ELABORACIÓN DE UN PLAN DE IMPLEMENTACIÓN DE LA ISO/IEC 27001:2013 PARA LA UNIDAD DE GST

Nombre Estudiante: María Fernanda Chaparro Ronderos

Programa: Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Área: Sistemas de Gestión de la Seguridad de la Información

Consultor: *Antonio José Segovia Henares*
Profesor responsable de la asignatura: Carles Garrigues Olivella
Centro: Universitat Oberta de Catalunya

Fecha entrega: 6 de junio de 2016

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013 para la unidad de GST*
Nombre del autor:	*María Fernanda Chaparro Ronderos*
Nombre del consultor/a:	*Antonio José Segovia Henares*
Nombre del PRA:	*Carles Garrigues Olivella*
Fecha de entrega (mm/aaaa):	06/2016
Titulación::	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Área del Trabajo Final:	*Sistemas de Gestión de la Seguridad de la Información*
Idioma del trabajo:	*Español*
Palabras clave	*Gestión, ISO 27001:2013, Seguridad.*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

El presente trabajo consiste en la elaboración de un plan de implementación de la norma ISO 27001:2013 en la unidad de Gerencia de Servicios Tecnológicos (GST) de una Corporación Universitaria ubicada en Colombia. El trabajo se dividió en las siguientes fases: recopilación de información del estado actual de la unidad en materia de sus procesos de seguridad de la información de acuerdo a los dominios y a las cláusulas, desarrollo del sistema de gestión documental básico, análisis de riesgos de los activos de la unidad, propuestas de proyectos para disminuir los niveles de riesgo, y la ejecución finalmente de una auditoría de cumplimiento.

Dentro de este proceso se elaboraron algunos de los documentos requeridos, tales como el plan de auditoría, y se propusieron proyectos que pretenden mejorar algunos dominios de seguridad que se encontraban desatendidos. Estos resultados serán visibles en el mediano plazo. Adicionalmente y a través de la auditoría, se evidenciaron las no conformidades que permitirán la formulación de acciones para algunos procesos de la unidad, de modo que se cumpla y mejore sus políticas de seguridad.

El desarrollo del proyecto encontró que la GST cuenta con un estado de madurez de la seguridad reproducible en el cual se hacen esfuerzos, pero que debe contar con un mayor acompañamiento y compromiso de la alta dirección en lo concerniente a la aprobación de las políticas, y la organización y planificación de la seguridad de la información.

Abstract (in English, 250 words or less):

The present paper consists of development of an ISO 27001:2013 implementation plan at the Management Unit Technology Services (GST) Corporation located in Colombia. The work was divided into the following phases: information gathering on the current status of the unit in terms of its information security processes according to the domains and the clauses, development of a basic document management system, risk analysis of the assets of the unit, proposals for projects to reduce risk levels, and finally the implementation of a compliance audit.

In this process there were prepared some of the required documents, such as the audit plan, and projects were proposed aiming to improve some security domains that were underserved. These results will be visible in the medium term. Additionally and through the audit, there were evident non conformities that will allow the formulation of actions for some unit processes, so that compliance and improve their security policies.

The project found that the GST has a maturity state of the reproducible security in which efforts are made, but they should have a greater support and commitment of senior management with regard to the adoption of policies, and the organization and planning of information security.

Índice

Lista de figuras

Lista de tablas

1. Introducción

1.1 Contexto y justificación del Trabajo

El Plan Director de Seguridad es uno de los elementos clave con que debe trabajar el Responsable de Seguridad de una organización. Este plan constituye la hoja de ruta que debe seguir la empresa para gestionar de una forma adecuada la seguridad, permitiendo no sólo conocer el estado de la misma, sino en qué líneas se debe actuar para mejorarla. Se habla, por tanto, de un modelo de mejora continua PDCA (Plan-Do-Check-Act).

El presente plan pretende reunir la definición de las políticas y los objetivos de seguridad, el análisis diferencial en base a la ISO/IEC 27001:2013 e ISO/IEC 27002, la identificación de los activos de valor corporativos para la metodología de análisis de riesgos, la elaboración de propuestas que lleven a la organización al cumplimiento de los objetivos propuestos, terminando con una evaluación de madurez y nivel existente dentro de una organización de tipo universitario en Colombia, específicamente en su área de TI de la sede principal (unidad de Gerencia de Servicios Tecnológicos), con el objetivo de establecer las bases de un SGSI (Sistema de Gestión de la Seguridad de la Información) teniendo en cuenta que lo que interesa son los Sistemas de Información que dan soporte a actividades y servicios de dicha área. Las áreas de docencia y administrativa no serán tenidas en cuenta en este estudio, debido a lo grande de la organización (Más de 10 sedes físicas).

1.2 Objetivos del Trabajo

1.2.1. Objetivo general

El objetivo general de este trabajo es integrar las estrategias de seguridad de la información, así como la documentación y políticas de la oficina de gerencia de Servicios Tecnológicos (GST), en un sistema de Gestión de la seguridad de la información, basados en la norma ISO/IEC 27001:2013, para mejorar en el corto, mediano y largo plazo los aspectos de seguridad de dicha oficina, relacionados con los dominios y las cláusulas que se encuentran en su estado inicial de maduración, de acuerdo con el análisis diferencial realizado. Con los resultados obtenidos de este trabajo se pretende sentar las bases para que la unidad de GST logré certificarse en ISO/IEC27001:2013 en el mediano plazo.

1.2.2. Objetivos específicos

- Alinear los procesos de la oficina de GST para cumplir con los requisitos de la norma ISO 27001:2013.

- Generar los planes de continuidad de negocio, o reducir el número de incidentes de seguridad no tratados.

- Identificar los procesos que permitan realizar los controles y gestionar el SGSI, además de la creación de la documentación necesaria en los formatos de gestión documental con los que cuenta la Corporación universitaria XX.

- Generar la confianza en los directivos, funcionarios administrativos y académicos, con respecto a las aplicaciones, sistemas de información que se desarrollan y utilizan normalmente.

- Generar el plan de capacitación y concientización tanto de los directivos, como de los funcionarios administrativos y académicos, para lograr una mejor educación en el manejo de los activos de información.

1.3 Enfoque y método seguido

El proyecto plantea el establecimiento de las bases para la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información). Dentro de las posibles estrategias a trabajar se encontraba la adaptación del sistema de gestión de seguridad de la empresa a un plan maestro ya existente, la creación de un plan maestro de seguridad desde ceros. Después de una revisión inicial se optó por desarrollar un plan maestro de seguridad

Documentación normativa sobre las mejores prácticas en seguridad de la información.
Definición clara de la situación actual y de los objetivos del SGSI.
Análisis de Riesgos.
Identificación y valoración de los activos corporativos como punto de partida a un análisis de riesgos.
Identificación de amenazas, evaluación y clasificación de las mismas
Evaluación del nivel de cumplimiento de la ISO/IEC 27002:2013 en la organización.
Propuestas de proyectos de cara a conseguir una adecuada gestión de la seguridad.
Esquema Documental.

1.4 Planificación del Trabajo

En el archivo ANEXO L “plan maestro”, se encuentra el diagrama de Gantt asociado con la descripción de actividades, tares, e hitos parciales de cada una de las PEC del proyecto.

1.5 Breve sumario de productos obtenidos

Los productos obtenidos del presente trabajo se describen a continuación, y la descripción detallada se hará en los capítulos siguientes.

- Informe Análisis Diferencial
- Esquema Documental ISO/IEC 27001
- Análisis de Riesgos
- Plan de Proyectos
- Auditoría de Cumplimiento
- Presentación de resultados

1.6 Breve descripción de los otros capítulos de la memoria

A lo largo del documento se irá haciendo una serie de análisis, desglose de información, propuestas y elaboración de documentos, que permitan la generación de una propuesta de plan director de seguridad de la información, teniendo en cuenta los pasos para su formulación. Se comenzará con un análisis del estado actual de la oficina (unidad) de GST en relación con la seguridad de la información ((Capítulo 2), mediante un análisis diferencial o de brecha, con respecto a las cláusulas de la norma ISO 27001:2013 y los dominios de control de ISO 27002:2013. Seguidamente, se abordará lo concerniente al esquema documental necesario para el cumplimiento normativo, de acuerdo a lo exigido por la propia norma. En este apartado (Capítulo 3) se explica la función de cada uno de ellos dentro del plan director, su objetivo, y su alcance. Se hace una identificación de la documentación existente y se elaboran y proponen los documentos faltantes. Seguidamente se genera el análisis de riesgos, basados en la metodología MAGERIT, identificando activos, criticidad, impacto, amenazas, riesgos tanto aceptable como residual. Con este análisis se llega finalmente a la propuesta de proyectos que ayuden a mitigar los mayores riesgos encontrados en el corto y mediano plazo. Finalmente se realiza una auditoría de cumplimiento para evaluar el estado de madurez de los controles implantados, y para determinar el nivel de las cláusulas de la norma. Esto le dará a la Universidad una pauta para desarrollar sus planes a corto y mediano plazo en materia de seguridad de la información.

1.7. Orígenes de la norma ISO 27001

Con el advenimiento de las TIC y de nuevas formas de comercio, la información se ha convertido en un activo de vital importancia para las empresas y las organizaciones hasta el punto de necesitar el aseguramiento de dicha información y los sistemas que la procesan y almacenan.

Para gestionar adecuadamente la seguridad de la información, se hizo necesaria la creación de un sistema que de forma metódica y a través de la documentación, cumpla con los objetivos de seguridad planteados por la organización y permita la evaluación de los riesgos a los que se ve sometida.

Debido a lo anteriormente dicho aparece el conjunto de estándares ISO/IEC 27000, los cuales proporcionan el marco para la gestión de la seguridad de la información de la organización, sea pública o privada. A continuación veremos un pequeño recorrido por la creación y actualización de dichos estándares hasta el día de hoy.

En el año de 1995, aparece por primera vez el "conjunto de buenas prácticas para la gestión de la seguridad de la información"; esta norma, denominada BS7799, fue diseñada por el British Standards Institution, entidad de normalización internacional creada en el año 1901.

"La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente[1]. La primera parte de esta norma fue adoptada sin grandes cambios por ISO en el año 2000 como ISO 17799.

En 2005, con numerosas empresas certificadas en BS7799-2, ISO publicó el estándar 27001, a la vez que se revisó y actualizó la ISO17799, norma que el año 2007 fue renombrada como ISO 27002:2005.

ISO/IEC 27001:2005 fue revisada y reorganizada en septiembre de 2013. "de la información" [2]. Esta es la norma que es certificable por auditores externos." En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados"(«ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información», s. f.). En España esta norma se publicó como UNE-ISO/IEC 27001:2014, con modificaciones

adicionales con respecto a la declaración de aplicabilidad en 2015 en el documento ISO/IEC 27001:2013/Cor.2:2015.

ISO/IEC 27002 es una guía de buenas prácticas en seguridad de la información, la cual no es certificable. Describe tanto los objetivos de control, como los controles recomendables para la organización. Consta de 11 dominios, 39 objetivos de control y 133 controles. En el año 2000 fue publicada por la ISO y por la comisión electrotécnica Internacional el estándar ISO/IEC 17799:2000 bajo el título de “Information technology - Security techniques - Code of practice for information security management”, después de haber sido publicada por primera vez por el British Standards Institution bajo el nombre de BS-7799-1. Tras un período de revisión y actualización de los contenidos de este estándar se publicó en el año 2005 como ISO/IEC 17799:2005. Con la aprobación de la norma ISO/IEZAC 27001 en octubre de 2005 y la reserva de la numeración 27.000 para la Seguridad de la Información, el estándar IGFSO/DIEC 17799:2005 pasó a ser renombrado como ISO/IEC 27002 en el año 2007. Fue publicada desde el 1 de julio de 2007. “Publicada en España como UNE-ISO/IEC 27002:2009 desde el 9 de Diciembre de 2009”(«ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información», s. f.). En Colombia se consigue bajo el nombre de (NTC-ISO-IEC 27002). Esta norma, al igual que 27001 fue recientemente actualizada (2013). Una gran novedad es la inclusión del teletrabajo.

