioso.
- ✓ Actualizaciones de software.
- ✓ Copias de seguridad.
- ✓ Seguridad lógica en las comunicaciones.
- ✓ Seguridad de accesos remotos no autorizados.
- ✓ Identificación automática de equipos no autorizados.
- ✓ Controles de acceso a registros del sistema.
- ✓ Sincronización de relojes.

Una vez establecidos los controles se debe realizar la verificación de su correcto funcionamiento, mediante el establecimiento previo de una serie de objetivos e indicadores que permitan su evaluación y seguimiento.

3.2.6 Formación y Concienciación

En esta fase, la Norma ISO 27001 establece que todo el personal debe estar involucrado y hacer parte activa de los procesos relacionados con el SGSI, es imprescindible la capacitación en seguridad informática a todo el personal: Docentes, Administrativos, Estudiantes, generando una cultura de uso y buenas prácticas de seguridad que permita minimizar las posibilidades de riesgo para la institución.

Igualmente se debe tener el apoyo manifiesto de las Directivas de la Institución, Consejo Directivo, Rectoría, Vicerrectorías, Decanaturas, Direcciones de Programa y Jefes de área para todo el proceso, ya que serán los encargados de conocer los riesgos del negocio y las obligaciones con los usuarios. Además, su responsabilidad tendrá que abarcar las estrategias para introducir los cambios de mentalidad, de procedimientos y de tareas que requiere el sistema por medio de planes de capacitación, divulgación y concienciación periódica.

3.2.7 Objetivos de Control e Indicadores

Dentro del plan de tratamiento de riesgo se deben incluir las acciones que se van a desarrollar para gestionar el riesgo, las cuales deben tener un objetivo e indicador que permitan medir la eficacia de los controles definidos con anterioridad, la medición se realizará teniendo en cuenta los registros del sistema y documentos soporte diligenciados durante un periodo de tiempo establecido, la información utilizada debe ser clara, precisa, oportuna y veraz.

Los indicadores que se establezcan deben tener en cuenta las variables que permitan el cumplimiento de los objetivos y deben reunir algunos criterios como:

- ✓ Pertinencia
- ✓ Disponibilidad
- ✓ Confiabilidad
- ✓ Utilidad
- ✓ Funcionalidad

En la siguiente tabla se incluyen algunos objetivos e indicadores para realizar la medición de la eficacia de los controles aplicados a la Fundación Universitaria Juan de Castellanos.

Tabla 8. Objetivos e Indicadores aplicados a la FU Juan de Castellanos.

Objetivo	Indicador	Fórmula	Unidad de Medida	Periodicidad	Meta			Responsable
					2014	Cumplimiento Meta	Nivel de cumplimiento	
Aumentar la disponibilidad del sistema	Disponibilidad del sistema	Número de horas fuera de servicio del sistema / Número de horas de disponibilidad del sistema X 100	%	Semestral	60%	50%	83%	Vicerrectoría administrativa Unidad de Asesoría y Sostenimiento Tecnológico
Usuarios: Estudiantes, Docentes y Administrativos.		**Observaciones:**						

Objetivo	Indicador	Fórmula	Unidad de Medida	Periodicidad	Meta			Responsable
					2014	Cumplimiento Meta	Nivel de cumplimiento	
Reducir las incidencias de seguridad por fallas del usuario.	Incidencias de seguridad por fallas del usuario.	Número de ocurrencias por fallos del usuario / Número de incidencia por fallos del usuario estimados X 100	%	Semestral	85%	55%	65%	Vicerrectoría administrativa Unidad de Asesoría y Sostenimiento Tecnológico.
Usuarios: Estudiantes, Docentes y Administrativos.		**Observaciones:**						

Objetivo	Indicador	Fórmula	Unidad de Medida	Periodicidad	Meta			Responsable
					2014	Cumplimiento Meta	Nivel de cumplimiento	
Medir los accesos no autorizados al sistema.	Efectividad en los controles de acceso.	Número de accesos no autorizados / Número total de accesos X 100	%	Semestral	90%	48%	53%	Vicerrectoría administrativa Unidad de Asesoría y Sostenimiento Tecnológico.
Usuarios: Estudiantes, Docentes y Administrativos.		**Observaciones:**						

Objetivo	Indicador	Fórmula	Unidad de Medida	Periodicidad	Meta			Responsable
					2014	Cumplimiento Meta	Nivel de cumplimiento	
Determinar la efectividad de los procesos de mantenimiento de equipos.	Efectividad en los controles de mantenimiento de equipos.	Número de equipos con mantenimiento / Número total de equipos X 100	%	Semestral	70%	45%	64%	Vicerrectoría administrativa Unidad de Asesoría y Sostenimiento Tecnológico.
Usuarios: Estudiantes, Docentes y Administrativos		**Observaciones:**						

Objetivo	Indicador	Fórmula	Unidad de Medida	Periodicidad	Meta			Responsable
					2014	Cumplimiento Meta	Nivel de cumplimiento	
Asegurar el nivel de capacitación y conocimiento de normas internas en cuanto a seguridad informática.	Nivel de concienciación del personal.	Número de capacitaciones realizadas al personal sobre seguridad informática / Número total de capacitaciones proyectadas según políticas de seguridad X 100	%	Semestral	95%	30%	32%	Vicerrectoría administrativa Unidad de Asesoría y Sostenimiento Tecnológico.
Usuarios: Estudiantes, Docentes y Administrativos.		**Observaciones:**						

3.3 Verificar

Posterior a la implementación del SGSI, la Universidad debe abordar la fase de verificación que consiste en realizar las siguientes actividades:

- ✓ Revisar el SGSI
- ✓ Medir la eficacia de los controles
- ✓ Revisar los riesgos residuales
- ✓ Realizar auditorías internas del SGSI
- ✓ Registrar eventos y acciones

3.3.1 Revisión del SGSI

La Norma ISO 27001 establece la revisión periódica del SGSI, por lo menos una vez al año, para establecer el grado de eficacia y pertinencia del sistema en concordancia con los objetivos del negocio. Esta revisión permite el análisis del sistema, detección de fortalezas debilidades y la toma de decisiones en cuento a planes de mejoramiento continuo.

