CAPÍTULO I

1. EL PROBLEMA

1.1 Tema:

Auditoría Informática y su incidencia en la funcionalidad del Sistema de Información Financiera de la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU).

1.2 Planteamiento del Problema

1.2.1 Contextualización

A nivel mundial la auditoría informática se realiza con carácter objetivo, crítico, sistemático y selectivo con el fin de evaluar la eficacia y eficiencia del uso adecuado de los recursos informáticos, de la gestión informática y si estas han brindado el soporte adecuado a los objetivos y metas del negocio.

La Auditoría Informática permite la revisión y la evaluación de los controles, sistemas, procedimientos informáticos, equipos de cómputo, su utilización, eficiencia y seguridad de la organización que está inmersa en el procesamiento de la información con el fin de lograr una utilización más eficiente y segura de la misma que servirá para una adecuada toma de decisiones.

En el país y en la región se evidencia el uso de grandes sistemas informáticos financieros que sin un control de su actividad, estos colapsarían y provocarían

grandes pérdidas para quienes dependen de ellos, proyectando una mala imagen de las mismas.

Las Auditorías Informáticas deben hacerse de forma periódica de tal forma que detecten las fallas o falencias y ayuden a corregirlas. Además hay que citar que el avance de la tecnología crece a pasos agigantados, creándose e inventándose día a día mejores y más sofisticados equipos que permiten optimizar la función de los Sistemas Informáticos Financieros.

La Cooperativa de Ahorro y Crédito Universitaria Ltda., es una Institución que cada día sigue creciendo poco a poco y es consciente que la información que se maneja debe estar bien protegida y manejada, por esta razón tiene la necesidad de realizar una auditoría informática que determine el estado actual del funcionamiento del Sistema de Información Financiera, así como determine posibles fallas y soluciones mediante un examen crítico con el objetivo de evaluar la eficiencia y eficacia de su gestión.

