GESTIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN CON BASE EN LA NORMA ISO/IEC 27005 DE 2011 ADAPTANDO LA METODOLOGÍA COBIT 5 AL CASO DE ESTUDIO: PROCEDIMIENTO RECAUDOS DE LA DIVISIÓN FINANCIERA DE LA UNIVERSIDAD DEL CAUCA.

LIBRO DE ANEXOS

MILENA NATALIA CRUCES CERÓN

JUAN PABLO MORA PALACIOS

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones

Departamento de Sistemas

Grupo de Tecnologías de la Información (GTI)

Popayán, Julio de 2016

GESTIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN CON BASE EN LA NORMA ISO/IEC 27005 DE 2011 ADAPTANDO LA METODOLOGÍA COBIT 5 AL CASO DE ESTUDIO: PROCEDIMIENTO RECAUDOS DE LA DIVISIÓN FINANCIERA DE LA UNIVERSIDAD DEL CAUCA.

LIBRO DE ANEXOS

Trabajo de Grado para optar al título de Ingeniero en Electrónica y Telecomunicaciones

Milena Natalia Cruces Cerón

Juan Pablo Mora Palacios

Director: Esp. Siler Amador Donado

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Sistemas
Grupo de Tecnologías de la Información (GTI)
Popayán, Junio de 2016

ANEXO A – Resolución R 005.

4.90.18

Universidad del Cauca

Rectoría

RESOLUCIÓN NUMERO R- 0 0 5 DE 2015
(7 ENERO)

Por la cual se autoriza la ejecución del proyecto "Implantación y Certificación del Sistema de Gestión de la Seguridad de la Información – SGSI de la Universidad del Cauca"

EL RECTOR DELEGATARIO DE LA UNIVERSIDAD DEL CAUCA, en uso de las funciones delegadas mediante resolución R-1017 DE 19 DE DICIEMBRE DE 2014.

C O N S I D E R A N D O

1. Que es función del Rector de la Universidad del Cauca evaluar y controlar el funcionamiento general de la Universidad.

2. La Universidad del Cauca cuenta actualmente con los siguientes sistemas de información que generan y manejan información crítica: SIMCA (Sistema Integrado de Matrícula y Control Académico); SRF Plus (Sistema de Recursos Físicos); Finanzas Plus (Sistema de Información Financiero); SQUID (Sistema de Ingresos, Facturación y Cartera); QUERYS SRH (Sistema Recursos Humanos); SIVRI (Sistema de Información Vicerrectoría de Investigaciones); Smart Acces Control (Sistema Control de Acceso); Unicornio (Sistema de Información Bibliográfica); Apolo (Sistema de Información para Hemeroteca), los cuales son las fuentes primarias de información institucional.

3. La Universidad del Cauca desarrolla actividades institucionales relacionadas con el manejo de información, que demandan la necesidad de garantizar su seguridad desde la perspectiva de la confidencialidad, la integridad y la disponibilidad, desde sus procesos administrativos hasta los sistemas de información que los soportan.

4. Es necesario proteger los activos de información y para tal efecto es indispensable la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI).

5. Se debe hacer uso de un proceso sistemático, documentado y conocido por toda la institución, desde un enfoque de riesgo empresarial, para garantizar que la seguridad de la información sea gestionada correctamente, este proceso es el que constituye un SGSI.

RESUELVE:

ARTÍCULO PRIMERO: EJECUTAR en la Universidad del Cauca el Proyecto: "IMPLANTACION Y CERTIFICACION DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN – SGSI DE LA UNIVERSIDAD DEL CAUCA", para garantizar la seguridad de la información desde la perspectiva de la confidencialidad, integridad y disponibilidad.

ARTÍCULO SEGUNDO: INFORMACIÓN. La Información requerida para el desarrollo del proyecto será suministrada por cada una de las dependencias responsables de la información institucional, acorde con los artículos cuarto y quinto de la Resolución R-030 de Enero 30 de 2012.

ARTICULO TERCERO: DIRECCIÓN. La Dirección del Proyecto estará a cargo del Jefe de la División de Tecnologías de la Información y las Comunicaciones, como funcionario institucional responsable de este proyecto de seguridad, enmarcado dentro del Proyecto de Desarrollo de esta dependencia.

ARTICULO CUARTO: ASESOR. Designar como ASESOR en la formulación y desarrollo del Proyecto al ingeniero: Siler Amador Donado – Docente adscrito al Departamento de Sistemas de la Facultad de Ingeniería Electrónica y Telecomunicaciones, con una dedicación de 10 horas semanales de su labor académica.

ARTÍCULO QUINTO: FUNCIONES DEL ASESOR. Las funciones del asesor de la División de las TIC en la formulación y desarrollo del Proyecto son:

1. Apoyar en la elaboración de las políticas, normas y procedimientos de seguridad de la información para el SGSI institucional.
2. Acompañar en la implementación y cumplimento de las políticas, normas, y procedimientos de seguridad de la información.
3. Asistir en la administración del SGSI acorde con las fases del modelo PDCA.
4. Apoyar en el análisis de riesgos, planes de contingencia y prevención de desastres relacionados con el SGSI.
5. Asistir en el desarrollo de las investigaciones sobre incidentes y problemas relacionados con la seguridad de la información.
6. Acompañar en las revisiones periódicas del SGSI.
7. Recomendar las medidas pertinentes.

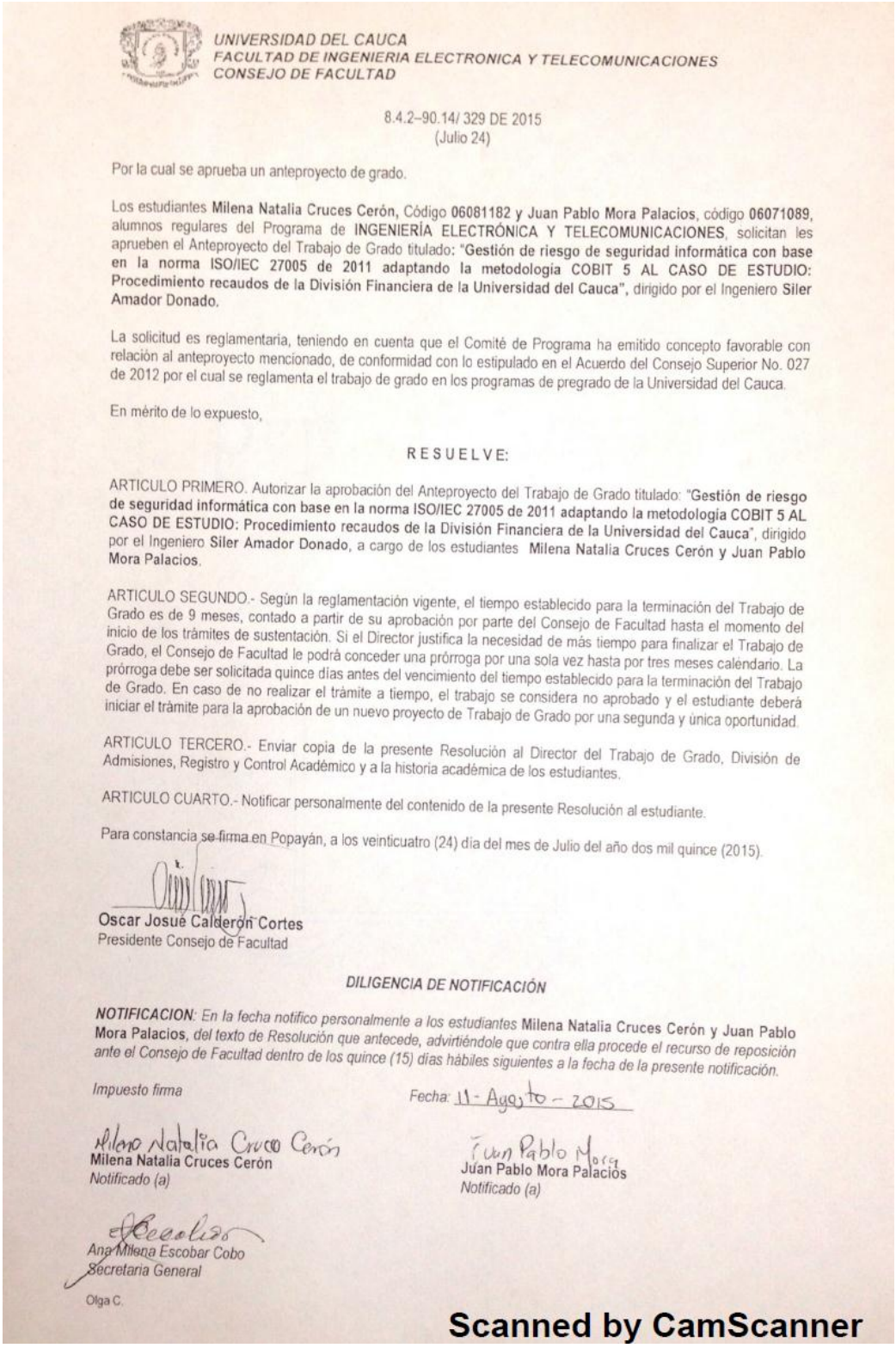
ARTÍCULO SEXTO: La presente resolución rige a partir de la fecha de su expedición y deroga las disposiciones que le sean contrarias, en especial la Resolución numero R. 051 de 2013.

COMUNIQUESE Y CUMPLASE

Se expide en Popayán, Ciudad Universitaria, a los siete (7) días del mes de enero. de 2015

EDGAR DE JESÚS VELÁSQUEZ RIVERA
Rector Delegatario

ANEXO B - Aprobacion de Anteproyecto



UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERIA ELECTRONICA Y TELECOMUNICACIONES
CONSEJO DE FACULTAD

8.4.2–90.14/ 329 DE 2015
(Julio 24)

Por la cual se aprueba un anteproyecto de grado.

Los estudiantes **Milena Natalia Cruces Cerón**, Código **06081182** y **Juan Pablo Mora Palacios**, código **06071089**, alumnos regulares del Programa de **INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES**, solicitan les aprueben el Anteproyecto del Trabajo de Grado titulado: **"Gestión de riesgo de seguridad informática con base en la norma ISO/IEC 27005 de 2011 adaptando la metodología COBIT 5 AL CASO DE ESTUDIO: Procedimiento recaudos de la División Financiera de la Universidad del Cauca"**, dirigido por el Ingeniero **Siler Amador Donado.**

La solicitud es reglamentaria, teniendo en cuenta que el Comité de Programa ha emitido concepto favorable con relación al anteproyecto mencionado, de conformidad con lo estipulado en el Acuerdo del Consejo Superior No. 027 de 2012 por el cual se reglamenta el trabajo de grado en los programas de pregrado de la Universidad del Cauca.

En mérito de lo expuesto,

RESUELVE:

ARTICULO PRIMERO. Autorizar la aprobación del Anteproyecto del Trabajo de Grado titulado: **"Gestión de riesgo de seguridad informática con base en la norma ISO/IEC 27005 de 2011 adaptando la metodología COBIT 5 AL CASO DE ESTUDIO: Procedimiento recaudos de la División Financiera de la Universidad del Cauca"**, dirigido por el Ingeniero **Siler Amador Donado**, a cargo de los estudiantes **Milena Natalia Cruces Cerón y Juan Pablo Mora Palacios.**

ARTICULO SEGUNDO.- Según la reglamentación vigente, el tiempo establecido para la terminación del Trabajo de Grado es de 9 meses, contado a partir de su aprobación por parte del Consejo de Facultad hasta el momento del inicio de los trámites de sustentación. Si el Director justifica la necesidad de más tiempo para finalizar el Trabajo de Grado, el Consejo de Facultad le podrá conceder una prórroga por una sola vez hasta por tres meses calendario. La prórroga debe ser solicitada quince días antes del vencimiento del tiempo establecido para la terminación del Trabajo de Grado. En caso de no realizar el trámite a tiempo, el trabajo se considera no aprobado y el estudiante deberá iniciar el trámite para la aprobación de un nuevo proyecto de Trabajo de Grado por una segunda y única oportunidad.

ARTICULO TERCERO.- Enviar copia de la presente Resolución al Director del Trabajo de Grado, División de Admisiones, Registro y Control Académico y a la historia académica de los estudiantes.

ARTICULO CUARTO.- Notificar personalmente del contenido de la presente Resolución al estudiante.

Para constancia se firma en Popayán, a los veinticuatro (24) día del mes de Julio del año dos mil quince (2015).

Oscar Josué Calderón Cortes
Presidente Consejo de Facultad

DILIGENCIA DE NOTIFICACIÓN

***NOTIFICACION**: En la fecha notifico personalmente a los estudiantes* **Milena Natalia Cruces Cerón y Juan Pablo Mora Palacios,** *del texto de Resolución que antecede, advirtiéndole que contra ella procede el recurso de reposición ante el Consejo de Facultad dentro de los quince (15) días hábiles siguientes a la fecha de la presente notificación.*

Impuesto firma Fecha: 11 - Agosto - 2015

Milena Natalia Cruces Cerón
Milena Natalia Cruces Cerón
Notificado (a)

Juan Pablo Mora
Juan Pablo Mora Palacios
Notificado (a)

Ana Milena Escobar Cobo
Secretaria General

Olga C.

Scanned by CamScanner

ANEXO C – Acuerdo de Confiabilidad

ACUERDO DE CONFIDENCIALIDAD

Popayán, 26 de Agosto del 2015 16847 SEP -2 P2:33

Señores
UNIVERSIDAD DEL CAUCA

GESTION DOCUMENTAL

Estimados señores:

En relación con mi intención de conocer los procesos organizacionales (en adelante el "Proceso" o los "Procesos") y evaluar la seguridad de la información en los procesos y procedimientos de **DIV. FINANCIERA (DIVISIÓN FINANCIERA DE LA UNIVERSIDAD DEL CAUCA)** (en adelante "Material de Evaluación"), declaro que estoy interesado en recibir información de los mismos, la cual puede contener información confidencial de propiedad de LA UNIVERSIDAD DEL CAUCA (en adelante la "Organización").

De igual forma le manifiesto que si después de leer y estudiar la información contenida en los Procesos decido investigar con mayor detalle y profundidad, soy consciente que la Organización estaría en condiciones de suministrar información adicional que pueda requerir sujeto a la posibilidad de que la Organización limite ese acceso en cualquier momento.

Reconozco desde ahora y de manera expresa, la naturaleza confidencial de todo el Material de Evaluación y el hecho de que es de propiedad exclusiva de la Organización. En consecuencia, yo acepto y estoy de acuerdo en que:

(i) Sólo utilizaremos el Material de Evaluación con el propósito exclusivo de ayudarnos a tomar un concepto de la seguridad de la información en el marco del Material de Evaluación.

(ii) No permitiremos el acceso, la reproducción o publicación del Material de Evaluación ni divulgaremos de manera parcial o total su contenido específico. Solo se divulgarán consolidados de todas las organizaciones que suministren Material de Evaluación.

(iii) No filtraremos o utilizaremos los conceptos, diseños de productos, ideas o modelos de negocio descritas o pertenecientes a los Procesos para desarrollar proyectos similares para beneficio propio o el de terceros de forma directa o por interpuesta persona, en territorio nacional o internacional y reconozco que tal conducta constituye una violación al presente Acuerdo.

Yo, mediante la firma del presente Acuerdo, quedo(a) obligado(a) a informarle a quien corresponda sobre la naturaleza confidencial del Material de Evaluación y sobre el hecho de que éste es de propiedad exclusiva de la Organización. En el evento en que nos veamos obligados a divulgar o entregar información, de manera parcial o total, del contenido de los Procesos por orden de autoridad judicial, aceptamos y nos obligamos a darle aviso escrito inmediato a la Organización, de manera que se puedan ejercer los correspondientes derechos de protección o de tutela, según corresponda.

Aceptamos y reconocemos que una indemnización monetaria no será suficiente para cubrir los perjuicios que resulten de la violación del presente Acuerdo por mi parte. Sin embargo, aceptamos que la Organización podrá cobrar y perseguir indemnización de perjuicios por cualquier daño, pérdida, costo o responsabilidad que se cause por la violación del presente Acuerdo y podrá también ejercer cualquier medio legal para evitar que se sigan ocasionando perjuicios como consecuencia de la violación.

Aceptamos y reconocemos igualmente, que la Organización no será responsable por las inexactitudes u omisiones que se puedan presentar en el Material de Evaluación, y que éste ha sido recopilado sobre la base del mejor esfuerzo posible.

Nos comprometemos a devolver o a destruir todo el Material de Evaluación tan pronto como se presente el primero de los siguientes eventos: (i) lo soliciten la Organización o (ii) la Organización informe que los procesos han terminado.

Aceptamos que este acuerdo hace parte integral de cada uno de los proyectos y que la obligación de confidencialidad no se extingue aún si no estamos interesados en participar en uno a varios de dichos proyectos.

El presente Acuerdo y la resolución de controversias que puedan derivarse de su ejecución se rigen por las leyes de la República de Colombia.

Sin otro particular, muy atentamente,

Milena Natalia Cruces Cerón
Firma
Nombre: Milena Natalia Cruces Cerón
CC: 1.088.972.924 de La Cruz Nariño

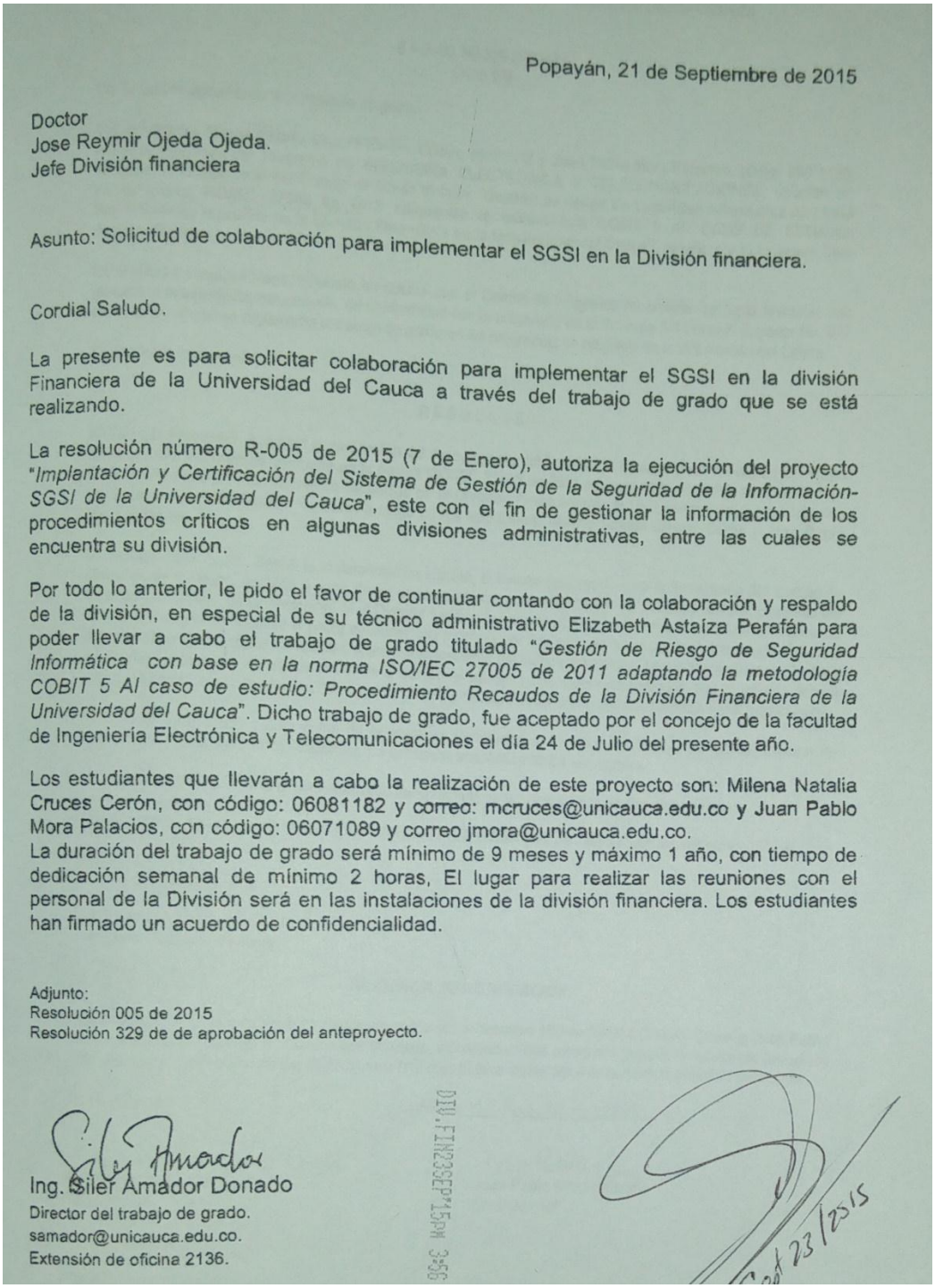
Juan Pablo Mora P
Firma
Nombre: Juan Pablo Mora Palacios
CC: 87.249.408 de La Cruz Nariño

Esta diligencia Notarial se realiza por diligencia de parte interesada

Notaría 1a de Popayán

RECONOCIMIENTO Y AUTENTICACIÓN
AL DESPACHO DE LA NOTARIA 1a. DE POPAYÁN
COMPARECIÓ
26 AGO 2015
Milena Natalia Cruces Cerón
QUIEN PRESENTO C.C. No 1088.972.924
EXPEDIDA EN La Cruz
Y MANIFESTÓ EN FORMA VOLUNTARIA Y ESPONTÁNEA QUE EL CONTENIDO DE EL DOCUMENTO ES SUYA. EL (LA) COMPARECIENTE ESTAMPA E IMPRIME HUELLA DIGITAL DEL DEDO ÍNDICE DERECHO
EL (LA) COMPARECIENTE Milena Natalia Cruces Cerón
Notario (a) Encargado (a)
COLOMBIA
POPAYÁN - CAUCA
Nancy Mery Muñoz Muñoz
Notaria Primera (Encargada)

ANEXO D - carta del jefe de la división financiera



Popayán, 21 de Septiembre de 2015

Doctor
Jose Reymir Ojeda Ojeda.
Jefe División financiera

Asunto: Solicitud de colaboración para implementar el SGSI en la División financiera.

Cordial Saludo.

La presente es para solicitar colaboración para implementar el SGSI en la división Financiera de la Universidad del Cauca a través del trabajo de grado que se está realizando.

La resolución número R-005 de 2015 (7 de Enero), autoriza la ejecución del proyecto "*Implantación y Certificación del Sistema de Gestión de la Seguridad de la Información-SGSI de la Universidad del Cauca*", este con el fin de gestionar la información de los procedimientos críticos en algunas divisiones administrativas, entre las cuales se encuentra su división.

Por todo lo anterior, le pido el favor de continuar contando con la colaboración y respaldo de la división, en especial de su técnico administrativo Elizabeth Astaíza Perafán para poder llevar a cabo el trabajo de grado titulado "*Gestión de Riesgo de Seguridad Informática con base en la norma ISO/IEC 27005 de 2011 adaptando la metodología COBIT 5 Al caso de estudio: Procedimiento Recaudos de la División Financiera de la Universidad del Cauca*". Dicho trabajo de grado, fue aceptado por el concejo de la facultad de Ingeniería Electrónica y Telecomunicaciones el día 24 de Julio del presente año.

Los estudiantes que llevarán a cabo la realización de este proyecto son: Milena Natalia Cruces Cerón, con código: 06081182 y correo: mcruces@unicauca.edu.co y Juan Pablo Mora Palacios, con código: 06071089 y correo jmora@unicauca.edu.co.
La duración del trabajo de grado será mínimo de 9 meses y máximo 1 año, con tiempo de dedicación semanal de mínimo 2 horas, El lugar para realizar las reuniones con el personal de la División será en las instalaciones de la división financiera. Los estudiantes han firmado un acuerdo de confidencialidad.

Adjunto:
Resolución 005 de 2015
Resolución 329 de de aprobación del anteproyecto.

Ing. Siler Amador Donado
Director del trabajo de grado.
samador@unicauca.edu.co.
Extensión de oficina 2136.

ANEXO E - Actas de reuniones: financiera y de las TIC

Universidad del Cauca	Oficina de Planeación y Desarrollo Institucional Acta general para actividades universitarias	
Código: PE-GE-2.2-FOR-6	Versión: 1	Fecha Vigencia: 21-02-2014

Ciudad	Popayán			Dependencia(s) responsable (s) de la actividad			
Fecha	2	09	2015	Hora Inicio	Hora Finalización	Lugar de desarrollo	ACTA No
	Día	Mes	Año	2:10 pm	3:30	División Financiera de la Universidad del Cauca	1

ORDEN DEL DIA

1. **Verificación de Asistencia**
2. **Lectura de acta anterior SI** ☐ **NO** ☐
3. **Temas a tratar**

No	TEMAS A TRATAR
1	Conocer y explicar el trabajo de grado "GESTION DE RIESGO DE SEGURIDAD INFORMATICA CON BASE EN LA NORMA ISO/IEC 27005 DE 2011, ADOPTANDO LA METODOLOGIA COBIT 5 AL CASO DE ESTUDIO: PROCEDIMIENTO RECAUDOS DE LA DIVISION FINANCIERA DE LA UNIVERSIDAD DEL CAUCA. "
2	Compromiso al desarrollo del trabajo de parte de los estudiantes como de la división.
3	Acordar horarios de reuniones.

DESARROLLO DE LA REUNIÓN

El desarrollo de la reunión fue de la siguiente manera:

- Se inició presentándose y dando una breve explicación del trabajo de grado que se realizara en la División financiera de la Universidad del Cauca, por parte de los estudiantes Milena Natalia Cruces y Juan Pablo Mora del parte del director e Ingeniero Siler Amador, como también de la manera que se ira desarrollando.
- Compromiso, responsabilidad, cumplimiento de los estudiantes Juan Pablo Mora y Milena Natalia Cruces para el desarrollo del trabajo
- Responsabilidad de Elizabeth Astaiza, de facilitar a los estudiantes la mayor información posible necesaria para dicho trabajo, lo cual se llevara a cabo por medio de reuniones que se realizaran en las instalaciones de la División financiera de la Universidad del Cauca.
- Respetar el acuerdo de confidencialidad por parte de los estudiantes.

RELACION PERSONAS ASISTENTES

No	NOMBRE Y APELLIDO	CARGO	DEPENDENCIA / ENTIDAD	FIRMA
1	Siler Amador Donado.	Docente/ Director		
2	Elizabeth Astaiza Perafan.	Técnico Administrativo		
3	Milena Natalia Cruces Cerón.	Estudiante		

Universidad del Cauca	Oficina de Planeación y Desarrollo Institucional Acta general para actividades universitarias		
Código: PE-GE-2.2-FOR-6	Versión: 1	Fecha Vigencia: 21-02-2014	

4	Juan Pablo Mora Palacios	Estudiante		

COMPROMISOS

No	COMPROMISO	RESPONSABLE	FECHA COMPROMISO	FECHA DE REALIZACIÓN
1	Dar la información necesaria para el buen desarrollo del trabajo de grado.	Elizabeth Astaiza Perafan		
2	Asistir puntualmente a las reuniones acordadas.	Elizabeth A. Milena Cruces Juan Pablo M.		
3	Responsabilidad con la información, catalogada como de confidencialidad.	Milena Cruces Juan Pablo M.		
4	Responsabilidad, efectividad, dedicación con el desarrollo del trabajo a realizar.	Milena Cruces Juan Pablo M. Siler Amador D.		
5	Cumplir el acuerdo de confidencialidad, el cual fue autenticado por la notaría y entregado a la Vicerrectora Administrativa	Milena Cruces. Juan Pablo M.		

OBSERVACIONES

SILER AMADOR DONADO

MILENA NATALIA CRUCES CERON.

ELIZABETH ASTAIZA PERAFAN.

JUAN PABLO MORA PALACIOS.

Universidad del Cauca	Oficina de Planeación y Desarrollo Institucional Acta general para actividades universitarias		
	Código: PE-GE-2.2-FOR-6	Versión: 1	Fecha Vigencia: 21-02-2014

Ciudad	Popayán			Dependencia(s) responsable (s) de la actividad			
Fecha	9	09	2015	Hora Inicio	Hora Finalización	Lugar de desarrollo	ACTA No
	Día	Mes	Año	2:10 pm	3:30	División Financiera de la Universidad del Cauca	2

ORDEN DEL DIA

1. **Verificación de Asistencia**
2. **Lectura de acta anterior SI ☐ NO ☐**
3. **Temas a tratar**

No	TEMAS A TRATAR
1	Conocer y explicar el funcionamiento de la división financiera del procedimiento recaudos, paso a paso desde el inicio del día hasta el final de este, las áreas implicadas y el software que se utiliza para cumplir las diferentes funciones.
2	Compromiso de empezar a desarrollar la elipse que contenga el funcionamiento de la división financiera.

DESARROLLO DE LA REUNIÓN

El desarrollo de la reunión fue de la siguiente manera:

- Se inició dando a conocer los aplicativos que se utilizan en recaudos, como es: SIMCA SQUID y finanzas plus, cómo a través de estos se generan los recaudos de la división y se reportan entre ellos.
- Se dio una explicación, de los pasos que se dan desde el inicio del día hasta el final de este y ejemplos de los formatos que cada división utiliza y genera para los recaudos que hace la universidad.