1.8. Contextualización

A continuación se realizará una contextualización de la empresa con la cual se trabajará, especificando su unidad de Gestión de Servicios tecnológicos (en adelante llamada GST), la cual es la unidad en la que se realizará el plan de implementación de la ISO 27001:2013, según las necesidades y requerimientos de la institución

1.8.1. La empresa

La Institución de educación Superior XX es un sistema universitario que cuenta con diversas sedes en Colombia, la cual brinda a más de 60.000 estudiantes, con un grupo aproximadamente de 4500 docentes, educación en los niveles de técnico profesional, tecnólogo, y profesional universitario, así como a nivel de posgrado y maestría. Estos servicios son prestados tanto en modalidad presencial como virtual y a distancia.

La estructura organizacional se detalla a continuación:

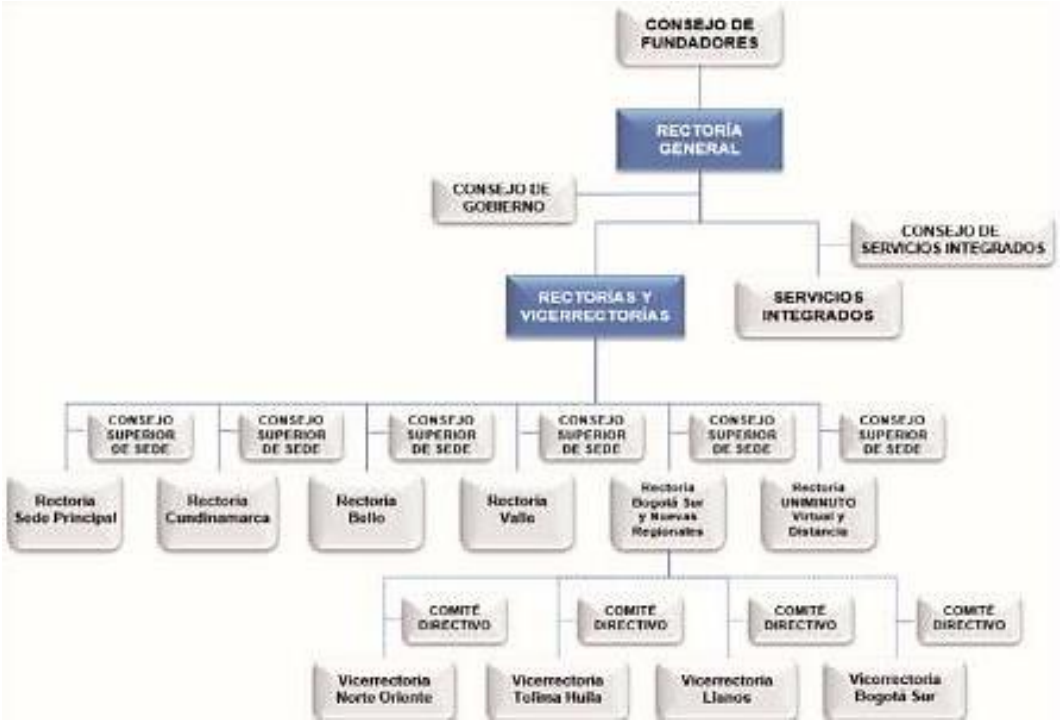


Imagen 1. Infraestructura Institución universitaria

Dentro de las áreas de apoyo se encuentra la unidad de Gerencia de Servicios tecnológicos (GST), la cual es la encargada del manejo de los proyectos y la coordinación de servicios TIC en cada una de las sedes de la Institución, el gobierno de TI, y por supuesto, la administración general de la infraestructura tecnológica existente (Servicios Web, infraestructura de red, etc.). Esta unidad se encuentra ubicada físicamente en la sede principal, la cual está localizada en la ciudad de Bogotá. En la imagen 2 se aprecia el esquema de infraestructura de GST.

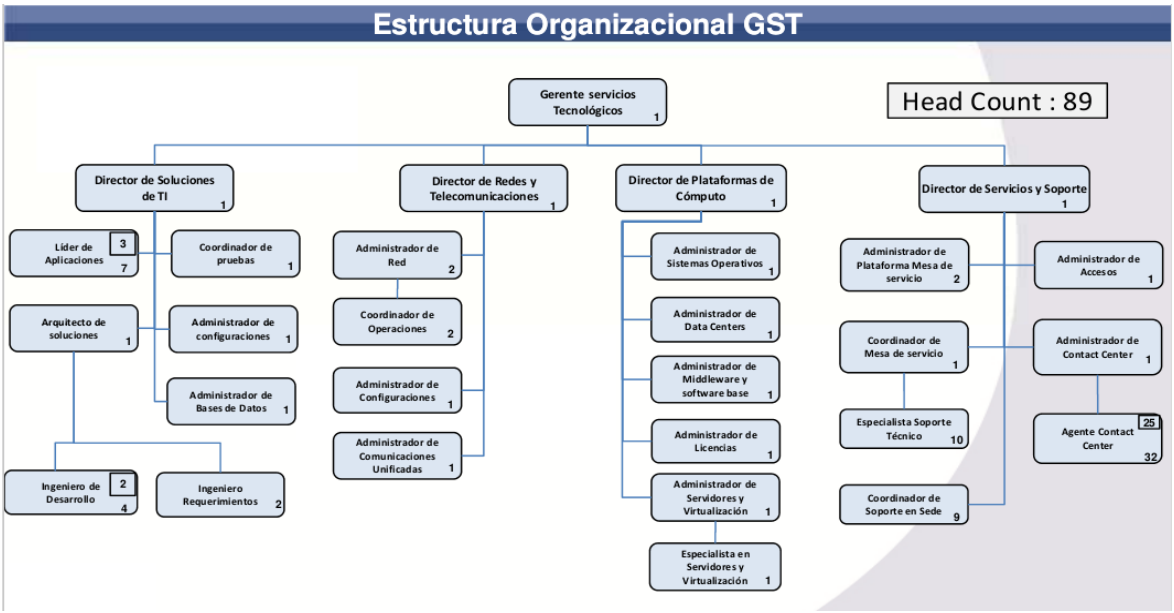


Imagen 2. Infraestructura Gerencia de Servicios Tecnológicos

El mapa de procesos de la Gerencia de Servicios Tecnológicos GST se detalla a continuación:

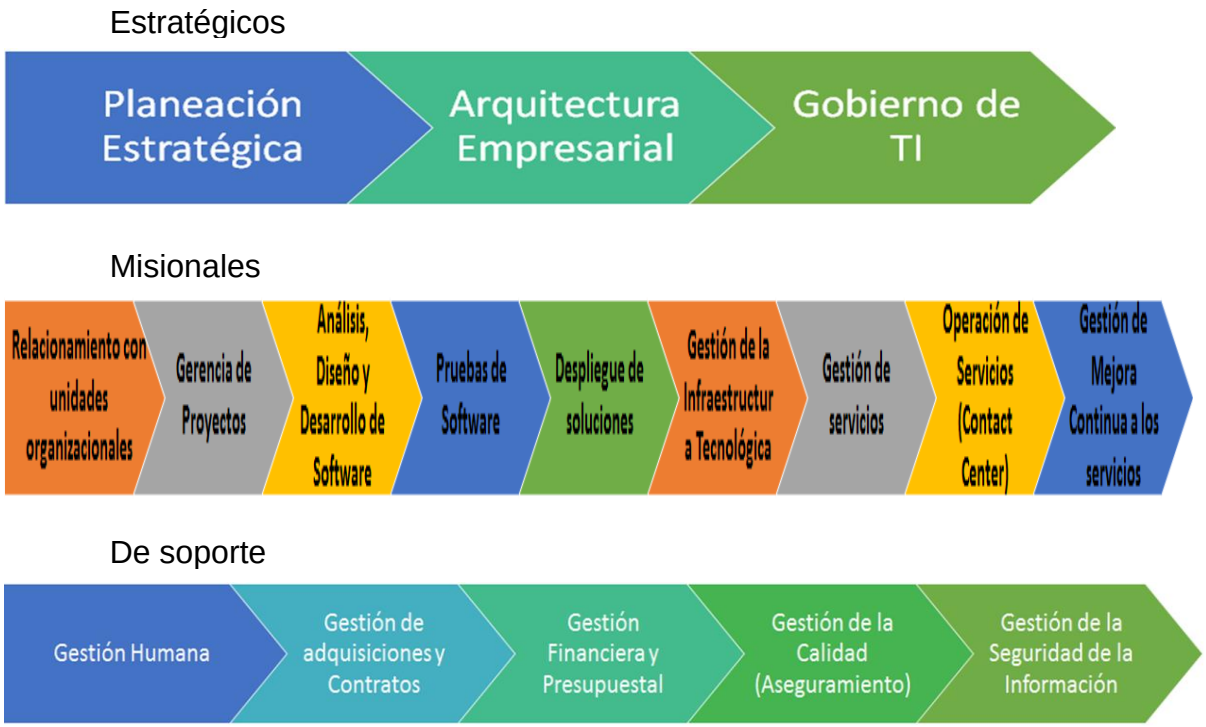


Imagen 3. Mapa de procesos de la GST

La institución cuenta con aplicaciones web, servidores basados en sistemas operativos Windows y Linux, aplicaciones a la medida, sistema de telefonía IP, varias VLAN, entre otros activos, además de tener su propio Call center.

Esta infraestructura es manejada en su totalidad por la unidad de GST, a través de un equipo multidisciplinario que se encarga de la gestión, administración e innovaciones tecnológicas, así como del análisis, diseño y desarrollo de software que permita prestar servicios eficientes y confiables a la comunidad educativa (Docentes, estudiantes y administrativos).

2. Análisis diferencial

Antes de iniciar el proyecto se realiza un análisis diferencial del estado actual de la oficina de GST en relación a la seguridad de la información, tomando como referente de comparación la ISO/IEC 27001:2013 y la ISO/IEC 27002:2013 (En su anexo A), lo cual permitirá observar el estado actual, formular las recomendaciones y los planes de mejora.

Análisis diferencial ISO/IEC 27001:2013

Se elaboró una herramienta en Excel la cual se encuentra en el anexo A, la cual permitió evaluar el estado actual de la oficina de GST, tanto para las cláusulas de la norma 27001: 2013, como para los dominios del Anexo A de la norma la ISO/IEC 27002:2013. En la tabla 1 se muestra la valorización dominios de la ISO/IEC 27002:2013, de acuerdo con los datos entregados por los responsables de la información:

%	Estado	Descripción Criterios clasificación
0	Inexistente (pnp)	Ausencia total de políticas, procedimientos, no hay documentación
10	Inicial (RD)	Hay evidencia de que la organización ha reconocido que los problemas existen y que necesitan ser re sueltos. Sin embargo, no hay procesos estandarizados pero en cambio hay métodos ad hoc que tienden a ser aplicados en forma individual o caso por caso.
50	Repetible (REP)	Los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares emprendiendo la misma tarea. No hay capacitación o comunicación formal de procedimientos estándar y la responsabilidad se deja a la persona
70	Definida (DEF)	Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes
90	Gestionado (MD)	El control se implementó pero no se documentó . Los procesos están bajo constante mejoramiento y proveen buena práctica. Se usa la automatización y herramientas en una forma limitada o fragmentada
100	Optimizado (D)	El control se implementó y se documentó

Tabla 1. Valorización para las cláusulas de requisitos de la ISO/IEC 27001:2013.