Árbol del Problema

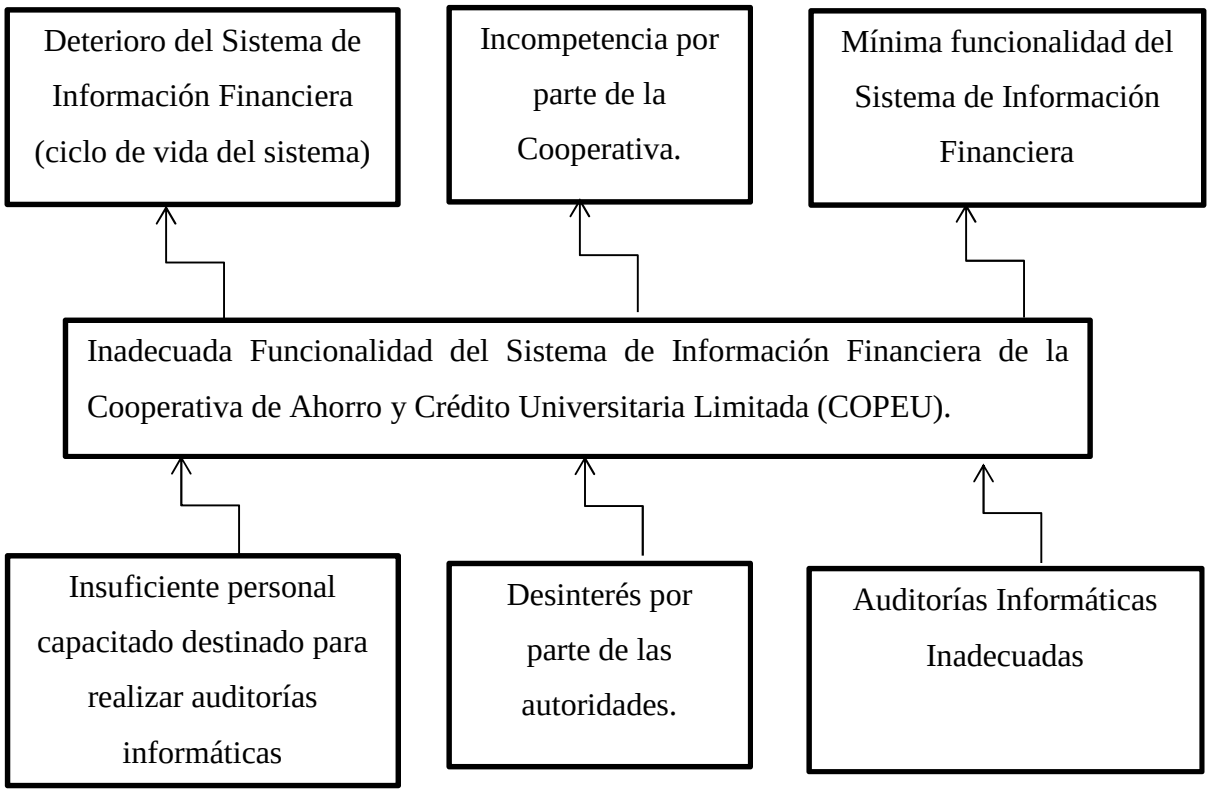


Figura 1: Árbol del Problema

1.2.2 Análisis Crítico

En la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU) de Ambato no existe personal capacitado para realizar una Auditoría Informática al Sistema de Información Financiera lo que ocasiona que la Cooperativa esté propensa a pérdidas económicas, desprestigio y desconfianza por deterioro del Sistema de Información Financiera.

Además existe poco interés por parte de las autoridades de la Cooperativa para realizar una Auditoría Informática al Sistema de Información Financiera de la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU) lo que ocasionaría Incompetencia en la Institución.

También las Auditorías Informáticas Inadecuadas al sistema de información financiera, por falta de personal capacitado para la actividad destinada lo que ocasiona que en la Cooperativa el sistema tenga una minina funcionalidad.

1.2.3 Prognosis

La falta de solución al inadecuado funcionamiento del Sistema de Información Financiera de la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU) podría agravar el problema y tener clientes insatisfechos, servicio insuficiente, pérdidas económicas así como también pérdida de prestigio y confianza de la misma, por lo que se hace necesaria la realización de una Auditoría Informática.

1.2.4 Formulación del Problema

¿Qué incidencia tiene una Inadecuada Auditoría Informática en la funcionalidad del Sistema Informático Financiero de la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU) en el período 2013?

1.2.5 Preguntas Directrices

- ¿Mediante que técnicas se obtiene información necesaria de la Auditoría Informática?

- ¿Qué errores y deficiencias existen actualmente en el Sistema de Información Financiera de la Cooperativa de Ahorro y Crédito Universitaria Limitada?

- ¿De qué manera se mejorará la funcionalidad o productividad del Sistema de Información Financiera de la Cooperativa de Ahorro y Crédito Universitaria Limitada?

1.2.6 Delimitación

Campo: Ingeniería en Sistemas Computacionales e Informáticos.

Área: Administrativas Informáticas.

Línea: Administración de Recursos.

Sublinea: Auditorias Informáticas.

Tiempo: Se desarrollará en 6 meses a partir de la aprobación del perfil del Proyecto.

Lugar: Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU).

1.3 Justificación

Las tendencias en la utilización de herramientas tecnológicas para el mejor desenvolvimiento laboral han generado gran interés en la sociedad. El hombre ha hecho del uso de la tecnología parte de su diario vivir.

Debido a que en la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU) de Ambato no se ha efectuado ninguna auditoría informática, se considera

de gran importancia que se ejecute una auditoría en la Cooperativa y permita tomar medidas correctivas, asegurando la funcionalidad y productividad del Sistema de Información Financiera encaminando a guiar al buen desarrollo y correcto funcionamiento del mismo, para de esta manera, en posteriores auditorías, se enfoque la auditoría a áreas específicas o áreas críticas existentes.

Con este proyecto se beneficiará principalmente la Cooperativa y sus clientes ya que mediante normas o estándares se verificará el correcto funcionamiento del Sistema de Información Financiera de la Cooperativa de Ahorro y Crédito Universitaria Limitada y que permitirá en el futuro el mejor desenvolvimiento de la institución.