RELACION PERSONAS ASISTENTES

No	NOMBRE Y APELLIDO	CARGO	DEPENDENCIA / ENTIDAD	FIRMA
1	Elizabeth Astaiza Perafan.	Técnico Administrativo		
2	Milena Natalia Cruces Cerón.	Estudiante		
3	Juan Pablo Mora Palacios	Estudiante		

Universidad del Cauca	Oficina de Planeación y Desarrollo Institucional Acta general para actividades universitarias		
Código: PE-GE-2.2-FOR-6	Versión: 1	Fecha Vigencia: 21-02-2014	

COMPROMISOS

No	COMPROMISO	RESPONSABLE	FECHA COMPROMISO	FECHA DE REALIZACIÓN
1	Dar la información necesaria para el buen desarrollo del trabajo de grado.	Elizabeth Astaiza Perafan		
2	Asistir puntualmente a las reuniones acordadas.	Elizabeth A. Milena Cruces Juan Pablo M.		
3	Responsabilidad con la información, catalogada como de confidencialidad.	Milena Cruces Juan Pablo M.		
4	Responsabilidad, efectividad, dedicación con el desarrollo del trabajo a realizar.	Milena Cruces Juan Pablo M. Siler Amador D.		
5	Cumplir el acuerdo de confidencialidad, el cual fue autenticado por la notaría y entregado a la Vicerrectora Administrativa	Milena Cruces. Juan Pablo M.		

OBSERVACIONES

Elizabe Astaiza P.
ELIZABETH ASTAIZA PERAFAN

Milena Natalia Cruces Ceron
MILENA NATALIA CRUCES CERON.

Juan Pablo Mora
JUAN PABLO MORA PALACIOS.

Universidad del Cauca	Oficina de Planeación y Desarrollo Institucional Acta general para actividades universitarias	
Código: PE-GE-2.2-FOR-6	Versión: 1	Fecha Vigencia: 21-02-2014

3Ciudad	Popayán			Dependencia(s) responsable (s) de la actividad			
Fecha	30	09	2015	Hora Inicio	Hora Finalización	Lugar de desarrollo	ACTA No
	Día	Mes	Año	2:10 pm	4:00	División Financiera de la Universidad del Cauca	3

ORDEN DEL DIA

1. **Verificación de Asistencia**
2. **Lectura de acta anterior SI ☐ NO ☐**
3. **Temas a tratar**

No	TEMAS A TRATAR
1	Conocer y explicar el funcionamiento de la división financiera del procedimiento recaudos, paso a paso desde el inicio del día hasta el final de este, las áreas implicadas y el software que se utiliza para cumplir las diferentes funciones.
2	Compromiso de empezar a desarrollar la elipse que contenga el funcionamiento de la división financiera.
3	Presentar al jefe de la División Financiera el trabajo que se desea realizar.

DESARROLLO DE LA REUNIÓN

El desarrollo de la reunión fue de la siguiente manera:

- Se inició aclarando ciertas inquietudes que se tenía ciertas dudas de la reunión pasada, respecto a los procedimientos de la División Financiera.
- Seguidamente se dio una breve explicación del trabajo de grado que se realizara en la División financiera de la Universidad del Cauca, por parte de los estudiantes, los cuales fueron presentados al jefe de la División Financiera el señor José Reimir Ojeda, como también de la manera que se irá desarrollando el cual dio todo el apoyo para el desarrollo del trabajo de grado.
- Posteriormente se recopilo con la explicación de los pasos, funciones que se presentan en la División Financiera.

RELACION PERSONAS ASISTENTES

No	NOMBRE Y APELLIDO	CARGO	DEPENDENCIA / ENTIDAD	FIRMA
1	Elizabeth Astaiza Perafan.	Técnico Administrativo	División Gestión Financiera	Elizabeth Astaiza P
2	Milena Natalia Cruces Cerón.	Estudiante		
3	Juan Pablo Mora Palacios	Estudiante		
4	José Reimir Ojeda Ojeda	Jefe de la División Financiera	División Gestión Fcia	

Universidad del Cauca	Oficina de Planeación y Desarrollo Institucional Acta general para actividades universitarias		
Código: PE-GE-2.2-FOR-6	Versión: 1	Fecha Vigencia: 21-02-2014	

COMPROMISOS

No	COMPROMISO	RESPONSABLE	FECHA COMPROMISO	FECHA DE REALIZACIÓN
1	Dar la información necesaria para el buen desarrollo del trabajo de grado.	Elizabeth Astaiza Perafan		
2	Asistir puntualmente a las reuniones acordadas.	Elizabeth A. Milena Cruces Juan Pablo M.		
3	Responsabilidad con la información, catalogada como de confidencialidad.	Milena Cruces Juan Pablo M.		
4	Responsabilidad, efectividad, dedicación con el desarrollo del trabajo a realizar.	Milena Cruces Juan Pablo M. Siler Amador D.		
5	Cumplir el acuerdo de confidencialidad, el cual fue autenticado por la notaría y entregado a la Vicerrectora Administrativa	Milena Cruces. Juan Pablo M.		
6	Brindar todo el apoyo, información, necesidades para el desarrollo del trabajo de grado.	José Reimir Ojeda Ojeda		

OBSERVACIONES

Elizabe Astaiza T.
ELIZABETH ASTAIZA PERAFAN

Milena Natalia Cruces Cerón
MILENA NATALIA CRUCES CERON.

Juan Pablo Mora.
JUAN PABLO MORA PALACIOS

JOSE REIMIR OJEDA OJEDA

Universidad del Cauca	Oficina de Planeación y Desarrollo Institucional Acta general para actividades universitarias		
Código: PE-GE-2.2-FOR-6	Versión: 1	Fecha Vigencia: 21-02-2014	

3Ciudad	Popayán			Dependencia(s) responsable (s) de la actividad			
Fecha	14	10	2015	Hora Inicio	Hora Finalización	Lugar de desarrollo	ACTA No
	Día	Mes	Año	2:10 pm	4:00	División Financiera de la Universidad del Cauca	4

ORDEN DEL DIA

1. **Verificación de Asistencia**
2. **Lectura de acta anterior SI ☐ NO ☐**
3. **Temas a tratar**

No	TEMAS A TRATAR
1	Hacer las respectivas aclaraciones frente a la elipse de la División Financiera de la Universidad del Cauca.
2	Compromiso de finalizar el desarrollo de la elipse que contenga el funcionamiento de la división financiera.

DESARROLLO DE LA REUNIÓN

El desarrollo de la reunión fue de la siguiente manera:

- Se inició aclarando ciertas inquietudes que se tenía ciertas dudas de la reunión pasada, respecto a los procedimientos de la División Financiera.
- Seguidamente se dio ciertas aclaraciones de la elipse, frente a procedimientos de la organización y a organizaciones extemas, que estaban establecidas por los procedimientos que fueron obtenidos dentro de la Universidad por los estudiantes
- Posteriormente se recopilo más información del comportamiento de los demás procesos frente a la División Financiera de los cuales hacían falta para completar u otros por corregir.
- Se completó la información del procedimiento de Recaudos de una manera más exhaustiva las organizaciones internas y extemas de la Universidad ya que esta es la del caso de estudio.

RELACION PERSONAS ASISTENTES

No	NOMBRE Y APELLIDO	CARGO	DEPENDENCIA / ENTIDAD	FIRMA
1	Elizabeth Astaiza Perafan.	Técnico Administrativo	División Gestion Financiera	Elizabeth Astaiza P.
2	Milena Natalia Cruces Cerón.	Estudiante		
3	Juan Pablo Mora Palacios	Estudiante		

Universidad del Cauca	Oficina de Planeación y Desarrollo Institucional Acta general para actividades universitarias		
Código: PE-GE-2.2-FOR-6	Versión: 1	Fecha Vigencia: 21-02-2014	

COMPROMISOS

No	COMPROMISO	RESPONSABLE	FECHA COMPROMISO	FECHA DE REALIZACIÓN
1	Dar la información necesaria para el buen desarrollo del trabajo de grado.	Elizabeth Astaiza Perafan		
2	Asistir puntualmente a las reuniones acordadas.	Elizabeth A. Milena Cruces Juan Pablo M.		
3	Responsabilidad con la información, catalogada como de confidencialidad.	Milena Cruces Juan Pablo M.		
4	Responsabilidad, efectividad, dedicación con el desarrollo del trabajo a realizar.	Milena Cruces Juan Pablo M. Siler Amador D.		
5	Cumplir el acuerdo de confidencialidad, el cual fue autenticado por la notaría y entregado a la Vicerrectora Administrativa	Milena Cruces. Juan Pablo M.		

OBSERVACIONES

Elizabeth Astaiza P.
ELIZABETH ASTAIZA PERAFAN

Milena Natalia Cruces Ceron
MILENA NATALIA CRUCES CERON.

Juan Pablo Mora P.
JUAN PABLO MORA PALACIOS

Universidad del Cauca	Oficina de Planeación y Desarrollo Institucional Acta general para actividades universitarias	
Código: PE-GE-2.2-FOR-6	Versión: 1	Fecha Vigencia: 21-02-2014

3Ciudad	Popayán			Dependencia(s) responsable (s) de la actividad			
Fecha	19	10	2015	Hora Inicio	Hora Finalización	Lugar de desarrollo	ACTA No
	Día	Mes	Año	2:10 pm	4:00	División Financiera de la Universidad del Cauca	5

ORDEN DEL DIA

1. **Verificación de Asistencia**
2. **Lectura de acta anterior SI ☐ NO ☐**
3. **Temas a tratar**

No	TEMAS A TRATAR
1	Hacer las respectivas aclaraciones frente a la elipse de la División Financiera de la Universidad del Cauca.
2	Compromiso de finalizar el desarrollo de la elipse que contenga el funcionamiento de la división financiera.
3	Identificación de Activos.

DESARROLLO DE LA REUNIÓN

El desarrollo de la reunión fue de la siguiente manera:

- Se inició aclarando las últimas inquietudes que se tenía, respecto a los procedimientos de la División Financiera y dando como fin el método de las elipses para dar como concluido el alcance.
- Seguidamente se inició dando a conocer información de los activos de la División Financiera, por parte del técnico administrativo. Los cuales fueron de manera muy minuciosa debido a ciertas dudas que se tenían frente a los activos de información.

RELACION PERSONAS ASISTENTES

No	NOMBRE Y APELLIDO	CARGO	DEPENDENCIA / ENTIDAD	FIRMA
1	Elizabeth Astaiza Perafan.	Técnico Administrativo	División Gestión Financiera	Elizabeth Astaiza P
2	Milena Natalia Cruces Cerón.	Estudiante		
3	Juan Pablo Mora Palacios	Estudiante		

COMPROMISOS

No	COMPROMISO	RESPONSABLE	FECHA COMPROMISO	FECHA DE REALIZACIÓN
1	Dar la información necesaria para el buen desarrollo del trabajo de	Elizabeth Astaiza Perafan		

	grado.			
2	Asistir puntualmente a las reuniones acordadas.	Elizabeth A. Milena Cruces Juan Pablo M.		
3	Responsabilidad con la información, catalogada como de confidencialidad.	Milena Cruces Juan Pablo M.		
4	Responsabilidad, efectividad, dedicación con el desarrollo del trabajo a realizar.	Milena Cruces Juan Pablo M. Siler Amador D.		
5	Cumplir el acuerdo de confidencialidad, el cual fue autenticado por la notaría y entregado a la Vicerrectora Administrativa	Milena Cruces. Juan Pablo M.		

OBSERVACIONES

Elizabeth Astaiza P.
ELIZABETH ASTAIZA PERAFAN

Milena Natalia Cruces Cerón
MILENA NATALIA CRUCES CERON.

Juan Pablo Mora.
JUAN PABLO MORA PALACIOS

ANEXO F - Lista de activos

No	ACTIVOS
1	Bases de Datos
2	Servidores Web
3	Servidores de Aplicaciones
4	Servicio de Correo
5	Sistema Académico Simca
6	SQUID
7	FPL
8	Sistema de Pagos PSE y WEBSERVICES
9	Internet
10	Matrices de Almacenamiento
11	Switches de Comunicación
12	Cableado Estructurado
13	Firewalls
14	Licencias SW
15	Certificados de Seguridad
16	Planta Eléctrica Div TIC
17	Aire acondicionado
18	Planillas de Bancos
19	Soportes de Conciliación
20	Soportes Diarios de Caja
21	Resoluciones
22	Computador
23	Fotocopiadora
24	Impresora
25	Red Telefónica
26	Ficheros
27	Medios Magnéticos
28	Planta Eléctrica Div TIC
29	Recauda y Registra
30	Técnico Administrativo
31	Mensajeros Internos/Externos
32	Tesorero
33	Password
34	Edificio Div TIC
35	Cliente

36	Edificio Div Financiera
37	Planta Eléctrica Div Financiera
38	UPS
39	Red Unicauca
40	Mobiliarios

ANEXO G - Clasificación de activos

TIPO	DEFINICION	ACTIVOS	
Servicio	Función que satisface una necesidad de los usuarios del servicio. Para la prestación de un servicio los servicios aparecen como activos de un análisis de riesgos bien como servicios finales (prestados por la Organización a terceros), bien como servicios instrumentales (donde los usuarios y los medios son propios), bien como servicios contratados (a otra organización que los proporciona con sus propios medios).	Recauda y Registra.	
Datos / Información	Elementos de información que de forma singular o agrupada de alguna forma, representan el conocimiento que se tiene de algo. Los datos son el corazón que permite a una organización prestar sus servicios.	Base de Datos, Resoluciones, Soportes Diarios de Caja, Soportes de Conciliación, Planillas de Bancos, Certificados de Seguridad, Password.	
Aplicaciones (Software)	Este tipo se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.	Servicios de aplicaciones, Servicio de correo, Sistema Académico Simca, SQUID, FPL, Sistema de Pagos PSE y Webservices, Firewalls, Licencias SW, Matrices de Almacenamiento.	
Equipos infor máticos (Hardware)	Dícese de los bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del proceso o la transmisión de datos.	Computador, Impresora, Fotocopiadora.	
Redes de Comunicacion es	Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.	Servidores Web, Red Unicauca, Cableado Estructurado, Red Telefónica, Internet, Switches de Comunicación.	
Soportes de Información	Se consideran dispositivos físicos que permiten almacenar información de forma permanente o al	Medios Magnéticos (memorias USB, Discos Duros).	

	menos durante largos periodos de tiempo.		
Equipamiento Auxiliar	Se consideran dispositivos físicos que permiten almacenar información de forma permanente o al menos durante largos periodos de tiempo.	Mobiliarios, Ficheros, Aire acondicionado, UPS.	
Instalaciones	Los lugares donde se hospedan los sistemas de información y comunicaciones.	Edificio Div TIC, Edificio Div Financiera, Planta Eléctrica Div Financiera, Planta Eléctrica Div TIC.	
Personal	Aparecen las personas relacionadas con los sistemas de información.	Técnico Administrativo, Cliente, Mensajeros Internos/Externos, Tesorero.	

ANEXO H - Tasación de activos

ACTIVOS	Confidencialidad	Integridad	Disponibilidad	Criticidad
Bases de Datos	5	5	5	5
Servidores Web	5	5	5	5
Servidores de Aplicaciones	5	5	5	5
Servicio de Correo	3	4	3	3
Sistema Académico Simca	3	4	5	4
SQUID	5	5	5	5
FPL	5	5	5	5
Sistema de Pagos PSE y WEBSERVICES	5	5	5	5
Internet	1	3	5	3
Matrices de Almacenamiento	5	5	5	5
Switches de Comunicación	2	4	3	3
Cableado Estructurado	2	2	4	3
Firewalls	5	5	5	5
Licencias SW	5	5	5	5
Certificados de Seguridad	2	3	5	3
Plantas Eléctricas Div TIC/Financiera	5	5	5	5
Aire acondicionado	1	5	5	4
Planillas de Bancos	5	5	5	5
Soportes de Conciliación	3	5	5	4
Soportes Diarios de Caja	3	5	5	4
Resoluciones	3	5	4	3
Computador	2	3	3	3
Fotocopiadora	1	3	5	3
Impresora	1	4	5	3
Red Telefónica	1	2	4	2
Ficheros	1	5	3	3
Medios Magnéticos	3	5	4	4
Recauda y Registra	2	5	5	4
Técnico Administrativo	1	3	5	3
Mensajeros Internos/Externos	1	3	5	3
Tesorero	1	3	5	3
Password	3	3	2	2
Edificios Div TIC/Div Financiera	5	3	5	4
Cliente	1	3	5	3
Edificio	5	3	5	4

UPS	5	5	5	5
Red Unicauca	1	3	5	3
Mobiliarios	2	3	5	3

ANEXO I - Identificación de amenazas y vulnerabilidades

Categorías de Recursos	ACTIVOS	Amenaza	Vulnerabilidades
Servicios SSI	-Bases de Datos -Servidores Web -Servidores de Aplicaciones -Recauda y Registra -Red Telefónica -Password	-Polvo, corrosión, congelamiento. -Incumplimiento en el mantenimiento del sistema de información. -Hurto de medios o documentos. - Abuso de los derechos	-Mantenimiento insuficiente/ instalación fallida de los medios de almacenamiento -Susceptibilidad a la húmeda, el polvo y la suciedad. -Variaciones de voltaje -Almacenamiento sin protección -Copia no controlada -Ausencia de “Terminación de la sesión” cuando se abandona la estación de trabajo
Plataformas o sistemas	-Servicio de Correo -Sistema Académico Simca -SQUID -FPL -Sistema de Pagos PSE y WEBSERVICES -Internet -Red Unicauca	-Abuso de los derechos. -Corrupción de datos. -Falsificación de derechos. -Mal funcionamiento del software. -Manipulación de software. -Abuso de derechos.	-Asignación errada de los derechos de acceso -Utilización de datos errados en los programas aplicación -Gestión deficiente de las contraseñas -Ausencia de control de cambios eficaz
Equipos y dispositivos	-Matrices de Almacenamiento -Switches de Comunicación -Cableado Estructurado -Firewalls -Licencias SW -Certificados de Seguridad -Aire acondicionado -Fotocopiadora -Computador -Medios Magnéticos -Planta Eléctrica Div TIC/ Div Financiera -Impresora -UPS	-Incumplimiento en el mantenimiento del sistema de información. -Abuso de los derechos. -Corrupción de datos. -Falsificación de derechos. -Manipulación de equipos. -Manipulación de Licencias. -Abuso de derechos. -Hurto de equipos.	-Conexión deficiente de los cables -Ausencia de identificación y autenticación de emisor receptor -Conexiones de red pública sin protección -Ausencia de procesamientos de monitoreo de los recursos de procesamientos de información - Ausencia de mecanismo de monitoreo establecidos para los equipos.

Soportes	-Planillas de Bancos -Soportes Diarios de Caja -Soportes de Conciliación -Resoluciones	-Abuso de los derechos -Corrupción de datos -Hurto de documentos.	- Error de uso. -Hurto de Documentos.
Personal	-Técnico Administrativo -Mensajeros Internos/Externos -Tesorero -Cliente	-Incumplimiento en la disposición del personal -Error en el uso -Hurto de medio o documentos	-Ausencia del personal -Uso incorrecto de software y hardware -Trabajo no supervisado del personal -Entrenamiento insuficiente de seguridad de personal.
	-Edificio Div TIC/ Div Financiera -Mobiliarios	-Destrucción de equipos o medios -Hurto de equipos / mobiliarios.	-Uso inadecuado o destrucción del control de acceso físico a las edificaciones y mensajería. -Ausencia de protección física de la edificación, puertas y ventanas

ANEXO J - Encuestas para los escenarios

Encuesta (Jefe División Financiera)

Gestión de riesgo de Seguridad Informática con base en la norma ISO/IEC 27005 de 2011 adaptando la metodología COBIT 5 Al caso de estudio: Procedimiento Recaudos de la División Financiera de la Universidad del Cauca.

ENCUESTA A LA DIVISION DE GESTION FINANCIERA DE LA UNIVERSIDAD DEL CAUCA

Conscientes de la importancia de la seguridad en el ámbito de las tecnologías de la información y la comunicación de nuestras organizaciones, esta encuesta pretende dar una visión general sobre el actual conocimiento de la División de Gestión Financiera de la universidad del cauca, esta encueta está hecha para recolectar información para el trabajo de grado titulado **"Gestión de Riesgo de Seguridad Informática con base en la norma ISO/IEC 27005 de 2011 adaptando la metodología COBIT 5 Al caso de estudio: Procedimiento Recaudos de la División Financiera de la Universidad del Cauca."** A cargo de los estudiantes: Milena Natalia Cruces Cerón y Juan Pablo Mora Palacios, con dirección del ingeniero Siler Amador Donado.

Lea atentamente las instrucciones:

1. Las preguntas tienen como propósito realizar un análisis sobre fin de conocer el tratamiento, hábitos de uso y medidas de seguridad empleadas en la información que se utiliza.
2. Para contestar marque con una X la opción.
3. Toda información proporcionada será utilizada solo con fines académicos bajo un acuerdo de Confidencialidad firmado y autenticado por los estudiantes encargados.

1. **¿La División de Gestión Financiera tiene definido un plan estratégico de TI?**

   a) SI

   b) Parcialmente

   c) N

2. **¿La División de Gestión Financiera tiene implantado políticas de TI?**

   a) SI

   b) Parcialmente

   c) No

   2.1 Si su respuesta es SI ¿con que frecuencia son renovadas dichas políticas de TI?

   a) Frecuentemente

   b) A veces

   c) Nunca

3. **¿Están identificados las amenazas y vulnerabilidades que afectan al normal desempeño de la División de Gestión Financiera?**

   a) SI

   b) Parcialmente

   c) No

   3.1 SI su respuesta es SI, ¿Cuáles son las amenazas y vulnerabilidades que causan mayor impacto en las operaciones de TI? Cite las más representativas

4. **¿Está usted preparado para los riesgos que se presenten en la División Financiera?**

   a) SI

   b) Parcialmente

   c) No

5. **¿Se establecen acuerdos de confidencialidad y no divulgación sobre el acceso e intercambio de información en la División de Gestión Financiera?**

   a) SI

   b) No

6. **¿La División de Gestión Financiera trata los activos (hardware, software, documentación, etc...)??**

   a) No

   b) La Institución dispone de un inventario parcial de activos

   c) La Institución dispone de un inventario completo y actualizado de los activos.

7. **¿Los activos de la Institución están convenientemente clasificados (según su grado de sensibilidad y criticidad)?**

   a) Si

b) Sí, pero de forma parcial

c) Sí, los activos están clasificados

d) No

8. ¿Las infraestructuras TIC críticas o con información sensible están ubicadas en entornos protegidos y con controles de acceso?

a) Sí, se encuentran en locales aislados

b) Sí, los locales están especialmente preparados contra daños externos (electricidad, fuego, agua, sabotajes, etc...)

c) Sí, existe control de acceso para el personal autorizado

d) Sí, existen directrices claras para visitar y/o trabajar en dichos entornos

e) Ninguna de las anteriores

9. ¿Cuántas evaluaciones de seguridad realiza a sus sistemas al año?

a) Una

b) Más de tres

c) Ninguna

10. ¿Ha tenido incidentes de seguridad de la información en estos 3 últimos años?

a) Una c) NO

b) Más de tres

11. Sobre la gestión de medios extraíbles (Cintas, CDs, DVDs, memorias flash, discos duros portátiles, etc.) y copias impresas

a) Existe un procedimiento documentado que incluye instrucciones de almacenamiento, transporte y destrucción de los medios extraíbles utilizados

b) Se almacenan en lugar seguro y protegido del fuego e inundaciones fuera del centro de proceso de datos

c) Se lleva un inventario completo

d) Se destruyen físicamente cuando llega el fin de su vida útil

e) Ninguna de las anteriores

12. ¿Existe una política de protección de la información cuando se produce un intercambio electrónico de la misma?

a) No

b) Sí

c) Si, y tiene en cuenta la protección frente a accesos no autorizados, modificaciones, disponibilidad del servicio y aspectos legales.

13. ¿Son los encargados conscientes de la responsabilidad que tienen para que sean eficaces los controles de acceso, en particular con las contraseñas, equipos informáticos y el entorno de trabajo?

a) No, no tienen consignas sobre uso de las contraseñas, sus equipos informáticos o escritorios

b) No, pero se aplican medidas técnicas que garantizan la calidad de las contraseñas y el bloqueo de los equipos informáticos desatendidos

c) Sí, además de lo anterior, se les informa expresamente sobre la forma de gestionar correctamente sus contraseñas, los equipos informático, sesiones desatendidas y el entorno de trabajo

14. ¿Qué procedimientos y medios para restringir el acceso al sistema operativo de los encargados se utilizan en La División de Gestión Financiera?

a) El personal tiene un identificador único

b) Se controla que no haya más de un número de intentos de acceso fallidos, tras el cual se producen eventos como registro, incrementos de los tiempos de respuesta, etc.

c) Se establecen tiempos de cierre por inactividad, así como tiempos máximos de conexión

d) Se limita el acceso a las funcionalidades del sistema a lo estrictamente necesario para el trabajo del usuario

e) Ninguna de las anteriores

15.¿Existe gestión de vulnerabilidades del software?

a) SI

b) No

16.¿Se aplican medidas para asegurar el cumplimiento de los requisitos legales ya sean estatutarias, reguladoras o contractuales?

a) No

b) Sí, es una responsabilidad delegada a los usuarios

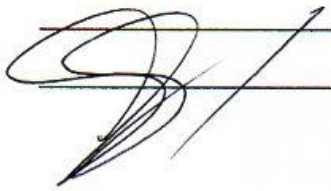
c) Sí, hay políticas definidas que regulan el uso legal del software y otros productos protegidos por leyes de propiedad intelectual

d) Sí, además de lo anterior se implementan controles para asegurar que se cumplen dichas políticas

e) Sí, además de lo anterior se realizan auditorías internas que velan por el cumplimiento de las mismas

Observaciones:

- Se Solicita que el Sistema obligue al cambio de Clave periodicamente
- Se Solicita tambien que la sesión al estar inactiva por lo menos una hora, se cierre, obligando a ingresar nuevamente al usuario.
- los BackUps del Sistema FPL se solicita que sean automaticos.
- Establecer un protocolo para el manejo de la información y entrada al Sistema.



José Reymir Ojeda Ojeda
Jefe División de Gestión Financiera

Encuestas (Técnico Administrativo Área Recaudos)

ENCUESTA AL AREA DE RECAUDOS DE LA DIVISION DE GESTION FINANCIERA DE LA UNIVERSIDAD DEL CAUCA

Conscientes de la importancia de la seguridad en el ámbito de las tecnologías de la información y la comunicación de nuestras organizaciones, esta encuesta pretende dar una visión general sobre el actual conocimiento de la división de gestión financiera de la universidad del cauca, esta encueta está hecha para recolectar información para el trabajo de grado titulado "**Gestión de Riesgo de Seguridad Informática con base en la norma ISO/IEC 27005 de 2011 adaptando la metodología COBIT 5 Al caso de estudio: Procedimiento Recaudos de la División Financiera de la Universidad del Cauca.**" A cargo de los estudiantes: Milena Natalia Cruces Cerón y Juan Pablo Mora Palacios, con dirección del ingeniero Siler Amador Donado.

Lea atentamente las instrucciones:

1. Las preguntas tienen como propósito realizar un análisis sobre fin de conocer el tratamiento, hábitos de uso y medidas de seguridad empleadas en la información que se utiliza.
2. Para contestar marque con una X la opción.
3. Toda información proporcionada será utilizada será utilizada solo con fines académicos bajo un acuerdo de Confidencialidad.

1. **¿El área de Recaudos de la División de Gestión Financiera tiene definido un plan estratégico de TI?**

   a) SI

   b) Parcialmente

   c) N

2. **¿La División de Gestión Financiera tiene implantado políticas de TI?**

   a) SI

   b) Parcialmente

   c) No

3. **¿Están identificados las amenazas y vulnerabilidades que afectan al normal desempeño del Área de Recaudos?**

   a) SI

   b) Parcialmente

   c) No

   3.1 SI su respuesta es SI, ¿Cuáles son las amenazas y vulnerabilidades que causan mayor impacto en las operaciones de TI? Cite las más representativas

   _____

   _____

   _____

   _____

4. **¿Está usted preparada para los riesgos que se presenten en el área de Recaudos?**

   a) SI

   b) Parcialmente

   (c) No

5. **¿Se establecen acuerdos de confidencialidad y no divulgación sobre el acceso e intercambio de información en el área de Recaudos?**

   a) SI

   (b) No

6. **¿El área de Recaudos gestiona los activos (hardware, software, documentación, etc...)??**

   a) No

   (b) La Institución dispone de un inventario parcial de activos

   c) La Institución dispone de un inventario completo y actualizado de los activos.