El cumplimiento de los requisitos se obtuvo como se observa en el siguiente diagrama radial:

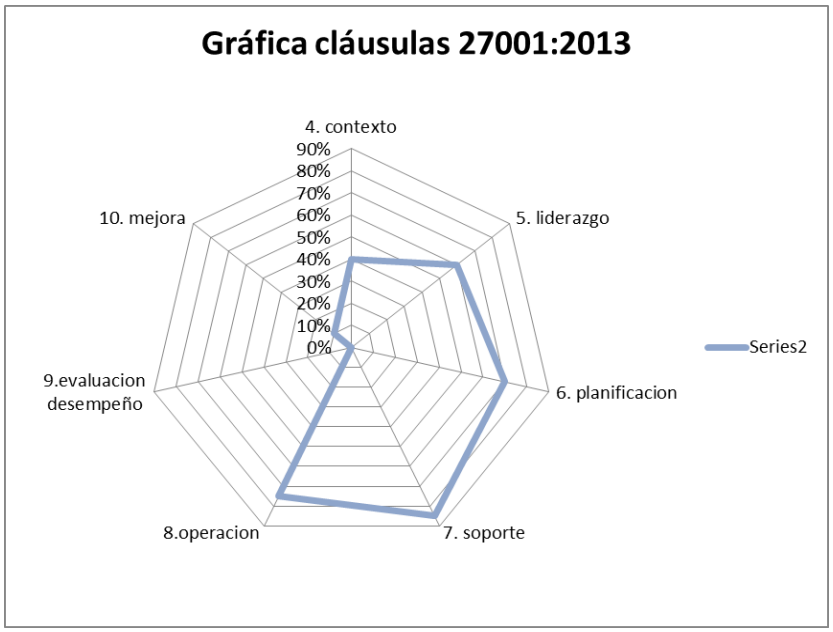


Imagen 4. Gráfica de resultado actual cláusulas unidad Gerencia de Servicios Tecnológicos

En el diagrama de barras a continuación, se observa el nivel de cumplimiento de cada cláusula de manera clara:

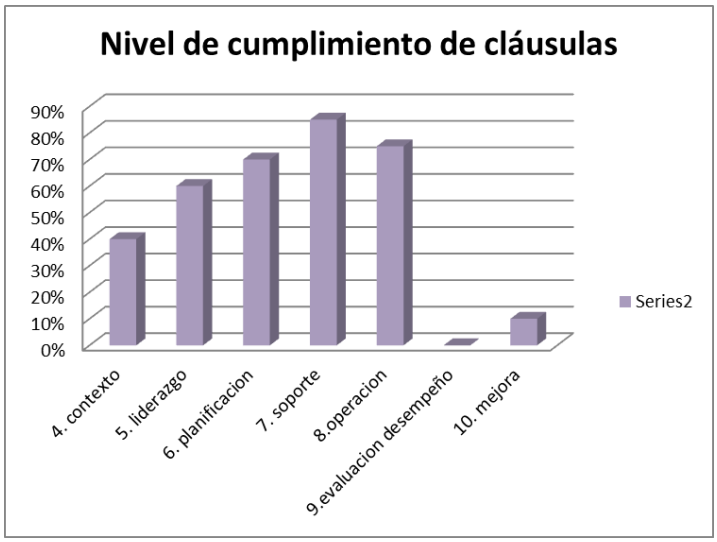


Imagen 5. Nivel cumplimiento porcentaje cláusulas

Análisis diferencial ISO/IEC 27002:2013

Mediante la herramienta de Excel mencionada anteriormente y que se observa en el Anexo A, y con el concurso de los responsables de la seguridad de la información de GST, se estableció el estado actual de los dominios existentes en la norma 27002:2013.

Códigos Status	Significado	Porcentaje
D	El control se documentó e implementó	100
MD	El Control se lleva a cabo y el proceso debe ser documentado para asegurar la repetibilidad del proceso y mitigar los riesgos.	90
RD	El control no cumple las normas y debe ser rediseñado para cumplir con las normas	50
PNP	El proceso no está en su lugar / no implementado. (Control requeridos ni documentado ni implementado)	0
NA (Not Applicable)	El control no es aplicable para la empresa ni para el negocio	0

Tabla 2. Valorización para los dominios establecidos en la ISO/IEC 27002:2013.

De igual forma, se obtuvo la siguiente gráfica radial, la cual muestra el estado actual del cumplimiento de los dominios por parte de la oficina de GST:

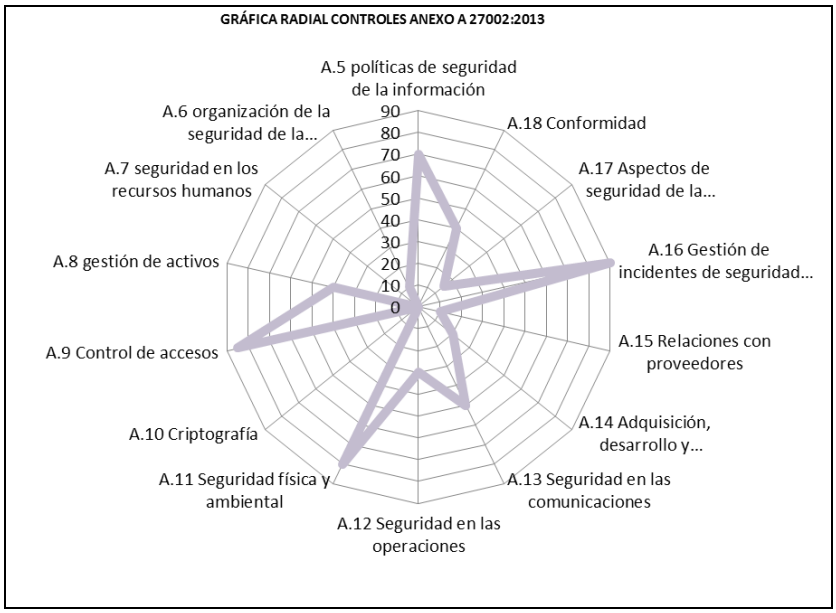


Imagen 6. Gráfica radial situación actual controles unidad de Gerencia de Servicios Tecnológicos.

Así mismo, la proporción de cumplimiento de los controles puede observarse en la siguiente tabla:

Area	Definiciones	% Cumplimiento
	Controles	
A.5	A.5 políticas de seguridad de la información	70
A.6	A.6 organización de la seguridad de la información	10
A.7	A.7 seguridad en los recursos humanos	0
A.8	A.8 gestión de activos	40
A.9	A.9 Control de accesos	85
A.10	A.10 Criptografía	0
A.11	A.11 Seguridad física y ambiental	80
A.12	A.12 Seguridad en las operaciones	30
A.13	A.13 Seguridad en las comunicaciones	50
A.14	A.14 Adquisición, desarrollo y mantenimiento de sistemas	20
A.15	A.15 Relaciones con proveedores	10
A.16	A.16 Gestión de incidentes de seguridad de la información	90
A.17	A.17 Aspectos de seguridad de la información dentro de la continuidad del negoc	15
A.18	A.18 Conformidad	40

Tabla 3. Proporción de cumplimiento de los controles de la ISO/IEC 27002:2013.

2.1. Resultados.

De lo anterior se puede ver claramente del análisis en ISO 27001:2013, que no existe ningún procedimiento relacionado con la evaluación del desempeño. No se han establecido tiempos ni asignaciones de responsabilidades en cuanto a los procesos y controles del SGSI, y no se cuenta con planes de auditoría interna en relación con la seguridad de la información. Esto conlleva por tanto a que la cláusula de mejora también se encuentre en un estado casi inexistente, mostrando la necesidad de generar procesos que ayuden en su formulación y posterior mejora.

En cuanto al soporte se encontró que en la unidad de GST se han esforzado por tener personal idóneo a nivel técnico, capaz de resolver los problemas que se encuentran, y evaluar y gestionar los riesgos asociados.

Con relación a los controles del Anexo A de la ISO 27002:2013, se evidencia claramente que la organización de la seguridad de la información, la criptografía, y la continuidad del negocio, no son prioridad para la oficina y se realiza lo mínimo para su funcionamiento. Con respecto a la seguridad ligada a los recursos humanos, se evidenció el desconocimiento de los procesos realizados por la oficina de recursos humanos al respecto.

3. Fase 2: sistema de gestión documental

3.1. Introducción

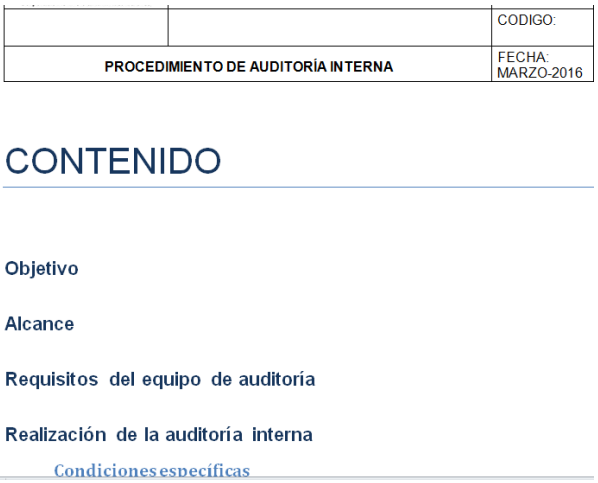
Todos los Sistemas de Gestión se apoyan en un cuerpo documental para el cumplimiento normativo. Esto significa que el Sistema de Gestión de Seguridad de la Información que se plantea debe tener una serie de documentos, los cuales vienen establecidos en la propia norma ISO/IEC 27001. A continuación se describen dichos documentos, los cuales pueden ser observados en los anexos correspondientes.

3.2. Esquema documental

Para el desarrollo del presente trabajo se tuvieron en cuenta los siguientes documentos:

- **Política de Seguridad**: Normativa interna de seguridad que regula las líneas sobre la forma en que trabajará la organización en el tema de seguridad de la información. “Su principal objetivo es recoger las directrices que debe seguir la seguridad de la información de acuerdo a las necesidades de la organización y a la legislación vigente.”[3]. (INCIBE). Con respecto a la actual política de la Corporación universitaria, cabe decir que todavía está en fase de actualización y aprobación por parte de la alta dirección, y en algunos aspectos todavía es genérica, por lo cual se recomienda a la organización que la ajuste antes de su aprobación para poder ser presentada a los colaboradores de la entidad. En el ANEXO B se observa la política de seguridad de la información actual.

- **Procedimiento de Auditorías Internas**: Documento que debe incluir una planificación de las auditorías que se llevarán a cabo durante la vigencia de la certificación (una vez se obtenga), requisitos que se establecerán a los auditores internos y se definirá el modelo de informe de auditoría. Para el caso particular, la Corporación no ha llevado a cabo ninguna acción relacionada con auditoría interna, salvo auditorías técnicas, por lo cual se construyó el documento propuesta para ser entregado al comité de Seguridad informática para su revisión, actualización, adaptación y aprobación. Se anexa el documento en el ANEXO C.