En el caso de la Universidad, la verificación del SGSI lo debe realizar el Consejo Directivo por medio de informes entregados por parte del encargado de la seguridad informática, el cual estará designado por la Vicerrectoría Administrativa para tal fin. Algunos de los insumos para el proceso de verificación pueden ser:

- ✓ Resultados de auditorías internas o externas e informes de revisiones del SGSI.
- ✓ Sugerencias y recomendaciones otorgadas por las partes interesadas(estudiantes, administrativos, docentes y personal externo).
- ✓ Procesos, procedimientos o técnicas que pudieran ser útiles para mejorar el nivel de eficiencia y eficacia del SGSI.
- ✓ Informes sobre el estado de acciones preventivas y correctivas realizadas al SGSI.
- ✓ Registros de vulnerabilidades o amenazas que no se hayan tratado adecuadamente en evaluaciones de riesgos anteriores.
- ✓ Resultados de las mediciones de eficacia y eficiencia según métricas de seguridad.
- ✓ Informes y estado de las acciones iniciadas como producto de revisiones anteriores al SGSI.
- ✓ Cambios realizados en la organización y que pueden afectar al SGSI.
- ✓ Recomendaciones establecidas por otros sistemas (SGC) de la institución.

La norma 27001 en su apartado 4.2.3, Monitorear y revisar el SGSI, establece los procedimientos que se deben llevar a cabo para realizar el seguimiento al SGS, así:

- ✓ Ejecutar procedimientos de monitoreo y revisión y otros controles.
- ✓ Realizar revisiones regulares del SGSI.
- ✓ Medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.
- ✓ Revisar la evaluación del riesgo a intervalos planeados y revisar el nivel de riesgo residual y riesgo aceptable identificado, teniendo en cuenta los cambios presentados a nivel de la organización.
- ✓ Realizar auditorías internas al SGSI por periodos de tiempo planeados.
- ✓ Realizar una revisión gerencial del SGSI sobre una base regular para asegurar que el alcance permanezca adecuado y se identifiquen las mejoras en el proceso del SGSI.
- ✓ Actualizar los planes de seguridad para tomar en cuenta los descubrimientos de las actividades de monitoreo y revisión.
- ✓ Registrar las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño del SGSI.

Teniendo en cuenta la anterior información, el Consejo Superior de la Universidad tomará la decisión de generar:

- ✓ Planes de acción para el mejoramiento del SGSI.
- ✓ Actualización de la gestión y evaluación del riesgo.
- ✓ Reestructuración o implementación de nuevos de los controles.
- ✓ Asignación de más recursos para el cumplimiento de los objetivos del SGSI.
- ✓ Cambios en los niveles de riesgo aceptables.
- ✓ Implementación de estrategias para medir la efectividad de los controles.
- ✓ Compromisos u obligaciones contractuales.
- ✓ Procesos eficaces la gestión de incidentes de seguridad de la información.
- ✓ Rediseño, eliminación e implementación de nuevos indicadores.

Para facilitar el proceso de verificación del SGSI se pueden implementar algunas herramientas como: Auditorías internas, cartas de control, planes deverificación del SGSI, balanced scorecard BSC o cuadro de mando integral CMI.

3.3.2 Auditorías Internas

Las Auditorías Internas se deben establecer dentro de la institución a fin de especificar los requisitos necesarios para establecer, implementar, mantener y mejorar el SGSI, ejerciendo

una labor de vigilancia y validación de la implementación de las disposiciones y lineamientos establecidos en la política de seguridad y los controles relacionados con la seguridad informática definidos dentro del SGSI.

El personal asignado para realizar las auditorías internas debe tener amplio conocimientos en la aplicación de la norma ISO 27001 y su Guía de buenas prácticas ISO 27002, así como del SGSI implementado en la institución, por cuanto este tendrá la función de evaluar y comprobar los controles y procedimientos informáticos más complejos, objeto de análisis, desarrollando y aplicando metodologías de auditoría.

Para realizar las auditorías internas se podrán utilizar técnicas, tales como: inspección, observación, entrevistas, documentación y procedimientos analíticos a los sistemas informáticos de la institución, al igual que aplicar herramientas de software o hardware para realizar la respectiva revisión.

El auditor será el responsable de llevar a cabo la auditoría en donde se deben incluir las siguientes actividades:

- ✓ Planificar la auditoría.
- ✓ Llevar a cabo las distintas tareas definidas en las fases de la auditoría.
- ✓ Escuchar y observar.
- ✓ Gestionar las desviaciones y riesgos que pudieran producirse durante la auditoría.
- ✓ Informar al Consejo Directivo y/o Rectoría de la institución acerca del diseño y funcionamiento de los controles implantados, la fiabilidad de la información suministrada, la suficiencia de las evidencias o la medida en la que sustentan las conclusiones de la auditoría.
- ✓ Uso de software de auditoría CAATS (Computer Assisted Audit Techniques) para verificar procesos automatizados que no son posible revisar manualmente.

Como resultado de las actividades antes descritas, el auditor debe presentará al Consejo Directivo de la Universidad un informe de auditoría que contendrá:

- ✓ Las conclusiones de la auditoría.
- ✓ Las no conformidades (menores, mayores y las evidencias relacionadas).
- ✓ Las observaciones con sus respectivas evidencias relacionadas.
- ✓ Una descripción de la auditoría con objetivo, alcance, fases y fechas, técnica o técnicas empleadas, áreas auditadas, entrevistados, entre otros.
- ✓ La relación de evidencias detectadas y, por cada una, su competencia y suficiencia.