7. **¿Los activos del área de Recaudos están convenientemente clasificados (según su grado de sensibilidad y criticidad)?**

   a) Si

   b) Sí, pero de forma parcial

   c) Sí, los activos están clasificados

   (d) No

8. **¿Cuántas evaluaciones de seguridad realiza a sus sistemas al año?**

   a) Una

   b) Más de tres

   (c) Ninguna

9. **¿Ha tenido incidentes de seguridad de la información en estos 3 últimos años?**

   a) Una

   b) Más de tres

10. **¿Existe un procedimiento para la aceptación de los nuevos sistemas, actualizaciones de aplicaciones, nuevas versiones de sistema operativo, cambio de hardware, etc...?**

    a) Si, existe un procedimiento

    (b) No, simplemente se realizan algunas pruebas

11. **¿Se toman medidas contra el código malicioso en el área de Recaudos?**

    (a) Tenemos antivirus y antimalware en todos los equipos de los usuarios

    b) Tenemos implantada una gestión centralizada de los equipos de la Institución para actualizaciones del sistema operativo y antivirus

    c) No.

12. **¿Respecto a las copias de seguridad?**

    a) No se realizan copias de seguridad

    (b) Se realizan copias de seguridad de software y datos

13.Sobre la gestión de medios extraíbles (Cintas, CDs, DVDs, memorias flash, discos duros portátiles, etc.) y copias impresas

a) Existe un procedimiento documentado que incluye instrucciones de almacenamiento, transporte y destrucción de los medios extraíbles utilizados

b) Se almacenan en lugar seguro y protegido del fuego e inundaciones fuera del centro de proceso de datos

c) Se lleva un inventario completo

d) Se destruyen físicamente cuando llega el fin de su vida útil

e) Ninguna de las anteriores

14.¿Existe una política de protección de la información cuando se produce un intercambio electrónico de la misma?

a) No

b) Sí

c) Si, y tiene en cuenta la protección frente a accesos no autorizados, modificaciones, disponibilidad del servicio y aspectos legales.

15.¿Existe una política de control de acceso a los sistemas de información tanto lógicos como físicos que está alineada con los requisitos de seguridad de la Institución así como con los requisitos legales?

a) No hay ninguna política de control

b) Sí, para los accesos lógicos

c) Sí, para los accesos físicos

d) Sí, y además está documentada

e) Sí, y además de lo anterior se revisa y se hace un seguimiento de cumplimiento

16. ¿Existen procedimientos para gestionar los privilegios de acceso del usuario autorizado a los sistemas de información durante todo su ciclo de vida, es decir, desde el alta de usuario, su evolución dentro del área de Recaudos así como la revocación de todos los privilegios tras su baja?

(a) No hay procedimientos formales

b) Sí, normalmente en el de alta, se le da acceso a los sistemas pero ni se le da por escrito sus derechos, ni sus obligaciones de acceso como la confidencialidad de las contraseñas, etc.

c) Sí, hay un registro formal de todo el proceso de alta, modificaciones y bajas pero ni se le da por escrito sus derechos, ni sus obligaciones de acceso, ni tampoco hay una revisión de los derechos una vez establecidos

d) Sí, además de lo anterior, se le da por escrito sus derechos y sus obligaciones de acceso, y periódicamente hay una revisión de los derechos una vez establecidos

17. ¿Existen procedimientos y medios para restringir adecuadamente el acceso a las aplicaciones y a la información contenida en su PC?

a) No

b) Sólo medidas de autenticación, pero no se aplican perfiles de acceso

(c) Sí, tengo restricciones según el perfil de acceso

d) Sí, tengo restricciones, alineadas con la política de control de acceso. Además se controla que la información confidencial sólo puede ser enviada a terminales autorizados

e) Sí, y además de lo anterior, se aíslan tanto lógica como físicamente los sistemas que manejan información confidencial, quedando documentada explícitamente la sensibilidad de dicha información y aplicación

18.¿Qué controles de seguridad incluyen las aplicaciones?

a) No se incluyen controles de forma sistemática

(b) Se incluyen controles de validación de los datos de entrada (rango, longitud, integridad, etc.)

c) Además de lo anterior, se incluyen validaciones en el proceso (orden de ejecución, consistencia de los datos, recuperación de fallos, etc.)

d) Además de lo anterior, se incluyen validaciones de los datos de salida (exactitud de los datos, integridad, seguridad, etc.)

19. Tiene su contraseña escrita en:

a) Agenda

b) Celular

(c) Ninguno

d) Otro

¿Cual?_____

20. ¿Ha permitido que otra persona ingrese con su Usuario?

(a) Si

b) No

Si su respuesta es afirmativa ¿Quién?

Personal autorizado

21.¿Su contraseña de acceso al sistema es conocida por personas diferentes a Usted?

a) Si

(b) No

Si su respuesta es afirmativa ¿Quién?

_____

22.¿Cambia su contraseña periódicamente?

a) Si

(b) No

Si su respuesta es afirmativa ¿cada cuánto?

_____

23.Cuando se levanta de su sitio de trabajo porque necesita ausentarse, usted:

a) Cierra sesión

(b) Activa el protector de Pantalla

c) Suspende el PC

d) Apaga el PC

e) Otra

¿Cual?_____

24.¿En su sitio de trabajo se dispone de un lugar seguro donde se guarden los documentos impresos?

a) Si

(b) No

25.¿Usted deja algunos documentos sobre el escritorio?

(a) Si

b) No

26.¿Existe gestión de vulnerabilidades del software?

a) SI

(b) No

27.¿Puede usted cambiar/eliminar información del sistema SQUIT?

(a) SI

b) No

28.¿Tiene alguien más acceso al sistema SQUIT?

(a) SI

b) No

Si su respuesta es afirmativa ¿Quién?

_____

29.¿Dado que se ausente por unos días de su trabajo, alguien más puede sustituir temporalmente sus funciones?

a) SI

(b) No

Si su respuesta es afirmativa ¿Quién?

_____

30.¿Se aplican medidas para asegurar el cumplimiento de los requisitos legales ya sean estatutarias, reguladoras o contractuales?

a) No

b) Sí, es una responsabilidad delegada a los usuarios

c) Sí, hay políticas definidas que regulan el uso legal del software y otros productos protegidos por leyes de propiedad intelectual

d) Sí, además de lo anterior se implementan controles para asegurar que se cumplen dichas políticas

e) Sí, además de lo anterior se realizan auditorías internas que velan por el cumplimiento de las mismas

* Universidad se rige por: Acuerdos, resoluciones, actos administrativos.

Observaciones:

Elizabeth Astaiza P.
POP - 13 - abril - 2016
Elizabeth Astaiza Perafan
Técnico Administrativo

Encuesta (Ingeniero Servidores)

ENCUESTA DIVISION DE LAS TIC DE LA UNIVERSIDAD DEL CAUCA

Conscientes de la importancia de la seguridad en el ámbito de las tecnologías de la información y la comunicación de nuestras organizaciones, esta encuesta pretende dar una visión general sobre el actual conocimiento de la División de Gestión financiera de la universidad del cauca, esta encueta está hecha para recolectar información para el trabajo de grado titulado **"Gestión de Riesgo de Seguridad Informática con base en la norma ISO/IEC 27005 de 2011 adaptando la metodología COBIT 5 Al caso de estudio: Procedimiento Recaudos de la División Financiera de la Universidad del Cauca."** A cargo de los estudiantes: Milena Natalia Cruces Cerón y Juan Pablo Mora Palacios, con dirección del ingeniero Siler Amador Donado.

Lea atentamente las instrucciones:

1. Las preguntas tienen como propósito realizar un análisis sobre fin de conocer el tratamiento, hábitos de uso y medidas de seguridad empleadas en la información que se utiliza.
2. Para contestar marque con una X la opción.
3. Toda información proporcionada será utilizada será utilizada solo con fines académicos bajo un acuerdo de Confidencialidad.

1. **¿La División de las TIC tiene definido un plan estratégico de TI?**

   X SI

   b) Parcialmente

   c) N

2. **¿La división de las TIC tiene implantado políticas de TI?**

   X SI

   b) Parcialmente

   c) No

3. **¿Están identificados las amenazas y vulnerabilidades que afectan al normal desempeño de la División de las TIC?**

   X SI

   b) Parcialmente

   c) No

   3.1 **SI su respuesta es SI, ¿Cuáles son las amenazas y vulnerabilidades que causan mayor impacto en las operaciones de TI? Cite las más representativas**

   Modulo de Riesgos Publicos Lumen.

4. **¿Está usted preparado para los riesgos que se presenten en la División de las TIC?**

   a) SI

   b) Parcialmente

   c) No

5. **¿Se establecen acuerdos de confidencialidad y no divulgación sobre el acceso e intercambio de información en la División de las TIC?**

   a) SI

   b) No

6. **¿La División de las TIC gestiona los activos (hardware, software, documentación, etc...)??**

   a) No

   b) La Institución dispone de un inventario parcial de activos

   c) La Institución dispone de un inventario completo y actualizado de los activos.

7. **¿Los activos de la División están convenientemente clasificados (según su grado de sensibilidad y criticidad)?**

   a) Si

   b) Sí, pero de forma parcial

   c) Sí, los activos están clasificados

   d) No

8. **¿Las infraestructuras TIC críticas o con información sensible están ubicadas en entornos protegidos y con controles de acceso?**

a) Sí, se encuentran en locales aislados

b) Sí, los locales están especialmente preparados contra daños externos (electricidad, fuego, agua, sabotajes, etc...)

c) Sí, existe control de acceso para el personal autorizado

d) Sí, existen directrices claras para visitar y/o trabajar en dichos entornos

e) Ninguna de las anteriores

9. ¿Cuántas evaluaciones de seguridad realiza a sus sistemas al año?

a) Una

b) Más de tres

c) Ninguna

10. ¿Ha tenido incidentes de seguridad de la información en estos 3 últimos años?

a) Una

b) Más de tres

11. ¿Existe un procedimiento para la aceptación de los nuevos sistemas, actualizaciones de aplicaciones, nuevas versiones de sistema operativo, cambio de hardware, etc...?

a) Si, existe un procedimiento

b) No, simplemente se realizan algunas pruebas

12. ¿Se toman medidas contra el código malicioso?

a) Tenemos antivirus y antimalware en todos los equipos de los usuarios

b) Tenemos implantada una gestión centralizada de los equipos de la Institución para actualizaciones del sistema operativo y antivirus

c) No.

13.Respecto a las copias de seguridad

a) No se realizan copias de seguridad

b) Se realizan copias de seguridad de software y datos

14.¿Sobre la gestión de medios extraíbles (Cintas, CDs, DVDs, memorias flash, discos duros portátiles, etc.) y copias impresas?

a) Existe un procedimiento documentado que incluye instrucciones de almacenamiento, transporte y destrucción de los medios extraíbles utilizados

b) Se almacenan en lugar seguro y protegido del fuego e inundaciones fuera del centro de proceso de datos

c) Se lleva un inventario completo

d) Se destruyen físicamente cuando llega el fin de su vida útil

e) Ninguna de las anteriores

15.¿Existe una política de protección de la información cuando se produce un intercambio electrónico de la misma?

a) No

b) Sí

c) Si, y tiene en cuenta la protección frente a accesos no autorizados, modificaciones, disponibilidad del servicio y aspectos legales.

16.¿Existe una política de control de acceso a los sistemas de información tanto lógicos como físicos que está alineada con los requisitos de seguridad de la Institución así como con los requisitos legales?

a) No hay ninguna política de control

b) Sí, para los accesos lógicos

c) Sí, para los accesos físicos

d) Sí, y además está documentada

e) Sí, y además de lo anterior se revisa y se hace un seguimiento de cumplimiento

17. ¿Existen procedimientos para gestionar los privilegios de acceso del usuario autorizado a los sistemas de información durante todo su ciclo de vida, es decir, desde el alta de usuario, su evolución dentro de la Dlision así como la revocación de todos los privilegios tras su baja?

a) No hay procedimientos formales

b) Sí, normalmente en el de alta, se le da acceso a los sistemas pero ni se le da por escrito sus derechos, ni sus obligaciones de acceso como la confidencialidad de las contraseñas, etc.

c) Sí, hay un registro formal de todo el proceso de alta, modificaciones y bajas pero ni se le da por escrito sus derechos, ni sus obligaciones de acceso, ni tampoco hay una revisión de los derechos una vez establecidos

d) Sí, además de lo anterior, se le da por escrito sus derechos y sus obligaciones de acceso, y periódicamente hay una revisión de los derechos una vez establecidos

18. ¿Qué procedimientos y medios para restringir el acceso al sistema operativo de los usuarios se utilizan en la División?

a) Los usuarios tiene un identificador único

b) Se controla que no haya más de un número de intentos de acceso fallidos, tras el cual se producen eventos como registro, incrementos de los tiempos de respuesta, etc.

c) Se establecen tiempos de cierre por inactividad, así como tiempos máximos de conexión

d) Se limita el acceso a las funcionalidades del sistema a lo estrictamente necesario para el trabajo del usuario

e) Ninguna de las anteriores

19.¿Existen procedimientos y medios para restringir adecuadamente el acceso a las aplicaciones y a la información contenida en ellas?

a) No

b) Sólo medidas de autenticación, pero no se aplican perfiles de acceso.

c) Sí, los usuarios tienen restricciones según su perfil de acceso

d) Sí, los usuarios tienen restricciones, alineadas con la política de control de acceso. Además se controla que la información confidencial sólo puede ser enviada a terminales autorizados.

e) Sí, y además de lo anterior, se aíslan tanto lógica como físicamente los sistemas que manejan información confidencial, quedando documentada explícitamente la sensibilidad de dicha información y aplicación

20.¿Qué controles de seguridad incluyen las aplicaciones?

a) No se incluyen controles de forma sistemática

b) Se incluyen controles de validación de los datos de entrada (rango, longitud, integridad, etc.)

c) Además de lo anterior, se incluyen validaciones en el proceso (orden de ejecución, consistencia de los datos, recuperación de fallos, etc.)

d) Además de lo anterior, se incluyen validaciones de los datos de salida (exactitud de los datos, integridad, seguridad, etc.)

21.¿Existe gestión de vulnerabilidades del software?

a) SI

b) No

22.¿Existe un servidor exclusivo para el manejo de la División Financiera (SQUIT, Finanzas Plus)?

~~c)~~ SI

d) No

e)

23.¿la Información de las División Financiera (SQUIT, Finanzas Plus) está debidamente protegida?

~~f)~~ SI

g) No

Si su repuesta es Si ¿Cómo?

-Usuario, Perfiles

-Autenticación.

-Dispositivos seguridad FW,

-Segregación lógica y física

24.¿Puede usted cambiar/eliminar información del servidor de la división financiera?

h) SI

i) No

25.¿Se aplican medidas para asegurar el cumplimiento de los requisitos legales ya sean estatutarias, reguladoras o contractuales?

a) No

b) Sí, es una responsabilidad delegada a los usuarios

c) Sí, hay políticas definidas que regulan el uso legal del software y otros productos protegidos por leyes de propiedad intelectual

d) Sí, además de lo anterior se implementan controles para asegurar que se cumplen dichas políticas

e) Sí, además de lo anterior se realizan auditorías internas que velan por el cumplimiento de las mismas

Observaciones:

ANEXO K - Mapeo de metas corporativas y metas TI

			Metas Corporativas																	
			01. Valor para las partes interesadas de las Inversiones de Negocio	02. Cartera de productos y servicios competitivos	03. Riesgos de negocio gestionados (salvaguarda de activo)	04. Cumplimiento de leyes y regulaciones externas	05. Transparencia financiera	06. Cultura de servicio orientada al cliente	07. Continuidad y disponibilidad del servicio de negocio	08. Respuestas ágiles a un entorno de negocio cambiante	09. Toma estratégica de Decisiones basadas en información	10. Optimización de costes de entrega del servicio	11. Optimización de la funcionalidad de los procesos de negocio	12. Optimización de los costes de los procesos de negocio	13. Programas gestionados de cambio en el negocio	14. Productividad operacional y de los empleados	15. Cumplimiento con las políticas internas	16. Personas preparadas y motivadas	17. Cultura de innovación del producto y del negocio
Metas Relacionas con las TI			**Financiera**					**Cliente**					**Interna**					**Aprendizaje y Crecimiento**	
Financiera	1	Alineamiento de TI y estrategia de negocio	P	P	S			P	S	P	P	S	P		P			S	S
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas			S	P											P		
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S					S	S		S		P			S	S
	4	Riesgos de negocio relacionados con las TI gestionados			P	S			P	S		P			S		S	S	
	5	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	P	P				S		S		S	S	P		S			S
	6	Transparencia de los costes, beneficios y riesgos de las TI	S		S		P				S	P		P					
Cliente	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
Interna	9	Agilidad de las TI	S	P	S			S		P			P		S	S		S	P
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones			P	P			P								P		
	11	Optimización de activos, recursos y capacidades de las TI	P	S						S		P	S	P	S	S			S
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	S	P	S			S		S		S	P	S	S	S			S
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	P	S	S			S				S		S	P				
	14	Disponibilidad de información útil y fiable para la toma de decisiones	S	S	S	S			P		P		S						
	15	Cumplimiento de las políticas internas por parte de las TI			S	S											P		
Aprendizaje	16	Personal del negocio y de las TI competente y motivado	S	S	P			S		S						P		P	S
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio	S	P				S		P	S		S		S			S	P

ANEXO L - Mapeo de metas TI y los Procesos

			Metas Relacionadas con las TI																
			1 Alineamiento de TI y estrategia de negocio	2 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	3 Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	4 Riesgos de negocio relacionados con las TI gestionados	5 Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	6 Transparencia de los costes, beneficios y riesgos de las TI	7 Entrega de servicios de TI de acuerdo a los requisitos del negocio	8 Uso adecuado de aplicaciones, información y soluciones tecnológicas	9 Agilidad de las TI	10 Seguridad de la información, infraestructura de procesamiento y aplicaciones.	11 Optimización de activos, recursos y capacidades de las TI	12 Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	13 Entrega de Programas que proporcionen beneficios a tiempo, dentro presupuesto y satisfaciendo los requisitos y normas de calidad.	14 Disponibilidad de información útil y fiable para la toma de decisiones	15 Cumplimiento de las políticas internas por parte de las TI	16 Personal del negocio y de las TI competente y motivado	17 Conocimiento, experiencia e iniciativas para la innovación de negocio
Procesos de Cobit 5			**Financiera**						**Cliente**		**Interna**							**Aprendizaje y Crecimiento**	
Evaluar, Orientar y Supervisar	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	Asegurar la Entrega de Beneficios	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	Asegurar la Optimización del Riesgo	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	Asegurar la Optimización de los Recursos	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	Asegurar la Transparencia hacia las partes interesadas	S	S	P			P	P						S	S	S		S
Alinear, Planificar y Organizar	APO01	Gestionar el Marco de Gestión de TI	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	APO02	Gestionar la Estrategia	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	Gestionar la Arquitectura Empresarial	P		S	S	S	S	S	S	P	S	P	S		S			S
	APO04	Gestionar la Innovación	S			S	P			P	P		P	S					P
	APO05	Gestionar el portafolio	P		S	S	P	S	S	S	S		S		P				S
	APO06	Gestionar el Presupuesto y los Costes	S		S	S	P	P	S	S			S		S				
	APO07	Gestionar los Recursos Humanos	P	S	S	S			S		S	S	P		P		S	P	P
	APO08	Gestionar las Relaciones	P		S	S	S	S	P	S			S	P	S		S	S	P
	APO09	Gestionar los Acuerdos de Servicio	S			S	S	S	P	S	S	S	S		S	P	S		
	APO10	Gestionar los Proveedores		S		P	S	S	P	S	P	S	S		S	S	S		S
	APO11	Gestionar la Calidad	S	S		S	P		P	S	S		S		P	S	S	S	S
	APO12	Gestionar el Riesgo		P		P		P	S	S	S	P			P	S	S	S	S
	APO13	Gestionar la Seguridad		P		P		P	S	S		P				P			
Construcción, Adquisición e Implementación	BAI01	Gestionar los Programas y Proyectos	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Gestionar la Definición de Requisitos	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Gestionar la Identificación y la Construcción de Soluciones	S			S	S		P	S			S	S	S	S			S
	BAI04	Gestionar la Disponibilidad y la Capacidad				S	S		P	S	S		P		S	P			S
	BAI05	Gestionar la introducción de Cambios Organizativos	S		S		S		S	P	S		S	S	P				P
	BAI06	Gestionar los Cambios			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Gestionar la Aceptación del Cambio y de la Transición				S	S		S	P	S	S	S	P	S	S	S		S
	BAI08	Gestionar el Conocimiento	S				S		S	S	P	S	S			S		S	P
	BAI09	Gestionar los Activos		S		S		P	S		S	S	P			S	S		
	BAI10	Gestionar la Configuración		P		S		S		S	S	S	P			P	S		
Entregar, dar Servicio y Soporte	DSS01	Gestionar las Operaciones		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Gestionar las Peticiones y los Incidentes del Servicio				P			P	S		S				S	S		S
	DSS03	Gestionar los Problemas		S		P	S		P	S	S		P	S		P	S		S
	DSS04	Gestionar la Continuidad	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	Gestionar los Servicios de Seguridad	S	P		P			S	S		P	S	S		S	S		
	DSS06	Gestionar los Controles de los Procesos del Negocio		S		P			P	S		S	S	S		S	S	S	S
Supervisión, Evaluación y Verificación	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno		P		P		S	S	S		S				S	P		S
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos		P		P	S		S			S					S		S

ANEXO M - listado total de los escenarios de riesgo de Cobit 5

Nuevos Escenarios Creados	
Escogido por inforamcion Obtenida	
Escogido por Actividades	

			Tipo de Riesgo					
No	**Ref de COBIT 5**	**Categoría de escenario de Riesgo**	**Habilitación de beneficio/ valor para TI**	**Entrega de programas y proyectos de TI**	**Entrega de operaciones y servicios de TI**	**Escenarios Negativos**	Procesos	Información
1	0101	**Establecimiento y mantenimiento del portafolio**	P	P	S	Se seleccionan programas erróneos para implementar que no se alinean con la estrategia y las prioridades corporativas.		
2	0102		P	P	S	Existen iniciativas duplicadas.		
3	0103		P	P	S	Un programa nuevo e importante genera incompatibilidad a largo plazo con la arquitectura empresarial.		
4	0104		P	P	S	Los recursos en competencia se asignan y gestionan en forma ineficiente y no se alinean con las prioridades del negocio.		
5	0105		P	S	S	Desconocimiento de las Políticas de TI		
6	0201	**Gestión del ciclo de vida de los programas/proyectos (inicio, aspectos económicos, entrega, calidad y finalización de los programas/ proyectos)**	P	P	S	No se completan los proyectos con fallas (debido a costos, demoras, arrastres en el alcance, prioridades cambiantes de negocios).		
7	0202		S	P	S	El presupuesto para proyectos de TI se encuentra excedido.		
8	0203		S	P		Ocasionalmente, se tienen entregas tardías de los proyectos de TI por un departamento interno de desarrollo.		
9	0204		P	P	S	Rutinariamente, existen importantes retrasos en la entrega de proyectos de TI.		

10	0205		P	P	S	Existen demoras excesivas en proyectos de desarrollo externalizado de TI.		
11	0206		P	P		Los programas/proyectos fallan debido a la falta de involucramiento activo de las partes interesadas (incluyendo al patrocinador) durante su ciclo de vida.		
12	0207		P	S	S	Degradación de la imagen de la entidad por su incapacidad para responder oportuna y asertivamente contra incidentes que afectan a los servicios entregados por proyectos ineficientes.		
13	0301	**Toma de decisiones sobre inversiones en TI**	P		S	Los gerentes de negocios o sus representantes no se involucran en las decisiones importantes sobre inversiones de TI (p.ej. nuevas aplicaciones u oportunidades tecnológicas, riorizaciones).		
14	0302		P		S	Se selecciona el software equivocado para implementar en términos de costos, desempeño, características, impatibilidad, etc.		
15	0303		P		P	Se selecciona la infraestructura equivocada para implementar, en términos de costos, desempeño, características, compatibilidad, etc.		
16	0304		P	P		Se adquiere software redundante.		
17	0401	Pericia y Habilidades TI	P	P	P	Faltan habilidades de TI o son incompatibles, p.ej., debido a nuevas tecnologías.		
18	0402		P	P	P	El personal de TI no comprende el negocio, lo que afecta la entrega de servicio/calidad de proyectos.		
19	0403		P	P	P	No existen suficientes habilidades para cubrir los requerimientos del negocio.		
20	0404		S	P	P	No existen habilidades para contratar personal de TI		
21	0405		S	P	P	No existe diligencia debida en el proceso de contratación del personal.		
22	0406		S	P	P	No existe un entrenamiento adecuado, lo que lleva a que el personal de TI abandone la empresa.		

23	0407		S	P	P	Existe un retorno insuficiente de la inversión en el entrenamiento debido a la desvinculación temprana del parte del personal capacitado de TI (p.ej., MBA).		
24	0408		S	P	P	Existe una dependencia excesiva del personal calve del TI		
25	0409		S	P	P	Existe una incapacidad para actualizar las habilidades de TI a un nivel apropiado a través del entrenamiento.		
26	0410		P		P	Falta de inversión en profesionales para el área debido al exceso desconfianza en el personal de TI.		
27	0411		P	S	S	Falta de concientización y participación del personal en acciones preventivas que se direccionen a evitar los riesgos de salud y seguridad en el trabajo.		
28	0501	Operaciones del personal (error humano e interno malicioso)	S	S	P	Se abusa de los derechos de acceso de roles anteriores		
29	0502		S		P	El equipo, es dañado por el personal accidentalmente.		
30	0503		S		P	Existen errores cometidos por el personal (durante las actualizaciones del sistema, copias de respaldo, mantenimiento)		
31	0504		S		P	La información es ingresada incorrectamente por el personal.		
32	0505		S		P	El centro de datos es destruido (por sabotaje, etc.) por el personal.		
33	0506		S		P	Un dispositivo con datos sensibles es robado por un miembro del personal.		
34	0507		S		P	Un componente clave de la infraestructura es robado por un miembro del personal.		
35	0508		P	S	P	Se configuran erróneamente los componentes de hardware.		
36	0509		S		P	Se configuran erróneamente los componentes de hardware.		
37	0510		S		P	El hardware fue dañado ntencionadamente (dispositivos de seguridad, etc.)		

38	0601	Información (brecha de datos: daño, fuga y acceso)	S		P	El personal interno ha dañado componentes de hardware, lo que conlleva la destrucción (parcial) de los datos informáticos.		
39	0602		S	S	P	La base de datos está corrupta, lo cual hace inaccesible a los datos.		
40	0603		S	S	P	Perdida y Revelación de medios portátiles que contiene datos sensibles de información (CD, USB, discos portátiles, etc.)		
41	0604		S	S	P	Se pierden y se revelan datos sensibles mediante ataques lógicos.		
42	0605		S	S	P	Se pierden o no se verifica la efectividad de los medios que contienen las copias de respaldo.		
43	0606		P	S	P	Se revela información sensible en forma accidental debido a fallas en el seguimiento de las guías de manejo de información.		
44	0607		P	S	P	Se modifican intencionadamente los datos (contables, vinculados a la seguridad, información, etc.)		
45	0608		P	S	P	Se revela información sensible a través del correo electrónico.		
46	0609		P	S	P	Se revela información sensible debido a ineficientes procedimiento de retención/archivo y eliminación.		
47	00610		P	S	P	Existen fugas de la propiedad intelectual (PI) y/o la información competitiva, debido a la desvinculación de miembros clave de la empresa.		
48	0611		P	S	P	La empresa tiene un flujo excesivo de datos y no puede extraer o deducir la información relevante para el negocio (p.ej., el problema del “big data”).		
49	0612	Información (Brecha de datos: daños fugas y accesos)			P	Filtración de la información debido al abandono del equipo de la institución.		
50	0613		S	S	P	Falta de un plan de continuidad que imposibilita responder a incidentes e interrupciones de servicios.		
51	0701	Arquitectura (visión y diseño)	P	P	P	La arquitectura empresarial es compleja e inflexible, bloqueando una mayor evolución y expansión, lo que lleva a la pérdida de oportunidades de negocio.		

52	0702		P	S	P	La arquitectura empresarial no se ajusta a su propósito y no respalda las prioridades del negocio		
53	0703		P	S	S	Existe una falla en la adopción y explotación oportuna de la nueva infraestructura.		
54	0704		P	S	S	Existe una falla en la adopción y explotación oportuna de un nuevo software (funcionalidad, optimización, etc.)		
55	0801	Infraestructura (hardware, sistemas operativos y tecnologías de control)	P	S	P	Se instala infraestructura nueva (innovadora) y como resultado los sistemas se tornan inestables, lo que lleva a incidentes operativos.		
56	0802		P	S	P	Los sistemas no pueden manejar los volúmenes de transacciones cuando estos se incrementan.		
57	0803		P	S	P	Los sistemas no pueden manejar la carga que se genera cuando se despliegan nuevas aplicaciones o iniciativas.		
58	0804		P	S	P	Existen fallas intermitentes en los servicios (telecomunicaciones, electricidad).		
59	0805		P	S	P	TI es obsoleta y no satisface los nuevos requerimientos del negocio (redes, seguridad, base de datos, almacenamiento, etc.).		
60	0806				P	Fallas en el hardware por exceso de calor.		
61	0807		S	S	P	Fallas en los registros y definición de acceso a los activos físicos de TI o el uso de dispositivos por parte del usuario para tratamiento de la información.		
62	0901	Software	P		S	No existen habilidades en el uso del software para materializar los resultados deseados (por ejemplo: fallas al implementar los modelos de negocio o los cambios requeridos).		
63	0902		P		S	Se implementa software inmaduro (adopción temprana, fallos, etc.)		
64	0903		P		S	Se selecciona e implementa software equivocado según costos, desempeño, características, compatibilidad, etc.		
65	0904		P		S	Existen dificultades operativas cuando se pone un nuevo software en producción.		
66	0905		P		S	Los usuarios no pueden utilizar ni explotar nuevo software aplicativo.		