		CODIGO:
PROCEDIMIENTO DE AUDITORÍA INTERNA		FECHA: MARZO-2016

CONTENIDO

Objetivo

Alcance

Requisitos del equipo de auditoría

Realización de la auditoría interna

Condiciones específicas

Imagen 7. Contenido procedimiento Auditoría Interna.

- **Gestión de Indicadores:** Es necesario definir indicadores para medir la eficacia de los controles de seguridad implantados en la organización. Es por esto que la Corporación ha definido que los indicadores deben estar alineados con su política de seguridad, teniendo en cuenta los procesos descritos a continuación:

  a) Seguridad del Personal
  b) Seguridad Física y Ambiental
  c) Seguridad en las Comunicaciones y las Operaciones
  d) Control de Accesos
  e) Seguridad en el Desarrollo y Mantenimiento de Sistemas
  f) Planificación de la Continuidad Operativa.

Igualmente es importante definir la sistemática para medir.
Aquí es importante decir que por motivos de confidencialidad, la Corporación no entregó los formatos requeridos, por lo cual acá se desarrolla uno alterno. Ver ANEXO D.

- **Procedimiento Revisión por Dirección**: La Dirección de la Organización debe revisar anualmente las cuestiones más importantes que han sucedido en relación al Sistema de Gestión de Seguridad de la Información. Para esta revisión, la ISO/IEC 27001:2013 define tanto los puntos de entrada, como los puntos de salida que se deben obtener de estas revisiones.
  En las revisiones se deben incluir consideraciones sobre:

  - El estado de las acciones con relación a las revisiones previas.
  - Cambios en el contexto de la empresa que sean pertinentes al SGSI.

A continuación se describe el procedimiento de revisión por dirección propuesto por la Corporación Universitaria:

"La revisión del Sistema de Gestión por la Alta Dirección la realiza la Rectoría General, la Vicerrectoría General académica, la Vicerrectoría académica UVD, las Direcciones general financiera y de Servicios al usuario y Calidad, la Dirección de Planeación y desarrollo y las Rectorías de sede como responsables de la administración del sistema de gestión integrado, verificando entre otros los siguientes puntos:

Las Políticas de Calidad, Seguridad y Salud Ocupacional, Seguridad de la información y Ambiental.

• El cumplimiento de los Objetivos de Calidad, seguridad de la información, objetivos ambientales y de seguridad y salud ocupacional.
• El desempeño en calidad, ambiental, seguridad de la información, y Salud Ocupacional.

• Los resultados de las auditorías internas y/o externas.

• Las acciones correctivas y/o preventivas necesarias para el mejoramiento del Sistema de Gestión, así como el estado de aquellas que se hayan identificado.

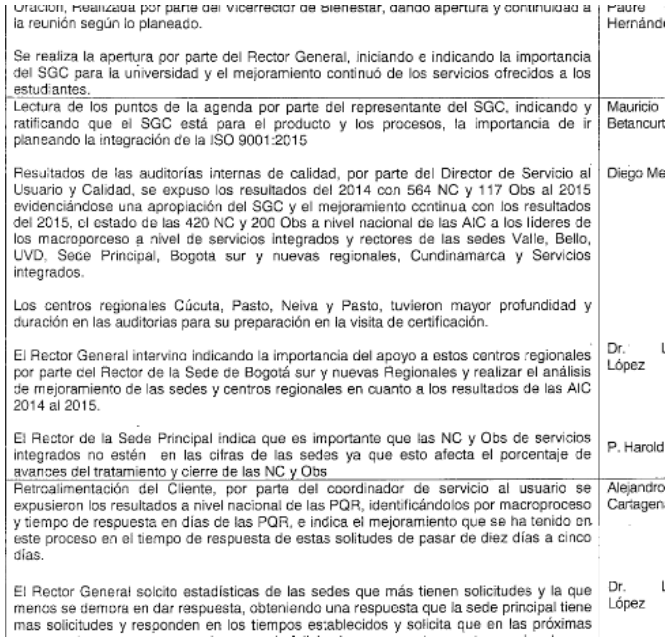
• Las acciones de seguimiento de las revisiones por la Dirección previas.
• Avance y cumplimiento de la implementación de los planes de tratamiento definidos para los riesgos identificados.

• Cambios y requerimientos organizacionales que podrían afectar al Sistema de Gestión.

• Recomendaciones para la mejora.

• Resultados de la gestión de riesgos corporativos, esto incluye vulnerabilidades o amenazas no tratadas en la valoración previa de riesgos.

Los resultados obtenidos en la revisión quedan plasmados en el formato de acta establecido por la institución (FR-CA-PSC-03 Vers.4.0), y deberán ejecutarse por lo menos una vez al año.”



Oración, Realizada por parte del Vicerrector de Bienestar, dando apertura y continuidad a la reunión según lo planeado. Se realiza la apertura por parte del Rector General, iniciando e indicando la importancia del SGC para la universidad y el mejoramiento continuó de los servicios ofrecidos a los estudiantes.	Padre Hernándo
Lectura de los puntos de la agenda por parte del representante del SGC, indicando y ratificando que el SGC está para el producto y los procesos, la importancia de ir planeando la integración de la ISO 9001:2015	Mauricio Betancurt
Resultados de las auditorías internas de calidad, por parte del Director de Servicio al Usuario y Calidad, se expuso los resultados del 2014 con 564 NC y 117 Obs al 2015 evidenciándose una apropiación del SGC y el mejoramiento continua con los resultados del 2015, el estado de las 420 NC y 200 Obs a nivel nacional de las AIC a los líderes de los macroporceso a nivel de servicios integrados y rectores de las sedes Valle, Bello, UVD, Sede Principal, Bogota sur y nuevas regionales, Cundinamarca y Servicios integrados. Los centros regionales Cúcuta, Pasto, Neiva y Pasto, tuvieron mayor profundidad y duración en las auditorias para su preparación en la visita de certificación.	Diego Me
El Rector General intervino indicando la importancia del apoyo a estos centros regionales por parte del Rector de la Sede de Bogotá sur y nuevas Regionales y realizar el análisis de mejoramiento de las sedes y centros regionales en cuanto a los resultados de las AIC 2014 al 2015.	Dr. l López
El Rector de la Sede Principal indica que es importante que las NC y Obs de servicios integrados no estén en las cifras de las sedes ya que esto afecta el porcentaje de avances del tratamiento y cierre de las NC y Obs	P. Harold
Retroalimentación del Cliente, por parte del coordinador de servicio al usuario se expusieron los resultados a nivel nacional de las PQR, identificándolos por macroproceso y tiempo de respuesta en días de las PQR, e indica el mejoramiento que se ha tenido en este proceso en el tiempo de respuesta de estas solitudes de pasar de diez días a cinco días.	Alejandro Cartagen
El Rector General solcito estadísticas de las sedes que más tienen solicitudes y la que menos se demora en dar respuesta, obteniendo una respuesta que la sede principal tiene mas solicitudes y responden en los tiempos establecidos y solicita que en las próximas	Dr. l López

Imagen 8. Desarrollo reunión revisión año 2014.

- **Gestión de Roles y Responsabilidades**: El Sistema de Gestión de Seguridad de la Información tiene que estar compuesto por un equipo que se encargue de crear, mantener, supervisar y mejorar el Sistema. Este equipo de trabajo, conocido habitualmente como Comité de Seguridad, debe estar compuesto al menos por una persona de Dirección, para que de esta manera las decisiones que se tomen puedan estar respaldadas por alguien de Dirección. Para el caso de la Corporación universitaria, la definición de roles y responsabilidades está siendo elaborada dentro de la nueva política de seguridad de la información que está siendo desarrollada por el equipo; a continuación se transcribe una parte de la definición de responsabilidades que aparece en el borrador de dicho documento:

  "Los siguientes entes serían responsables, en distintos grados, de la seguridad en la Institución:

  - El Comité de Seguridad Informática, compuesto por los representantes de los distintos departamentos de la Institución, así como por el Gerente de Servicios Tecnológicos, el Director de Infraestructura Tecnológica, el Administrador de Seguridad de la Información, el encargado de Redes y Telecomunicaciones, el Administrador de Servidores y el Abogado o representante legal de la Institución. Este Comité está encargado de elaborar y actualizar las políticas, normas, pautas y procedimientos relativos a seguridad en informática y telecomunicaciones. También es responsable de coordinar el análisis de riesgos, planes de contingencia y prevención de desastres. Durante sus reuniones trimestrales o según cronograma, el Comité efectuará la evaluación y revisión

de la situación de la Institución en cuanto a seguridad informática, incluyendo el análisis de incidentes ocurridos y que afecten la seguridad.

- La Dirección de Infraestructura Tecnológica es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la organización, todo esto en coordinación con la Junta Directiva y la Gerencia de Servicios Tecnológicos. También es responsable de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances." (Chaparro R, 2016). Se anexó documento de responsabilidades extraído de borrador de política de seguridad de la información en construcción (ANEXO E).

- **Metodología de Análisis de Riesgos**: Establece la sistemática que se seguirá para calcular el riesgo, lo cual deberá incluir básicamente la identificación y valoración de los activos, amenazas y vulnerabilidades. En el ANEXO F se entrega la matriz de riesgos y las fichas de probabilidad de amenazas definidas por la organización. La metodología de análisis de riesgos definida por el oficial de seguridad se basa en MAGERIT.

- **Declaración de Aplicabilidad**: Documento que incluye todos los controles de Seguridad establecidos en la Organización, con el detalle de su aplicabilidad, estado y documentación relacionada. Para el caso de estudio, se identificó la inexistencia de la declaración de aplicabilidad, por lo cual ha sido desarrollada una propuesta que fue entregada a la dirección de seguridad de la información para su revisión y aprobación. Se anexa la Declaración de aplicabilidad propuesta (ANEXO G).

3.3. Resultados

Después de la revisión correspondiente del esquema documental básico, se encuentra que la Corporación Universitaria carece de la mayoría de documentación requerida, por lo cual se hizo necesario la realización de propuestas de Declaración de aplicabilidad, Plan de auditoría y Gestión de Indicadores, los cuales requieren la revisión y aprobación por parte del oficial de seguridad de la información en conjunto con el Comité de Seguridad de la información y la Gerencia de Servicios Tecnológicos. Estas aprobaciones son fundamentales para poder llevar a cabo las diferentes actividades de implantación, como son la realización del

análisis de riesgos, implantación de controles necesarios, implantación de proyectos, realización de auditoría interna, etc.

4. Fase 3: Análisis de riesgos.

4.1. Introducción

No podemos proteger aquello que no conocemos. Es por ello, que la primera etapa hacia la consecución del Plan de Implementación de un SGSI consistirá en la evaluación de nuestros activos, considerando las dependencias existentes entre ellos y realizando una valoración de los mismos.

¿Por qué realizarlo?
Los motivos por los que se debe realizar un análisis de riesgos son los siguientes:
• Permite identificar los diferentes riesgos a los que se encuentra expuesta la organización desde el punto de vista de la seguridad y que podrían afectar al desarrollo de las diferentes actividades de negocio de la organización.
• Permite a la organización realizar una selección de medidas de seguridad que se deben implantar en ella, mucho más ajustada a las necesidades de la misma.
Para esta fase solo se trabaja con los activos que son responsabilidad directa de la oficina de GST, sean de software, hardware o personal y que se encuentran relacionados con los procesos misionales de la unidad. Así pues, se procederá a realizar el análisis de riesgos a través de las siguientes etapas: Inventario y valoración de activos, amenazas, determinación del impacto potencial, determinación del riego potencial.