1.4 Objetivos

Objetivo General

- Determinar la incidencia de las Auditorías Informáticas en la funcionalidad del Sistema de Información Financiera de la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU) en el período 2013.

Objetivos Específicos

- Determinar las inconsistencias de las Auditorías Informáticas realizadas en el Sistema de Información Financiera de la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU).
- Establecer el funcionamiento del Sistema de Información Financiera de la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU).
- Plantear una solución factible al problema de funcionalidad del Sistema de Información Financiera de la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU).

CAPÍTULO II

2. MARCO TEÓRICO

2.1 Antecedentes Investigativos:

En la biblioteca de la Universidad Técnica De Ambato, en la Facultad de Ingeniería en Sistemas Electrónica e Industrial reposa la tesis "Auditoría Informática para optimizar el manejo de la información y equipamiento informático en el MIES INFA Tungurahua" de la Autora Castro Núñez Diana Margoth trabajo realizado en Tungurahua-Ecuador en el año 2012 en cuyas conclusiones expresan lo siguiente:

"De la investigación se concluye que los funcionarios del MIES – INFA en su mayoría deja a visibilidad las contraseñas de sus ordenadores bajo teclados, en hojas adhesivas en los monitores lo que hace posible que terceros puedan ingresar libremente y tomar información importante".

"No existe un plan de contingencia en la institución en el ámbito informático ante cualquier eventualidad que puede suscitarse la cual puede afectar de manera significativa el desempeño de la institución".

"Los funcionarios del MIES – INFA poseen en sus computadores software que en gran parte no es utilizado, lo cual ocupa espacio de memoria y lentitud en sus equipos".

“El antivirus utilizado por la institución es deficiente por lo que la proliferación de virus en los computadores es frecuente”.

“No existe mantenimiento periódico de los equipos de cómputo de la institución lo que evitaría fallos recurrentes en los ordenadores y molestias en los funcionarios”.

En la biblioteca de la Universidad Técnica De Ambato, en la Facultad de Ingeniería en Sistemas Electrónica e Industrial reposa la tesis “Auditoría Informática para los Departamentos Comercial, Acometidas y Procesamiento de Datos de la Empresa Municipal de Agua Potable y Alcantarillado de Ambato” de la Autora Adriana Elizabeth Aguilar Arcos trabajo realizado en Tungurahua-Ecuador en el año 2007 en cuyas conclusiones y recomendaciones expresan lo siguiente:

“Las funciones y reglamentos que se encuentran establecidas en la empresa deben ser dadas a conocer al personal para un mejor desempeño de las mismas”.

“Para la adquisición de software y hardware los miembros de la Sección de Procesamiento de Datos ven las necesidades de los departamentos, de acuerdo a esto solicitan lo necesario a gerencia y al departamento de proveeduría justificando los beneficios que se obtendrá en EMAPA adquiriendo este producto”.

“La Sección de Procesamiento de Datos realiza un plan informático anual para una mejor organización de todo lo que conlleva la sección”.

“Existe software ilegal instalado en las diferentes computadoras, los cuales son instalados por el personal, sin la autorización de los encargados de la Sección de Procesamiento de Datos”.

“Consta de una buena organización en la seguridad de ingreso de usuarios, mediante el uso de validación de contraseñas dando privilegios a cada uno para su acceso a la información”.

“Actualmente la Empresa no dispone de procedimientos a seguir para la restauración de la información en el caso de suceder cualquier tipo de desastre”.

“La falta de capacitación de los usuarios en cuanto a aplicaciones computacionales como en el manejo de dispositivos externos, las computadoras están expuestos al ingreso de virus el cual puede provocar un sinnúmero de daños”.