3.4 Actuar

En esta última fase, se implementan las medidas correctivas y planes de mejora obtenidos como resultado de la verificación del SGSI. Las disposiciones y procedimiento a llevar a cabo se encuentran descritas en el capítulo 8 de la Guía de buenas prácticas ISO 27002, algunas de las actividades que se deben realizar en esta etapa corresponden a:

- ✓ Mantener y mejorar el SGSI.
- ✓ Definir planes de acción en cuanto a medidas correctivas, preventivas y planes de contingencia.
- ✓ Identificar las no conformidades encontrada en el SGSI, producto de las auditorías internas.
- ✓ Aplicar los planes de mejoramiento al SGSI, propuesto en la fase de verificación.
- ✓ Realizar análisis y estudio de casos y análisis de causa-efecto.
- ✓ Implementación de cambios propuestos y ejecución de recursos asignados.
- ✓ Evaluar la efectividad de los planes de mejora del SGSI, teniendo en cuenta los resultados de acciones implementadas anteriormente.
- ✓ Comunicar las acciones de mejora del SGSI a las partes interesadas.
- ✓ Actualizar los planes de seguridad en los sistemas informáticos en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de seguimiento y revisión.
- ✓ Verificar la correcta implementación de las mejoras propuestas al SGSI.

Estarán involucrados en la fase de actuar, las Directivas de la Fundación Universitaria Juan de Castellanos, así como personal administrativo, cuerpo docente y estudiantes quienes deben ejecutar las acciones de mejora planteadas como resultado de la autoevaluación realizada por parte de las auditorías internas y externas (si es el caso), lo cual permitirá la implementación de controles para el logro de los objetivos del SGSI.

A continuación se resumen los insumos, responsables y productos a tener en cuenta en la fase de verificación.

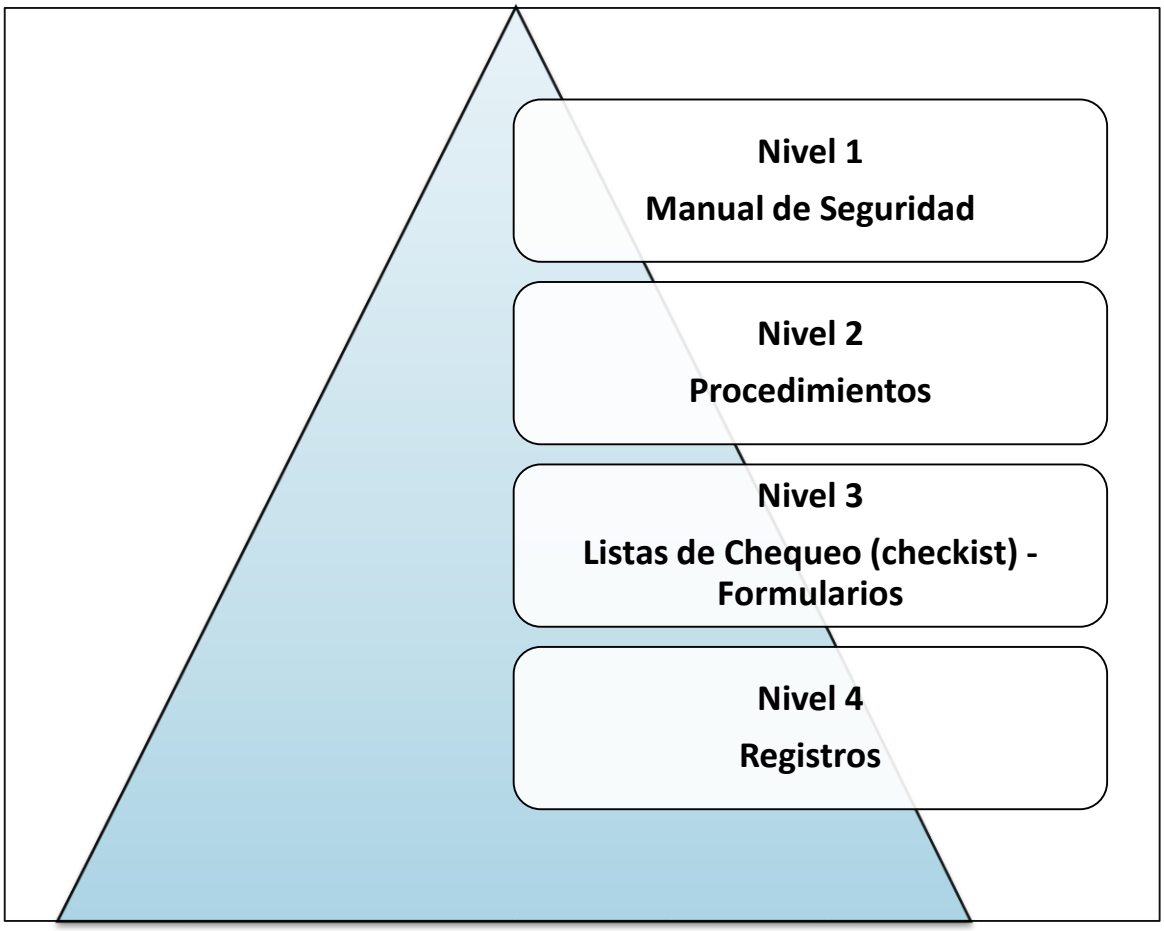
Tabla 9. Insumos, Responsables y Productos de la Fase de Actuar.

INSUMOS	RESPONSABLES	PRODUCTOS
Informes de auditorías internas y externas.	Equipo de auditores internos o externos.	Informe de Plan de acción ejecutado con descripción de actividades, responsables, porcentajes de cumplimiento, objetivos, impacto de las mejoras al SGSI.
Informes de no conformidades.	Equipo de auditores internos o externos.	
Informes de la etapa de revisiones al sistema.	Vicerrectoría Académica – Unidad de Asistencia y Sostenimiento Tecnológico.	
Planes de acción y mejora de etapas anteriores.	Consejo Superior – Rectoría - Vicerrectoría Académica – Unidad de Asistencia y Sostenimiento Tecnológico	
Propuestas de mejora de otras entidades o áreas de negocios.	Ministerio de Educación Nacional – Secretaría de Educación Departamental – Municipal – Otras Instituciones Universitarias.	

3.5 Documentos del SGSI

El SGSI que se implemente en la Fundación Universitaria Juan de Castellanos debe tener el soporte documental establecido para su correcto funcionamiento, para tal fin la norma ISO 9001, estándar de los Sistemas de Gestión de Calidad,indica que los documentos se deben integrar en cuatro niveles, los cuales aplicados al modelo del SGSI de acuerdo a la norma ISO 27001 son los siguientes:

Figura 10. Niveles de los documentos del SGSI.