67	0906		P		S	Modificación intencional del software conduce a datos erróneos o acciones fraudulentas.		
68	0907		P		S	Modificación no intencional del software conduce a resultados inesperados.		
69	0908		P		S	Ocurren errores no intencionales en la gestión de configuraciones y de cambios.		
70	0909		P		S	Regularmente, ocurren fallas en el funcionamiento del software o de las aplicaciones críticas.		
71	0910		P		S	Intermitentemente, ocurren problemas con el software de sistemas importantes		
72	0911		P		S	El software aplicativo es obsoleto (p.ej., tecno-logías anticuadas, pobremente documentadas, costosas de mantener, difíciles de extender, no integradas en la arquitectura vigente).		
73	0912		P		S	No existen habilidades para retornar a versiones anteriores en caso de problemas operativos con nuevas versiones.		
74	1001	Propiedad del negocio sobre la TI	P	P	S	El negocio no asume la responsabilidad que debería sobre las áreas de TI, p.ej., los requerimientos funcionales, las rioridades en el desarrollo, la evaluación de oportunidades a través de nuevas tecnologías		
75	1002		P	S	S	Existe una dependencia y uso excesivos de aplicaciones de usuario final y de soluciones ad-hoc para necesidades importantes de la información, lo que lleva a deficiencias en la seguridad, datos imprecisos o incrementos en los costos y el uso ineficiente de recursos.		
76	1003		P	S	S	Se generan costos o poca efectividad en las compras de TI que se concretan fuera de los procesos de adquisición.		
77	1004				P	Requerimientos inadecuados llevan a acuerdos de nivel de servicios (SLAs) poco efectivos.		
78	1101	Selección / desempeñodel proveedor, cumplimientocontractual,discontinuidad del servicio y trasferencia.		S	P	Falta de debida diligencia respecto a la viabilidad financiera, capacidad de entrega y sustentabilidad de los servicios del proveedor.		

79	1102			S	P	Se aceptan términos de los proveedores de TI que no razonables para el negocio.		
80	1103			S	P	El soporte y la entrega de servicios por los proveedores son inadecuados y no alineados con los acuerdos de niveles de servicio (SLA).		
81	1104			S	P	El desempeño de los servicios externalizados es inadecuado en los acuerdos de gran escala y largo alcance.		
82	1105			S	P	Pueden existir incumplimientos de las licencias de software (uso y/o distribución de software sin las correspondientes licencias, etc.)		
83	1106			S	P	Incapacidad para transferir a provisores alternativos debido a una confianza excesiva en el provisor actual.		
84	1107			S	P	Los servicios en la nube son adquiridos por el negocio sin consultar/involucrar a TI, lo que resulta en la incapacidad de integrar el servicio con los prestados en forma interna.		
85	1201	Cumplimiento regulatorio	P	S	S	No se cumple con regulaciones, que tienen que ver con la privacidad, contabilidad, manufactura, etc.		
86	1202		P	S	S	El desconocimiento de cambios potenciales en la regulación tiene un impacto en el ambiente operativo		
87	1203		P	S	S	El regulador impide el flujo de datos a través de las fronteras debido a controles insuficientes.		
88	1301	Geopolitico			P	No se tiene acceso debido a incidentes disruptivos en otros ambientes de la empresa.		
89	1302				P	La interferencia del Estado y las políticas nacionales limitan las capacidades de los servicios		
90	1303				P	Las acciones dirigidas contra la empresa resultan en la destrucción de la infraestructura		
91	1401	Robo o destrucción de la infraestructura	S	S	P	Se ha producido el robo de un dispositivo con datos sensibles.		
92	1402		S	S	P	Se ha producido el robo de una importante cantidad de servidores de desarrollo.		
93	1403		S	S	P	Se destruye el centro de datos (sabotaje, etc.).		

94	1404		S	S	P	Dispositivos individuales se destruyen accidentalmente.		
95	1405		P	S	P	Ineficiencia o ausencia de dispositivos que detectan las amenazas del entorno, debido a la falta de supervisión, mantenimiento y actualización de los mismos.		
96	1406				P	Libre acceso a las instalaciones de procesamiento sin peticiones formales.		
97	1501	Código Maliciosos	S		P	Se ha producido una intrusión de código malicioso en los servidores operativos.		
98	1502		S		P	Los computadores portátiles se infectan frecuentemente con código malicioso.		
99	1503		S		P	Un empleado insatisfecho implementa una bomba lógica que produce la pérdida de datos importantes.		
100	1504		S		P	Roban los datos de la compañía a través de accesos no autorizados obtenidos mediante ataques.		
101	1505	Códigos maliciosos	P	S	P	Desactualización de los usuarios respecto a configuraciones de tráfico entrante, uso de correos electrónicos, contraseñas y descargas lo cual facilita el acceso de software.		
102	1601	Ataques lógicos	S		P	Usuarios no autorizados tratan de forzar el ingreso a los sistemas.		
103	1602		S		P	Existen interrupciones en los servicios debido a ataques de denegación de servicios.		
104	1603		S		P	El sitio web sufre un ataque que modifica su apariencia (“defacement”).		
105	1604		S		P	Se registran casos de espionaje industrial.		
106	1605		S		P	Existen ataques de virus.		
107	1606		S		P	Se registran casos de hacktivismo (“hacktivism”).		
108	1701	Acción industrial	S	S	P	No es posible acceder a las instalaciones y edificios debido a una huelga gremial.		
109	1702		S	S	P	El personal clave no se encuentra disponible debido a impedimentos de la industria (por ejemplo, huelga en el transporte).		
110	1703		S	S	P	Un tercero no puede proveer servicios por una huelga.		

111	1704		S	S	P	No hay acceso al capital debido a una huelga del sector bancario.		
112	1801	Ambiental	S	S	P	El equipamiento utilizado no es amigable en cuanto al medio ambiente (por ejemplo, en el consumo de energía, embalajes, etc.)		
113	1901	Actos de la Naturaleza	S	S	P	Hay un terremoto.		
114	1902		S	S	P	Hay un tsunami.		
115	1903		S	S	P	Hay fuertes tormentas y ciclones tropicales.		
116	1904		S	S	P	Hay un gran incendio fuera de control.		
117	1905		S	S	P	Hay una inundación.		
118	1906		S	S	P	Hay una crecida en el nivel del agua.		
119	2001	Innovación	P	S	S	No se identifican tendencias nuevas e importantes de TI.		
120	2002		P		S	Hay una falla en la adopción y en el aprovechamiento oportuno de un nuevo software (funcionalidad, optimización, etc.).		
121	2003		P		S	No se identifican tendencias nuevas e importantes de software (consumismo en TI).		

ANEXO N - Evaluación de escenarios de riesgos

No	Ref de COBIT 5	Categoría de escenario de Riesgo	Escenarios Negativos	Impacto	Frecuencia	Riesgo
1	105	Establecimiento y mantenimiento del portafolio.	Desconocimiento de las Políticas de TI.	8	5	40
2	207	Gestión del ciclo de vida del programa o proyecto	Degradación de la imagen de la entidad por su incapacidad para responder oportuna y asertivamente contra incidentes que afectan a los servicios entregados por proyectos ineficientes.	5	2	10
3	301	Toma de decisiones sobre inversiones en TI	Los gerentes de negocios o sus representantes no se involucran en las decisiones importantes sobre inversiones de TI (por ejemplo: nuevas aplicaciones u oportunidades tecnológicas, priorizaciones).	5	4	20
4	401	Pericia y Habilidades TI	Faltan habilidades de TI o son incompatibles, por ejemplo: debido a nuevas tecnologías.	5	3	15
5	408		Existe una dependencia excesiva del personal clave de TI.	8	5	40
6	409		Existe una incapacidad para actualizar las habilidades de TI a un nivel apropiado a través del entrenamiento.	8	3	24
7	411		Falta de inversión en profesionales para el área debido al exceso desconfianza en el personal de TI	5	1	5
8	412		Falta de concientización y participación del personal en acciones preventivas que se direccionen a evitar los riesgos de salud y seguridad en el trabajo.	5	1	5
9	502	Operaciones del personal (error humano e interno malicioso)	El equipo de TI es dañado accidentalmente por el personal.	8	2	16
10	503		Existen errores cometidos por el personal (durante las actualizaciones del sistema, copias de respaldo, mantenimiento)	8	3	24
11	504		La información es ingresada incorrectamente por el personal.	8	4	32
12	505		El centro de datos es destruido (por sabotaje, etc.) por el personal.	8	2	16
13	506		Un dispositivo con datos sensibles es robado por un miembro del personal.	8	3	24
14	507		Un componente clave de la infraestructura es robado por un miembro del personal.	5	3	15
15	509		Se configuran erróneamente los componentes de hardware.	5	3	24
16	510		El hardware fue dañado intencionadamente (dispositivos de seguridad, etc.)	5	1	5
17	601	Información	El personal interno ha dañado componentes de hardware, lo que conlleva la destrucción (parcial) de los datos informáticos.	8	1	8
18	602		La base de datos está corrupta, lo cual hace inaccesible a los datos.	8	1	8
19	603		Perdida y Revelación de medios portátiles que contiene datos sensibles de información (CD, USB, discos portátiles, etc.)	8	3	24
20	604		Se pierden y se revelan datos sensibles mediante ataques lógicos.	8	3	24

21	605	(brecha de datos: daño, fuga y acceso)	Se pierden o no se verifica la efectividad de los medios que contienen las copias de respaldo.	5	4	20
22	606		Se revela información sensible en forma accidental debido a fallas en el seguimiento de las guías de manejo de información.	8	4	32
23	607		Se modifican intencionadamente los datos (contables, vinculados a la seguridad, información, etc.)	8	5	40
24	608		Se revela información sensible a través del correo electrónico.	5	2	10
25	609		Se revela información sensible debido a ineficientes procedimiento de retención/archivo y eliminación.	8	3	24
26	612		Filtración de la información debido al abandono del equipo de la institución.	8	5	40
27	613		Falta de un plan de continuidad que imposibilita responder a incidentes e interrupciones de servicios.	5	2	10
28	801	Infraestructura (hardware, sistemas operativos y tecnologías de control)	Se instala infraestructura nueva (innovadora) y como resultado los sistemas se tornan inestables, lo que lleva a incidentes operativos.	5	1	5
29	802		Los sistemas no pueden manejar los volúmenes de transacciones cuando estos se incrementan.	3	1	3
30	803		Los sistemas no pueden manejar la carga que se genera cuando se despliegan nuevas aplicaciones o iniciativas.	2	1	2
31	804		Existen fallas intermitentes en los servicios (telecomunicaciones, electricidad).	8	4	32
32	806		Fallas en el hardware por exceso de calor.	2	1	2
33	807		Fallas en los registros y definición de acceso a los activos físicos de TI o el uso de dispositivos por parte del usuario para tratamiento de la información.	5	4	20
34	901	Software	No existen habilidades en el uso del software para materializar los resultados deseados (por ejemplo: fallas al implementar los modelos de negocio o los cambios requeridos).	8	2	16
35	902		Se implementa software inmaduro (adopción temprana, fallos, etc.)	5	1	5
36	903		Se selecciona e implementa software equivocado según costos, desempeño, características, compatibilidad, etc.	5	2	10
37	904		Existen dificultades operativas cuando se pone un nuevo software en producción.	5	1	5
38	905		Los usuarios no pueden utilizar ni explotar nuevo software aplicativo.	2	1	2
39	906		Modificación intencional del software conduce a datos erróneos o acciones fraudulentas.	3	1	3
40	907		Modificación no intencional del software conduce a resultados inesperados.	5	3	15
41	908		Ocurren errores no intencionales en la gestión de configuraciones y de cambios.	8	4	32
42	909		Pude ocurrir fallas en el funcionamiento del software o de las aplicaciones críticas.	2	1	2
43	910		Ocurren problemas con el software de sistemas importantes.	2	1	2
44	1105	Selección/ desempeño del proveedor, cumplimiento contractual, discontinuidad del servicio y trasferencia.	Pueden existir incumplimientos de las licencias de software (uso y/o distribución de software sin las correspondientes licencias, etc.)	8	2	16
45	1106		Incapacidad para transferir a provisores alternativos debido a una confianza excesiva en el provisor actual.	3	2	6
46	1201	Cumplimiento regulatorio	No se cumple con regulaciones, que tienen que ver con la privacidad, contabilidad, manufactura, etc.	5	2	10
47	1202		El desconocimiento de cambios potenciales en la			

			regulación tiene un impacto en el ambiente operativo	8	3	24
48	1401	Robo o destrucción de la infraestructura	Se ha producido el robo de un dispositivo con datos sensibles.	8	5	40
49	1403		Se destruye el centro de datos (sabotaje, etc.).	8	5	40
50	1404		Dispositivos individuales se destruyen accidentalmente.	8	4	32
51	1405		Ineficiencia o ausencia de dispositivos que detectan las amenazas del entorno, debido a la falta de supervisión, mantenimiento y actualización de los mismos.	5	5	25
52	1406		Libre acceso a las instalaciones de procesamiento sin peticiones formales.	8	5	40
53	1501	Código Maliciosos	Se ha producido una intrusión de código malicioso en los servidores operativos.	8	1	8
54	1502		Los computadores portátiles se infectan frecuentemente con código malicioso.	8	2	16
55	1503		Un empleado insatisfecho implementa una bomba lógica que produce la pérdida de datos importantes.	8	5	40
56	1504		Roban los datos de la compañía a través de accesos no autorizados obtenidos mediante ataques.	8	5	40
57	1505		Desactualización de los usuarios respecto a configuraciones de tráfico entrante, uso de correos electrónicos, contraseñas y descargas lo cual facilita el acceso de software.	5	5	25
58	1601	Ataques lógicos	Usuarios no autorizados tratan de forzar el ingreso a los sistemas.	8	5	40
59	1605		Existen ataques de virus.	3	2	6
60	1701	Acción industrial	No es posible acceder a las instalaciones y edificios debido a una huelga gremial.	3	2	6
61	1702		El personal clave no se encuentra disponible debido a impedimentos de la industria (por ejemplo, huelga en el transporte).	5	2	10
62	1801	Ambiental	El equipamiento utilizado no es amigable en cuanto al medio ambiente (por ejemplo, en el consumo de energía, embalajes, etc.)	8	3	24
63	1901	Actos de la Naturaleza	Hay un terremoto.	8	5	40
64	1903		Hay fuertes tormentas y ciclones tropicales.	8	5	40
65	1904		Hay un gran incendio fuera de control.	8	5	40

Tabla #: Evaluación de Escenarios de Riesgos

ANEXO O - Matriz de riesgos

Riesgo= Frecuencia * Impacto							
Desastroso	**Impacto**	**8**	**8** 1501-601-602	**16** 502-505-901-1105-1502-	**24** 409-506-509-603-604-609-1202-1801-503-	**32** 504-606-804-908-1404-	**40** 408-607-1401-1403-1406-1503-1504-1601-105-612-1901-1903-1904
Mayor		**5**	**5** 510-801-902-904-410-411	**10** 608-903-1702-1201-207-613	**15** 507-907-401	**20** 605-807-301	**25** 1405-1505
Moderado		**3**	**3** 906-802	**6** 1106-1605-1701-	**9**	**12**	**15**
Menor		**2**	**2** 905-909-910-803-806	**4**	**6**	**8**	**10**
Insignificante		**1**	**1**	**2**	**3**	**4**	**5**
			1	**2**	**3**	**4**	**5**
		Frecuencia					
			Raro	**M. Bajo**	**Bajo**	**Medio**	**Alto**

ANEXO P - Tablas de referencias de Cobit 5

Ref de COBIT 5	Categoría de Escenario de Riesgo	Escenario de Riesgo	Actor		Tipo de Amenaza				Evento							Activo / Recurso				
			Interno	Externo	Maliciosa	Accidental	Error	Falla	Revelación	Interrupción	Modificación	Robo	Destrucción	Reglas y Regulaciones	Ejecución Inefectiva	Personas y habilidades	Estructuras Organizativas	Infraestructuras	Información	Aplicaciones
105	Establecimiento y mantenimiento del portafolio	Desconocimiento de las Políticas de TI.																		
301	Toma de decisiones sobre inversiones en TI	Los gerentes de negocios o sus representantes no se involucran en las decisiones importantes sobre inversiones de TI (por ejemplo: nuevas aplicaciones u oportunidades tecnológicas, priorizaciones).																		
408	Pericia y habilidades de TI	Existe una dependencia excesiva del personal clave de TI.																		
409		Existe una incapacidad para actualizar las habilidades de TI a un nivel apropiado a través del entrenamiento.																		
410		Inexistencia de métodos para evaluar el personal.																		
503	Operaciones del personal (error humano e intento malicioso)	Existen errores cometidos por el personal (durante las actualizaciones del sistema, copias de respaldo, mantenimiento)																		
504		La información es ingresada incorrectamente por el personal.																		
506		Un dispositivo con datos sensibles es																		

		robado por un miembro del personal.																			
509		Se configuran erróneamente los componentes de hardware.																			
603	Información (brecha de datos: daño, fuga y acceso)	Pérdida y Revelación de medios portátiles que contiene datos sensibles de información (CD, USB, discos portátiles, etc.)																			
604		Se pierden y se revelan datos sensibles mediante ataques lógicos.																			
605		Se pierden o no se verifica la efectividad de los medios que contienen las copias de respaldo.																			
606		Se revela información sensible en forma accidental debido a fallas en el seguimiento de las guías de manejo de información.																			
607		Se modifican intencionadamente los datos (contables, vinculados a la seguridad, información, etc.)																			
609		Se revela información sensible debido a ineficientes procedimiento de retención/archivo y eliminación.																			
612		Filtración de la información debido al abandono del equipo de la institución.																			
804	Infraestructura (hardware, sistemas operativos y tecnología de control) (selección/ implementación, operaciones y desmantelamiento)	Existen fallas intermitentes en los servicios (telecomunicaciones, electricidad).																			
807		Fallas en los registros y definición de acceso a los activos físicos de TI o el uso de dispositivos por parte del usuario para tratamiento de la información.																			
908	Software	Ocurren errores no intencionales en la gestión de configuraciones y de cambios.																			
1202	Cumplimiento Regulatorio	El desconocimiento de cambios potenciales en la regulación tiene un impacto en el ambiente operativo																			
1401		Se ha producido el robo de un dispositivo con datos sensibles.																			
1403		Se destruye el centro de datos (sabotaje, etc.).																			

1404	Robo o destrucción de la infraestructura	Dispositivos individuales se destruyen accidentalmente.																				
1405		Ineficiencia o ausencia de dispositivos que detectan las amenazas del entorno, debido a la falta de supervisión, mantenimiento y actualización de los mismos.																				
1406		Libre acceso a las instalaciones de procesamiento sin peticiones formales.																				
1503	Código malicioso	Un empleado insatisfecho implementa una bomba lógica que produce la pérdida de datos importantes.																				
1504		Roban los datos de la compañía a través de accesos no autorizados obtenidos mediante ataques.																				
1505		Desactualización de los usuarios respecto a configuraciones de tráfico entrante, uso de correos electrónicos, contraseñas y descargas lo cual facilita el acceso de software.																				
1601	Ataques lógicos	Usuarios no autorizados tratan de forzar el ingreso a los sistemas																				
1801	Ambiental	El equipamiento utilizado no es amigable en cuanto al medio ambiente (por ejemplo, en el consumo de energía, embalajes, etc.)																				
1901	Actos de la Naturaleza	Hay un terremoto.																				
1903		Hay fuertes tormentas y ciclones tropicales.																				
1904		Hay un gran incendio fuera de control.																				

ANEXO Q - Tabla de Procesos

Lista de Escenarios de Riesgos Calificados de tipo Riesgo Inaceptable.												
				Actividades								
				Activo / Recurso					Responsables			
Ref. de COBIT 5	Escenario de Riesgo	Nivel de Riesgo	Descripción	Personas y habilidades	Estructuras Organizativas	Infraestructuras	Información	Aplicaciones	Responsable ¿Quién hace?	Rinde Cuentas ¿Quién comunica?	Métricas Relacionadas	
105	Desconocimiento de las Políticas de TI.	40	Diseñar y plantear políticas para garantizar el control de la Div de Gestión Financiera.						Institución: Jefe de la Vicerrectoría Administrativa y jefe de la Div de Gestión Financiera	Jefe de la Div Gestión Financiera	Políticas soportadas por estándares y prácticas internacionales, certificadas. Por tanto realizar frecuentemente la revisión y actualización de las políticas, las cuales deben ser documentadas y actualizadas.	
301	Los gerentes de negocios o sus representantes no se involucran en las decisiones importantes sobre inversiones de TI (por ejemplo: nuevas aplicaciones u oportunidades tecnológicas, priorizaciones).	20	Involucrarse en las decisiones importantes sobre las inversiones, las cuales permitan dar opiniones respecto a los beneficios que se tengan a la nueva tecnología.						Institución: Jefe de la Vicerrectoría Administrativa, jefe y personal de la Div de Gestión Financiera.	Jefe de la Div Gestión Financiera	Número de empleados identificados frente a los conocimientos de las nuevas aplicaciones u oportunidades tecnológicas.	
408	Existe una dependencia excesiva del personal clave de TI.	40	Identificar las competencias y habilidades del personal para que no exista dependencia entre ellos.						Institución: el Jefe de la y el personal encargado de cada una de las dependencia que conforman la Div de Gestión Financiera.	Personal Div Gestión Financiera	Número de empleados evaluados según sus competencias del área de Recaudos.	

409	Existe una incapacidad para actualizar las habilidades de TI a un nivel apropiado a través del entrenamiento.	24	Gestionar la creación de foros de capacitación en temas de ocurrencia cotidiana evitando la generación de trámites extensos.						Institución: Jefe de la Vicerrectoría Administrativa junto al jefe de la Div de Gestión Financiera.	Jefe de la Div Gestión Financiera	Nivel de satisfacción de las partes interesadas con la capacitación del personal con los programas y servicios planeados.
503	Existen errores cometidos por el personal (durante las actualizaciones del sistema, copias de respaldo, mantenimiento)	24	Desarrollar un plan de mantenimiento de los errores cometidos y tratarlos de manera que resuelvan los problemas para adquirir las copias de respaldo.						Institución: personal de la Div de Gestión Financiera, encargado de los sistemas de copias de respaldo	Personal Div Gestión Financiera	Número de incidentes significativos relacionados por errores cometidos que no fueron identificados en la evaluación de riesgos.
504	La información es ingresada incorrectamente por el personal.	32	Implementar mecanismos de protección ante el ingreso de información errada.						Institución: personal de la Div de Gestión financiera, encargado de corroborar e ingresar datos correctamente al sistema.	Técnico Administrativo	Número de incidentes significativos relacionados por ingresar incorrectamente la información que no fueron identificados en la evaluación de riesgos.
506	Un dispositivo con datos sensibles es robado por un miembro del personal.	16	Definir políticas de control relacionadas con los dispositivos ingresados y salientes de la Div Financiera.						Institución: el jefe y la Seguridad privada contratada para la Div de Gestión Financiera.	Personal Div Gestión Financiera	Porcentaje de inversiones de TI en los que la realización del beneficio se monitoriza través del ciclo de vida económico completo.
509	Se configuran erróneamente los componentes de hardware.	24	Capacitar al personal ante la configuración de hardware.						Institución: personal encargado del manejo de hardware de la Div de Gestión Financiera	Técnico Administrativo	Número de vulnerabilidades. Porcentaje de pruebas periódicas de los dispositivos de seguridad.
603	Pérdida y Revelación de medios portátiles que contiene datos sensibles de información (CD, USB, discos portátiles, etc.)	24	Proveer el fácil reconocimiento ante la pérdida de dispositivos que contengan información sensible.						Institución: el jefe y la Seguridad privada contratada para la Div de Gestión Financiera.	Personal Div Gestión Financiera	Número de incidentes identificados por pérdida y revelación de información sensible.
604	Se pierden y se revelan datos sensibles mediante ataques lógicos.	24	Implementar mecanismos de protección ante la manipulación de ataques lógicos.						Institución: Unidad de operación de Sistemas informáticos.	Jefe de la Div Gestión Financiera	Porcentaje de mejoras acordadas que han sido reflejadas. Porcentaje de asuntos identificados que se han incluido satisfactoriamente.
605	Se pierden o no se verifica la efectividad de los medios que contienen las copias de respaldo.	20	Verificación y actualización de los medios que contienen información sensible.						Institución: jefe de la DIv de Gestión Financiera. Jefe de la Div de las TIC.	Jefe de la Div Gestión Financiera	Nivel de concienciación y comprensión de las posibilidades de la pérdida de las copias de respaldo.
606	Se revela información sensible en forma accidental debido a fallas en el seguimiento de las guías de manejo de	32	Implementar mecanismos de protección de información, en los diferentes sistemas que se maneja información sensible.						Institución: personal y jede de la Div de Gestión Financiera. jefel y el personal encargado de	Personal Div Gestión Financiera	Nivel de concienciación y comprensión de las posibilidades de la revelación de información sensible de la institución.

	información.								las Base de datos de la Div TIC		
607	Se modifican intencionadamente los datos (contables, vinculados a la seguridad, información, etc.)	40	Identificar, analizar y confirmar las modificaciones de los datos, que se desean cambiar teniendo presente la autorización del jefe.						Institución: personal encargado del control de datos sensibles de institución.	Técnico Administrativo	Número de vulnerabilidades. Nivel de conciencia ante las modificaciones de los datos delicados de la institución.
609	Se revela información sensible debido a ineficientes procedimientos de retención / archivo y eliminación.	24	Capacitar adecuadamente al personal encargado de la retención/archivo y eliminación de información.						Institución: personal encargado de archivar la información tanto en la Div de Gestión Financiera como de la Div de las TIC.	Técnico Administrativo	Porcentaje de puestos vacantes. Frecuencia de las evaluaciones del personal entrante como antiguo.
612	Filtración de la información debido al abandono del equipo de la institución.	40	Dejar el equipo apagado o bloqueado al momento de tener que abandonarlo.						Institución: jefe, personal de la Div de Gestión Financiera.	Personal Div Gestión Financiera	Número de vulnerabilidades. Nivel de conciencia ante la filtración de información debido al abandono del equipo de trabajo.
804	Existen fallas intermitentes en los servicios (telecomunicaciones, electricidad).	32	Instalar equipamiento de buena calidad y de alerta inmediata al momento de alguna falla de los servicios de telecomunicaciones o de electricidad.						Institución: Jefe de la Div de las TIC. Unidad de operaciones de sistemas informáticos.	Jefe DIv TIC	Número de interrupciones del negocio debidas a incidentes en el servicio de telecomunicaciones, electricidad.
807	Fallas en los registros y definición de acceso a los activos físicos de TI o el uso de dispositivos por parte del usuario para tratamiento de la información.	20	Registrar y emplear el uso dispositivos capaces de robar algún tipo de información como al acceso a los activos físicos de TI.						Institución: seguridad privada de las instalaciones de la Div de Gestión Financiera.	Personal Div Gestión Financiera	Porcentaje de tipos de eventos operativos críticos cubiertos por los sistemas de detección automática.
908	Ocurren errores no intencionales en la gestión de configuraciones y de cambios.	32	Gestionar de inmediato el tratamiento frente a los errores cometidos no intencionales.						Institución: Rectoría, Vicerrectoría Administrativa, Div de Gestión Financiera, Div de las TIC.	Técnico Administrativo	Número de incidentes que impliquen dispositivos de usuario final. Número de dispositivos de usuario final no autorizados detectados en la red o en el entorno.
1202	El desconocimiento de cambios potenciales en la regulación tiene un impacto en el ambiente operativo	24	Informar y Capacitar al personal de los cambios que tienen un impacto en el ambiente operativo.						Institución: Consejo Superior, Rectoría, Vicerrectoría Administrativa, Div de Gestión Financiera, Div de las TIC.	Personal Div Gestión Financiera	Número de incidentes que impliquen el desconocimiento de cambios potenciales.
1401	Se ha producido el robo de un dispositivo con datos sensibles.	40	Registras los dispositivos de la Div Financiera que al momento de salir puedan ser fácilmente						Institución: compañía de seguridad privada de las instalaciones de la Div de	Jefe de la Div Gestión Financiera	Número de incidentes de seguridad causantes por la pérdida de robo de un dispositivo

			identificados por los miembros de seguridad.						Gestión Financiera.		con datos sensibles. Interrupciones del servicio o pérdida de imagen así como también los relacionados con seguridad física.
1403	Se destruye el centro de datos (sabotaje, etc.).	40	Tener el adecuado control de vigilancia de cámaras al centro de datos.						Institución: compañía de seguridad privada de las instalaciones de la Div de Gestión Financiera y la Div de las TIC.	Jefe DIv TIC	Número de incidentes por la destrucción del centro de datos. Interrupciones del servicio o pérdida de imagen así como también los relacionados con seguridad física.
1404	Dispositivos individuales se destruyen accidentalmente.	32	Adquirir el conocimiento adecuado del funcionamiento de dispositivos.						Institución: personal de la Div de Gestión Financiera y de la Div de las TIC.	Personal Div Gestión Financiera	Número de vulnerabilidades. Nivel de conciencia ante la destrucción de dispositivos delicados de la Div de Gestión Financiera.
1405	Ineficiencia o ausencia de dispositivos que detectan las amenazas del entorno, debido a la falta de supervisión, mantenimiento y actualización de los mismos.	25	Instalación de equipos capaces de la Identificación amenazas en el entorno.						Institución: Consejo Superior, Rectoría, Vicerrectoría Administrativa, Div de Gestión Financiera, Div de las TIC.	Rectoría	Número de vulnerabilidades. Nivel de conciencia ante la ausencia de dispositivos que detectan las amenazas del entorno de la Div de Gestión Financiera.
1406	Libre acceso a las instalaciones de procesamiento sin peticiones formales.	40	Registrar y emplear el uso de tarjetas o placas de identidad con su previa autorización y supervisión a todos los visitantes de las instalaciones.						Institución: Vicerrectoría Administrativa, Div de Gestión Financiera, Div de las TIC.	Jefe de la Div Gestión Financiera	Porcentaje de usuarios registrados y entregados tarjetas o placas de autorización para su ingreso a las diferentes áreas administrativas de la universidad. Porcentaje del personal que se actualizado su acceso.
1503	Un empleado insatisfecho implementa una bomba lógica que produce la pérdida de datos importantes.	40	Control y evaluación al personal de la Div Financiera frente a sus respectivos puestos de trabajo.						Institución: personal de la Div de Gestión Financiera.	Jefe de la Div Gestión Financiera	Número de vulnerabilidades. Porcentaje de pruebas periódicas de los empleados para saber el grado de satisfacción en el que se encuentren.
1504	Roban los datos de la Div de Gestión Financiera, a través de accesos no autorizados obtenidos mediante ataques.	40	Instalación de cámaras para el control de los lugares donde se tiene información sensible de la DIv Financiera						Institución: Consejo Superior, Rectoría, Vicerrectoría Administrativa, Div de Gestión Financiera, Div de las TIC.	Jefe de la Div Gestión Financiera	Número de vulnerabilidades. Nivel de conciencia ante el robo de datos de la Div de Gestión financiera, debido accesos no autorizados.
1505	Desactualización del personal respecto a configuraciones de tráfico entrante, uso de	25	Definir políticas relacionadas con los permisos para las descargas, cambio constante de contraseñas						Institución: personal de la Div de Gestión Financiera y personal	Personal Div	Número de vulnerabilidades. Porcentaje de pruebas periódicas de los dispositivos de seguridad.