En la biblioteca de la Universidad Técnica De Ambato, en la Facultad de Ingeniería en Sistemas Electrónica e Industrial reposa la tesis “Auditoría Informática en los Departamentos de Personal, Médico, Trabajo Social, Coactivas, Planificación de la Empresa Municipal de Agua Potable y Alcantarillado” de la Autora Evelin Fernanda Canseco Estrella trabajo realizado en Tungurahua-Ecuador en el año 2007 en cuyas conclusiones y recomendaciones expresan lo siguiente:

“Para la obtención del personal que trabajará en la Empresa el Jefe de Personal tiene un Manual de elección de Personal, el mismo que esta diseño para cubrir las necesidades de cada uno de los puestos para los departamentos y secciones”.

“Es importante aclarar que todo aspirante a cualquier puesto de trabajo debe tener conocimientos básicos en computación para que su desempeño laboral sea óptimo”.

“La relación existente entre los departamentos y secciones es muy ambigua, ya que para labores de cada uno de los departamentos se cumple con la jerarquía del organigrama vigente, pero en el tema informático cada uno de los usuarios solicita directamente ayuda a la sección de Procesamiento de Datos sin cumplir con el orden jerárquico establecido ya que este podría tardar mucho tiempo y el usuario necesita ayuda inmediata”.

“La ubicación de los elementos de la red en el departamento de planificación es pésima ya que estos están colocados en forma desorganizada sin cumplir con las Normas existentes en el ámbito de redes”.

Todos los departamentos poseen un porcentaje alto de software ilegal, el mismo que debe ser corregido para evitar problemas graves”.

“Los equipos tienen falencias en las seguridades ya sean físicas como lógicas, ya que no tienen los implementos (alarmas, extintores) para un caso de emergencia y el antivirus

colocado en cada uno de los equipos no tienen actualizaciones periódicas más seguidas y esto puede producir errores en los equipos".

"La sección de Procesamiento de Datos no tiene un plan de capacitación actualizado para mejorar el conocimiento de los usuarios".

Se toman como antecedentes ya que tienen bases investigativas que sirven como punto de partida sobre cómo realizar la Auditoría Informática para verificar la funcionalidad del Sistema de Información Financiera de la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU) lo cual puede tomarse como una solución.

2.2 Fundamentación Legal

LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS
LEY 2002-67 (REGISTRO OFICIAL 557-S, 17-IV-2002)
CONGRESO NACIONAL
Título I
DE LOS MENSAJES DE DATOS

Capítulo I
PRINCIPIOS GENERALES

Art. 5.- Confidencialidad y reserva.- Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención.

Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia.

Art. 9.- Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.

No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.

CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR

ASAMBLEA CONSTITUYENTE 2008

Capítulo sexto

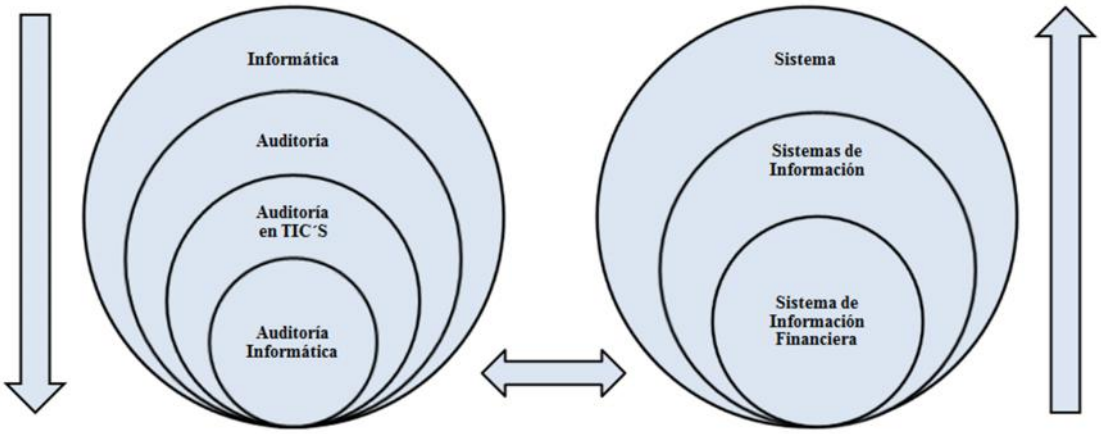
Derechos de libertad

Art. 66.- Se reconoce y garantizará a las personas:

19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

2.3 Categorías Fundamentales

Figura 2: Inclusión de Variables



Constelación De Ideas

Figura 3: Auditoría Informática

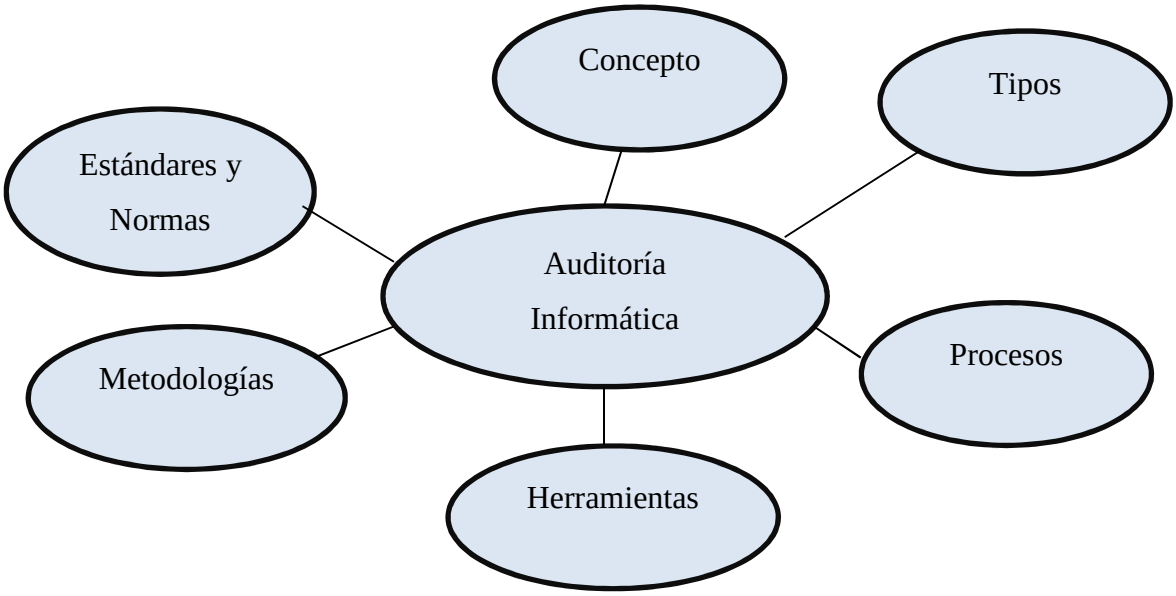
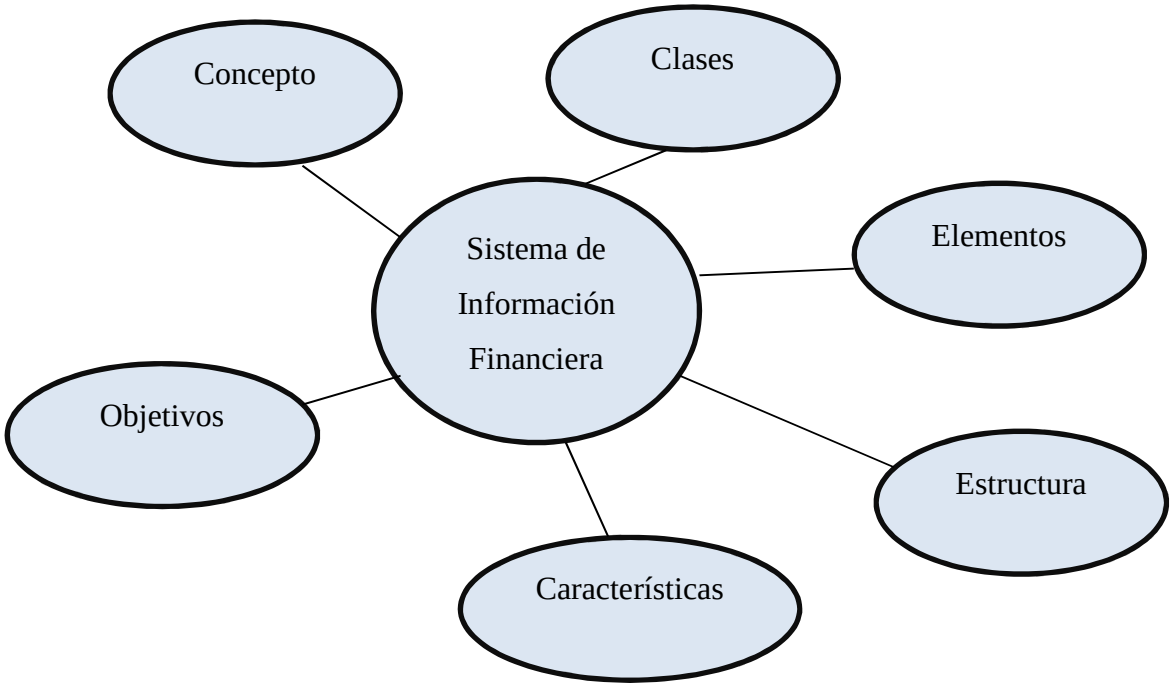