Fuente: Alemán, (2015)

3.5.1 Documentos Nivel 1 - Manual de seguridad

Es el documento que permitirá orientar y describir los lineamientos de todo el SGSI, en él se deben incluir: objetivos, alcances, responsabilidades, políticas, directrices, funciones y especificaciones relacionadas con los procesos y procedimientos que tienen que ver con la seguridad de los sistemas informáticos de la Institución, por su categoría debe ser un análogo al Manual de Calidad.

3.5.2 Documentos Nivel 2 - Procedimientos

Corresponden a la estandarización de los procesos operativos que se llevan a cabo dentro de la organización y que tienen que ver con la seguridad de los sistemas informáticos, garantizan la planificación, operación y control.

3.5.3 Documentos Nivel 3 - Instrucciones, checklists y formularios

Documentos que registran las tareas y actividades específicas relacionadas con la seguridad de la información.

3.5.4 Documentos Nivel 4 - Registros

Están compuestos por el conjunto de evidencias que comprueban el cumplimiento de los requisitos del SGSI, se encuentran asociados a documentos de otros niveles como resultado que demuestra el cumplimiento de lo establecido en los mismos.

Otros de los documentos que son requisitos para el SGSI, según la Norma ISO 27001 y que la Fundación Universitaria Juan de Castellanos debe mantener, son los documentos que soportan cada una de las fases del ciclo PDCA, anteriormente descritos, y que corresponden a:

- ✓ Alcance
- ✓ Políticas y objetivos de seguridad
- ✓ Procedimientos y mecanismos de control
- ✓ Enfoque de evaluación de riesgos
- ✓ Informe de evaluación de riesgos
- ✓ Plan de tratamiento de riesgos
- ✓ Procedimientos documentados
- ✓ Registros
- ✓ Declaración de aplicabilidad (objetivos de control y los controles del SGSI)

3.6 Control de documentos

Es necesario establecer para los documentos generados procedimientos que definan y garanticen las siguientes acciones:

- ✓ Aprobación antes de su emisión.
- ✓ Revisión y actualización.
- ✓ Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.
- ✓ Disponibilidad de las versiones relevantes de documentos vigentes disponibles en los lugares de empleo.
- ✓ Garantizar que los documentos se mantienen legibles y fácilmente identificables.
- ✓ Garantizar la disponibilidad de los documentos de acuerdo con los requerimientos del personal y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación.
- ✓ Identificar los documentos procedentes de entidades externas.
- ✓ Controlar la distribución de documentos.

- ✓ Prevenir la utilización de documentos obsoletos.
- ✓ Realizar la identificación apropiada a documentos que son retenidos con algún propósito.

4 CONCLUSIONES

Los SGSI en las organizaciones son un elemento indispensable que permiten administrar y gestionar la seguridad de los sistemas informáticos, su implementación implica el diseño de una metodología que permita direccionar el proceso paso a paso, garantizando la integridad, disponibilidad y confidencialidad de la información que se maneja dentro y fuera de ella.

Al plantear la metodología propuesta fue necesario determinar los procesos claves de negocio de la Fundación Universitaria Juan de Castellanos, revisar la clasificación de los activos de información, determinar un análisis de riesgos y controles que permitieron contextualizar los alcances del SGSI, lo cual será de utilidad en el momento de su aplicación y facilitará el desarrollo de las fases del ciclo PHVA (Planear, Hacer, Verificar y Actuar) a nivel institucional.

La presente metodología, basada en la Norma ISO 27001 y su guía de buenas prácticas ISO 27002, permitirán a la Fundación Universitaria Juan de Castellanos organizar, diseñar y administrar de manera sistemática su SGSI, otorgándole beneficios, tales como: Integración del SGSI al SGC (ISO 9001), requisito indispensable para la certificación institucional de alta calidad ante el Ministerio de Educación Nacional, conformidad con las normas legales vigentes en cuanto a seguridad de los sistemas informáticos, mejoramiento de la imagen institucional a nivel nacional e internacional, continuidad del negocio, confianza ante el personal interno y externo que utilice los servicios que ofrece la institución, aumento de la seguridad con base en la gestión por procesos, reducción de costes y mejora de los procesos y servicios, entre otros.

La metodología propuesta y aplicación del SGSI le permitirá a su vez a las directivas de la Universidad mantener una visión general del estado de los sistemas informáticos, plantear estrategias de cambio y mejora de los mismos, verificar las medidas de seguridad aplicadas y los resultados obtenidos, valorar y asegurar sus activos de posibles riesgos y vulnerabilidades presentes, permitiendo la toma de

decisiones de manera consecuente, argumentada y documentada, involucrando a todo el personal en un proceso global que le proporcionará la mejora continua, además de darle las bases para que se considere la certificación del SGSI bajo la Norma ISO 27001.

REFERENCIAS

27001 Academy. (s.f.). *Norma ISO 27001*. Recuperado el 15 de Diciembre de 2014, de http://www.iso27001standard.com: http://www.iso27001standard.com/es/que-es-iso-27001/

Audisec. (Febrero de 2010). *www.audisec.es*. Recuperado el 14 de Diciembre de 2014, de www.globalsgsi.com: http://www.criptored.upm.es/descarga/GUIA_AUDISEC_GLOBALSGSI.pdf

Blog corporativo. (5 de Diciembre de 2013). *Implementación de la norma ISO 27001*. Recuperado el 11 de Diciembre de 2014, de isotools: http://www.isotools.org/2013/12/05/en-inventario-de-activos-en-la-implementacion-de-la-norma-iso-27001/

Chavez, R. (25 de Septiembre de 2013). *Gestión de riesgos de seguridad en la información*. Recuperado el 23 de 11 de 2014, de slideshare: http://es.slideshare.net/roberth.chavez/gestin-del-riesgos-de-seguridad-de-la-informacin

Equipo consultoría Digiware. (26 de Diciembre de 2008). *Modelo de seguridad de la información*. Recuperado el 9 de Diciembre de 2014, de programa.gobiernoenlinea: http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/ModeloSeguridad_SANSI_SGSI.pdf

Fundacion Universitaria Juan de Castellanos. (04 de Diciembre de 2014). Recuperado el 21 de Diciembre de 2014, de http://www.jdc.edu.co/: http://www.jdc.edu.co/nosotros/estructura-organizacional

Gómez, L. (s.f.). *Guía de Aplicación de la Norma UNE-ISO/IEC 2001.* Asociación Española de Normalización y Certificación.