	correos electrónicos, contraseñas y descargas lo cual facilita el acceso de software.								encargado en la Div de las TIC.	Gestión Financiera	
1601	Usuarios no autorizados tratan de forzar el ingreso a los sistemas.	40	Controles con una alta protección a los sistemas que contengan información sensible.						Personal de la Div TIC.	Jefe de la Div Gestión Financiera	Número de vulnerabilidades. Porcentaje de pruebas periódicas ante usuarios que intentan ingresar al sistema sin ser autorizadas.
1801	El equipamiento utilizado no es amigable en cuanto al medio ambiente (por ejemplo, en el consumo de energía, embalajes, etc.)	24	Adquirir equipamiento amigable con el medio ambiente capaz de soportar el funcionamiento de toda la Div de Gestión Financiera.						Institución: Rectoría, Vicerrectoría Administrativa, Div de Gestión Financiera, Div de las TIC.	Vicerrectoría Administrativa	Número de vulnerabilidades. Nivel de conciencia ante el equipamiento, utilizado como respaldo para el seguimiento del servicio.
1901	Hay un terremoto.	40							Institución: Concejo académico Rectoría, Vicerrectoría Administrativa, Div de Gestión Financiera, Div de las TIC.	Rectoría	
1903	Hay fuertes tormentas y ciclones tropicales.	40									
1904	Hay un gran incendio fuera de control.	40									

ANEXO R - Tabla de riesgo residual

Ref de COBIT 5	Escenarios Negativos	Nivel de Riesgo	Riesgo residual Calculado		
			Impacto	Frecuencia	Riesgo Residual
105	Desconocimiento de las Políticas de TI.	40	2	3	6
301	Los gerentes de negocios o sus representantes no se involucran en las decisiones importantes sobre inversiones de TI (por ejemplo: nuevas aplicaciones u oportunidades tecnológicas, priorizaciones).	20	5	2	10
408	Existe una dependencia excesiva del personal clave de TI.	40	3	3	9
409	Existe una incapacidad para actualizar las habilidades de TI a un nivel apropiado a través del entrenamiento.	24	5	2	10
503	Existen errores cometidos por el personal (durante las actualizaciones del sistema, copias de respaldo, mantenimiento)	24	5	2	10
504	La información es ingresada incorrectamente por el personal.	32	3	3	9
506	Un dispositivo con datos sensibles es robado por un miembro del personal.	24	5	3	15
509	Se configuran erróneamente los componentes de hardware.	24	5	2	10
603	Pérdida y Revelación de medios portátiles que contiene datos sensibles de información (CD, USB, discos portátiles, etc.)	24	5	3	15
604	Se pierden y se revelan datos sensibles mediante ataques lógicos.	24	3	3	9
605	Se pierden o no se verifica la efectividad de los medios que contienen las copias de respaldo.	20	5	3	15
606	Se revela información sensible en forma accidental debido a fallas en el seguimiento de las guías de manejo de información.	32	5	3	15
607	Se modifican intencionadamente los datos (contables, vinculados a la seguridad, información, etc.)	40	5	2	10
609	Se revela información sensible debido a ineficientes procedimiento de retención/archivo y eliminación.	24	5	3	15
612	Filtración de la información debido al abandono del equipo de la institución.	40	5	3	15
804	Existen fallas intermitentes en los servicios (telecomunicaciones, electricidad).	32	3	3	9
807	Fallas en los registros y definición de acceso a los activos físicos de TI o el uso de dispositivos por parte del usuario para tratamiento de la información.	20	5	3	15
908	Ocurren errores no intencionales en la gestión de configuraciones y de cambios.	32	8	1	8
1202	El desconocimiento de cambios potenciales en la regulación tiene un impacto en el ambiente operativo	24	3	2	6
1401	Se ha producido el robo de un dispositivo con datos sensibles.	32	5	3	15
1403	Se destruye el centro de datos (sabotaje, etc.).	40	5	3	15
1404	Dispositivos individuales se destruyen accidentalmente.	32	5	3	15
1405	Ineficiencia o ausencia de dispositivos que detectan las amenazas del entorno, debido a la falta de supervisión, mantenimiento y actualización de los mismos.	40	5	3	15
1406	Libre acceso a las instalaciones de procesamiento sin peticiones formales.	40	5	3	15

1503	Un empleado insatisfecho implementa una bomba lógica que produce la pérdida de datos importantes.	40	5	3	15
1504	Roban los datos de la compañía a través de accesos no autorizados obtenidos mediante ataques.	40	5	3	15
1505	Desactualización de los usuarios respecto a configuraciones de tráfico entrante, uso de correos electrónicos, contraseñas y descargas lo cual facilita el acceso de software.	25	3	3	9
1601	Usuarios no autorizados tratan de forzar el ingreso a los sistemas.	40	8	1	8
1801	El equipamiento utilizado no es amigable en cuanto al medio ambiente (por ejemplo, en el consumo de energía, embalajes, etc.)	24	5	3	15
1901	Hay un terremoto.	40	5	3	15
1903	Hay fuertes tormentas y ciclones tropicales.	40	5	3	15
1904	Hay un gran incendio fuera de control.	40	5	3	15

Riesgo Residual.

Riesgo= Frecuencia * Impacto							
Desastroso	**Impacto**	**8**	**8** 1501-601-602-908-1601-	**16** 502-505-901-1105-1502-	**24**	**32**	**40**
Mayor		**5**	**5** 510-801-902-904-410-411	**10** 608-903-1702-1201-207-613-409-503-509-607-301	**15** 507-907-506-603-605-606-609-612-807-1401-1403-1404- 405-1406-1503-1504-1801-1901-1903-1904	**20**	**25**
Moderado		**3**	**3** 906-802	**6** 1106-1605-1701-1202-	**9** 408-504-604-804-1505-	**12**	**15**
Menor		**2**	**2** 905-909-910-803-806	**4**	**6** 105	**8**	**10**
Insignificante		**1**	**1**	**2**	**3**	**4**	**5**
			1	**2**	**3**	**4**	**5**
		Frecuencia					
			Raro	**M. Bajo**	**Bajo**	**Medio**	**Alto**

ANEXO S - Entregables

UNIVERSIDAD DEL CAUCA

Caso de estudio: Procedimiento de Recaudos en la División de Gestión Financiera.

DOCUMENTO SOBRE LA OBTENCION DE LA APROBACION DE LA DIRECCION PARA INICIAR UN PROYECTO DE SGSI.

Código	
Versión:	1.0
Fecha de la versión:	30/11/2015
Creado por:	Milena Cruces – Juan Pablo Mora
Aprobado por:	
Nivel de confidencialidad:	Alto

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación

Tabla de contenido

1. Objetivo, obtener la aprobación por la dirección para iniciar el proyecto SGSI.

El Objetivo de esta fase es definir detalladamente la obtención de la aprobación de la dirección para iniciar el proyecto de SGSI. Se requiere el aval de la dirección, para esto la tabla 1, muestra cada uno de los pasos a considerar para la obtención de la aprobación de la dirección para dar inicio a la implementación del SGSI.

2. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001:2013 numeral 4,3
- COBIT 5
- [Sistema de gestión de la seguridad de la información de la Universidad del Cauca. Septiembre de 2015]
- [R005 del 7 de Enero de 2015]

- Carta de compromiso de la División de Gestión financiera de la Universidad del Cauca.

3. OBTENCION DE LA APROBACION DE LA DIRECCION PARA INICIAR UN PROYECTO DE SGSI.

Para llegar a obtener la aprobación de la dirección para dar inicio a un proyecto de un Sistema de Gestión de Seguridad de la Información o SGSI se recomienda crear un caso de negocio que incluya las prioridades y objetivos al implementar un SGSI, el resultado de este numeral son:

a. Obtener objetivos del negocio de la organización.
b. Lograr la comprensión de los sistemas de gestión existentes.

3.1. PANORAMA GENERAL PARA LA OBTENCION DE LA APROBACION DE LA DIRECCION PARA INICIAR EL PROYECTO DE SGSI.

Un panorama general para llegar a obtener la aprobación de la dirección, se inicia obteniendo ciertos objetivos del negocio los cuales permitan dar una breve descripción de lo que se desea realizar al implementar un SGSI.

- **Objetivos estratégicos, prioridades de la seguridad de la información y los requisitos organizacionales para un SGSI:**

  - Realizar un análisis de la seguridad de la información de toda la División de Gestión financiera con el propósito de evaluar el riesgo de la información.
  - Motivar y capacitar al personal de la División de Gestión Financiera sobre la implantación de un sistema de gestión de seguridad de la información.
  - Analizar la información recolectada y proponer las estrategias que le permiten la protección de los activos de información.

- Implantar el plan estratégico, del Sistema de Gestión de Seguridad de la Información en las áreas en las que se halla determinado el riesgo de la información de la División de Gestión Financiera.

➢ **Comprensión de los sistemas de gestión existentes.**

Al no existir un SGSI en la Universidad del Cauca, no se aplica un modelo de gestión de la seguridad, ni se contemplan unos procedimientos adecuados y se evidencia una debilidad en la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos, trayendo como consecuencia que la disponibilidad de los servicios críticos, la confidencialidad y la integridad de los datos tengan un alto nivel de riesgo.

3.2. ACLARACION DE LAS PRIORIDADES DE LA ORGANIZACIÓN PARA DERARROLLAR UN SGSI:

Se debe incluir los objetivos al implementar un SGSI, considerando las prioridades y los requisitos de seguridad de la información de la organización.

➢ **Objetivos estratégicos, prioridades de la seguridad de la información y los requisitos organizacionales para un SGSI:**

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer políticas y procedimientos en relación a los objetivos estratégicos de la División de Gestión Financiera, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. Los objetivos estratégicos de la División de Gestión Financiera de la Universidad del Cauca son:

- Realizar un análisis de la seguridad de la información de toda la División de Gestión financiera con el propósito de evaluar el riesgo de la información.
- Motivar y capacitar al personal de la División de Gestión Financiera sobre la implantación de un sistema de gestión de seguridad de la información.
- Analizar la información recolectada y proponer las estrategias que le permiten la protección de los activos de información.
- Implantar el plan estratégico, del Sistema de Gestión de Seguridad de la Información en las áreas en las que se halla determinado el riesgo de la información de la División de Gestión Financiera.

Las prioridades de seguridad de la información y los requisitos de la Universidad del Cauca para un SGSI, es garantizar a las respectivas dependencias, los riesgos que afecten la seguridad de la información sean identificados y evaluados, esto con el fin de implantar contramedidas, procesos y procedimientos para su apropiado control, tratamiento y mejora continua. Las prioridades y requisitos a tener presente serán:

- Hacer un análisis de riesgos, identificando amenazas, vulnerabilidades e impactos en los sistemas de información, ofreciendo la oportunidad de optimizar las áreas, dentro de la Universidad relacionada con la información que más le importe, mejorando la gestión de la seguridad dando garantía de continuidad y disponibilidad del negocio.
- Generar un valor a la Universidad, aumentando su costo comercial y de esta manera, darle una mejorar imagen.
- Una gran prioridad es la certificación en el manejo de la información, ya que garantiza su conformidad con la implantación de la ISO /IEC 27001, su eficacia,

etc. La cual contribuye a fomentar las actividades de protección de la información en las organizaciones, mejorando su imagen y generando confianza frente a terceros.

- Disminuir el impacto de los riegos potenciales sin necesidad de grandes cambios para mantenerlo en un nivel aceptable, permitiendo hacer mejoras a la información de una manera más económica y rápida.
- Garantizar la fiabilidad y disponibilidad del servicio en el mantenimiento rutinario. Se deben realizar auditorías periódicas para evaluar la efectividad de los controles e implementar las mejoras solicitadas. Garantizar la seguridad en los cambios que se hicieron.

- **Requisitos reglamentarios, contractuales y de la industria, relacionados con la seguridad de la información de la organización:**

La intervención y el interés que hace el gobierno y la Universidad del Cauca, frente a la seguridad de la información, se ve reflejado en los siguientes decretos y resoluciones, los cuales se tienen como soportes para ser implementado el SGSI:

- Resolución 005 de 2015 por la cual se autoriza la ejecución del proyecto "Implantación y Certificación del Sistema de Gestión de la Seguridad de la Información-SGSI de la Universidad del Cauca" para garantizar la seguridad de la información desde las perspectiva de la confidencialidad, integridad y disponibilidad.
- Decreto número 2573 de 2015 por el cual se establece los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la ley 1341 de 2009 y se dicta otras disposiciones (1)
- Documento Conpes 3701 busca generar lineamientos de política de ciberseguridad y ciberdefensa orientado a desarrollas una estrategia nacional que contraste el incremento de las amenazas informáticas que afectan significativamente al país.(2)
- Resolución 785 de 2015 (7 de octubre de 2015). Establece las políticas de seguridad de la información de la Universidad del Cauca, donde se tiene que la política del SGSI es la declaración general que representa la posición de la Dirección de la Universidad del Cauca con respecto a la protección de los activos de información.

En aplicación a las normas de regulación colombiana para la seguridad de la información: Ley 527 de Comercio electrónico y firma digital del 18 de Agosto de 1999, Ley 1266 Habeas data del 31 de Diciembre del 2008, Ley 1273 de Delitos informáticos del 5 de Enero de 2009, Ley 1581 para Protección de Datos Personales del 17 de Octubre de 2012, Decreto 1704: Seguridad de los Operadores de Servicios de Telecomunicaciones del 15 de Agosto de 2012, Decreto 1377: Protección de Datos Personales del 25 de Junio de 2013, Decreto 2573: Lineamientos Generales de la Estrategia de Gobierno el línea del 12 de Diciembre de 2014. Que teniendo en cuenta lo anterior, se ha ce necesario definir

las políticas del sistema de gestión de seguridad de la información que aplicara a la Universidad del Cauca.

- **Un bosquejo de las características del negocio, la organización, su ubicación, activos y tecnología.**

Características del negocio del Área Recaudos pereciente a la división financiera de la Universidad del Cauca

El Área de Recaudos de la División Financiera se encarga de reconocer, revelar, controlar, garantizar el recaudo y registro de los recursos financieros a los cuales la Universidad tiene derecho, enmarcados en la normatividad bancaria, presupuestal y contable vigente para el cumplimiento de la misión social, Inicia con los actos administrativos que determinan la prestación del servicio, fijan las tarifas de cobro a facturar en SIMCA y SQUID y termina con el archivo de los documentos.

- **Ubicación organizacional del Área Recaudos:**
  En la siguiente ilustración podemos ver la ubicación del Área de Recaudos tanto organizacional como física de acuerdo al organigrama de la Universidad.

Figura 2: Organización física del área de Recaudos.

- **Ubicación Física del Área de Recaudos**
  Calle.4 # 5-30, Centro histórico de la ciudad de Popayán, Cauca

3.3. DEFINIR EL ALCANCE PRELIMINAR DEL SGSI:

Definir alcance preliminar del SGSI, dando como salida Alcance Preliminar y definición de roles y responsabilidades del SGSI:

- **Desarrollar el alcance preliminar:**

Los requisitos para la gestión de seguridad de la información establecidos por la dirección de la organización en la División de Gestión Financiera de la Universidad del Cauca se centran en:

- La necesidad de establecer una política y unos objetivos.
- Implementar controles para gestionar los riesgos en el contexto del negocio.
- Monitorizar el rendimiento del SGSI.
- Mejora continua.

La obligación impuesta que la Universidad del Cauca debe hacer es, al personal que realizar la implantación del SGSI, ya que se requiere de personal capacitado preferible auditor interno ISO 27001.

La División de Gestión Financiera está compuesta por nueve procedimientos, los cuales son: Conciliaciones Bancarias y saldos de tesorería y contabilidad; Declaraciones tributarias; Egresos por devoluciones y descuentos; Egresos presupuestales; Legalización de comisión y avance; Modificaciones Presupuestales; Plan anual de caja PAC; Recaudos; y Estados Financieros. Estos procedimientos se comunican de manera indirecta, lo que implica que todos interactúan con todos sin ningún tipo de orden o secuencia a seguir. Esto debido a que la función principal de recaudos consiste en, recaudar los ingresos de la institución y realizar los pagos a los diferentes proveedores de bienes y servicios prestados a la universidad del Cauca.

La lista de objetivos de negocio de la gestión de seguridad de la información en la División de gestión Financiera será:

- Determinar los riesgos que se presenten con la información que se maneja en la División de Gestión financiera, en el área de Recaudos de la Universidad del Cauca.
- Clasificar el nivel de Impacto de los riesgos.
- Construir planes de mitigación de riesgo (disminuir los riesgos).
- Brindar apoyo y asesoría a las diferentes dependencias en seguridad de la información.

La División de Gestión Financiera, se encuentra en constantes amenazas y riegos por diversos factores que ponen en peligro la información, en especial el área de Recaudos, estas amenazas pueden provenir desde el interior o exterior de la Universidad. El objetivo del área de recaudos es, reconocer, relevar, controlar, garantizar, el recaudo y los registros de los recursos financieros a los cuales la universidad tiene derecho, enmarcados en la normatividad bancaria, presupuestal y contable vigente para el cumplimiento de la misión social. El funcionamiento de recaudos inicia con los actos administrativos que determinan la prestación del servicio, fijan las tarifas de cobro a facturación SIMCA (Sistema de Integrado de Matriculas y control académico) y SQUID (Sistema de facturación y gestión de recaudos), realiza la interface de SQUID a Finanzas Plus (Sistema de información financiera) de todas las facturas generadas por el cobro de servicios prestados en la institución y determina con el archivo de documentos. La ubicación geográfica a la cual se le aplicara el SGSI es la Calle. 5 # 4-70, Centro histórico de la ciudad de Popayán, Cauca.

Al no existir un SGSI en la Universidad del Cauca, no se aplica un modelo de gestión de la seguridad, ni se contemplan unos procedimientos adecuados y se evidencia una debilidad en la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos, trayendo como consecuencia que la disponibilidad de servicios críticos, la confidencialidad y la integridad de los datos tengan un alto nivel de riesgo.

Las características del negocio son de carácter institucional a beneficio de la comunidad universitaria con conocimientos y habilidades adquiridas en el camino.

3.4. DEFINIR ROLES Y RESPOSABILIDADES PARA EL ALCANCE PRELIMINAR DEL SGSI:

Rol	Breve descripción de la responsabilidad
Nivel Directivo	
Comité de dirección de la Universidad del Cauca	Responsable con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento, mejora, auditorías y certificación del SGSI y la Asignar tiempo y recursos para que sus activos de información estén lo suficientemente protegidos.
Nivel Estratégico	
Comité de seguridad de la Información	Responsables de los temas relacionados con la seguridad de la información, asignar responsables, tareas, actividades y tomar decisiones en cuanto a seguridad de la información se refiere respaldado por el COMITÉ DE DIRECCIÓN, buscando siempre la mejora del SGSI.
Nivel Táctico	
Cisco (Oficial de Seguridad de la Información)	Responsable máximo de planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones con el fin de mejorar la seguridad de la información dentro de sus pilares fundamentales de confidencialidad, integridad y disponibilidad.
Asesor	Apoyar en la elaboración de las políticas, normas y procedimientos de la seguridad de la información, acompañar la implementación de estas, apoyar en el análisis de riesgos, planes de contingencia y prevención de desastres relacionados con el SGSI
Nivel Técnico Y operativo	
Líderes Técnicos de las Aplicaciones	Profesionales adscritos a la División de las TIC de la Universidad, responsables de mantener operando las respectivas Aplicaciones software y de ayudar a los usuarios finales a ser más eficaces en el desempeño de su labor.
Administrador de Base de datos	Profesionales adscritos a la División de las TIC de la Universidad, responsables del normal funcionamiento de las respectivas Bases de Datos de las correspondientes Aplicaciones de los Sistemas de Información Institucionales.

Líderes Funcionales de las aplicaciones	Todas las Aplicaciones utilizadas en la Universidad, deben contar con su respectivo Líder Funcional que garantice la calidad e integridad de la información. Estos funcionarios son responsables de los correspondientes activos de información institucionales. Los Líderes Funcionales de las Aplicaciones son los respectivos Jefes de las Dependencias universitarias o sus delegados
Jefe de la División Financiera	Encargado de velar por el correcto desempeño del SGSI y revisar minuciosamente cualquier documento del SGSI para su aprobación.
Usuarios Finales de las aplicaciones	Los usuarios finales de las Aplicaciones, corresponden a los funcionarios de cada Dependencia de la Universidad, que registran y actualizan la información en forma permanente en su respectiva Aplicación que hace parte de los Sistemas de Información Institucionales
Técnico Administrativo	Reconocer, revelar, controlar, garantizar el recaudo y registro de los recursos financieros a los cuales la Universidad tiene derecho, fijan las tarifas de cobro a facturar en SIMCA y SQUID y termina con el archivo de los documentos.(Finanzas Plus)

Tabla 2: Roles y Responsabilidades para el alcance preliminar.

3.5. CREAR EL CASO DE NEGOCIO Y EL PLAN DE PROYECTO PARA APROBACION POR LA DIRECCION:

En esta actividad se debe crear el caso de negocio y el plan de proyecto para aprobación de la dirección para iniciar un proyecto para implementar un SGSI, dando como salida 2 Documentos, los cuales contengan lo siguiente:

- **Caso del Negocio:**

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios.

Las metas y los objetivos por parte de la Universidad del Cauca es definir la estructura organizacional y los recursos necesarios para la implantación de un Sistema de Gestión de Seguridad de la Información. Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante un sistema definido, documentado y conocido por todos, que se revisa y mejora constantemente.

La meta principal, es la Certificación de un SGSI es un proceso mediante el cual una Entidad de Certificación externa, independiente y acreditada, audita el sistema

determinando su conformidad con ISO/IEC 27001:2013, su grado de implantación real y su eficacia y, en caso positivo, emite el correspondiente certificado.

Los beneficios que trae la implantación de un SGSI para la Universidad del Cauca, se enmarca en:

- Reducción de Costos: los beneficios que trae por ejemplo, es en la reducción de las primas de seguros en algunas pólizas debido a la justificación de la protección de los activos asegurados, o evitando a indemnizar a usuarios por malas gestiones.
- Mantener y mejorar la imagen: los usuarios percibirán a la División de Gestión Financiera como una entidad responsable, comprometida con la mejora de sus procesos y servicios. Un SGSI implantado en la Universidad del Cauca y en especial a la División de Gestión Financiera, en una posición de reconociendo ante la ciudadanía y a sus pares. Una imagen consolidada y de confianza, facilita la gestión general y habilita nuevas posibilidades para la toma de necesidades.
- Cumplimiento legal y reglamentario: día a día el marco normativo referido a la seguridad de la información se afianza y se consolida, por medio de decretos, leyes, resoluciones estipuladas por el gobierno nacional (Min TIC) como de la Universidad, para la implementación del SGSI.

De todos los nueve procedimientos que comprenden la División de Gestión Financiera, se encuentran varios sistemas de información que manejan información crítica y los cuales requieren de un sistema de gestión de seguridad de la información. Pero para este trabajo de grado se ha optado por el área de Recaudos ya que la Universidad por medio del Rector y soportado por la Resolución 005 de 2015, da a conocer la necesidad que tiene de la implementación de un SGSI en el área de Recaudos, esto debido a que esta área es una de las más importantes, ya que en ella se maneja toda la información de ingresos presupuestales de la universidad, de donde se requiere de la necesidad de un sistema de gestión de seguridad de la información para la protección de los activos de información que se encuentran en esta área.

El plan general que se desea, es la implementación de un “Sistema de Gestión de Seguridad de la Información de la Universidad del Cauca”. Este proyecto es requerido por la Universidad por medio de la Resolución 005 de 2015, esto con el fin de garantizar la seguridad de la información desde la perspectiva de la confidencialidad, integridad y disponibilidad. La dirección del proyecto está a cargo bajo del jefe de la División de Tecnologías de la información y las comunicaciones.

El plan de implementación que se desea, se observa en la figura 3.

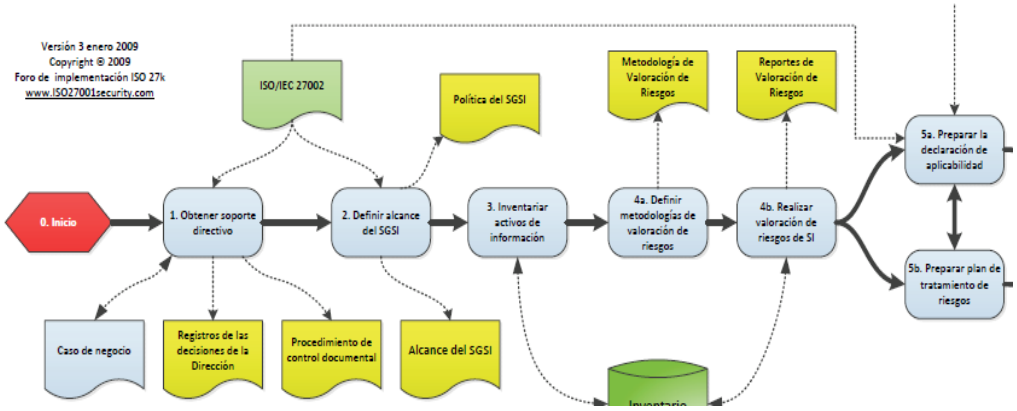


Figura 3: Plan de implementación.

De donde se obtiene que:

1. Obtener Soporte Directivo: Para lograr el objetivo de la implantación, es fundamental contar con el respaldo de los niveles directivos dentro de la entidad y ser conscientes de los beneficios que se puede obtener de la seguridad.

2. Definir el alcance del SGSI: es el punto de partida para establecer el SGSI, permitiendo identificar claramente las dependencias, relaciones y límites de la organización, incluyendo aquellas partes que no se tiene a considerar, dentro y fuera de la organización. Dentro del alcance se determina las políticas de información, las cuales se define como un contexto de planificación y control para establecer límites de conducta aceptable, limitar las decisiones y estándares, su objetivo es proporcionar apoyo por la alta gerencia de acuerdo con los requerimientos de la empresa.

3. Inventarios de activos de Información: las organizaciones poseen información que deben proteger frente a riesgos y amenazas para asegurar el correcto funcionamiento de su negocio. Este tipo de información es de vital importancia para las diferentes empresas es lo que se denomina activo de información. su protección es el objetivo de todo sistema de gestión de seguridad de la información.