4.2. Inventario y valoración de activos.

De acuerdo con [UNE 71504:2008], un activo es un “componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización”. Los activos pueden ser: información, datos, servicios, software (aplicaciones), hardware, comunicaciones, recursos administrativos, recursos físicos y humanos. (AENOR, 2008).

Para el presente estudio, se realizará un análisis de todos los activos que se encuentran a cargo de GST utilizando la tradicional metodología MAGERIT,
Nuestro primer punto para el análisis es analizar los activos vinculados a la información. Es habitual agrupar los activos por grupos. En nuestro caso, podemos agrupar los activos en grupos acordes con la metodología MAGERIT. Esta metodología es realmente un método para realizar análisis y gestión de riesgos, diseñada inicialmente para la administración española por el Consejo Superior de Administración Electrónica, pero que debido a su buena definición y aceptación, puede ser aplicada en otros contextos. (De MAGERIT se tomará en cuenta el libro 2: catálogo de elementos para realizar la definición de amenazas, y el libro I: método).

Así pues, como primera medida, se hizo un levantamiento de información del inventario que posee la oficina de GST, teniendo en cuenta el valor en pesos y la criticidad que tiene en las cinco dimensiones de seguridad para la organización cada uno de ellos, de la siguiente forma:

Valor cualitativo	Valor en Pesos Col (COP)
Bajo (B)	< $50.000.000,00
Medio (M)	$50.000.001 - $100.000.000
Alto (A)	$100.000.001,00 - $450.000.000,00
Muy Alto (MA)	> $450.000.000,00

Tabla 4. Valoración de los activos para GST.

Las dimensiones de seguridad tenidas en cuenta fueron: Disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad, de acuerdo con el libro 1: método de MAGERIT.

Criticidad	
Valor cualitativo	Valor cuantitativo
Bajo (B)	1 - 2.99
Medio (M)	3 - 3.99
Alto (A)	4
Muy Alto (MA)	5

Tabla 5. Valores cualitativo y cuantitativo de criticidad de los activos.

La tabla obtenida se observa en el ANEXO H, pestaña Activos, debido a su gran extensión. Por tal motivo, en el presente documento solo se presenta una porción de la tabla con fines ilustrativos, como se observa a continuación:

					Aspectos críticos				
Ámbito	ID	Activo	Valor	Valor ($ PESOS COP)	D	I	C	T	A
Hardware									
		Computadores	A	$ 250.000.000,00	4	2	3	2	4
		Impresoras	B	$ 50.000.000,00	3	2	1	1	1
		memorias USB	B	$ 10.000.000,00	3	2	5	3	4
		PBX	M	$ 60.000.000,00	4	2	2	3	3
		Portátiles	M	$ 90.000.000,00	4	3	4	3	3
		Teléfonos celulares	B	$ 5.000.000,00	3	2	2	2	1
Red									
		Switch core		$ 40.000.000,00	4	3	3	5	5
		Equipos de la red cableada (router)	M	$ 150.000.000,00	4	4	3	5	5

		Equipos de la red inalámbrica (router)	M	$ 60.000.000,00	4	3	3	5	4
		Equipos de la red inalámbrica (punto de acceso)	M	$ 60.000.000,00	3	3	3	4	4
		Cortafuego (Firewall)			5	1	2	2	2
		Routers de borde	M	$ 90.000.000,00	5	2	3	5	3
Instalaciones									
		Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)	MA	$ 10.000.000.000,00	4	5	2	1	1
Información									
		Gestión Documental (Alfresco).	MA	$ 500.000.000,00	4	3	4	3	3
		Infraestructura (Planes, Documentación, etc.)	MA	$ 400.000.000,00	4	4	5	3	4
		Informática (Planes, Documentación, etc.)	A	$ 600.000.000,00	4	4	5	3	4
		Datos e información no institucionales	MA	$ 500.000.000,00	3	4	3	3	2
Datos									
		Finanzas (SAP)	M	$ 400.000.000,00	4	5	5	3	3
		Académico (Banner)	A	$ 500.000.000,00	5	4	4	3	3
		Directorio de Contactos	B	$ 50.000.000,00	4	4	3	3	1

Tabla 6. Activos con sus ámbitos de acuerdo a MAGERIT para la oficina de GST.

Aquí cabe aclarar que el valor que se observa en el inventario no es el valor comercial de los activos, sino un compendio entre el valor comercial y el valor que el activo posee para la Universidad, para cumplir con su misión y visión.

4.3. Análisis de amenazas

Una vez definidos los activos y su valor para la organización se debe realizar un análisis que muestre cuales amenazas pueden llegar a afectar a dichos activos, para posteriormente estimar cuán vulnerable es el activo a la materialización de dicha amenaza, así como también a la frecuencia estimada de la misma.
De acuerdo con lo anterior, se procedió a realizar la clasificación de las amenazas utilizando las tablas existentes en el libro 2: Catálogo de elementos de MAGERIT, el cual sugiere la agrupación de las amenazas en cuatro grandes grupos:

Desastres naturales, accidentes industriales, errores y fallos no intencionados, y Amenazas intencionales presenciales (Ministerio de hacienda y administraciones públicas , 2012), obteniéndose la siguiente tabla de amenazas:

		DIMENSIÓN AFECTADA					ACTIVOS AFECTADOS								
	AMENAZA	D	I	C	T	A	hardware	Red	Instalaciones	Software (aplicaciones	Información	Datos	Servicios	Personal	logs
DESASTRES NATURALES	[N.1] Fuego	X					X	X	X		X				
	[N.2] daños por agua	X					X	X	X		X				
	[N.3] inundación	X					X	X	X		X				
	[N.4] Siniestro mayor	X					X	X	X		X				
	[N.5]Fenómeno sísmico	X					X	X	X		X				
	[N.6]Fenómeno meteorológico	X					X	X	X		X				
ACCIDENTES DE ORIGEN INDUSTRIAL	[I.1] Fuego	X					X	X	X		X				
	[I.2] daños por agua	X					X	X	X		X				
	[I.12] Sobrecarga eléctrica	X					X	X	X		X				
	[I.13] Fluctuación eléctrica	X	X				X	X		X	X				
	[I.3] Contaminación mecánica	X					X								
	[I.4] Contaminación electromagnética	X					X		X						
	[I.5] Avería de origen físico o lógico	X	X				X			X					
	[I.6] Corte del suministro eléctrico	X					X	X	X						
	[I.7] Condiciones inadecuadas de temperatura o humedad	X	X				X		X		X				
	[I.8] fallos de servicios de comunicaciones	X						X							
	[I.9] Interrupción de otros servicios y suministros esenciales	X					X								
	[I.10] Degradación de los soportes de almacenamiento de la información	X									X				
	[I.11] Emanaciones electromagnéticas			X			X		X	X					
ERRORES Y FALLOS NO INTENCIONADOS	[E.1] Errores de los usuarios	X	X	X						X	X	X	X		
	[E.2] Errores del administrador	X	X	X			X	X		X	X	X	X		
	[E.3] Errores de monitorización (log)		X		X						X				
	[E.4] Errores de configuración		X									X			
	[E.7] Deficiencias en la organización	X												X	
	[E.8] Difusión de software dañino	X	X	X						X					
	[E.9] Errores de re-encaminamiento			X				X		X			X		
	[E.10] Errores de secuencia		X					X		X			X		
	[E.14] Escapes de información			X											
	[E.18] Destrucción de información	X	X					X	X	X		X	X		
	[E.19] Fugas de información			X						X	X	X	X	X	
	[E.20] Vulnerabilidades de los programas (software)	X	X	X						X					
	[E.21] Errores de mantenimiento / actualización de programas (software)	X	X							X					
	[E.23] Errores de mantenimiento /	X					X	X							

	actualización de equipos (hardware)														
	[E.24] Caída del sistema por agotamiento de recursos	X					X	X					X		
	[E.25] Pérdida de equipos	X		X			X								
	[E.28] Indisponibilidad del personal	X												X	
AMENAZAS INTENCIONALES PRESENCIALES	[A.3] Manipulación de los registros de actividad (log)		X		X										
	[A.4] Manipulación de la configuración	X	X			X									
	[A.5] Suplantación de la identidad del usuario		X	X		X		X		X		X	X		
	[A.6] Abuso de privilegios de acceso	X	X	X			X	X		X	X	X	X		
	[A.7] Uso no previsto	X	X	X			X	X	X	X		X	X		
	[A.8] Difusión de software dañino	X	X	X						X					
	[A.9] [Re-]encaminamiento de mensajes			X				X		X			X		
	[A.10] Alteración de secuencia		X					X		X			X		
	[A.11] Acceso no autorizado		X	X			X	X	X	X	X	X	X		
	[A.12] Análisis de tráfico			X				X							X
	[A.13] Repudio		X		X								X		X
	[A.14] Interceptación de información (escucha)			X				X							
	[A.15] Modificación deliberada de la información		X					X	X	X	X	X	X		
	[A.18] Destrucción de información	X							X	X		X	X		
	[A.19] Divulgación de información		X						X	X	X	X	X		
	[A.22] Manipulación de programas	X	X	X						X					
	[A.23] Manipulación de los equipos	X		X			X								
	[A.24] Denegación de servicio	X					X	X					X		
	[A.25] Robo	X		X			X								
	[A.26] Ataque destructivo	X					X		X		X				
	[A.28] Indisponibilidad del personal	X												X	
	A.29] Extorsión	X	X	X										X	
	[A.30] Ingeniería social (picaresca)	X	X	X										X	

Tabla 7. Amenazas según libro II: Catálogo de elementos MAGERIT.

Ahora es el momento de hacer la definición de la probabilidad de ocurrencia de la materialización de cada amenaza con respecto a los activos que se tienen (frecuencia estimada/días del año), atendiendo las sugerencias hechas para el caso por MAGERIT, y de acuerdo con las necesidades de la oficina de GST:

Vulnerabilidad (frecuencia estimada/días del año)	Rango	Valor
Frecuencia Extrema	1 vez al día	1
Frecuencia alta	1 vez al mes	12/365 = 0,03287
Frecuencia media	1 vez cada 6 meses	2/365 = 0,005479
Frecuencia baja	1 vez al año	1/365 = 0,002739

Tabla 8. Probabilidad de ocurrencia de los eventos.

Adicionalmente se ha determinado el impacto de la siguiente manera:

Impacto		Valor
insignificante	I	[5% -19%]
bajo	B	[20% - 49%]
medio	M	[50% - 90%]
alto	A	[91%- 100%]

Tabla 9. Relación del impacto.