Gutiérres, H. (2010). *Calidad total y productividad.* Ciudad de México: Mc. Graw Hill.

ISO 9001: 2008. (2008). Sistema de Gestión de la Calidad-Requisitos. Ginebra.

Moreno, F. (2009). La ISO/IEC 27005 en la búsqueda de información más segura. Normas y Calidad. ICONTEC.

Ricón, D. (2002). Modelos para la implementación de un sistema de gestión de calidad basado en la norma ISO 9001. *Universidad EAFIT No. 126*, 47-55.

Walton, M. (1992). *El Método de Deming en la Práctica.* Barcelona: Norma.

ANEXOS

Anexo 1. Controles y Objetivos de Control para FU Juan de Castellanos

Sección	Subsección	Objetivo	Control	Aplicar Sí/No	Justificación
A.5 Política de Seguridad	A.5.1 Política de Seguridad de la Información	Proporcionar dirección gerencial y apoyo a la seguridad de la información mediante los requerimientos Institucionales, Locales, Nacionales, legislación y	5.1.1 Documento de la Política de Seguridad de la Información	SÍ	Establecida y exigida por la Norma UNE/ISO – IEC 27001. Se recomienda seguir la Guía de buenas prácticas ISO 27002:2008, donde se establece la normatividad para la implementación de la política de seguridad informática.

		regulación del sector Educativo en la Fundación Universitaria Juan de Castellanos.	5.1.2 Revisión de la política de Seguridad de la Información	SÍ	Establecida y exigida por la Norma UNE/ISO – IEC 27001
A.6 Organización de la Seguridad de la Información	A.6.1 Organización Interna	Manejar la seguridad de la información dentro de la Universidad.	6.1.1 Compromiso del Consejo Superior con la seguridad de la información	SÍ	Establecida y exigida por la Norma UNE/ISO – IEC 27001.
			6.1.2 Coordinación de la seguridad de la información	SÍ	Establecida y exigida por la Norma UNE/ISO – IEC 27001.
			6.1.3 Asignación de responsabilidades	SÍ	Establecida y exigida por la Norma UNE/ISO – IEC 27001.

			en seguridad de la información		
			6.1.4 Proceso de autorización para los medios de procesamiento de información	SÍ	Establecida y exigida por la Norma UNE/ISO – IEC 27001.
			6.1.5 Acuerdos de confidencialidad	SÍ	Establecida y exigida por la Norma UNE/ISO – IEC 27001.
			6.1.6 Contacto con las autoridades	SÍ	Se requiere tener contacto con las autoridades relevantes.
			6.1.7 Contacto con grupos de interés especial	SÍ	Se requiere mantener contactos especializados, listas de correo, revistas, sitios web, periódicos, etc.

			6.1.8 Revisión independiente de la seguridad de la información	SÍ	Los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información, si es el caso, se pueden revisar independientemente a intervalos planeados o cuando ocurran cambios significaciones para la implementación de la seguridad.
	A.6.2 Entidades Externas – Terceras partes	Mantener la seguridad de la información y los medios de procesamiento de información a los cuales entidades	6.2.1 Identificación de riesgos relacionados con terceras partes o entidades externas	SÍ	Se deben identificar los riesgos que corre la información y los medios de procesamiento de datos de la Universidad e implementar los controles apropiados antes de dar

		externas tienen acceso y procesan.			acceso a terceras personas.
			6.2.2 Gestión de la Seguridad al tratar con clientes (estudiantes)	SÍ	Identificar y tratar todos los requerimientos de seguridad antes de otorgar acceso a los estudiantes a la información o activos de la Universidad.
			6.2.3 Gestión de la Seguridad en contratos con terceras partes o con entidades externas	SÍ	Todos los acuerdos que involucran acceso, procesamiento, comunicación o manejo de información por parte de terceras personas deben tener en cuenta los requerimientos de seguridad necesarios y relevantes.
A.7 Gestión de Activos	A.7.1 Responsabilidades de los activos	Lograr y mantener la protección apropiada de los	7.1.1 Inventario de activos	SÍ	Establecida y exigida por la Norma UNE/ISO – IEC 27001.

		activos. organizacionales.			
			7.1.2 Propiedad de los activos	SÍ	Establecida y exigida por la Norma UNE/ISO – IEC 27001.
			7.1.3 Utilización aceptable de los activos	SÍ	Se deben colocar parámetros de uso aceptable de los activos.
	A.7.2 Clasificación de la información	Garantizar que la información reciba un nivel de protección adecuado.	7.2.1. Guía de clasificación	SÍ	Establecida y exigida por la Norma UNE/ISO – IEC 27001.
			7.2.2 Etiquetado y tratamiento de información	SÍ	Establecida y exigida por la Norma UNE/ISO – IEC 27001.

A.8 Seguridad de la Gestión de los Recursos Humanos	A.8.1 Antes de la contratación	Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades y sean adecuados para los roles asignados con el propósito de reducir el riesgo de robo, fraude o mal uso de los medios.	8.1.1 Roles y responsabilidades	SÍ	Es necesario tener en cuenta este ítem por el tipo de contratación que maneja la Universidad (contratos de corta duración). Definición y documentación de roles y responsabilidades de seguridad de los empleados y terceros de acuerdo con la política de seguridad.
			8.1.2 Análisis y Selección	SÍ	Control del proceso de selección de personal académico y administrativo.
			8.1.3 Términos y condiciones de empleos	SÍ	Se deben documentar dentro de cláusulas en los contratos de trabajo, dando a conocer al