4. Definir metodologías de valoración de riesgos: la metodología propone un organigrama que establece los roles necesarios y como se vinculan entre sí. Una metodología de valoración de riesgo, se emplea para realizar la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos que estén relacionados a los activos de información, mencionados en el alcance.

Los recursos requeridos para la implementación del SGSI en el área de Recaudos de la División de Gestión Financiera de la Universidad del Cauca, es la Información necesaria de parte del área para el buen desarrollo de la implementación del SGSI.

Las consideraciones de implementación que incluyan la seguridad de la información existente, es un acta de confidencialidad, autenticada sobre la información actual, por parte de las personas responsables de la implementación del Sistema de Gestión de Seguridad de la Información en el área de Recaudos de la División de Gestión Financiera de la Universidad del Cauca.

La línea temporal con todos sus hitos más importantes, se describen en el siguiente cronograma establecido para la implementación del SGSI:

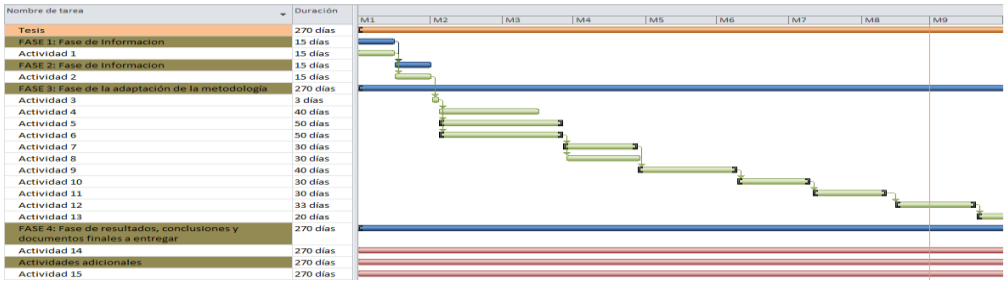


Figura 4: Cronograma de actividades.

Los costos esperados, se muestran en la siguiente tabla 3:

RUBROS		FUENTES		TOTAL
		ESTUDIANTES	DEPARTAMENTO	
Recursos Humanos		$33.819.120	$ 1.878.840	$ 35.697.960
	Equipos de Laboratorio (120Hs)	$1.923.037	$ 0	$1.923.037
	Impresora (100Hs)	$ 20.000	$ 0	$ 20.000
	Computador	$ 750.000	$ 0	$ 750.000
Recursos Software		$ 65.076,94	$ 0	$ 65.076,94
Bibliografía		$ 280.000	$ 0	$ 280.000
Materiales		$ 250.000	$ 0	$ 250.000
SUBTOTAL		$ 37.631.557,49	$ 1.878.840	$ 39.970.397,49
Comunicaciones (2%)		$ 861.831,1498	$ 0	$ 861.831,1498
A.U.I (20% del costo total del trabajo de grado)		$ 8.618.311,498	$ 0	$ 8.618.311,498
TOTAL		$ 47.114.700,1378	$ 1.878.840	$ 48.990.540,1378

Tabla 3. Recursos y Presupuesto.

Los factores críticos de éxito de la no implementación seria: la pérdida de información confidencial, la pérdida de dinero, desprestigio al buen nombre de la Universidad, estos destacados como los más críticos.

- **Propuesta del Proyecto SGSI al Área de recaudos de las División Financiera de la Universidad del Cauca:**

Desarrollar la fase de plan del SGSI, para determinar el análisis de seguridad de la información Adaptando la metodología COBIT como mecanismo para la valoración del riesgo siguiendo la ISO/IEC 27003 como guía de implementación y al final calibrar y ajustar el mecanismo para la valoración del riesgo a partir de los resultados obtenidos al aplicar la metodología al caso de estudio y formular estrategias de mejora. Todo esto estará plasmado en un Documento guía con recomendaciones y estrategias sobre la adaptación de la metodología de la información COBIT 5 como metodología de valoración del riesgo en 27001 y un documento con los resultados obtenidos, con la identificación de los procedimientos, requerimientos y herramientas necesarias para poder implementar un SGSI para la división financiera de la Universidad del Cauca.

UNIVERSIDAD DEL CAUCA

Caso de estudio: Procedimiento de Recaudos en la División de Gestión Financiera.

DEFINIR EL ALCANCE LOS LÍMITES Y LA POLITICA DEL SGSI.

Código	
Versión:	1.0
Fecha de la versión:	
Creado por:	Milena Cruces – Juan Pablo Mora
Aprobado por:	
Nivel de confidencialidad:	Alto

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación

Tabla de contenido

1. OBJETIVO, DEFINIR EL ALCANCE Y LOS LÍMITES DETALLADOS Y DESARROLLAR LA POLITICA DEL SGSI, ASI COMO OBTENER EL RESPALDO DE LA DIRECCION.

El Objetivo de esta fase es definir detalladamente el alcance y los limites detallados y desarrollar la política del SGSI, así como obtener el respaldo de la dirección. De esta manera, definiendo el alcance se tiene en detalles los activos críticos de información en la organización y evaluar mecanismos de seguridad viables.

2. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001:2013
- [Sistema de gestión de la seguridad de la información de la Universidad del Cauca. Septiembre de 2015]
- [R005 del 7 de Enero de 2015]

3. OBTENCION DEL ALCANCE Y LOS LÍMITES DETALLADOS Y DESARROLLAR LA POLITICA DEL SGSI, ASI COMO OBTENER EL RESPALDO DE LA DIRECCIÓN.

Para llegar a obtener el alcance y los límites detallados y desarrollar la política del SGSI, así como obtener el respaldo de la dirección. Es posible definir el alcance de un SGSI de maneta que comprenda toda la organización, o una parte de ella, tal como una división o subdivisión claramente determinada, como es nuestro caso de estudio, la División de Gestión Financiera de la Universidad del Cauca, más concretamente en la subdivisión el área de Recaudos.

Para llegar a obtener el alcance y desarrollar la política del SGSI, así como el respaldo de la dirección se tienen los siguientes numerales:

3.1. PANORAMA GENERAL DE LA DEFINICION DEL ALCANCE, LOS LÍMITES Y LA POLITICA DEL SGSI.

La aprobación de la dirección para la implementación de un SGSI se basa en el alcance preliminar, en el caso de negocio y el plan de proyecto inicial del SGSI. Los principales factores para su implementación exitosa son:

a. La definición detallada del alcance y los límites, la definición de la política, y la aceptación y el respaldo por parte de la dirección.

Por tanto se necesitan las siguientes actividades, con el fin de cumplir el objetivo de “Definir el alcance y los límites detallados del SGSI” de los cuales son:

- Definir el alcance y los límites de la organización.

- Definir el alcance y los límites de las tecnologías de la información y las comunicaciones (TIC);
- Definir el alcance y los límites físicos;
- Las características específicas en los numerales 4.2.1 a) y b) de la norma NTC- ISO/IEC 27001, es decir los aspectos del negocio, la organización, la ubicación, los activos y la tecnología , del alcance, los límites y la política, se determinen en el proceso de definir este alcance y limites
- Integrar el alcance y los límites elementales para obtener el alcance y los límites del SGSI.

Se recomienda determinar el alcance detallado del SGSI considerando los activos críticos de información de la organización.

La definición del alcance y los límites de la organización, del alcance y los límites de las TIC, y del alcance y los límites físicos, no siempre se llevan a cabo de manera secuencial. Sin embargo, cuando se definen nuevos alcances y limites es útil hacer referencia a los alcances y limites ya obtenidos.

3.2. DEFINIR EL ALCANCE Y LOS LÍMITES DE LA ORGANIZACIÓN:

La División de Gestión Financiera de la Universidad del Cauca, se encuentra en constantes amenazas y riegos por diversos factores que ponen en peligro la información, estas amenazas pueden proceder desde el interior o exterior de la Universidad. Por ello es necesario la seguridad de la información, ahora bien, el objetivo de implementar un SGSI es de reconocer, relevar, controlar, garantizar y los registros de los recursos financieros a los cuales la universidad tiene derecho, enmarcados en la normatividad bancaria, presupuestal, legal y contable vigente para el cumplimiento de la misión social. Es por eso que la Resolución R005 del 7 de enero del 2015, mirando que actualmente existen sistemas de información que generan y manejan información crítica en los cuales se encuentra la División de Gestión Financiera en el área de Recaudos.

Las funciones y estructuras de aquellas partes de la División de Gestión Financiera que se encuentran dentro del alcance, permiten:

- Dirigir y coordinar los aspectos referentes a la administración financiera de la Universidad del Cauca.
- Elaborar informes periódicos sobre la gestión financiera, presupuestaria y contable.
- Dirigir, coordinar y controlar las actividades de las dependencias bajo su responsabilidad.
- Realizar los pagos a los diferentes proveedores y servicios prestados a la Universidad del Cauca

La estructura de la División de Gestión financiera cuenta con nueve procedimientos, nombrados a continuación:

1. Conciliaciones Bancarias y Saldos de Tesorería y Contabilidad.

2. Declaraciones Tributarias.
3. Egresos por Devoluciones y Descuentos.
4. Egresos Presupuestales.
5. Legalización de Comisión y Avance.
6. Modificaciones Presupuestales.
7. Plan Anual de Caja PAC.
8. Recaudos.
9. Estados Financieros.

Cada procedimiento cuenta con una serie de actividades las cuales se llevan a cabo para cumplir con sus objetivos en la División de Gestión Financiera. Dentro de este marco, la comunicación que tienen los procedimientos mediante el intercambio de información, sin duda es de mucho cuidado ya que todos dependen de todos. De igual manera existe comunicación con entidades dentro y fuera de la institución. De perder alguna información la división entraría en un nivel muy alto riesgo debido a la pérdida de la información.

Desde el punto de vista de los negocios, un sistema de información es una solución organizacional y administrativa, y responsabilidad sobre los activos de información dentro y fuera del alcance, consta de definir, coordinar y controlar la gestión necesaria para mitigar los riesgos asociados a la seguridad de la información y reportar al comité encargado de la seguridad de la información, esto con el objetivo de cumplir y soportar las actividades de seguridad de la información.

3.3. DEFINIR EL ALCANCE Y LOS LÍMITES DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (TIC):

Los límites de las TIC son:

- Problemáticas técnicas: incompatibilidades entre diversos tipos de ordenador y sistemas operativos.
- Falta de información: las necesidades de unos conocimientos teóricos y prácticos que todas las personas deben aprender, la necesidad de aptitudes y actitudes favorables a la utilización de nuevas y existentes herramientas manejadas en la división.
- Problemas de seguridad: circunstancias como el riesgo de que se produzcan accesos no autorizados a los ordenadores de alguna entidad que están conectados a internet y el posible robo de códigos o claves con las que se tengan acceso a información.
- Barreras económicas: el abaratamiento de los equipos y programas informáticos
- Barreras culturales: el idioma dominante, el inglés, en el que viene muchas referencias e información de internet; la tradición en el uso de instrumentos tecnológicos avanzados

Por otra parte, se encuentran los riesgos lógicos relacionados con la propia tecnología, la cual aumentan día a día. Hackers, robos de identidad, spam, virus, robos de información y espionaje industrial, por nombrar algunos.

La infraestructura de las comunicaciones de la Universidad del Cauca es la base sobre la que se garantiza el aprovechamiento eficiente de las comunicaciones y es determinante en el éxito del buen funcionamiento dentro de la institución.

La red de internet de la Universidad está compuesta por: routers, clave, torre, servidores, proveedores de salas de internet, así como protocolos y otros software requeridos para el funcionamiento. Para la infraestructura de comunicaciones se requiere de: una red o sistema telefónico, el tendido eléctrico y un sistema de red.

La Red corresponde a las instalaciones de alambres conductores de cables multipares o de acometida soportados sobre postes, incluyendo además la instalación del cable de suspensión, riendas de retención, sistema de puesta a tierra, herrajes de montaje de los mismos y otros accesorios. Las redes murales corresponden al cable instalado, grapado o enchapetado sobre las paredes exteriores de las edificaciones de la Universidad del Cauca, vinculando las cajas terminales de manera que su distribución logre la mayor cercanía a los domicilios de abonados y usuarios.

3.4. DEFINIR EL ALCANCE Y LOS LIMITES FISICOS:

- La División de Gestión financiera de la Universidad del Cauca dentro del organigrama institucional se encuentra descrita de la siguiente manera:

Figura #: Organización física del área de Recaudos.

- **Ubicación Física del Área de Recaudos de la División de Gestión financiera de la Universidad del Cauca:**
  Calle. 4 # 5-30, Centro histórico de la ciudad de Popayán, Cauca.

Las oficinas especiales utilizadas para almacenar o contener el hardware de las TIC o los datos dentro del alcance basándose en las limitaciones de las TIC, se tiene las instalaciones de la División de las TIC de la Universidad del Cauca, ubicada en la Facultad de Ciencias Naturales, Exactas y de la Educación- Campus Tulcán en la dirección calle 2 No. 3N-100, de la ciudad de Popayán- Cauca.

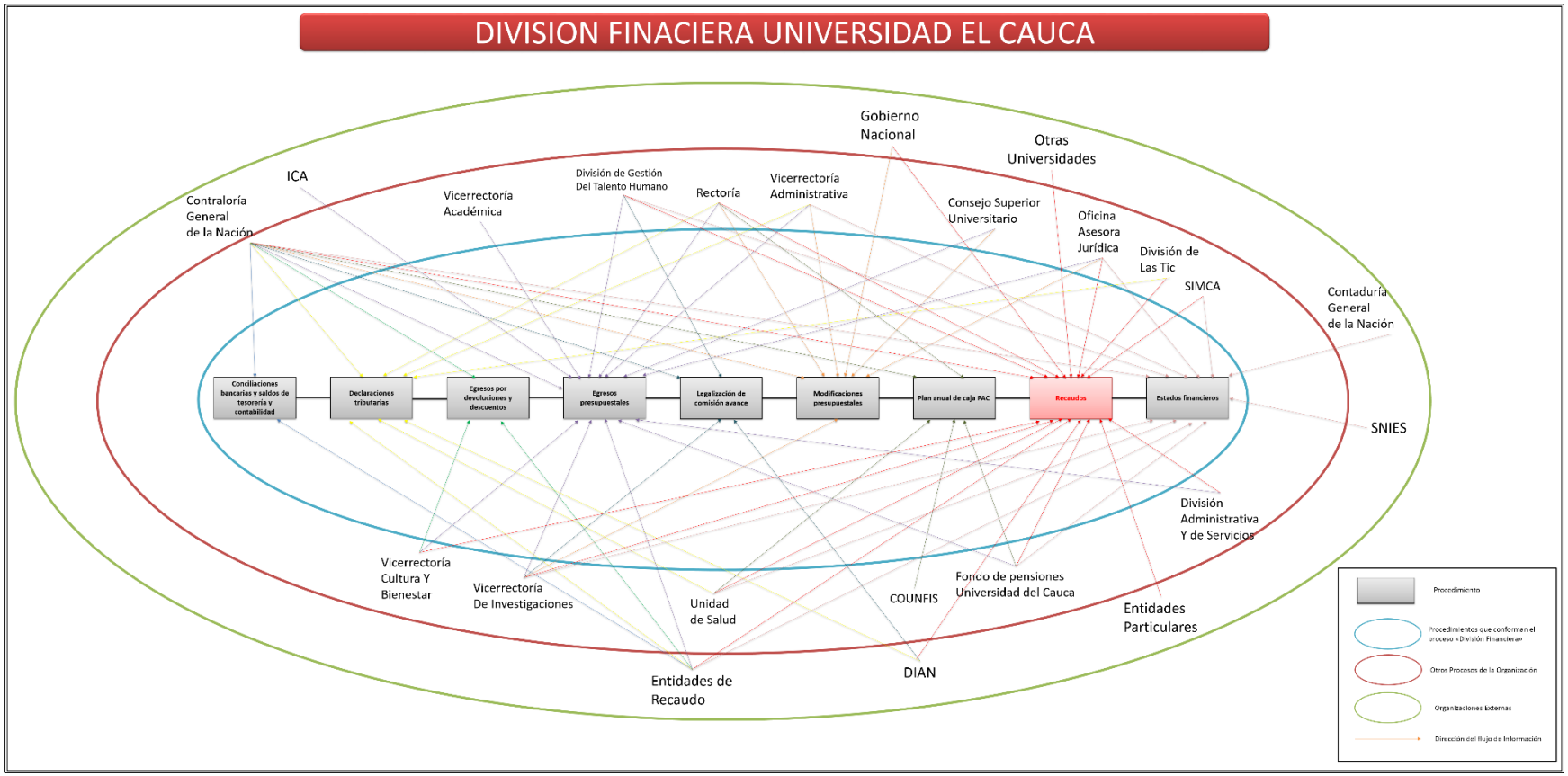
3.5. INTEGRAR CADA ALCANCE Y LOS LÍMITES PARA OBTENER EL ALCANCE Y LOS LÍMITES DEL SGSI:

Al momento d definir el alcance, se opta por escoger un método el cual sea capaz de definir el alcance. Para nuestro caso de estudio se ha tomado el método de las elipses. Este método de las elipses, permite inicialmente distinguir los procesos y subprocesos que conforman el proceso. La División de Gestión Financiera consta

de nueve procedimientos con sus respectivas actividades. A cada proceso se le identifica sus respectivos procesos. En la elipse intermedia, consiste en identificar las distintas relaciones que los procesos de la elipse concéntrica tienen con otros procesos de la organización. Y finalmente en la elipse externa, se identifican aquellas organizaciones que no hacen parte de la empresa pero tiene un tipo de interacción con los procesos y subprocesos de la elipse concéntrica. A esto le añade la dirección que lleva la información, las cuales se representan por flechas en las respectivas elipses.

El procedimiento crítico escogido por la organización es “Recaudos”, esto debido a que el área cuenta con información crítica, por tanto requiere de un sistema de gestión de seguridad de la información.

DIVISION FINACIERA UNIVERSIDAD EL CAUCA



3.6. DESARROLLAR LA POLITICA DEL SGSI Y OBTENER LA APROBACION DE LA DIRECCION.

Establecer las los objetivos del SGSI con base en los requisitos y en las prioridades de seguridad de la información de la organización son:

- Realizar un análisis de la seguridad de la información de toda la División de Gestión financiera con el propósito de evaluar el riesgo de la información.
- Motivar y capacitar al personal de la División de Gestión Financiera sobre la implantación de un sistema de gestión de seguridad de la información.
- Analizar la información recolectada y proponer las estrategias que le permiten la protección de los activos de información.
- Implantar el plan estratégico, del Sistema de Gestión de Seguridad de la Información en las áreas en las que se halla determinado el riesgo de la información de la División de Gestión Financiera.

Los requisitos legales o regulatorios de la Universidad del Cauca y las obligaciones contractuales de la universidad relacionados con la seguridad de la información, para la aplicación a las normas de regulación Colombiana son:

Ley 527 de Comercio electrónico y firma digital del 18 de Agosto de 1999, Ley 1266 Habeas data del 31 de Diciembre del 2008, Ley 1273 de Delitos informáticos del 5 de Enero de 2009, Ley 1581 para Protección de Datos Personales del 17 de Octubre de 2012, Decreto 1704: Seguridad de los Operadores de Servicios de Telecomunicaciones del 15 de Agosto de 2012, Decreto 1377: Protección de Datos Personales del 25 de Junio de 2013, Decreto 2573: Lineamientos Generales de la Estrategia de Gobierno el línea del 12 de Diciembre de 2014. Que teniendo en cuenta lo anterior, se ha ce necesario definir las políticas del sistema de gestión de seguridad de la información que aplicara a la Universidad del Cauca.

El contexto dentro de la Universidad del Cauca, es la no existencia de un SGSI, por tanto no se aplica un modelo de gestión de la seguridad de la información, ni se contemplan procedimientos adecuados y se evidencia una debilidad en la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos, trayendo como consecuencia que la disponibilidad de servicios críticos, la confidencialidad y la integridad de los datos tengan un alto nivel de riesgo.

Las políticas de seguridad que soportan el sistema de gestión de seguridad de la información SGSI de la División de Gestión Financiera de la Universidad del Cauca son:

1. La Universidad del Cauca y en especial la División de Gestión Financiera, ha decidido definir implementar y operar de manera continua un Sistema de Gestión de Seguridad de la Información-SGSI, llevado a la necesidad que requiera la División de Gestión Financiera.

2. La División de Gestión Financiera protegerá la información generada, procesada o resguardada de todos sus procedimientos, su infraestructura tecnológica y sus activos de riesgo que se generen dentro de esta.
3. La División de Gestión Financiera protegerá la información creada, procesada, transmitida o resguardada por sus procedimientos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de la información.
4. La División de Gestión Financiera protegerá las instalaciones de procesamiento y la infraestructura, las cuales soportan los procesos de la institución.
5. La División de Gestión Financiera implantara controles de acceso a la información, sistemas y recursos de las redes de datos.

   La División de Gestión Financiera garantizara el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas para garantizar la seguridad de la Información.

UNIVERSIDAD DEL CAUCA

Caso de estudio: Procedimiento de Recaudos en la División de Gestión Financiera.

REALIZAR EL ANALISIS DE LOS REQUISITOS DE SEGURIDAD DE LA INFORMACION.

Código	
Versión:	1.0
Fecha de la versión:	
Creado por:	Milena Cruces – Juan Pablo Mora
Aprobado por:	
Nivel de confidencialidad:	Alto

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación

Tabla de Contenido

1. OBJETIVO, DEFINIR LOS REQUISITOS MÁS IMPORTANTES.

2. QUE DEBE SUSTENTAR EL SGSI, IDENTIFICAR LOS ACTIVOS DE INFORMACION Y OBTENER EL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACION DENTRO DEL ALCANCE.

El Objetivo de esta fase es definir detalladamente los requisitos más importantes que debe sustentar el SGSI. Identificar los activos de información y obtener el estado actual de la seguridad de la información dentro del alcance que se identificó en el punto anterior (punto 6 de la norma 27003).

3. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27003
- [Sistema de gestión de la seguridad de la información de la Universidad del Cauca. Septiembre de 2015]
- [R005 del 7 de Enero de 2015]
- Procedimientos de la División de Gestión Financiera.

4. OBTENCION DE LOS REQUISITOS MAS IMPORTANTES QUE DEBE SUSTENTAR EL SGSI, DE IGUAL MANERA IDENTIFICAR LOS ACTIVOS DE INFORMACION Y OBTENER EL ESETADO ACTUAL DE LA SEGURIDAD DE LA INFORMACION DENTRO DEL ALCANCE.

Para llegar a obtener los requisitos más importantes que debe sustentar el SGSI implica en la recolección de toda la información de apoyo para el SGSI. Para este procedimiento se necesita una decisión en términos de la criticidad de la información, es decir, el nivel de protección requerido. Se recomienda determinar una variedad de las condiciones internas que puedan afectar la seguridad de la información.

Para llegar a obtener los requisitos más importantes que debe sustentar el SGSI, como también identificar los activos de información y así obtener el estado actual de la seguridad de la información, se tiene los siguientes numerales:

4.1. PANORAMA GENERAL DE LA REALIZACION DEL ANALISIS DE LOS REQUISITOS DE SEGURIDAD DE LA INFORMACION.

Es importante analizar la situación actual en la que se encuentra la organización, ya que es recomendable considerar los requisitos y activos de información existentes al implementar un SGSI. El principal factor para es:

b. Definir los requisitos importantes que debe sustentar el SGSI identificar los activos de información y obtener el estado actual de la seguridad de la información dentro del alcance.

Se recomienda que la información que fue recolectada durante el análisis se seguridad de la información:

a. Brinde a la dirección un punto de partida, en su defecto datos básicos correctos.
b. Identifique y documente las condiciones dadas para la implementación.
c. Facilite un entendimiento claro y bien definido de parte de la organización.
d. Tener en cuenta las circunstancias y la situación particular de la organización.
e. Identifique el nivel deseado de protección de la información, y
f. Determine la recopilación de información necesaria para toda la empresa o una parte de ella dentro del alcance propuesto para el desarrollo de la implementación.

4.2. DEFINIR LOS REQUISITOS DE SEGURIDAD DE LA INFORMACION PARA EL PROCESO DEL SGSI.

En esta actividad se recomienda analizar y definir los requisitos de seguridad de la información detallados para el proceso del SGSI, teniendo presente las prioridades y los requisitos de seguridad de la información de la organización.

El primer paso implica en la obtención de toda la información; donde se llega a la identificación de los nueve (9) procedimientos cuenta la División de Gestión Financiera, los cuales mencionamos a continuación: Conciliaciones Bancarias y Saldos de Tesorería y Contabilidad, Declaraciones Tributarias, Egresos por Devoluciones y Descuentos, Egresos Presupuestales, Legalización de Comisión y Avance, Modificaciones Presupuestales, Plan Anual de Caja PAC, Recaudos, Estados Financieros. Estos nueve (9) procesos son los encargados de recaudar los ingresos institucionales y realizar los pagos a los diferentes proveedores de bienes y servicios prestados a la Universidad del Cauca. El

lugar donde se encuentra la División Financiera es en la Calle 4 # 5 - 30, Centro histórico de la ciudad de Popayán, Cauca. Las redes de comunicación de la División con otras dependencias dentro de la institución y otras entidades fuera de ella, se hace por medio de correo electrónico institucional soportado por la red de la Universidad del Cauca, como también se comunican por medio del mensajero encargado de prestar el servicio.

Los requisitos de la organización que trata sobre la confidencialidad, disponibilidad e integridad, se dan de la siguiente manera:

- Confidencialidad: los activos de información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.
- Disponibilidad: Los activos de información solo pueden ser obtenidos a corto plazo por los usuarios que tengan permisos adecuados.
- Integridad: El contenido de los activos de información debe permaneces inalterado y completo. Las modificaciones deben ser registradas asegurando su confiabilidad.

Los requisitos estatutarios, reglamentarios y contractuales con los que la Universidad del Cauca debe definir los controles, medidas y responsabilidades específicos para su cumplimiento. Los registros importantes, confidenciales o sensibles de la organización se deben proteger contra la perdida, destrucción y falsificación, por lo tanto se deben guardar de forma segura, para cumplir con los requisitos estatutarios, legales, contractuales. Los funcionarios de la organización y usuarios de terceras partes deben estar informados que no es permitido otro acceso que no sea el autorizado a los sistemas y servicios de los procesamientos de información. Los controles criptográficos i de cifrado que se utilicen en la organización deben cumplir con todos los acuerdos, leyes y reglamentos pertinentes.

Con toda la información recolectada se llega a la identificación de vulnerabilidades, las cuales están asociadas a debilidades de los activos de información. Las vulnerabilidades en el contexto de los sistemas de información, es considerada como la ausencia o debilidad de controles que ayudan a mitigar un riesgo, aumentando el nivel de impacto y el factor de exposición

La lista de vulnerabilidades conocidas de la información, se describen a continuación:

Tipos	Ejemplos de vulnerabilidades
Hardware	Mantenimiento insuficiente /instalación fallida de los medios de almacenamiento.
	Falta de esquemas de reemplazo periódico. Susceptibilidad a la húmeda, el polvo y la suciedad.
	Sensibilidad a la radiación electromagnética
	Falta de control de cambio con configuración eficiente
	Susceptibilidad a las variaciones de tensión
	Susceptibilidad a las variaciones de temperatura
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Falta o insuficiencia de la prueba del software
	Defectos bien conocidos en el software
	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado
	Falta de pruebas de auditoría
	Distribución errada de los derechos de acceso
	Software de distribución amplia
	Utilización de los programas de aplicación a los datos errados en términos de tiempo
	Interface de usuario complicada
	Falta de documentación
	Configuración incorrecta de parámetros
	Fechas incorrectas
	Falta de mecanismos de identificación y autentificación, como la autentificación de usuario
	Tablas de contraseñas sin protección
	Gestión deficiente de las contraseñas
	Habilitación de servicios innecesarios
	Software nuevo o inmaduro
	Especificaciones incompletas o no claras para los desarrolladores
	Falta de control eficaz del cambio
	Descarga y uso no controlados de software
	Falta de copias de respaldo
	Falta de protección física de las puertas y ventanas de la edificación
	Falla en la producción de informes de gestión
	Falta de prueba del envío o la recepción de mensajes
	Líneas de comunicación sin protección

Red	Tráfico sensible sin protección
	Conexión deficiente de los cables.
	Punto único de falla
	Falta de identificación y autentificación de emisor y recepto
	Arquitectura insegura de la red
	Transferencia de contraseñas autorizadas
	Gestión inadecuada de la red (capacidad de recuperación del enrutamiento)
	Conexiones de red pública sin protección
Personal	Ausencia del personal
	Procedimientos inadecuados de contratación
	Entrenamiento insuficiente en seguridad
	Uso incorrecto de software y hardware
	Falta de conciencia acerca de la seguridad
	Falta de mecanismos de monitoreo
	Trabajo no supervisado del personal externo o de limpieza
	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos

Tabla 4: Listado de vulnerabilidades.