Con la información recopilada se da lugar a una tabla resumen como la que se muestra a continuación, la cual muestra cada uno de los activos del inventario frente a las posibles amenazas que lo pueden afectar en determinado ámbito de seguridad, y la frecuencia de que dicha amenaza pueda materializarse en el activo en la figura siguiente para un activo determinado. En definitiva, para cada tipo de activo se analizará la frecuencia con que puede producirse la amenaza, así como su impacto en las distintas dimensiones de la seguridad del activo. A continuación se muestran los datos obtenidos para el activo “computadores”:

Activo	Amenaza	Frecuencia estimada	D	I	C	T	A
COMPUTADORES	[N.1] Fuego	0,002739	80%				
	[N.2] daños por agua	0,002739	80%				
	[N.3] inundación	0,002739	80%				
	[N.4] Siniestro mayor	0,002739	95%				
	[I.1] Fuego	0,002739	80%				
	[I.12] Sobrecarga eléctrica	0,002739	30%				
	[I.13] Fluctuación eléctrica	0,005479	30%	60%			
	[I.5] Avería de origen físico o lógico	0,005479	50%	80%			
	[E.2] Errores del administrador	0,005479	50%	80%			
	[E.8] Difusión de software dañino	0,03287	80%	95%	80%		
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,005479	50%				
	[E.25] Pérdida de equipos	0,002739	90%		80%		
	[A.6] Abuso de privilegios de acceso	0,002739	40%	60%	60%		
	[A.25] Robo	0,002739	80%		80%		
	[A.26] Ataque destructivo	0,002739	90%				

Tabla 10. Análisis amenazas GST.

En el ANEXO H, pestaña “Análisis de amenazas” se observa la tabla completa.

Nótese como en la fila identificadora del activo, se coloca como impacto el máximo de los impactos que pueden provocar las diferentes amenazas.

4.4. Impacto potencial y nivel de riesgo aceptable

Una vez realizada la tabla anterior, y dado que se tiene conocimiento de los valores de los diferentes activos, se puede determinar el impacto potencial que puede suponer para la empresa la materialización de las amenazas. "Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema" (Ministerio de Haciendas y administraciones públicas, 2012).

Para poder hacer el cálculo del impacto potencial, se realizó la multiplicación del valor del activo por la frecuencia de ocurrencia estimada por el mayor de los impactos calculados en las cinco dimensiones de seguridad para cada una de las amenazas ($Impacto\ potencial = valor_{activo} * frecuencia_{ocurrencia} * impacto_{mayor}$).

De igual forma, la oficina de GST determinó la suma de $ 657.400,00, como su valor de nivel de riesgo aceptable, por lo tanto todos aquellos valores que den por encima de este valor deberán estar sujetos al diseño y selección de salvaguardas. En la tabla 11 puede observarse resaltados en color rosa, los valores obtenidos por encima de este límite. La tabla completa se observa en el ANEXO H, pestaña "análisis de amenazas".

Activo	Amenaza	Frecuencia estimada	D	I	C	T	A	Valor activo	Impacto potencial
COMPUTADORES	[N.1] Fuego	0,002739	80%					$ 250.000.000,00	$ 547.800,00
	[N.2] daños por agua	0,002739	80%					$ 250.000.000,00	$ 547.800,00
	[N.3] inundación	0,002739	80%					$ 250.000.000,00	$ 547.800,00
	[N.4] Siniestro mayor	0,002739	95%					$ 250.000.000,00	$ 650.512,50
	[I.1] Fuego	0,002739	80%					$ 250.000.000,00	$ 547.800,00
	[I.12] Sobrecarga eléctrica	0,002739	30%					$ 250.000.000,00	$ 205.425,00
	[I.13] Fluctuación eléctrica	0,005479	30%	50 %				$ 250.000.000,00	$ 684.875,00
	[I.5] Avería de origen físico o lógico	0,005479	50%	70 %				$ 250.000.000,00	$ 958.825,00
	[E.2] Errores del administrador	0,005479	50%	70 %				$ 250.000.000,	$ 958.825,00

								00	
	[E.8] Difusión de software dañino	0,03287	80%	95 %	70 %			$ 250.000.000,00	$ 7.806.625,00
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,005479	50%					$ 250.000.000,00	$ 684.875,00
	[E.25] Pérdida de equipos	0,002739	80%		80 %			$ 250.000.000,00	$ 547.800,00
	[A.6] Abuso de privilegios de acceso	0,002739	40%	50 %	60 %			$ 250.000.000,00	$ 342.375,00
	[A.25] Robo	0,002739	80%		80 %			$ 250.000.000,00	$ 547.800,00
	[A.26] Ataque destructivo	0,002739	90%					$ 250.000.000,00	$ 616.275,00

Tabla 11. Impacto potencial con salvaguardas a crear.

4.5. Nivel de riesgo aceptable y riesgo residual

Una vez establecido el control, se reducirá el riesgo, pero este seguirá existiendo (lo deseable es conseguir reducirlo para que esté por debajo del nivel aceptable), a este riesgo que seguirá existiendo después de aplicar los controles de seguridad, se denomina riesgo residual.

Una vez establecidos aquellos riesgos que no pueden ser asumidos por la empresa, se debe definir una serie de controles o “salvaguardas”, los cuales dependen del tipo de activo a proteger, la dimensión o dimensiones de seguridad a cubrir, y las amenazas de las que deba protegerse a los activos.
Debe tenerse en cuenta que para algunos activos se debe tener salvaguardas preventivas, es decir que disminuyen la probabilidad de ocurrencia, mientras que para otra clase de activos se cuenta con salvaguardas que disminuyen o limitan el impacto causado por la materialización de una amenaza.

Después de definir los controles de la organización y calcular el riesgo residual, se encontró que para todos los activos el nuevo riesgo se encuentra por debajo del valor establecido, con excepción de las instalaciones donde el riesgo disminuye, pero sigue estando por encima del valor umbral. En la tabla 12 se observa una porción de la tabla de riesgo e impacto residual obtenido. En el ANEXO I se observa la tabla completa.

Activo	Amenaza	Salvaguarda	Frecuencia estimada	D	I	C	T	A	Valor activo	Impacto Residual
COMPUTADORES	[N.1] Fuego		0,002739	80 %					$ 250.000.000	$ 547.800
	[N.2] daños por agua		0,002739	80 %					$ 250.000.000	$ 547.800
	[N.3] inundación		0,002739	80 %					$ 250.000.000	$ 547.800
	[N.4] Siniestro mayor		0,002739	95 %					$ 250.000.000	$ 650.512
	[I.1] Fuego		0,002739	80 %					$ 250.000.000	$ 547.800
	[I.12] Sobrecarga eléctrica		0,002739	30 %					$ 250.000.000	$ 205.425
	[I.13] Fluctuación eléctrica	UPS	0,002739	5%	10%				$ 250.000.000	$ 68.475
	[I.5] Avería de origen físico o lógico	Ciclo de mantenimiento	0,002739	5%	10%				$ 250.000.000	$ 68.475
	[E.2] Errores del administrador	Capacitación	0,005479	10 %	10%				$ 250.000.000,00	$ 136.975
	[E.8] Difusión de software dañino	Antivirus	0,005479	10 %	10%	10 %			$ 250.000.000	$ 136.975
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Capacitación personal	0,005479	20 %					$ 250.000.000	$ 273.950
	[E.25] Pérdida de equipos		0,002739	80 %		80 %			$ 250.000.000	$ 547.800
	[A.6] Abuso de privilegios de acceso		0,002739	40 %	50%	60 %			$ 250.000.000	$ 342.375
	[A.25] Robo		0,002739	80 %		80 %			$ 250.000.000	$ 547.800
	[A.26] Ataque destructivo		0,002739	90 %					$ 250.000.000	$ 616.275

Tabla 12. Impacto y riesgo residual para el activo "computadores".

4.6. Resultados

Una vez realizadas las tareas contempladas en esta fase, se encontró lo siguiente:

Se encontró que los activos más relevantes para la unidad son: la información contenida en ALFRESCO, SAP, y la infraestructura. Así mismo, los datos de SAP FINANCIERO, BANNER, Recursos humanos y respaldos (copias de seguridad), se constituyen en los activos que le

dan el valor agregado al negocio, haciendo de la universidad una de las de mayor crecimiento y cobertura en el país.

Después de hacer el análisis de las posibles amenazas se ubicaron las siguientes como las posibles sobre los sistemas de información:
Todas las relacionadas con desastres naturales sobre las instalaciones, encontrándose que el impacto en caso de materializarse, dejaría inoperativa la unidad.
Las amenazas de difusión de software dañino y destrucción de información, se constituyen en las que más activos impactan, teniendo un valor muy alto en caso de materializarse. Esto es debido a que los procesos dentro de la universidad son manejados en un 90% desde sistemas informáticos, por lo cual si no se protege el canal de datos, los equipos y las aplicaciones de manera apropiada, se puede tener una caída del negocio, dejándolo inoperativo durante cierto tiempo, y creando traumatismos en todos los procesos de la universidad (docencia, administrativo, investigación, proyección social, entre otros). En áreas como la de docencia virtual, el servicio puede verse interrumpido creando retraso en los procesos educativos y pérdidas tanto para la universidad, como para los estudiantes.

5. Fase 4: Propuestas de proyectos

5.1. Introducción

En este momento ya se conoce el estado actual de la Universidad, y específicamente los de GST, y los riesgos residuales que afronta, por lo cual debe plantearse proyectos que ayuden a alcanzar los niveles de seguridad que se esperan.

Los proyectos que se proponen a continuación son resultado del análisis de riesgos hecho en conjunto con el ingeniero de seguridad de la Universidad, y obedecen tanto a los resultados obtenidos, como a las solicitudes hechas por la alta dirección. Para el caso particular se presentarán dos proyectos los cuales consisten en el plan de capacitación y de continuidad del negocio; además se formulará un plan de concientización en seguridad de la información para el personal de GST.

5.2. Propuestas

Objetivos
Los objetivos de los proyectos presentados son:
Para el plan de capacitación:

- Construir y mejorar los niveles de educación en el manejo de la seguridad de la información de la organización.

Para el plan de continuidad:

- Asegurar la continuidad del negocio ante diversas situaciones
- Llevar los riesgos a un nivel aceptable.

Para el plan de mitigación de riesgos

- Establecer acciones para mitigar los riesgos por difusión de software dañino, interceptación de información, y destrucción de información.

Los proyectos planteados son el resultado del análisis de riesgos, ya que se detectó un nivel bajo en capacitación y concienciación del personal, junto con problemas de recuperación en caso de desastres. Adicionalmente se pudo establecer con este análisis la necesidad de acciones adicionales en la red y los equipos de cómputo que ayuden a mitigar la difusión de software dañino.

La siguiente tabla muestra la relación de los proyectos con los riesgos identificados para mitigar, y el pilar que se ve impactado:

Proyecto	Amenazas identificados	Pilar	Acciones	impacto	Prioridad desarrollo
Plan de capacitación	[E.1] Errores de los usuarios.	Integridad	Cursos de capacitación Campaña publicitaria Concienciación	Alto Medio Alto	Medio
	[E.2] Errores del administrador.	Integridad			
	[E.7] Deficiencias en la organización.	disponibilidad			
	[E.18] Destrucción de información.	integridad			
	[E.19] Fugas de información.	confidencialidad			
Plan de continuidad del negocio	[I.1] Fuego	Disponibilidad	Generación plan de acción. Establecimiento grupos de respuesta. Estudio, diseño e implementación Centro de Datos alterno	Alto Medio Alto	Alto
	[I5] avería de origen físico o lógico.	Disponibilidad			
	[I.6] Corte del suministro eléctrico.	Disponibilidad			
	[I.12] Sobrecarga eléctrica.	Disponibilidad			
	[I13] fluctuación eléctrica.	Disponibilidad			
	[N.1] Fuego	Disponibilidad			
	[N.2] daños por agua.				
	[N.3] inundación.				
	[N.4] Siniestro mayor.				
	[N.5] Fenómeno sísmico.				
	[A.18] Destrucción de información.				
	[A.26] Ataque destructivo.				
Plan de mitigación de riesgos	[A.14] Interceptación de información (escucha).	Integridad, disponibilidad	Bloqueo de puertos de comunicación empleados por software. Inspección de tráfico, bloqueo de tráfico. Inspección y medición del tráfico para control de canal. Establecimiento de políticas de uso de software, políticas de intercambio de información y actualización de políticas de uso de TI.	Medio Medio Medio	Alto
	[A.18] Destrucción de información	Disponibilidad			
	[E.8] Difusión de software dañino	Disponibilidad, Integridad			

Tabla 13. Relación de proyectos con riesgos identificados por encima del valor aceptable, con acciones a tomar.