					empleado y ratificando mediante su firma.
	A.8.2 Durante el Empleo	Asegurar que todos los empleados, contratista y terceros estén al tanto de las amenazas y vulnerabilidades relacionadas con la seguridad de la información, sus responsabilidades y obligaciones y que se encuentren equipados para apoyar la política de seguridad organizacional dentro de su desempeño laboral.	A.8.2.1 Gestión de responsabilidades	SÍ	Requisitos de aplicabilidad de la seguridad de la información por parte de empleados, contratistas terceros de acuerdo con la política de seguridad de la información establecida.
			A.8.2.2. Concienciación, formación y entrenamiento sobre seguridad de la información	SÍ	Se deben realizar jornadas de concienciación, formación y entrenamiento sobre seguridad informática teniendo en cuenta que esto puede ser un factor de amenaza.
			A.8.2.3 Proceso Disciplinario	Aplicar	Debe existir un manual de sanciones y aplicación

					de procesos disciplinarios para los empleados que incurran en faltas contra la seguridad de la información.
	A.8.3 Terminación o Cambio de Empleo	Asegurar que el personal administrativo o docente, salgan de la Institución o cambien de empleo de una manera ordenada y segura.	A.8.3.1 Responsabilidades ante la terminación de la vinculación	SÍ	Se debe crear un manual de responsabilidades y deberes del empleado como del empleador para asegurar la correcta desvinculación de los empleados, contratistas y terceros que salen de la Universidad, teniendo en cuenta la legislación vigente.

			A.8.3.2 Devolución de activos	SÍ	Cuando el empleado cesa debe devolver todos los activos a cargo, proceso soportado mediante acta de entrega y firma de paz y salvo.
			A.8.3.3 Retirada de los derechos de acceso	SÍ	Proceso para evitar los accesos a la información por parte de personal retirado de la Institución.
A.9. Seguridad física y del entorno	A.9.1 Áreas Seguras	Evitar accesos físicos no autorizados, daño e interferencia a las Sedes e información Institucional.	A.9.1.1 Perímetro de seguridad física	SÍ	Aplicación de controles físicos de entrada proporcionales al tamaño y actividad de la Institución.
			A.9.1.2 Controles de entradas físicos	SÍ	Aplicación de controles físicos de entrada proporcionales al tamaño y actividad de la Institución.

			A.9.1.3 Seguridad de oficinas, unidades, salas de cómputo e instalaciones	SÍ	Aseguramiento de todas las dependencias e instalaciones de la Universidad, acorde con la legislación y normas de seguridad vigentes.
			A.9.1.4 Protección contra amenazas externas y ambientales	SÍ	Aseguramiento de todas las dependencias e instalaciones de la Universidad, acorde con la legislación y normas de seguridad vigentes.
			A.9.1.5 Trabajo en áreas seguras	SÍ	Diseño y aplicación de protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastres naturales o creados por el hombre en todas las

					dependencias, unidades, salas de informáticas.
			A.9.1.6 Áreas de acceso público entrega y cargue	SÍ	Control de puntos de acceso zonas de entrega y descarga suministros de almacén, correspondencia, traslado de inmuebles, parqueaderos, etc., aislamiento de las áreas de proceso de información para evitar accesos no autorizados.
	A.9.2 Seguridad de equipo	Evitar la pérdida de daño robo o compromiso de los activos y la interrupción de las actividades de la Institución.	A.9.2.1 Ubicación y protección de equipos	SÍ	Los equipos deben estar protegidos de accesos no autorizados mediante ubicaciones físicas y lógicas seguras en áreas controladas por personal autorizado y salas cerradas bajo llave.

			A.9.2.2. Servicios públicos de soporte	SÍ	Se cuenta con Planta de energía para proteger los equipos de fallas de energía y otras interrupciones de los servicios públicos.
			A.9.2.3 Seguridad en el cableado	SÍ	Garantizar que las instalaciones y disposición del cableado sea segura.
			A.9.2.4 Mantenimiento de los equipos	SÍ	Los equipos deben tener un proceso de mantenimiento que garantice su continuidad y correcto funcionamiento.
			A.9.2.5 Seguridad del equipo fuera de las instalaciones	SÍ	Aplicación de seguridad a los equipos que se trasladen fuera de la instalaciones de la organización, claves de acceso, autorización y

					procedimiento de salida y entrega del mismo.
			A.9.2.6 Eliminación o re-uso seguros de equipos	SÍ	Procedimiento de chequeo de equipos con medios de almacenamiento, para asegurar que se haya removido o sobre – escrito de manera segura cualquier dato confidencial y software con licencia antes de su eliminación. Formateo de equipos en el momento de su reutilización.
			A.9.2.7 Extracción de elementos de la propiedad	SÍ	Procedimiento de autorización de entradas y salidas de elementos.
A.10 Gestión de las	A.10.1 Procedimientos	Asegurar la operación correcta y segura de los	A.10.1.1 Procedimientos	SÍ	Establecida y exigida por la Norma UNE/ISO – IEC 27001.

comunicaciones y las operaciones	operativos y responsabilidades	medios de procesamiento de información.	operativos documentados		
			A.10.1.2 Gestión de cambios	SÍ	Se deben controlar los cambios en los medios y sistemas de procesamiento de información.
			A.10.1.3 Separación de funciones	SÍ	Separar las funciones y áreas de responsabilidad para reducir el riesgo de modificación o pérdida de información (intencionadamente o no) y el mal uso de los activos de la Institución.
			A.10.1.4 Separación de las instalaciones de desarrollo, prueba y operación	SÍ	No se considera que este control influya, toda vez que se contrata con entidades externas el desarrollo de software

					que requiere la institución.
	A.10.2 Gestión de los servicios suministrados por terceros.	Implementar y mantener el nivel apropiado de seguridad de la información y entrega del servicio en línea con los contratos de entrega del servicio de terceros.	A.10.2.1 Suministro del servicio	SÍ	Asegurar que los terceros operen y mantengan los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en los contratos de servicios con terceros.
			A.10.2.2 Monitoreo y revisión de servicios de terceras partes	SÍ	Los servicios, reportes y registros provistos por terceros deben ser monitoreados y revisados y las auditorías se deben llevar a cabo periódicamente.
			A.10.2.3 Gestión de cambios a los	SÍ	Procedimiento que permita manejar los

			servicios de terceras partes		cambios en la provisión de servicios con terceros.
	A.10.3 Planeación y aceptación del sistema.	Minimizar el riesgo de fallas en los sistemas.	A.10.3.1 Gestión de capacidad	SÍ	Monitorear, afinar y realizar proyección del uso de los recursos para asegurar el desempeño del sistema requerido.
			A.10.3.2 Aceptación del sistema	SÍ	Procedimiento y criterios de aceptación para los sistemas nuevos, actualizaciones y versiones nuevas, establecimiento de pruebas adecuadas antes de su aceptación y adquisición.
	A.10.4 Protección contra software malicioso y código móvil	Proteger la integridad del software y la información.	A.10.4.1 Controles contra software malicioso	SÍ	Implementar mecanismos de control, identificación y eliminación de software malicioso (antivirus, anti spyware).