4.3. IDENTIFICAR LOS ACTIVOS DENTRO DEL ALCANCE DEL SGSI:

Los activos de información que conforman el área de Recaudos de la División de Gestión Financiera se identifican respondiendo las siguientes preguntas, las cuales se realizaron al personal encargado como el jefe de la división:

Preguntas	Respuestas
¿Qué sistemas el personal de Recaudos necesitan para realizar su trabajo?	Oficina cómoda, mesa grande y cómoda, un equipo de cómputo, radioteléfono, los servidores que contenga las plataformas de SIMCA, SQUID, FINANZAS PLUS.
¿Qué información el personal de Recaudos necesitan para realizar su trabajo?	Recibe la información obtenida del administrador del SQUID y la administración de SIMCA sobre los actos que fijan tasas y directrices en materia de recaudo. Requiere de la copia de los comprobantes de consignación por reintegros o retenciones aplicados en pagos con avances para ser anexadas a la relación.
¿Qué aplicaciones el personal de Recaudos necesitan para realizar su trabajo?	Correo electrónico institucional, sistema integrado de recaudo (SQUID), base de datos de personas inscritas en la

	Universidad, SIMCA, FINANZAS PLUS.
¿Qué servicios el personal de Recaudos necesitan para realizar su trabajo?	Energía eléctrica, servicio de internet, red interna, iluminación planta eléctrica, red telefónica.
¿Qué personas tienen una habilidad especial o conocimiento que es vital para su organización y sería difícil de reemplazar? ¿Qué habilidades tienen estas personas?	Ingeniero de soporte (desarrollo), Técnico administrativo (conocer el proceso y reglamentación institucional), profesional universitario (conocer el proceso y reglamentación institucional).
¿Qué activos intangibles el personal de Recaudos necesita para realizar su trabajo?	Reputación e imagen.

Tabla: Identificación de activos.

De las preguntas anteriores se llega a la identificación de los siguientes activos de información del área de Recaudos de la División de Gestión Financiera:

No	ACTIVOS
1	Bases de Datos
2	Servidores Web
3	Servidores de Aplicaciones
4	Servicio de Correo
5	Sistema Académico Simca
6	SQUID
7	FPL
8	Sistema de Pagos PSE y WEBSERVICES
9	Internet
10	Matrices de Almacenamiento
11	Switches de Comunicación
12	Cableado Estructurado
13	Firewalls
14	Licencias SW
15	Certificados de Seguridad
16	Planta Eléctrica Div TIC
17	Aire acondicionado
18	Planillas de Bancos
19	Soportes de Conciliación
20	Soportes Diarios de Caja
21	Resoluciones
22	Computador

23	Fotocopiadora
24	Impresora
25	Red Telefónica
26	Ficheros
27	Medios Magnéticos
28	Planta Eléctrica Div TIC
29	Recauda y Registra
30	Técnico Administrativo
31	Mensajeros Internos/Externos
32	Tesorero
33	Password
34	Edificio Div TIC
35	Cliente
36	Edificio Div Financiera
37	Planta Eléctrica Div Financiera
38	UPS
39	Red Unicauca
40	Mobiliarios

Tabla: Lista de activos de información.

Para la clasificación de los activos, se tienen los siguientes tipos de:

TIPO	DEFINICION	ACTIVOS
Servicio	Función que satisface una necesidad de los usuarios del servicio. Para la prestación de un servicio los servicios aparecen como activos de un análisis de riesgos bien como servicios finales (prestados por la Organización a terceros), bien como servicios instrumentales (donde los usuarios y los medios son propios), bien como servicios contratados (a otra organización que los proporciona con sus propios medios).	Recauda y Registra.
Datos / Información	Elementos de información que de forma singular o agrupada de alguna forma, representan el conocimiento que se tiene de algo. Los datos son el corazón que permite a una organización prestar sus servicios.	Base de Datos, Resoluciones, Soportes Diarios de Caja, Soportes de Conciliación, Planillas de Bancos, Certificados de Seguridad, Password.
Aplicaciones	Este tipo se refiere a tareas que ha	Servicios de aplicaciones,

(Software)	n sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.	Servicio de correo, Sistema Académico Simca, SQUID, FPL, Sistema de Pagos PSE y Webservices, Firewalls, Licencias SW, Matrices de Almacenamiento.
Equipos informáticos (Hardware)	Dícese de los bienes materiales, físicos, de stinados a soportar directa o indirectamente los servicios que presta la organización, siendo depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del proceso o la transmisión de datos.	Computador, Impresora, Fotocopiadora.
Redes de Comunicaciones	Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.	Servidores Web, Red Unicauca, Cableado Estructurado, Red Telefónica, Internet, Switches de Comunicación.
Soportes de Información	Se consideran dispositivos físicos que perm iten almacenar información de forma permanente o al menos durante largos periodos de tiempo.	Medios Magnéticos (memorias USB, Discos Duros).
Equipamiento Auxiliar	Se consideran dispositivos físicos que per miten almacenar información de forma permanente o al menos durante largos periodos de tiempo.	Mobiliarios, Ficheros, Aire acondicionado, UPS.
Instalaciones	Los lugares donde se hospedan los sistema s de información y comunicaciones.	Edificio Div TIC, Edificio Div Financiera, Planta Eléctrica Div Financiera, Planta Eléctrica Div TIC.
Personal	Aparecen las personas relacionadas con lo s sistemas de información.	Técnico Administrativo, Cliente, Mensajeros Internos/Externos, Tesorero.

Tabla: Clasificación de activos.

4.4. REALIZAR UNA EVALUACION DE LA SEGURIDAD DE LA INFORMACION:

En esta actividad se genera una evaluación de la seguridad de la información.

El estado y evaluación de seguridad de la organización, incluidos los controles de seguridad de la información existente. El área de Recaudos de la División de Gestión Financiera de la Universidad del Cauca, no cuenta con un sistema de seguridad de Información, ni tampoco con controles de seguridad, por lo cual lleva a tomar la decisión de implementar un Sistema de Gestión de Seguridad de la Información (SGSI), debido a que actualmente cuenta con sistemas de información que genera y maneja información crítica.

La Universidad del Cauca desarrolla actividades institucionales relacionadas con el manejo de información, que demanda la necesidad de garantizar su seguridad desde la perspectiva de la confidencialidad, la integridad y la disponibilidad, desde sus procesos administrativos hasta los sistemas de información que los soportan.

Por lo tanto, No existen documentos de las deficiencias de la Universidad del Cauca valoradas o evaluadas por algún sistema de gestión.

UNIVERSIDAD DEL CAUCA

Caso de estudio: Procedimiento de Recaudos en la División de Gestión Financiera.

REALIZAR LA VALORACION DE RIESGOS Y PLANTEAR EL TRATAMIENTO DE RIESGOS.

Código	
Versión:	1.0
Fecha de la versión:	
Creado por:	Milena Cruces – Juan Pablo Mora
Aprobado por:	
Nivel de confidencialidad:	Alto

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación

Tabla de contenido

1. OBJETIVO, REALIZAR LA VALORACION DE RIESGOS Y PLANTEAR EL TRATAMINETO DE RIESOS.

El Objetivo de esta fase es definir la metodología para valorar los riesgos, identificar, analizar y evaluar los riesgos de seguridad de la información para seleccionar las opciones de tratamiento de riesgos, los objetivos de control y controles.

2. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001
- COBIT 5
- [Sistema de gestión de la seguridad de la información de la Universidad del Cauca. Septiembre de 2015]
- [R005 del 7 de Enero de 2015]

- Carta de compromiso de la División de Gestión financiera de la Universidad del Cauca.

3. OBTENCION DE LA VALORACION DE RIESGOS Y PLANTEAR EL TRATAMIENTO DE RIESGOS.

Para llegar a obtener la valoración de riesgos y plantear el tratamiento de riesgos se recomienda la identificación, la evaluación y la planificación del tratamiento de riesgos, la selección de los objetivos de control y de los controles son pasos importantes en la implementación de un SGSI y se recomienda tenerlos en cuenta en esta etapa.

Para llegar a la obtención de la valoración de riesgos y plantear el tratamiento de riesgos se tienen los siguientes numerales:

3.1. PANORAMA GENERAL DE LA REALIZACION DE LA VALORACION DE RIESGOS Y PLANIFICACION DEL TRATAMIENTO DE RIESGOS.

La División Financiera se encuentra en constantes amenazas y riegos, por lo que se requiere estar preparados para cualquier imprevisto, de esta forma reaccionar instantáneamente para responder con medidas adecuadas y eficientes, siendo necesario la implementación de un Sistema de Gestión de Seguridad de la Información con el cual se analizaran los posibles riesgos, de esta manera poder solventarlos con controles y medidas que puedan evaluar su impacto, y de este modo anticipar cualquier circunstancia que derive en problemas, mediante la elaboración de un plan estratégico, para lograr prevenir y responder ante cualquier posible amenaza.

3.2. REALIZAR LA VALORACION DE RIESGOS:

La División de Gestión Financiera de la Universidad del Cauca, se encuentra en constantes amenazas y riegos por diversos factores que ponen en peligro la información, estas pueden proceder desde el interior o exterior de la Universidad. Por ello, es

necesaria la seguridad de la información, lo cual se puede lograr al implementar un SGSI cuyo objetivo es reconocer, relevar, controlar, garantizar y registrar los recursos financieros a los cuales la universidad tiene derecho, enmarcados en la normatividad bancaria, presupuestal, legal y contable vigente para el cumplimiento de la misión social.

Dicho lo anterior, el método de las elipses, permite inicialmente distinguir a la División de Gestión Financiera los procedimientos con sus respectivas actividades y a cada proceso identificarle su respectivo subprocesos.

El método de las elipses permite determinar los procedimientos de la División de Gestión Financiera que conforman el proceso, a cada procedimiento se le identifican sus respectivos procedimientos ; en la elipse intermedia, se determinan las diferentes relaciones que los procedimientos de la elipse concéntrica tiene con otros procesos de la Universidad del Cauca; y finalmente en la elipse externa, se resaltan aquellas organizaciones que no hacen parte de la Universidad del Cauca pero tienen algún tipo de interacción con los procesos y subprocesos de la elipse concéntrica.

La Metodología de Evaluación del Riesgo, propone un organigrama que establece los roles necesarios y como se vinculan entre sí en cada una de las etapas de implementación del SGSI. Esta metodología, se emplea para realizar la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos que estén relacionados a los activos de información, mencionados en el alcance. Este proceso es dirigido a estimar la magnitud de aquellos riesgos que no hayan podido evitarse de alguna manera. Es por eso que se decide probar a COBIT 5, el cual por medio de un estudio de Jonathan Carrillo llamado “Gestión del Riesgo en las Metodologías de Proyectos de Tecnologías de Información y Comunicaciones” permite concluir que puede ser apta para el desarrollo.

3.3. SELECCIONAR LOS OBJETIVOS DE CONTROL Y LOS CONTROLES:

Cobit 5 utiliza un modelo de procesos de mejora continua que ayuda al cumplimiento de metas TI las cuales aseguran el cumplimiento de las metas empresariales, manteniendo así un nivel operativo que asegura el valor de la entidad.

A continuación se crearan tres objetivos relacionados directamente con la seguridad de la información, políticas, activos, riesgo entre otros, que van ligados a los objetivos de esta tesis, de esta forma posteriormente identificar las metas empresariales y las metas TI, que nos llevaran a encontrar los procesos planteados en COBIT 5.

1. *Mejorar y mantener las habilidades del personal de tal forma que su cocimiento vaya enfocado en el desempeño de actividades relacionadas con las Tecnologías de la Información.*

Se bebe de educar al personal en TI para que tenga una mayor productividad, así como la realización de capacitaciones y actividades que mejoren sus habilidades, adquieran buenas prácticas y desarrollen metodologías para el desarrollo e implantación de software.

2. *Mejorar la infraestructura de TI disponible mediante la optimización de costos que permitan invertir en medidas de seguridad para de esta forma conseguir los diferentes objetivos y metas planteadas en la entidad.*

Consiste en permitir la protección y salvaguardar la información confidencial gracias al mejoramiento y actualización de la infraestructura que se maneja en la entidad, así como actualización de software y cambio de equipos obsoletos, todo esto a través de la optimización de los costos.

3. *Identificar, analizar, evaluar y reducir los riesgos en la entidad a través de la implementación de un sistema de seguridad de la información que cumpla las políticas internas.*

Se enfoca directamente en la creación de un SGSI, que identifique activos y escenarios de riesgo, así como evaluarlos y crear un plan estratégico para la respuesta a los riesgos y se debe de crear políticas de seguridad que cumpla con la normativa interna y externa.

			Tipo de Riesgo			
No	**Ref de COBIT 5**	**Categoría de escenario de Riesgo**	**Habilitación de beneficio/valor para TI**	**Entrega de programas y proyectos de TI**	**Entrega de operaciones y servicios de TI**	**Escenarios Negativos**
1	301	Toma de decisiones sobre inversiones en TI	P		S	Los gerentes de negocios o sus representantes no se involucran en las decisiones importantes sobre inversiones de TI (p.ej. nuevas aplicaciones u oportunidades tecnológicas, priorizaciones).
2	401	Pericia y Habilidades TI	P	P	P	Faltan habilidades de TI o son incompatibles, por ejemplo: debido a nuevas tecnologías.
3	408		S	P	P	Existe una dependencia excesiva del personal clave de TI.
4	409		S	P	P	Existe una incapacidad para actualizar las habilidades de TI a un nivel apropiado a través del entrenamiento.
5	502	Operaciones del personal (error humano e interno malicioso)	S		P	El equipo de TI es dañado accidentalmente por el personal.
6	503		S		P	Existen errores cometidos por el personal (durante las actualizaciones del sistema, copias de respaldo, mantenimiento)
7	504		S		P	La información es ingresada incorrectamente por el personal.
8	505		S		P	El centro de datos es destruido (por sabotaje, etc.) por el personal.
9	506		S		P	Un dispositivo con datos sensibles es robado por un miembro del personal.
10	507		S		P	Un componente clave de la infraestructura es robado por un miembro del personal.
11	509		S		P	Se configuran erróneamente los componentes

						de hardware.
12	510		S		P	El hardware fue dañado intencionadamente (dispositivos de seguridad, etc.)
13	601	Información (brecha de datos: daño, fuga y acceso)	S		P	El personal interno ha dañado componentes de hardware, lo que conlleva la destrucción (parcial) de los datos informáticos.
14	602		S	S	P	La base de datos está corrupta, lo cual hace inaccesible a los datos.
15	603		S	S	P	Perdida y Revelación de medios portátiles que contiene datos sensibles de información (CD, USB, discos portátiles, etc.)
16	604		S	S	P	Se pierden y se revelan datos sensibles mediante ataques lógicos.
17	605		S	S	P	Se pierden o no se verifica la efectividad de los medios que contienen las copias de respaldo.
18	606		P	S	P	Se revela información sensible en forma accidental debido a fallas en el seguimiento de las guías de manejo de información.
19	607		P	S	P	Se modifican intencionadamente los datos (contables, vinculados a la seguridad, información, etc.)
20	608		P	S	P	Se revela información sensible a través del correo electrónico.
21	609		P	S	P	Se revela información sensible debido a ineficientes procedimiento de retención/archivo y eliminación.
22	801	Infraestructura (hardware, sistemas operativos y tecnologías de control)	P	S	P	Se instala infraestructura nueva (innovadora) y como resultado los sistemas se tornan inestables, lo que lleva a incidentes operativos.
23	802		P	S	P	Los sistemas no pueden manejar los volúmenes de transacciones cuando estos se incrementan.
24	803		P	S	P	Los sistemas no pueden manejar la carga que se genera cuando se despliegan nuevas aplicaciones o iniciativas.
25	804		P	S	P	Existen fallas intermitentes en los servicios (telecomunicaciones, electricidad).
26	806				P	Fallas en el hardware por exceso de calor.
27	901	Software	P		S	No existen habilidades en el uso del software para materializar los resultados deseados (por ejemplo: fallas al implementar los modelos de negocio o los cambios requeridos).
28	902		P		S	Se implementa software inmaduro (adopción temprana, fallos, etc.)
29	903		P		S	Se selecciona e implementa software equivocado según costos, desempeño, características, compatibilidad, etc.
30	904		P		S	Existen dificultades operativas cuando se pone un nuevo software en producción.
31	905		P		S	Los usuarios no pueden utilizar ni explotar nuevo software aplicativo.
32	906		P		S	Modificación intencional del software conduce a datos erróneos o acciones fraudulentas.

33	907		P		S	Modificación no intencional del software conduce a resultados inesperados.
34	908		P		S	Ocurren errores no intencionales en la gestión de configuraciones y de cambios.
35	909		P		S	Pude ocurrir fallas en el funcionamiento del software o de las aplicaciones críticas.
36	910		P		S	Pocas veces, ocurren problemas con el software de sistemas importantes.
37	1105	Selección / desempeño del proveedor, cumplimiento contractual, discontinuidad del servicio y trasferencia.		S	P	Pueden existir incumplimientos de las licencias de software (uso y/o distribución de software sin las correspondientes licencias, etc.)
38	1106			S	P	Incapacidad para transferir a provisores alternativos debido a una confianza excesiva en el provisor actual.
39	1201	Cumplimiento regulatorio	P	S	S	No se cumple con regulaciones, que tienen que ver con la privacidad, contabilidad, manufactura, etc.
40	1202		P	S	S	El desconocimiento de cambios potenciales en la regulación tiene un impacto en el ambiente operativo
41	1401	Robo o destrucción de la infraestructura	S	S	P	Se ha producido el robo de un dispositivo con datos sensibles.
42	1403		S	S	P	Se destruye el centro de datos (sabotaje, etc.).
43	1404		S	S	P	Dispositivos individuales se destruyen accidentalmente.
44	1501	Código Maliciosos	S		P	Se ha producido una intrusión de código malicioso en los servidores operativos.
45	1502		S		P	Los computadores portátiles se infectan frecuentemente con código malicioso.
46	1503		S		P	Un empleado insatisfecho implementa una bomba lógica que produce la pérdida de datos importantes.
47	1504		S		P	Roban los datos de la compañía a través de accesos no autorizados obtenidos mediante ataques.
48	1601	Ataques lógicos	S		P	Usuarios no autorizados tratan de forzar el ingreso a los sistemas.
49	1605		S		P	Existen ataques de virus.
50	1701	Acción industrial	S	S	P	No es posible acceder a las instalaciones y edificios debido a una huelga gremial.
51	1702		S	S	P	El personal clave no se encuentra disponible debido a impedimentos de la industria (por ejemplo, huelga en el transporte).
52	1801	Ambiental	S	S	P	El equipamiento utilizado no es amigable en cuanto al medio ambiente (por ejemplo, en el consumo de energía, embalajes, etc.)
53	1901	Actos de la Naturaleza	S	S	P	Hay un terremoto.
54	1903		S	S	P	Hay fuertes tormentas y ciclones tropicales.
55	1904		S	S	P	Hay un gran incendio fuera de control.

Teniendo seleccionados los Escenarios de Riesgos, se procede a su evaluación. Esta evaluación se hace considerando calificaciones al probable impacto de ocurrencia en caso de que el riesgo se materialice; y la frecuencia con la posibilidad de ocurrencia del riesgo.

Cabe mencionar, el riesgo es la probabilidad de que un evento ocurra y cause consecuencias (daños o pérdidas) que afecten la habilidad de alcanzar los objetivos; este se mide a través de la probabilidad de que una amenaza se materialice explotando una vulnerabilidad ocasionando así un impacto.

No	Ref de COBIT 5	Categoría de escenario de Riesgo	Escenarios Negativos	Impacto	Frecuencia	Riesgo
1	105	Establecimiento y mantenimiento del portafolio.	Desconocimiento de las Políticas de TI.	8	5	40
2	207	Gestión del ciclo de vida del programa o proyecto	Degradación de la imagen de la entidad por su incapacidad para responder oportuna y asertivamente contra incidentes que afectan a los servicios entregados por proyectos ineficientes.	5	2	10
3	301	Toma de decisiones sobre inversiones en TI	Los gerentes de negocios o sus representantes no se involucran en las decisiones importantes sobre inversiones de TI (por ejemplo: nuevas aplicaciones u oportunidades tecnológicas, priorizaciones).	5	4	20
4	401	Pericia y Habilidades TI	Faltan habilidades de TI o son incompatibles, por ejemplo: debido a nuevas tecnologías.	5	3	15
5	408		Existe una dependencia excesiva del personal clave de TI.	8	5	40
6	409		Existe una incapacidad para actualizar las habilidades de TI a un nivel apropiado a través del entrenamiento.	8	3	24
7	411		Falta de inversión en profesionales para el área debido al exceso desconfianza en el personal de TI	5	1	5
8	412		Falta de concientización y participación del personal en acciones preventivas que se direccionen a evitar los riesgos de salud y seguridad en el trabajo.	5	1	5
9	502	Operaciones del personal (error humano e interno malicioso)	El equipo de TI es dañado accidentalmente por el personal.	8	2	16
10	503		Existen errores cometidos por el personal (durante las actualizaciones del sistema, copias de respaldo, mantenimiento)	8	3	24
11	504		La información es ingresada incorrectamente por el personal.	8	4	32
12	505		El centro de datos es destruido (por sabotaje, etc.) por el personal.	8	2	16
13	506		Un dispositivo con datos sensibles es robado por un miembro del personal.	8	3	24
14	507		Un componente clave de la infraestructura es robado por un miembro del personal.	5	3	15
15	509		Se configuran erróneamente los componentes de hardware.	5	3	24
16	510		El hardware fue dañado intencionadamente (dispositivos de seguridad, etc.)	5	1	5
17	601		El personal interno ha dañado componentes de hardware, lo que conlleva la destrucción (parcial) de los datos informáticos.	8	1	8
18	602		La base de datos está corrupta, lo cual hace inaccesible a los datos.	8	1	8

19	603	Información (brecha de datos: daño, fuga y acceso)	Perdida y Revelación de medios portátiles que contiene datos sensibles de información (CD, USB, discos portátiles, etc.)	8	3	24
20	604		Se pierden y se revelan datos sensibles mediante ataques lógicos.	8	3	24
21	605		Se pierden o no se verifica la efectividad de los medios que contienen las copias de respaldo.	5	4	20
22	606		Se revela información sensible en forma accidental debido a fallas en el seguimiento de las guías de manejo de información.	8	4	32
23	607		Se modifican intencionadamente los datos (contables, vinculados a la seguridad, información, etc.)	8	5	40
24	608		Se revela información sensible a través del correo electrónico.	5	2	10
25	609		Se revela información sensible debido a ineficientes procedimiento de retención/archivo y eliminación.	8	3	24
26	612		Filtración de la información debido al abandono del equipo de la institución.	8	5	40
27	613		Falta de un plan de continuidad que imposibilita responder a incidentes e interrupciones de servicios.	5	2	10
28	801	Infraestructura (hardware, sistemas operativos y tecnologías de control)	Se instala infraestructura nueva (innovadora) y como resultado los sistemas se tornan inestables, lo que lleva a incidentes operativos.	5	1	5
29	802		Los sistemas no pueden manejar los volúmenes de transacciones cuando estos se incrementan.	3	1	3
30	803		Los sistemas no pueden manejar la carga que se genera cuando se despliegan nuevas aplicaciones o iniciativas.	2	1	2
31	804		Existen fallas intermitentes en los servicios (telecomunicaciones, electricidad).	8	4	32
32	806		Fallas en el hardware por exceso de calor.	2	1	2
33	807		Fallas en los registros y definición de acceso a los activos físicos de TI o el uso de dispositivos por parte del usuario para tratamiento de la información.	5	4	20
34	901	Software	No existen habilidades en el uso del software para materializar los resultados deseados (por ejemplo: fallas al implementar los modelos de negocio o los cambios requeridos).	8	2	16
35	902		Se implementa software inmaduro (adopción temprana, fallos, etc.)	5	1	5
36	903		Se selecciona e implementa software equivocado según costos, desempeño, características, compatibilidad, etc.	5	2	10
37	904		Existen dificultades operativas cuando se pone un nuevo software en producción.	5	1	5
38	905		Los usuarios no pueden utilizar ni explotar nuevo software aplicativo.	2	1	2
39	906		Modificación intencional del software conduce a datos erróneos o acciones fraudulentas.	3	1	3
40	907		Modificación no intencional del software conduce a resultados inesperados.	5	3	15
41	908		Ocurren errores no intencionales en la gestión de configuraciones y de cambios.	8	4	32
42	909		Pude ocurrir fallas en el funcionamiento del software o de las aplicaciones críticas.	2	1	2
43	910		Ocurren problemas con el software de sistemas importantes.	2	1	2
44	1105	Selección/ desempeño del proveedor, cumplimiento contractual, discontinuidad del	Pueden existir incumplimientos de las licencias de software (uso y/o distribución de software sin las correspondientes licencias, etc.)	8	2	16
45	1106		Incapacidad para transferir a provisores alternativos debido a una confianza excesiva en el provisor actual.	3	2	6

		servicio y trasferencia.				
46	1201	Cumplimiento regulatorio	No se cumple con regulaciones, que tienen que ver con la privacidad, contabilidad, manufactura, etc.	5	2	10
47	1202		El desconocimiento de cambios potenciales en la regulación tiene un impacto en el ambiente operativo	8	3	24
48	1401	Robo o destrucción de la infraestructura	Se ha producido el robo de un dispositivo con datos sensibles.	8	5	40
49	1403		Se destruye el centro de datos (sabotaje, etc.).	8	5	40
50	1404		Dispositivos individuales se destruyen accidentalmente.	8	4	32
51	1405		Ineficiencia o ausencia de dispositivos que detectan las amenazas del entorno, debido a la falta de supervisión, mantenimiento y actualización de los mismos.	5	5	25
52	1406		Libre acceso a las instalaciones de procesamiento sin peticiones formales.	8	5	40
53	1501	Código Maliciosos	Se ha producido una intrusión de código malicioso en los servidores operativos.	8	1	8
54	1502		Los computadores portátiles se infectan frecuentemente con código malicioso.	8	2	16
55	1503		Un empleado insatisfecho implementa una bomba lógica que produce la pérdida de datos importantes.	8	5	40
56	1504		Roban los datos de la compañía a través de accesos no autorizados obtenidos mediante ataques.	8	5	40
57	1505		Desactualización de los usuarios respecto a configuraciones de tráfico entrante, uso de correos electrónicos, contraseñas y descargas lo cual facilita el acceso de software.	5	5	25
58	1601	Ataques lógicos	Usuarios no autorizados tratan de forzar el ingreso a los sistemas.	8	5	40
59	1605		Existen ataques de virus.	3	2	6
60	1701	Acción industrial	No es posible acceder a las instalaciones y edificios debido a una huelga gremial.	3	2	6
61	1702		El personal clave no se encuentra disponible debido a impedimentos de la industria (por ejemplo, huelga en el transporte).	5	2	10
62	1801	Ambiental	El equipamiento utilizado no es amigable en cuanto al medio ambiente (por ejemplo, en el consumo de energía, embalajes, etc.)	8	3	24
63	1901	Actos de la Naturaleza	Hay un terremoto.	8	5	40
64	1903		Hay fuertes tormentas y ciclones tropicales.	8	5	40
65	1904		Hay un gran incendio fuera de control.	8	5	40

Finalmente con el análisis anteriormente realizado sobre la gestión de riesgos concluye en la presentación del Plan de Acciones para el Tratamiento de los Riesgos, en el que se sintetiza los riesgos con su respectivo nivel, las actividades, responsables e indicadores para evaluar la eficiencia de dichas medidas. Adicionalmente se define el nivel de respuesta al riesgo que se va a alcanzar con las acciones propuestas en el caso de ser implementadas.

Ref. de COBIT		**Respuesta**

	Escenarios Negativos	Mitigar	Compartir / Trasferir	Aceptar	Evitar
105	Desconocimiento de las Políticas de TI.				
207	Degradación de la imagen de la entidad por su incapacidad para responder oportuna y asertivamente contra incidentes que afectan a los servicios entregados por proyectos ineficientes.				
301	Los gerentes de negocios o sus representantes no se involucran en las decisiones importantes sobre inversiones de TI (por ejemplo: nuevas aplicaciones u oportunidades tecnológicas, priorizaciones).				
401	Faltan habilidades de TI o son incompatibles, por ejemplo: debido a nuevas tecnologías.				
408	Existe una dependencia excesiva del personal clave de TI.				
409	Existe una incapacidad para actualizar las habilidades de TI a un nivel apropiado a través del entrenamiento.				
411	Falta de inversión en profesionales para el área debido al exceso desconfianza en el personal de TI				
412	Falta de concientización y participación del personal en acciones preventivas que se direccionen a evitar los riesgos de salud y seguridad en el trabajo.				
502	El equipo de TI es dañado accidentalmente por el personal.				
503	Existen errores cometidos por el personal (durante las actualizaciones del sistema, copias de respaldo, mantenimiento)				
504	La información es ingresada incorrectamente por el personal.				
505	El centro de datos es destruido (por sabotaje, etc.) por el personal.				
506	Un dispositivo con datos sensibles es robado por un miembro del personal.				
507	Un componente clave de la infraestructura es robado por un miembro del personal.				
509	Se configuran erróneamente los componentes de hardware.				
510	El hardware fue dañado intencionadamente (dispositivos de seguridad, etc.)				
601	El personal interno ha dañado componentes de hardware, lo que conlleva la destrucción (parcial) de los datos informáticos.				
602	La base de datos está corrupta, lo cual hace inaccesible a los datos.				
603	Pérdida y Revelación de medios portátiles que contiene datos sensibles de información (CD, USB, discos portátiles, etc.)				
604	Se pierden y se revelan datos sensibles mediante ataques lógicos.				
605	Se pierden o no se verifica la efectividad de los medios que contienen las copias de respaldo.				