A continuación se hace una breve descripción de los proyectos que se han planteado. En el ANEXO J se anexa el cronograma de los proyectos y los proyectos.

5.2.1. Plan de continuidad del negocio

ALCANCE:
El plan de continuidad del negocio está circunscrito a la dependencia de GST, y busca generar las pautas que permitan restituir en el menor tiempo posible la operatividad del negocio (servicios críticos prestados por GST) en caso de que el centro principal (Bogotá) quede inoperativo

a causa de un evento que impida su funcionamiento de manera parcial o total.
Lo que supone que los procedimientos planteados en este documento, contemplan solamente las acciones a realizar con relación al Hardware, Software y Equipos Activos involucrados en los procesos críticos definidos en este Plan.

Adicionalmente, se consideran los riesgos y soluciones del ambiente físico, relacionados con la operación de los procesos del Centro de Cómputo principal para ser implementados en el Data Center alterno en Bello.
El plan de continuidad del negocio busca reducir el nivel de riesgo de las amenazas de [I13] fluctuación eléctrica, [I5] avería de origen físico o lógico, [N.1] Fuego, [N.2] daños por agua, [N.3] inundación, [N.4] Siniestro mayor, [N.5] Fenómeno sísmico, [I.1] Fuego, [I.12] Sobrecarga eléctrica, [I.6] Corte del suministro eléctrico, [A.18] Destrucción de información, y [A.26] Ataque destructivo, con respecto a la disponibilidad en el centro de datos principal, el cual posee alojados los servidores con las aplicaciones críticas para el negocio (Banner, SAP, ALFRESCO, GÉNESIS, entre otros).

FASES:
Evaluación del estado actual: El equipo realizará un análisis de riesgos para identificar los activos con que cuenta, activos críticos a ser protegidos, el estado de los controles actuales y la definición de los equipos que deben ser adquiridos y los procesos y procedimientos que deben ser desarrollados. Esto se ha desarrollado a lo largo del documento.

Estrategia de respaldo: la universidad después de discutir diferentes alternativas decidió contar con un centro replicado ubicado en la ciudad de Bello, el cual le permita trasladar en el menor tiempo posible la operación para continuar con sus actividades. Esta decisión fue tomada desde el año pasado por el Consejo de Fundadores y la Gerencia de Servicios Tecnológicos. Este sitio pertenece a la sede de Bello. Los recursos técnicos y humanos para su adecuación vienen siendo contemplados desde el año anterior y se encuentran en fase de compra, contratación e instalación.

Desarrollo del plan: En esta etapa se definirán los equipos necesarios para un desarrollo adecuado del plan, además de sus responsabilidades y funciones. También se hará una descripción de los procedimientos de alerta y actuación ante los eventos que pueden llegar a activar el plan. Y finalmente el procedimiento de vuelta a la normalidad.

Pruebas: Acá se realizarán las pruebas pertinentes para verificar que el plan funciona de manera correcta.

Capacitación: Se realizará la capacitación y el entrenamiento respectivo al personal a cargo del plan de contingencias, y se realizará un plan de concientización entre todo el personal de GST.

Puesta en marcha del plan.

Adicionalmente, se consideran los riesgos y soluciones del ambiente físico, relacionados con la operación de los procesos del Centro de Cómputo principal para ser implementados en el Data Center alterno.

5.2.2. Plan de capacitación

ALCANCE:
El plan de capacitación involucra a personal administrativo y docente. En etapas posteriores también involucrará a estudiantes de la Universidad de modo que se tenga educación en aspectos básicos de seguridad de la información. Así mismo, para las personas que son críticas en los procesos de seguridad de la Universidad, se tienen contempladas capacitaciones de nivel medio y jurídico, de modo que se mejore el proceso de educación y concienciación en manejo de la seguridad de la información.
El plan de concienciación está orientado a disminuir el nivel de riesgo presente con respecto a [E.7] Deficiencias en la organización, y [E.19] Fugas de información, las cuales fueron identificadas en todo el personal de GST.

FASES:
Diseño del plan de sensibilización: En esta etapa se diseñaran las estrategias para sensibilizar a todos los actores de la Universidad. Para ello se utilizarán diferentes estrategias, las cuales serán seleccionadas y planteadas en este proyecto. Se calcula un tiempo de 8 días para esta fase.

Diseño del plan de capacitación: Durante esta fase se revisará y diseñará los cursos relacionados con seguridad de la información para personal clave, así como talleres prácticos para otros actores de la comunidad educativa (administrativos, docentes, estudiantes). Se calcula un tiempo de 15 días para el desarrollo de esta fase.

Consecución de recursos: En esta etapa se realizará la gestión de los recursos financieros y de personal que se necesitan para poner en funcionamiento el plan de sensibilización y capacitación. Debido a los tiempos administrativos y financieros, se calcula que esta fase puede tardar hasta 5 meses.

Ejecución del plan: De acuerdo con lo planeado, la ejecución del plan de capacitación tendrá una duración de 6 meses.

Entrega de memorias y documentos soportes del plan de capacitación: esta fase durará 8 días.

Cierre del proyecto.

5.2.3. Plan de mitigación de riesgos

ALCANCE:
El plan de mitigación de riesgos busca establecer acciones y recursos que restrinjan de la mejor forma posible la propagación de software autoejecutable o que intercambie información tanto en los equipos de cómputo, como en las aplicaciones y las redes utilizadas por la Universidad. Así mismo, se busca con este plan restringir el acceso a la información contenida en los discos duros de los equipos de cómputo, de acuerdo con los niveles de acceso.

OBJETIVOS:
Establecer las acciones encaminadas a mitigar los riesgos más relevantes detectados en el análisis de riesgos aplicado a los procedimientos de la Gerencia de Servicios Tecnológicos (GST) para la Corporación Universitaria XX y otras entidades de la CMD, ante la eventualidad de toda acción que lo pueda paralizar, ya sea de forma parcial o total.

6. Fase 5: Auditoría de cumplimiento

6.1. Introducción

Llegados a esta fase, se conoce los activos de la empresa y se ha realizado una evaluación de las amenazas. Es el momento de hacer una evaluación para saber hasta qué punto la empresa cumple con las buenas prácticas en materia de seguridad. La ISO/IEC 27002:2013 sirve como marco de control del estado de la seguridad. La realización de esta evaluación servirá como punto de partida para la formulación de los planes y proyectos de mejora en materia de seguridad de la información a corto, mediano y largo plazo, marcando las pautas de desarrollo de los mismos.

6.2. Metodología

El estándar ISO/IEC 27002:2013, agrupa un total de 114 controles o salvaguardas sobre buenas prácticas para la Gestión de la Seguridad de la Información organizado en 14 dominios y 35 objetivos de control. Éste estándar es internacionalmente reconocido y es perfectamente válido para la mayoría de organizaciones.

Para la realización de la auditoría interna al SGSI de la Universidad para evaluar el nivel de cumplimiento, se tienen en cuenta los dominios de control y los controles planteados por ISO/IEC 27002:2013. Para lo anterior se definió un plan de auditoría (el cual contempla las exclusiones de acuerdo a la declaración de aplicabilidad), una lista de verificación, y se utilizan los formatos de “solicitud de acciones” con que se cuenta dentro del sistema de calidad de la Universidad.

6.3. Evaluación de la madurez

El objetivo de esta fase del proyecto es evaluar la madurez de la seguridad en lo que respecta a los diferentes dominios de control y los 114 controles planteados por la ISO/IEC 27002:2013.
De forma resumida, los dominios que deben analizarse son:

- Política de seguridad
- Organización de la seguridad de la información.
- Gestión de activos.
- Seguridad en los recursos humanos
- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones.
- Control de acceso.
- Adquisición, desarrollo y mantenimiento de Sistemas de Información
- Gestión de incidentes

- Gestión de continuidad de negocio
- Cumplimiento.

El estudio realizó una revisión de los controles planteados por la norma para cumplir con los diferentes objetivos de control. Esta estimación se realizó basándose en el Modelo de Madurez de la Capacidad (CMM), utilizando la siguiente tabla:

EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
0%	**L0**	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	**L1**	Inicial / Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
50%	**L2**	Reproducible, pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	**L3**	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	**L4**	Gestionado y medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	**L5**	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Tabla 14. Estado madurez capacidad del negocio.

La forma de hacer esta valoración es evaluando los diferentes controles, a partir de los cuales se realizará un cálculo del nivel de cumplimiento del objetivo de control. El nivel de cumplimiento del dominio será tomado del cálculo del promedio de cumplimiento de los objetivos de control que lo componen. En el Anexo K se encuentra la valoración de todos los controles y dominios, así como el plan de auditoría interna y los soportes utilizados para la misma.

6.4. Presentación de resultados

Como resultado de la evaluación realizada se encontró lo siguiente:

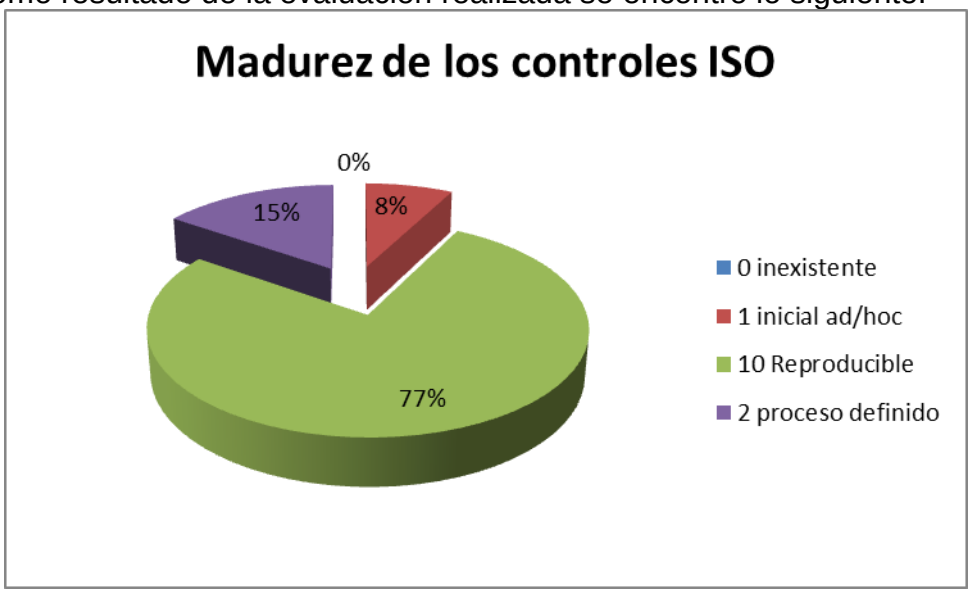


Imagen 9. Diagrama estado madurez.