Figura 4: Sistema de Información Financiera



2.3.1.1 Informática

Según Sánchez, Verónica (Internet, 05/07/2011, 11/03/2013 17:38) menciona que

"Es la ciencia que trata la información y se ocupa de los fundamentos y la utilización de las instalaciones de procesamiento de datos, asistida por computadores u otros procesadores de información.

La cantidad de datos que se puede conocer, recordar y manejar gracias a la informática es infinitamente superior que la que se puede conseguir por nuestros propios medios o en una biblioteca".

Según TORRES, Alcides (Internet, 25/03/2012, 11/03/2013 17:58) menciona que

"El término Informática se creó en Francia en el año 1.962 bajo la denominación INFORMATIQUE y procede de la contracción de las palabras INFORmation

autoMATIQUE. Posteriormente fue reconocido por el resto de países, siendo adoptado en España en 1.968 bajo el nombre INFORMÁTICA.

La informática es la ciencia que estudia el tratamiento automático y racional de la información. Se dice que el tratamiento es automático por ser máquinas las que realizan los trabajos de captura, procesos y presentación de la información, y se habla de racional por estar todo el proceso definido a través del programa. Que siguen el razonamiento humano. Dentro de la ciencia de la informática se encuentra incluidas una serie de funciones de las que mencionamos a continuación: a) El desarrollo de nuevas máquinas. b) El desarrollo de nuevos métodos de trabajos. c) La construcción de aplicaciones informáticas".

Según el análisis se podría concluir que la Informática es una ciencia destinada al estudio y atención que se le da a la información para tratarla de forma automática, utilizando sistemas computacionales y los componentes electrónicos que para ello se utilizan; mediante los conocimientos de un individuo para el tratamiento automático de la misma.

2.3.1.2 Auditoría

Según HURTADO, Pablo (Internet, 29/11/2005, 11/03/2013 23:23) menciona que

"Es el examen profesional, objetivo e independiente, de las operaciones financiera y/o Administrativas, que se realiza con posterioridad a su ejecución en las entidades públicas o privadas y cuyo producto final es un informe conteniendo opinión sobre la información financiera y/o administrativa auditada, así como conclusiones y recomendaciones tendientes a promover la economía, eficiencia y eficacia de la gestión empresarial o gerencial, sin perjuicio de verificar el cumplimiento de las leyes y regulaciones aplicables".

Según AUDITORÍA DE INFORMÁTICA (Internet, 30/07/2010, 11/03/2013 23:30) menciona que

“Es un examen crítico que se realiza con el fin de evaluar la eficiencia y eficacia de una organización.

Es una revisión metódica, periódica e intelectual de los registros, tareas y resultados de la empresa, con el fin de diagnosticar el comportamiento global en el desarrollo de sus actividades y operaciones.