606	Se revela información sensible en forma accidental debido a fallas en el seguimiento de las guías de manejo de información.				
607	Se modifican intencionadamente los datos (contables, vinculados a la seguridad, información, etc.)				
608	Se revela información sensible a través del correo electrónico.				
609	Se revela información sensible debido a ineficientes procedimiento de retención/archivo y eliminación.				
612	Filtración de la información debido al abandono del equipo de la institución.				
613	Falta de un plan de continuidad que imposibilita responder a incidentes e interrupciones de servicios.				
801	Se instala infraestructura nueva (innovadora) y como resultado los sistemas se tornan inestables, lo que lleva a incidentes operativos.				
802	Los sistemas no pueden manejar los volúmenes de transacciones cuando estos se incrementan.				
803	Los sistemas no pueden manejar la carga que se genera cuando se despliegan nuevas aplicaciones o iniciativas.				
804	Existen fallas intermitentes en los servicios (telecomunicaciones, electricidad).				
806	Fallas en el hardware por exceso de calor.				
807	Fallas en los registros y definición de acceso a los activos físicos de TI o el uso de dispositivos por parte del usuario para tratamiento de la información.				
901	No existen habilidades en el uso del software para materializar los resultados deseados (por ejemplo: fallas al implementar los modelos de negocio o los cambios requeridos).				
902	Se implementa software inmaduro (adopción temprana, fallos, etc.)				
903	Se selecciona e implementa software equivocado según costos, desempeño, características, compatibilidad, etc.				
904	Existen dificultades operativas cuando se pone un nuevo software en producción.				
905	Los usuarios no pueden utilizar ni explotar nuevo software aplicativo.				
906	Modificación intencional del software conduce a datos erróneos o acciones fraudulentas.				
907	Modificación no intencional del software conduce a resultados inesperados.				
908	Ocurren errores no intencionales en la gestión de configuraciones y de cambios.				
909	Pude ocurrir fallas en el funcionamiento del software o de las aplicaciones críticas.				
910	Ocurren problemas con el software de sistemas importantes.				
1105	Pueden existir incumplimientos de las licencias de software (uso y/o distribución de software sin las correspondientes licencias, etc.)				
1106	Incapacidad para transferir a provisores alternativos debido a una confianza excesiva en el provisor actual.				

1201	No se cumple con regulaciones, que tienen que ver con la privacidad, contabilidad, manufactura, etc.				
1202	El desconocimiento de cambios potenciales en la regulación tiene un impacto en el ambiente operativo				
1401	Se ha producido el robo de un dispositivo con datos sensibles.				
1403	Se destruye el centro de datos (sabotaje, etc.).				
1404	Dispositivos individuales se destruyen accidentalmente.				
1405	Ineficiencia o ausencia de dispositivos que detectan las amenazas del entorno, debido a la falta de supervisión, mantenimiento y actualización de los mismos.				
1406	Libre acceso a las instalaciones de procesamiento sin peticiones formales.				
1501	Se ha producido una intrusión de código malicioso en los servidores operativos.				
1502	Los computadores portátiles se infectan frecuentemente con código malicioso.				
1503	Un empleado insatisfecho implementa una bomba lógica que produce la pérdida de datos importantes.				
1504	Roban los datos de la compañía a través de accesos no autorizados obtenidos mediante ataques.				
1505	Desactualización de los usuarios respecto a configuraciones de tráfico entrante, uso de correos electrónicos, contraseñas y descargas lo cual facilita el acceso de software.				
1601	Usuarios no autorizados tratan de forzar el ingreso a los sistemas.				
1605	Existen ataques de virus.				
1701	No es posible acceder a las instalaciones y edificios debido a una huelga gremial.				
1702	El personal clave no se encuentra disponible debido a impedimentos de la industria (por ejemplo, huelga en el transporte).				
1801	El equipamiento utilizado no es amigable en cuanto al medio ambiente (por ejemplo, en el consumo de energía, embalajes, etc.)				
1901	Hay un terremoto.				
1903	Hay fuertes tormentas y ciclones tropicales.				
1904	Hay un gran incendio fuera de control.				

Tabla: Respuesta al Riesgo.

3.4. OBTENER LA AUTORIZACION DE LA DIRECCION PARA IMPLEMENTAR Y OPERAR UN SGSI:

Lista de Escenarios de Riesgos Calificados de tipo Riesgo Inaceptable.												
				Actividades								
				Activo / Recurso					Responsables			
Ref. de COBIT 5	Escenario de Riesgo	Nivel de Riesgo	Descripción	Personas y habilidades	Estructuras Organizativas	Infraestructuras	Información	Aplicaciones	Responsable ¿Quién hace?	Rinde Cuentas ¿Quién comunica?	Métricas Relacionadas	
105	Desconocimiento de las Políticas de TI.	40	Diseñar y plantear políticas para garantizar el control de la Div de Gestión Financiera.						Institución: Jefe de la Vicerrectoría Administrativa y jefe de la Div de Gestión Financiera	Jefe de la Div Gestión Financiera	Políticas soportadas por estándares y prácticas internacionales, certificadas. Por tanto realizar frecuentemente la revisión y actualización de las políticas, las cuales deben ser documentadas y actualizadas.	
301	Los gerentes de negocios o sus representantes no se involucran en las decisiones importantes sobre inversiones de TI (por ejemplo: nuevas aplicaciones u oportunidades tecnológicas, priorizaciones).	20	Involucrarse en las decisiones importantes sobre las inversiones, las cuales permitan dar opiniones respecto a los beneficios que se tengan a la nueva tecnología.						Institución: Jefe de la Vicerrectoría Administrativa, jefe y personal de la Div de Gestión Financiera.	Jefe de la Div Gestión Financiera	Número de empleados identificados frente a los conocimientos de las nuevas aplicaciones u oportunidades tecnológicas.	
408	Existe una dependencia excesiva del personal clave de TI.	40	Identificar las competencias y habilidades del personal para que no exista dependencia entre ellos.						Institución: el Jefe de la y el personal encargado de cada una de las dependencia que conforman la Div de Gestión Financiera.	Personal Div Gestión Financiera	Número de empleados evaluados según sus competencias del área de Recaudos.	
409	Existe una incapacidad para actualizar las habilidades de TI	24	Gestionar la creación de foros de capacitación en temas de						Institución: Jefe de la Vicerrectoría	Jefe de la Div Gestión	Nivel de satisfacción de las partes interesadas con la capacitación	

	a un nivel apropiado a través del entrenamiento.		ocurrencia cotidiana evitando la generación de trámites extensos.						Administrativa junto al jefe de la Div de Gestión Financiera.	Financiera	del personal con los programas y servicios planeados.
503	Existen errores cometidos por el personal (durante las actualizaciones del sistema, copias de respaldo, mantenimiento)	24	Desarrollar un plan de mantenimiento de los errores cometidos y tratarlos de manera que resuelvan los problemas para adquirir las copias de respaldo.						Institución: personal de la Div de Gestión Financiera, encargado de los sistemas de copias de respaldo	Personal Div Gestión Financiera	Número de incidentes significativos relacionados por errores cometidos que no fueron identificados en la evaluación de riesgos.
504	La información es ingresada incorrectamente por el personal.	32	Implementar mecanismos de protección ante el ingreso de información errada.						Institución: personal de la Div de Gestión financiera, encargado de corroborar e ingresar datos correctamente al sistema.	Técnico Administrativo	Número de incidentes significativos relacionados por ingresar incorrectamente la información que no fueron identificados en la evaluación de riesgos.
506	Un dispositivo con datos sensibles es robado por un miembro del personal.	16	Definir políticas de control relacionadas con los dispositivos ingresados y salientes de la Div Financiera.						Institución: el jefe y la Seguridad privada contratada para la Div de Gestión Financiera.	Personal Div Gestión Financiera	Porcentaje de inversiones de TI en los que la realización del beneficio se monitoriza través del ciclo de vida económico completo.
509	Se configuran erróneamente los componentes de hardware.	24	Capacitar al personal ante la configuración de hardware.						Institución: personal encargado del manejo de hardware de la Div de Gestión Financiera	Técnico Administrativo	Número de vulnerabilidades. Porcentaje de pruebas periódicas de los dispositivos de seguridad.
603	Pérdida y Revelación de medios portátiles que contiene datos sensibles de información (CD, USB, discos portátiles, etc.)	24	Proveer el fácil reconocimiento ante la pérdida de dispositivos que contengan información sensible.						Institución: el jefe y la Seguridad privada contratada para la Div de Gestión Financiera.	Personal Div Gestión Financiera	Número de incidentes identificados por pérdida y revelación de información sensible.
604	Se pierden y se revelan datos sensibles mediante ataques lógicos.	24	Implementar mecanismos de protección ante la manipulación de ataques lógicos.						Institución: Unidad de operación de Sistemas informáticos.	Jefe de la Div Gestión Financiera	Porcentaje de mejoras acordadas que han sido reflejadas. Porcentaje de asuntos identificados que se han incluido satisfactoriamente.
605	Se pierden o no se verifica la efectividad de los medios que contienen las copias de respaldo.	20	Verificación y actualización de los medios que contienen información sensible.						Institución: jefe de la DIv de Gestión Financiera. Jefe de la Div de las TIC.	Jefe de la Div Gestión Financiera	Nivel de concienciación y comprensión de las posibilidades de la pérdida de las copias de respaldo.
606	Se revela información sensible en forma accidental debido a fallas en el seguimiento de las guías de manejo de información.	32	Implementar mecanismos de protección de información, en los diferentes sistemas que se maneja información sensible.						Institución: personal y jede de la Div de Gestión Financiera. jefel y el personal encargado de las Base de datos de la Div TIC	Personal Div Gestión Financiera	Nivel de concienciación y comprensión de las posibilidades de la revelación de información sensible de la institución.

607	Se modifican intencionadamente los datos (contables, vinculados a la seguridad, información, etc.)	40	Identificar, analizar y confirmar las modificaciones de los datos, que se desean cambiar teniendo presente la autorización del jefe.						Institución: personal encargado del control de datos sensibles de institución.	Técnico Administrativo	Número de vulnerabilidades. Nivel de conciencia ante las modificaciones de los datos delicados de la institución.
609	Se revela información sensible debido a ineficientes procedimientos de retención / archivo y eliminación.	24	Capacitar adecuadamente al personal encargado de la retención/archivo y eliminación de información.						Institución: personal encargado de archivar la información tanto en la Div de Gestión Financiera como de la Div de las TIC.	Técnico Administrativo	Porcentaje de puestos vacantes. Frecuencia de las evaluaciones del personal entrante como antiguo.
612	Filtración de la información debido al abandono del equipo de la institución.	40	Dejar el equipo apagado o bloqueado al momento de tener que abandonarlo.						Institución: jefe, personal de la Div de Gestión Financiera.	Personal Div Gestión Financiera	Número de vulnerabilidades. Nivel de conciencia ante la filtración de información debido al abandono del equipo de trabajo.
804	Existen fallas intermitentes en los servicios (telecomunicaciones, electricidad).	32	Instalar equipamiento de buena calidad y de alerta inmediata al momento de alguna falla de los servicios de telecomunicaciones o de electricidad.						Institución: Jefe de la Div de las TIC. Unidad de operaciones de sistemas informáticos.	Jefe DIv TIC	Número de interrupciones del negocio debidas a incidentes en el servicio de telecomunicaciones, electricidad.
807	Fallas en los registros y definición de acceso a los activos físicos de TI o el uso de dispositivos por parte del usuario para tratamiento de la información.	20	Registrar y emplear el uso dispositivos capaces de robar algún tipo de información como al acceso a los activos físicos de TI.						Institución: seguridad privada de las instalaciones de la Div de Gestión Financiera.	Personal Div Gestión Financiera	Porcentaje de tipos de eventos operativos críticos cubiertos por los sistemas de detección automática.
908	Ocurren errores no intencionales en la gestión de configuraciones y de cambios.	32	Gestionar de inmediato el tratamiento frente a los errores cometidos no intencionales.						Institución: Rectoría, Vicerrectoría Administrativa, Div de Gestión Financiera, Div de las TIC.	Técnico Administrativo	Número de incidentes que impliquen dispositivos de usuario final. Número de dispositivos de usuario final no autorizados detectados en la red o en el entorno.
1202	El desconocimiento de cambios potenciales en la regulación tiene un impacto en el ambiente operativo	24	Informar y Capacitar al personal de los cambios que tienen un impacto en el ambiente operativo.						Institución: Consejo Superior, Rectoría, Vicerrectoría Administrativa, Div de Gestión Financiera, Div de las TIC.	Personal Div Gestión Financiera	Número de incidentes que impliquen el desconocimiento de cambios potenciales.
1401	Se ha producido el robo de un dispositivo con datos sensibles.	40	Registras los dispositivos de la Div Financiera que al momento de salir puedan ser fácilmente identificados por los miembros de seguridad.						Institución: compañía de seguridad privada de las instalaciones de la Div de Gestión Financiera.	Jefe de la Div Gestión Financiera	Número de incidentes de seguridad causantes por la pérdida de robo de un dispositivo con datos sensibles. Interrupciones del servicio o

											pérdida de imagen así como también los relacionados con seguridad física.
1403	Se destruye el centro de datos (sabotaje, etc.).	40	Tener el adecuado control de vigilancia de cámaras al centro de datos.						Institución: compañía de seguridad privada de las instalaciones de la Div de Gestión Financiera y la Div de las TIC.	Jefe DIv TIC	Número de incidentes por la destrucción del centro de datos. Interrupciones del servicio o pérdida de imagen así como también los relacionados con seguridad física.
1404	Dispositivos individuales se destruyen accidentalmente.	32	Adquirir el conocimiento adecuado del funcionamiento de dispositivos.						Institución: personal de la Div de Gestión Financiera y de la Div de las TIC.	Personal Div Gestión Financiera	Número de vulnerabilidades. Nivel de conciencia ante la destrucción de dispositivos delicados de la Div de Gestión Financiera.
1405	Ineficiencia o ausencia de dispositivos que detectan las amenazas del entorno, debido a la falta de supervisión, mantenimiento y actualización de los mismos.	25	Instalación de equipos capaces de la Identificación amenazas en el entorno.						Institución: Consejo Superior, Rectoría, Vicerrectoría Administrativa, Div de Gestión Financiera, Div de las TIC.	Rectoría	Número de vulnerabilidades. Nivel de conciencia ante la ausencia de dispositivos que detectan las amenazas del entorno de la Div de Gestión Financiera.
1406	Libre acceso a las instalaciones de procesamiento sin peticiones formales.	40	Registrar y emplear el uso de tarjetas o placas de identidad con su previa autorización y supervisión a todos los visitantes de las instalaciones.						Institución: Vicerrectoría Administrativa, Div de Gestión Financiera, Div de las TIC.	Jefe de la Div Gestión Financiera	Porcentaje de usuarios registrados y entregados tarjetas o placas de autorización para su ingreso a las diferentes áreas administrativas de la universidad. Porcentaje del personal que se actualizado su acceso.
1503	Un empleado insatisfecho implementa una bomba lógica que produce la pérdida de datos importantes.	40	Control y evaluación al personal de la Div Financiera frente a sus respectivos puestos de trabajo.						Institución: personal de la Div de Gestión Financiera.	Jefe de la Div Gestión Financiera	Número de vulnerabilidades. Porcentaje de pruebas periódicas de los empleados para saber el grado de satisfacción en el que se encuentren.
1504	Roban los datos de la Div de Gestión Financiera, a través de accesos no autorizados obtenidos mediante ataques.	40	Instalación de cámaras para el control de los lugares donde se tiene información sensible de la DIv Financiera						Institución: Consejo Superior, Rectoría, Vicerrectoría Administrativa, Div de Gestión Financiera, Div de las TIC.	Jefe de la Div Gestión Financiera	Número de vulnerabilidades. Nivel de conciencia ante el robo de datos de la Div de Gestión financiera, debido accesos no autorizados.
1505	Desactualización del personal respecto a configuraciones de tráfico entrante, uso de correos electrónicos, contraseñas y descargas lo	25	Definir políticas relacionadas con los permisos para las descargas, cambio constante de contraseñas						Institución: personal de la Div de Gestión Financiera y personal encargado en la Div de las TIC.	Personal Div Gestión Financiera	Número de vulnerabilidades. Porcentaje de pruebas periódicas de los dispositivos de seguridad.

	cual facilita el acceso de software.										
1601	Usuarios no autorizados tratan de forzar el ingreso a los sistemas.	40	Controles con una alta protección a los sistemas que contengan información sensible.						Personal de la Div TIC.	Jefe de la Div Gestión Financiera	Número de vulnerabilidades. Porcentaje de pruebas periódicas ante usuarios que intentan ingresar al sistema sin ser autorizadas.
1801	El equipamiento utilizado no es amigable en cuanto al medio ambiente (por ejemplo, en el consumo de energía, embalajes, etc.)	24	Adquirir equipamiento amigable con el medio ambiente capaz de soportar el funcionamiento de toda la Div de Gestión Financiera.						Institución: Rectoría, Vicerrectoría Administrativa, Div de Gestión Financiera, Div de las TIC.	Vicerrectoría Administrativa	Número de vulnerabilidades. Nivel de conciencia ante el equipamiento, utilizado como respaldo para el seguimiento del servicio.
1901	Hay un terremoto.	40							Institución: Concejo académico Rectoría, Vicerrectoría Administrativa, Div de Gestión Financiera, Div de las TIC.	Rectoría	
1903	Hay fuertes tormentas y ciclones tropicales.	40									
1904	Hay un gran incendio fuera de control.	40									

Se seleccionan los objetivos más adecuados para los riesgos identificados cuyo tratamiento fue de Mitigar, en el mapa de riesgos identificando anteriormente (Figura #: Matriz de Riesgo Final). Por lo cual para el desarrollo de los controles nos remitimos nuevamente al estándar ISO/IEC 27000, más específicamente al estándar ISO/IEC 27002: 2013, el cual permite determinar cuáles controles son aplicables al área de Recaudos de la División de Gestión Financiera de la Universidad del Cauca; los cuales cabe resaltar que únicamente son nombrados mas no ejecutados, esto debido a que únicamente su identificación es parte de la fase plan, el cual es nuestro objetivo para nuestro trabajo de grado.

La siguiente tabla muestra los controles aplicables a nuestro trabajo de grado.

Ref. de COBIT 5	Escenarios de Riesgos	Objetivo de Control	Control
105	Desconocimiento de las Políticas de TI.	5. Políticas de la seguridad de la Información.	5.1.1: Políticas para la seguridad de la información.
301	Los gerentes de negocios o sus representantes no se involucran en las decisiones importantes sobre inversiones de TI (por ejemplo: nuevas aplicaciones u oportunidades tecnológicas, priorizaciones).	14. Adquisición, desarrollo y mantenimiento de sistemas	14.2.5: Principios de construcción de los sistemas seguros.
408	Existe una dependencia excesiva del personal clave de TI.	6. Organización de la seguridad de la Información.	6.1.1: Roles y responsabilidades para la seguridad de la información.
		13. Seguridad de las comunicaciones.	13.2.4: Acuerdos de confidencialidad o de no divulgación de información.
409	Existe una incapacidad para actualizar las habilidades de TI a un nivel apropiado a través del entrenamiento.	6. Organización de la seguridad de la Información.	6.1.4: Contactos con grupos de interés especial.
		7. Seguridad de los recursos humanos.	7.2.2: Toma de conciencia, educación y formación en la seguridad de la información
503	Existen errores cometidos por el personal (durante las actualizaciones del sistema, copias de respaldo, mantenimiento)	6. Organización de la seguridad de la Información.	6.1.3: contacto con las autoridades.
504	La información es ingresada incorrectamente por el personal.	6. Organización de la seguridad de la Información.	6.1.3: contacto con las autoridades.
506	Un dispositivo con datos sensibles es robado por un miembro del personal.	7. Seguridad de los recursos humanos.	7.2.3: Proceso disciplinario.
509	Se configuran erróneamente los componentes de hardware.	11. Seguridad física y del entorno.	11.2.4: Mantenimiento de equipo.
603	Pérdida y Revelación de medios portátiles que contiene datos sensibles de información (CD, USB, discos portátiles, etc.)	11. Seguridad física y del entorno.	11.2.1: Ubicación y protección de equipos.
604	Se pierden y se revelan datos	9. Control de Acceso.	9.4.5: control de acceso a códigos

	sensibles mediante ataques lógicos.		fuente de programas.
605	Se pierden o no se verifica la efectividad de los medios que contienen las copias de respaldo.	11. Seguridad física y del entorno.	11.2.1: Ubicación y protección de equipos.
		12. Seguridad de las operaciones.	12.1.1: Procedimientos de operación documentada.
			12.3.1: Respaldo de la información.
606	Se revela información sensible en forma accidental debido a fallas en el seguimiento de las guías de manejo de información.	6. Organización de la seguridad de la información.	6.2.1: Políticas para dispositivos móviles.
		8. Gestión de activos.	8.3.1: Gestión de medios removibles.
607	Se modifican intencionadamente los datos (contables, vinculados a la seguridad, información, etc.)	6. Organización de la seguridad de la información.	6.2.2: teletrabajo.
		9. Control de Acceso.	9.4.4: uso de programas utilitarios privilegiados.
609	Se revela información sensible debido a ineficientes procedimiento de retención / archivo y eliminación.	6. Organización de la seguridad de la información.	6.2.1: Políticas para dispositivos móviles.
			6.2.2: Teletrabajo.
		10. Criptografía.	10.1.1: política sobre el uso de controles criptográficos.
		11. Seguridad física y del entorno.	11.1.6: Áreas de Despacho y carga
612	Filtración de la información debido al abandono del equipo de la institución.	6. Organización de la seguridad de la información	6.2.2: Teletrabajo.
		9. Control de Acceso.	9.4.3: sistema de gestión de contraseñas.
		11. Seguridad física y del entorno.	11.1.2: Controles de acceso
804	Existen fallas intermitentes en los servicios (telecomunicaciones, electricidad).	9. Control de Acceso.	9.1.2: Acceso a la redes y a servicios e red.
		11. Seguridad física y del entorno.	11.2.3: seguridad del cableado.
		14. Adquisición, desarrollo, y mantenimiento de sistemas.	14.1.3: protección de transacciones de los servicios de las aplicaciones.
807	Fallas en los registros y definición de acceso a los activos físicos de TI o el uso de dispositivos por parte del usuario para tratamiento de la información.	9. Control de Acceso.	9.1.1: Política de control de acceso.
908	Ocurren errores no intencionales en la gestión de configuraciones y de cambios.	12. Seguridad de las operaciones.	12.4.1: Registro de eventos.
			12.1.2: Gestión de Cambios
		8. Gestión de activos.	8.3.1: Gestión de medios removibles.
1202	El desconocimiento de cambios potenciales en la regulación tiene un impacto en el ambiente operativo	14. Adquisición, desarrollo, y mantenimiento de sistemas.	14.2.9: prueba de aceptación de sistemas.
		12. Seguridad de las operaciones.	12.1.2: Gestión de Cambios
1401	Se ha producido el robo de un dispositivo con datos sensibles.	9. Control de Acceso.	9.2.2: Suministro de acceso de usuarios.
		11. Seguridad física y del entorno.	11.1.2: Controles de acceso
			11.2.1: Ubicación y protección de equipos.
1403	Se destruye el centro de datos (sabotaje, etc.).	11. Seguridad física y del entorno.	11.2.1: Ubicación y protección de los equipos.
1404	Dispositivos individuales se destruyen accidentalmente.	11. Seguridad física y del entorno.	11.2.2: servicios de suministro.

1405	Ineficiencia o ausencia de dispositivos que detectan las amenazas del entorno, debido a la falta de supervisión, mantenimiento y actualización de los mismos.	11. Seguridad física y del entorno.	11.2.1: Ubicación y protección de equipos.
1406	Libre acceso a las instalaciones de procesamiento sin peticiones formales.	9. Control de Acceso.	9.1.1: Política de control de acceso.
1503	Un empleado insatisfecho implementa una bomba lógica que produce la pérdida de datos importantes.	12. Seguridad de las operaciones.	12.2.1: controles contra códigos maliciosos.
1504	Roban los datos de la compañía a través de accesos no autorizados obtenidos mediante ataques.	9. Control de Acceso	9.4.4: uso de programas utilitarios privilegiados.
		12. Seguridad de las operaciones.	12.2.1: controles contra códigos maliciosos.
1505	Desactualización de los usuarios respecto a configuraciones de tráfico entrante, uso de correos electrónicos, contraseñas y descargas lo cual facilita el acceso de software.	9. Control de Acceso	9.4.1: restricción de acceso a la información.
			9.4.3: Sistemas de gestión de contraseñas.
1601	Usuarios no autorizados tratan de forzar el ingreso a los sistemas.	9. Control de Acceso	9.4.3: Sistemas de gestión de contraseñas.
1801	El equipamiento utilizado no es amigable en cuanto al medio ambiente (por ejemplo, en el consumo de energía, embalajes, etc.)	8. Gestión de activos.	8.2.3: Manejo de activos.
1901	Hay un terremoto.	11. Seguridad física y del entorno.	11.1.4: Protección contra amenazas externas y ambientales.
1903	Hay fuertes tormentas y ciclones tropicales.		
1904	Hay un gran incendio fuera de control.		

Tabla: Controles a implementar.

Se considera la evaluación o definición del nuevo nivel de riesgo de la entidad en relación con los riesgos priorizados a los cuales se hizo su respectivo análisis y poder minimizar el riesgo de alguna manera.

Con la obtención del nivel de riesgo residual se puede realizar una comparación con el nivel de riesgo actual, de manera que se observen los efectos posteriores al decidir implementar las acciones para el tratamiento del riesgo.

Ref de COBIT 5	**Escenarios Negativos**	**Nivel de Riesgo Actual**	**Riesgo Residual**

105	Desconocimiento de las Políticas de TI.	40	6
301	Los gerentes de negocios o sus representantes no se involucran en las decisiones importantes sobre inversiones de TI (por ejemplo: nuevas aplicaciones u oportunidades tecnológicas, priorizaciones)	20	10
408	Existe una dependencia excesiva del personal clave de TI.	40	9
409	Existe una incapacidad para actualizar las habilidades de TI a un nivel apropiado a través del entrenamiento.	24	10
503	Existen errores cometidos por el personal (durante las actualizaciones del sistema, copias de respaldo, mantenimiento)	24	10
504	La información es ingresada incorrectamente por el personal.	32	9
506	Un dispositivo con datos sensibles es robado por un miembro del personal.	24	15
509	Se configuran erróneamente los componentes de hardware.	24	10
603	Pérdida y Revelación de medios portátiles que contiene datos sensibles de información (CD, USB, discos portátiles, etc.)	24	15
604	Se pierden y se revelan datos sensibles mediante ataques lógicos.	24	9
605	Se pierden o no se verifica la efectividad de los medios que contienen las copias de respaldo.	20	15
606	Se revela información sensible en forma accidental debido a fallas en el seguimiento de las guías de manejo de información.	32	15
607	Se modifican intencionadamente los datos (contables, vinculados a la seguridad, información, etc.)	40	10
609	Se revela información sensible debido a ineficientes procedimiento de retención/archivo y eliminación.	24	15
612	Filtración de la información debido al abandono del equipo de la institución.	40	15
804	Existen fallas intermitentes en los servicios (telecomunicaciones, electricidad).	32	9
807	Fallas en los registros y definición de acceso a los activos físicos de TI o el uso de dispositivos por parte del usuario para tratamiento de la información.	20	15
908	Ocurren errores no intencionales en la gestión de configuraciones y de cambios.	32	8
1202	El desconocimiento de cambios potenciales en la regulación tiene un impacto en el ambiente operativo	24	6
1401	Se ha producido el robo de un dispositivo con datos sensibles.	32	15
1403	Se destruye el centro de datos (sabotaje, etc.).	40	15
1404	Dispositivos individuales se destruyen accidentalmente.	32	15
1405	Ineficiencia o ausencia de dispositivos que detectan las amenazas del entorno, debido a la falta de supervisión, mantenimiento y actualización de los mismos.	40	15
1406	Libre acceso a las instalaciones de procesamiento sin peticiones formales.	40	15
1503	Un empleado insatisfecho implementa una bomba lógica que produce la pérdida de datos importantes.	40	15
1504	Roban los datos de la compañía a través de accesos no autorizados obtenidos mediante ataques.	40	15
1505	Desactualización de los usuarios respecto a configuraciones de tráfico entrante, uso de correos electrónicos, contraseñas y descargas lo cual facilita el acceso de software.	25	9

1601	Usuarios no autorizados tratan de forzar el ingreso a los sistemas.	40	8
1801	El equipamiento utilizado no es amigable en cuanto al medio ambiente (por ejemplo, en el consumo de energía, embalajes, etc.)	24	15
1901	Hay un terremoto.	40	15
1903	Hay fuertes tormentas y ciclones tropicales.	40	15
1904	Hay un gran incendio fuera de control.	40	15

Tabla: Comparación del Riesgo Actual / Riesgo Residual.