De la auditoría se encontró que el 77% de los controles (10 dominios) se encuentran en estados reproducibles, mientras que solo el 15% están en estado "proceso definido" (90% de cumplimiento), debido a varias causas: la primera es que las políticas y los procedimientos en su gran mayoría están redactados y son usados por algunas personas de la unidad de GST, pero carecen de la revisión y aprobación de la alta dirección, que en este caso es la Dirección de Infraestructura Tecnológica, la Gerencia de GST, el comité de seguridad, el Rector de la Universidad, y el Consejo de Fundadores.
Otra causa es que algunos procesos dependen de varias unidades de la Universidad, y por lo tanto de varias aprobaciones, como la seguridad en los recursos humanos o la seguridad física y ambiental, causando que la ejecución de proyectos y actividades sea demorada, y por lo tanto retrasando los procesos de mejora.

Una visión más detallada es la que se presenta como 'diagrama de radar' más adelante, la cual muestra el nivel de cumplimiento por capítulo ISO. En dicho diagrama se presenta un comparativo del estado actual comparada con el estado deseado:

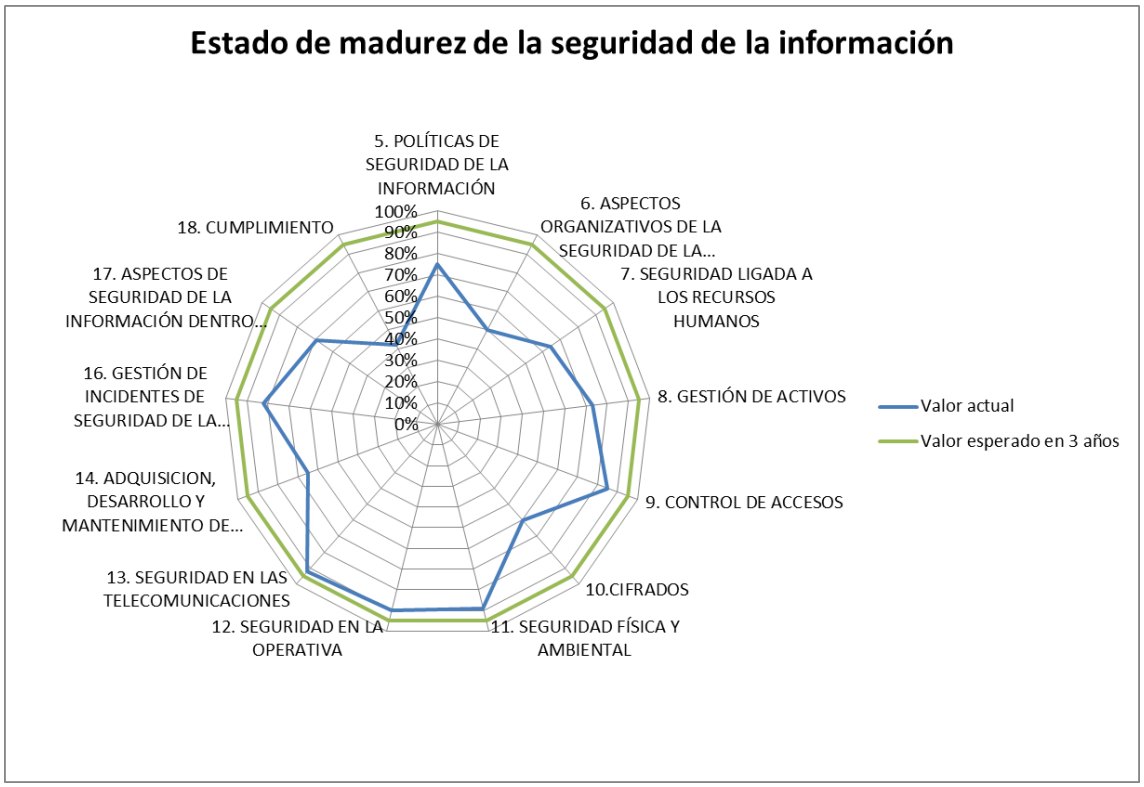


Imagen 10. Diagrama radial "estado madurez controles Anexo A 27002:2013".

Dentro de los resultados obtenidos en la auditoría se encontraron once (11) no conformidades, clasificadas en cuatro (4) no conformidades menores y siete (7) mayores, las cuales evidencian fallas en cláusulas como liderazgo, evaluación del desempeño y mejora. En el anexo J se encuentra el informe de auditoría con las no conformidades, observaciones y oportunidades de mejora encontrados.

6.5. Resultados

Como se observa, los dominios de SEGURIDAD EN LA OPERATIVA Y SEGURIDAD EN LAS COMUNICACIONES son los que se encuentran con un estado de madurez mayor, sin desconocer que existen otros dominios en los que la oficina de GST se esfuerza por llegar a un estado de madurez óptimo. Aquí cabe destacar que durante este trabajo se mejoraron los aspectos relacionados con la continuidad del negocio, pasando de un 15% de cumplimiento en el análisis diferencial, a un 69% en la auditoría realizada, lo cual muestra el esfuerzo realizado por alcanzar la mejora continua desde la oficina de seguridad de la información.

Se debe realizar un esfuerzo desde la dirección por implementar los planes de capacitación en legislación relacionada, implementar los controles de protección de los registros y la realización del plan de auditoría para mejorar los niveles de cumplimiento, ya que en este momento no llegan al 50%.

También se encuentra que si bien existe interés desde la alta dirección por la implementación y puesta a punto del sistema de gestión de seguridad de la información, es claro que en algunos roles de la entidad todavía hay falta de compromiso para su cumplimiento, lo cual sugiere que debe reforzarse las acciones de toma de conciencia y apropiación del tema.

7. Conclusiones

El presente trabajo permitió desarrollar en un ámbito real un plan maestro de seguridad de la información, el cual ayudó a mejorar distintas habilidades, como por ejemplo el manejo de metodologías específicas como MAGERIT y la realización de informes finales de auditoría, las cuales permiten desarrollar de forma más especializada trabajos concernientes a la gestión de la seguridad de la información.

Al ser un trabajo implementado, se encontró uno de los obstáculos más grandes que hay a la hora de desarrollar trabajos de este tipo, como es el contar con el apoyo y liderazgo de la alta dirección, lo cual es fundamental para el éxito de este tipo de proyectos. Lograr la concienciación de la gerencia en cuanto al manejo seguro de la información en todos sus ámbitos, permite que la Universidad vea mejorados razonablemente sus procesos y procedimientos en relación a esta área en el corto, mediano y largo plazo.

Con respecto a los objetivos planteados inicialmente, se puede concluir lo siguiente:

El análisis de riesgos mostró la necesidad de crear un plan de continuidad de negocio que permita a la GST estar lista en caso de incidentes que comprometan el funcionamiento normal de las operaciones críticas. Su propuesta y diseño permitió inscribirlo dentro de los planes administrativos y financieros de la entidad.

Durante el proceso se evidenció la necesidad de involucrar no solo al personal de GST en el alineamiento de los procesos de la oficina para cumplir con la norma ISO 27001:2013, sino a otras unidades como la rectoría general de la institución, y la dirección administrativa y financiera, ya que el trabajo en conjunto de éstas permite generar los recursos humanos, técnicos y de capital que se necesitan para modificar y alinear dichos procesos.

De los procesos que tiene la GST, se identificó que los procesos estratégicos planeación estratégica, arquitectura empresarial y gobierno de TI, así como los misionales (gestión de la infraestructura tecnológica y gerencia de proyectos) son fundamentales dentro de la alineación con la norma. Sin embargo, los procesos de soporte son los que dan el sustento al sistema de gestión de seguridad de la información en la Universidad, y su buen manejo es fundamental para el desarrollo de un proceso exitoso.

De los análisis diferencial y de riesgos desarrollados, y de la actualización y desarrollo de la gestión documental, se pudo evidenciar la baja capacitación que tiene el personal de la GST y de las unidades que manejan procesos críticos; la propuesta de un plan de capacitación y concienciación que involucre a funcionarios de distinto nivel, y que

permita mejorar los ámbitos relacionados con normativa legal, política y tratamiento de riesgos, ayudará a generar una cultura de seguridad que permita disminuir eventos como destrucción de información y errores de los usuarios, los cuales se constituyen en amenazas con alto impacto y frecuencia dentro de la organización.

Para que las estrategias de seguridad de la información puedan ser implementadas y mantenidas en el tiempo, es vital el apoyo económico que permita contar con más personal y equipos hardware o software. Conseguir personal capacitado y certificado para realizar las auditorías internas y desarrollar un análisis de carga para establecer el número de personas que deben ser adicionadas para el tratamiento y la respuesta a incidentes, ya que en este momento solo se cuenta con el ingeniero de seguridad para resolverlas.
También debe destinarse parte de los rubros conseguidos para la adquisición de software de análisis y gestión de riesgos, ya que el gran volumen de activos que se maneja hace difícil su correcta gestión sin una ayuda de este tipo.

Es necesario que se realice una segunda auditoría interna, la cual permita establecer el estado de los controles que fueron propuestos en esta primera parte del proyecto y que no han sido implantados en su totalidad a este momento. Dicha auditoría permitirá establecer los pasos a seguir, como nuevos proyectos a ejecutar, cuáles controles deben ser reforzados o cambiados para mejorar el nivel de madurez en cuestiones de seguridad dentro de la organización.

Algo que cabe destacar dentro de este apartado es la mejora obtenida en el dominio 17 “ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DENTRO DE LA CONTINUIDAD DEL NEGOCIO”, pasando de un 15% en el análisis diferencial a un 69% en la auditoría de cumplimiento. Esto, debido a la generación de acciones comenzadas a raíz del análisis de riesgos que evidenciaron la falta de acciones en esta área. También nombrar el dominio 8 “GESTION DE ACTIVOS”, el cual pasó del 40% al 73%, al identificar fallas en el procedimiento y la política de etiquetado y manipulado de la información, y en los inventarios de activos, los cuales fueron corregidos.

8. Glosario

Activo: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [UNE 71504:2008].

Amenaza: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008].

Impacto: Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema. (Minsiterio de hacienda y administraciones públicas).

Riesgo: Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.
El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo (Minsiterio de hacienda y administraciones públicas).

9. Bibliografía

[1] INCIBE, [En línea]. Available: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/swf/video_06.swf. [Último acceso: 2016].

[2] M. F. Chaparro R, *Responsabilidades,* Bogotá, Cundinamarca, 2016.

[3] AENOR, «Norma española UNA 71504,» Madrid, 2008.

[4] Ministerio de hacienda y administraciones públicas , «MAGERIT-Versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información: Libro II Catálogo de elementos,» Madrid, 2012.

[5] Ministerio de hacienda y administraciones públicas, «MAGERIT V3.0: Metodología de análisis y gestión de riesgos. Libro I: Método,» Madrid.

[6] «() - doc_iso27000_all.pdf».

[7] «ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información». [En línea]. Disponible en: http://www.iso27000.es/iso27000.html. [Accedido: 24-mar-2016].

[8] [En línea]. Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/swf/video_06.swf. [Accedido: 25-mar-2016].

10. Anexos

ANEXO A. ANÁLISIS GAP.
ANEXO B. POLÍTICA DE SEGURIDAD.
ANEXO C. PROCEDIMIENTO AUDITORÍA.
ANEXO D. GESTIÓN INDICADORES.
ANEXO E. RESPONSABILIDADES.
ANEXO F. RIESGOS.
ANEXO G. DECLARACIÓN APLICABILIDAD.
ANEXO H. ACTIVOS GST.
ANEXO I. IMPACTO RESIDUAL.
ANEXO J. PROYECTOS.
ANEXO K. AUDITORÍA CUMPLIMIENTO.
ANEXO L. GANTT PLAN MAESTRO
ANEXO M. PRESENTACIONES.