					Procedimientos de concienciación adecuados.
			A.10.4.2 Controles contra código móvil	SÍ	Implementar mecanismos para evitar la ejecución de código móvil no autorizado.
	A.10.5 Copias de seguridad	Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.	A.10.5.1 Back – ups o respaldo de información	SÍ	Se requiere realizar copias de seguridad de la información para evitar pérdida de información y realizar su verificación de acuerdo con la política.
	A.10.6 Gestión de Seguridad de Redes	Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.	A.10.6.1 Controles de Red	SÍ	Uso de firmas digitales para transmisión de datos sensibles, manejo y control adecuado de las redes para protección de la información en tránsito.

			A.10.6.2 Seguridad de los servicios de red	NO	El costo de implementación supera el beneficio obtenido.
	A.10.7 Gestión de medios	Evitar la divulgación, modificación, eliminación o destrucción no autorizada de los activos y la interrupción de las actividades.	A.10.7.1 Gestión de soportes removibles	SÍ	Se requiere para evitar riesgos de pérdida de información.
			A.10.7.2 Descarte de medios de almacenamiento de información	SÍ	Establecer procedimiento para eliminación de medios de manera segura.
			A.10.7.3 Procedimiento de manejo de la información	SÍ	Aplicar procedimiento para el manejo de información para evitar su divulgación o mala utilización.

			A.10.7.4 Seguridad de documentación del sistema	SÍ	Proteger la documentación de un acceso no autorizado.
	A.10.8 Intercambio de Información	Mantener la seguridad de la información y software intercambiados dentro de la Institución y con entidades externas.	A.10.8.1 Procedimientos y políticas de intercambio de información	SÍ	Establecer políticas, procedimientos y controles de intercambio de información a través de cualquier medio de información.
			A.10.8.2 Acuerdos de intercambio	NO	No se realizan intercambios de información.
			A.10.8.3 Soportes físicos en tránsito	NO	No se manejarán soportes físicos fuera de las instalaciones de la institución.
			A.10.8.4 Mensajería electrónica	SÍ	Se deben proteger adecuadamente los mensajes electrónicos.

			A.10.8.5 Sistemas de información de negocio	NO	Este control no reduciría el riesgo de exposición de los activos identificados.
	A.10.9 Servicio de comercio electrónico	Garantizar la seguridad de los servicios de comercio electrónico.	A.10.9.1 Comercio Electrónico	NO	No se maneja servicio de comercio electrónico por parte de la institución.
			A.10.9.2 Transacciones en línea	SÍ	Establecer procedimientos y políticas que permitan proteger la información involucrada en las transacciones en línea, evitando transmisión incompleta, rutas equivocadas, alteración no autorizada del mensaje, divulgación no autorizada, y duplicación

					o re-envío no autorizado del mensaje.
			A.10.9.3 Información	SÍ	Procedimientos de control y revisión de la información disponible al público para evitar daños en su integridad, autenticidad y disponibilidad.
	A.10.10 Monitoreo	Detectar actividades de procesamiento de información no autorizados.	A.10.10.1 Registros de auditoría	SÍ	Aplicar mecanismos de control de acceso y producción de registros de eventos, auditoría, excepciones y mantenerlos durante un periodo establecido como soporte para realizar seguimiento y auditorías futuras.
			A.10.10.2 Uso del sistema de monitorización	SÍ	Establecer procedimientos para monitoreo de los

					sistemas informáticos y revisar estas actividades.
			A.10.10.3 Protección de la información de log	SÍ	Procedimiento para la protección de los medios de registro y la información del registro contra alteraciones y accesos no autorizados.
			A.10.10.4 Registros del administrador y operador	SÍ	Se debe realizar el registro de actividades del administrador y operador del sistema (propietario, usuarios, estudiantes, docentes, etc.)
			A.10.10.5 Registros de Fallos	SÍ	Procedimiento para registro, análisis y tratamiento de fallos presentados en el sistema.

			A.10.10.6 Sincronización de relojes	SÍ	Realizar sincronización de relojes a los sistemas de procesamiento de información más relevante con una fuente de tiempo exacta acordada.
A.11 Control de Accesos	A.11.1 Requerimientos institucionales para el control de acceso	Controlar el acceso a la información.	A.11.1.1 Política de acceso	SÍ	Establecer, documentar y revisar la política de control de acceso con base en los requerimientos institucionales y de seguridad.
	A.11.2 Gestión del Acceso del usuario	Asegurar el acceso al sistema a los usuarios autorizados y restringir a los no autorizados.	A.11.2.1 Registro de usuarios	SÍ	Procedimiento para accesos y restricciones de usuarios de los sistemas de información.
			A.11.2.2 Gestión de privilegios	SÍ	Asignación, control y revisión de asignación de

					privilegios de usuarios y administrador de los sistemas de información. Administración a nivel de servidor.
			A.11.2.3 Gestión de contraseñas de usuarios	SÍ	Proceso de gestión formal de la asignación y uso de claves de usuarios.
			A.11.2.4 Revisión de los derechos de acceso del usuario	SÍ	Se aplicaría bajo petición del responsable directo del usuario.
	A.11.3 Responsabilidades del usuario	Garantizar la seguridad ante accesos no autorizados, robo o alteración de la información y/o medios de procesamiento.	A.11.3.1 Uso de contraseñas	SÍ	Requisitos de buenas prácticas de seguridad en el manejo y uso de contraseñas por parte de los usuarios.

			A.11.3.2 Equipo desatendido por el usuario	SÍ	Requisitos de seguridad para la protección de los equipos por parte de los usuarios.
			A.11.3.3 Política de mesas y pantallas limpias	SÍ	Adopción y documentación de política de mesas y pantallas limpias para los documentos, medios de almacenamiento removibles y medios de procesamiento de información.
	A.11.4 Control de acceso a la red	Evitar el acceso no autorizado a los servicios en red.	A.11.4.1 Política sobre el uso de servicios en red	SÍ	Especificación de acceso a usuarios a la red.
			A.11.4.2 Autenticación de usuarios para conexiones externas	SÍ	Uso de métodos de autenticación de usuarios para controlar el acceso de usuarios remotos.

			A.11.4.3 Identificación de equipos en red	SÍ	Uso de identificadores de equipos que se conectan a la red (Wi-Fi)
			A.11.4.4 Protección del puerto de diagnóstico remoto	SÍ	Control de acceso físico y lógico a los puertos de diagnóstico y configuración.
			11.4.5 Segmentación de redes	SÍ	Dividir servicios de información, usuarios y sistemas de información en redes separadas.
			11.4.6 Control de conexión de redes	SÍ	Restringir la capacidad de conexión de los usuarios en las redes compartidas, sobre todo aquellas que están fuera de los límites institucionales, de acuerdo con la política de control de acceso.
			A.11.4.7. Control de re	SÍ	Garantizar que las conexiones de red y los

			encaminamiento de redes		flujos de información no se salgan de los límites establecidos en la política de control de acceso.
	A.11.5 Control de acceso a los sistemas de operación	Evitar accesos no autorizados a los sistemas operativos.	A.11.5.1 Procedimiento de registro en el terminal	SÍ	Control de acceso a los sistemas de información y límite de intentos de ingreso.
			A.11.5.2 Identificación y autenticación del usuario	SÍ	Cada usuario (docentes, administrativos y estudiantes) contarían con un usuario y una contraseña de acceso al sistema.
			A.11.5.3 Sistemas de Gestión de Contraseñas	SÍ	Proceso de asignación, control, monitoreo y cancelación de usuario y contraseña por usuario.
			A.11.5.4. Uso de utilidades del sistema	SÍ	Restricción y acceso a las utilidades del sistema dependiendo el tipo de usuario.

			A.11.5.5 Sesión Inactiva	SÍ	Controlar los tiempos de uso de sesión para evitar accesos no autorizados en aplicaciones y equipos.
			A.11.5.6 limitación en el tiempo de conexión	SÍ	Establecimiento de controles de tiempo de conexión para evitar mal uso del servicio.
	A.11.6 Control de acceso a las aplicaciones y la información	Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.	A.11.6.1 Restricciones de acceso a la información	SÍ	Administración de acceso por usuarios teniendo en cuenta sus funciones y necesidades del servicio.
			A.11.6.2 Aislamiento de sistemas sensibles	SÍ	La información sensible de los usuarios se debe resguardar en lugares y medios aislados y dedicados para su seguridad.

	A.11.7 Computación móvil y teletrabajo	Garantizar la seguridad de la información cuando se utilicen medios de computación móvil y teletrabajo.	A.11.7.1 Computación móvil comunicaciones	SÍ	Adopción de política, plan de operación y procedimientos para el uso de medios de computación y comunicaciones móviles.
			A.11.7.2 Teletrabajo	NO	No se utiliza este servicio en la Institución y no se considera que el costo de implementación del control supere el beneficio obtenido.
OTROS CONTROLES A TENER EN CUENTA					
Sección			**Subsección**		**Descripción**
A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información			A.12.1.1		Especificar los controles de seguridad para los sistemas de información nuevos o actualizaciones de los existentes.
A.12.2 Procesamiento correcto en las aplicaciones			A.12.2.1, A12.2.2, A.12.2.3, A.12.2.4		Aplicar mecanismos de seguridad en las

		aplicaciones para evitar fallas de autenticación, integridad o disponibilidad de la misma. Establecer requisitos de seguridad al realizar la adquisición del software.
A.12.3. Controles Criptográficos	A.12.3.1, A12.3.2	Uso de medios criptográficos en las aplicaciones para proteger la información.
A.12.4. Seguridad en los archivos del sistema	A.12.4.1, A12.4.2, A.12.4.3	Proteger los archivos del sistema garantizando su seguridad y administración desde el servidor para evitar modificaciones.
A.12.5 Seguridad en los procesos de desarrollo y soporte	A.12.5.1, A12.5.2, A.12, 5.3, A.12.5.4, A.12.5.5,	Mantenimiento de la seguridad del software e información del sistema.

A.12.6 Gestión de vulnerabilidad técnica	A.12.6.1	Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.
A.13 Gestión de incidentes en la seguridad de la información	A.13.1,1, A.13.1.2	Procedimiento para el manejo de eventos y debilidades en la seguridad de los sistemas de información y toma de acciones correctivas y oportunas.
A.13.2 Gestión de incidentes y mejoras en la seguridad de la información	A.13.2.1, A.13.2.2, A.13.2.3	Asegurar que se aplique un enfoque consistente y efectivo a la gestión de la información.
A.14 Gestión de la continuidad del negocio	A.14.1.1, A14.1,2, A.14.1.3, A.14.1.4, A.14.1.5	Contrarrestar las interrupciones de las actividades del negocio y proteger los procesos críticos.

A.15 Cumplimiento	A.15.1.1, A15.1,2, A.15.1.3, A.15.1.4, A.15.1.5. A.15.1.6	Cumplimiento de requerimientos legales para evitar cualquier violación y requerimiento sancionatorio.
A.15.2 Cumplimiento con las políticas y estándares de seguridad y el cumplimiento técnico	A.15.2.1, A.15.2.2	Asegurar el cumplimiento de los sistemas con la política y estándares de seguridad institucionales.
A.15.3 Consideraciones de auditoría de los sistemas de información	A.15.3.1, A.15.3.2	Maximizar la efectividad y minimizar la interferencia desde el proceso de auditoría de los sistemas de información.