Clasificación de la auditoría por su lugar de origen

Auditoría externa y Auditoría interna.

Clasificación de auditorías por su área de aplicación

Auditoría financiera (contable), Auditoría administrativa, Auditoría operacional, Auditoría integral, Auditoría gubernamental, Auditoría informática”.

Según el análisis se podría concluir que la Auditoría La Auditoría es aquel instrumento de gestión que ha de incluir una evaluación sistemática, documentada y objetiva de la eficacia del sistema de prevención para lo cual deberá ser realizada de acuerdo con las normas técnicas establecidas o que puedan establecerse, y teniendo en cuenta la información recibida de los trabajadores.

2.3.1.3 Auditoría en TIC’S (Tecnologías de Información y Comunicación)

Según ARANGUIZ, Giselle, CABELLO, Nadia, RIQUELME, Eduardo, RIVAS, Carla, RODRÍGUEZ, Jenny, SILVA, Romina (Internet, 12/06/2010, 12/03/2013 00:49) menciona que

“Tecnologías de la Información y la comunicación (TIC) : Cuando unimos estas tres palabras hacemos referencia al conjunto de avances tecnológicos que nos proporcionan la informática, las telecomunicaciones y las tecnologías audiovisuales, que comprenden los desarrollos relacionados con los ordenadores, Internet, la telefonía, los "más media", las aplicaciones multimedia y la realidad virtual. Estas tecnologías básicamente nos proporcionan información, herramientas para su proceso

y canales de comunicación.
El ciclo de vida básico de una auditoría es el siguiente:

a) Inicio de la auditoría
b) Revisión de la documentación y preparación de las actividades
c) Desarrollo del plan de auditoría
d) Preparación del informe de la auditoría y presentación de resultados".

Según NORMAS DE AUDITORÍA GUBERNAMENTAL NAG 270 Y CORRELATIVA (Internet, 15/04/2006, 12/03/2013 01:23) menciona que

"Es el examen objetivo, crítico, metodológico y selectivo de evidencia relacionada con políticas, prácticas, procesos y procedimientos en materia de Tecnologías de la Información y la Comunicación, para expresar una opinión independiente respecto:

a) A la confidencialidad, integridad, disponibilidad y confiabilidad de la información.

b) Al uso eficaz de los recursos tecnológicos.

c) A la efectividad del sistema de control interno asociado a las Tecnologías de la Información y la Comunicación".

Según el análisis se podría concluir que la Auditoría en TIC'S La Auditoria en TIC´S son un conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente un sistema informático, telecomunicaciones, redes o equipamiento, con el fin de proteger actividades y recursos, verificar si las actividades se desarrollan eficientemente y de acuerdo con la normatividad informática y general en cada empresa o institución, para conseguir la eficacia exigida por la organización.

2.3.1.4 Auditoría Informática

Según PIATTINI, Mario, DEL PESO, Emilio (2001, Auditoría Informática Un Enfoque Práctico, pág. 28) menciona que

“La Auditoría Informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

También RIVAS, Gonzalo (1998, Auditoría Informática, pág. 39) menciona que

“La auditoría informática es un examen metódico del servicio informático, o de un sistema informático en particular, realizado de una forma puntual y de modo discontinuo, a instancias de la Dirección, con la intención de ayudar a mejorar conceptos como la seguridad, la eficacia, y la rentabilidad del servicio, o del sistema, que resultan auditados”.

Además CASTRO, Diana (2012) “Auditoría Informática para optimizar el manejo de la información y equipamiento informático en el MIES INFA Tungurahua, previo a la obtención del Título de Ingeniera en Sistemas Computacionales e Informáticos, Universidad Técnica de Ambato, Facultad de ingeniería en sistemas Electrónica e Industrial, Ciudad Ambato, Ecuador.

“Auditoría Informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo de una entidad, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

2.3.1.4.1. Tipos de Auditoría Informática

Auditoría Física, Auditoria Ofimática, Auditoría de Base de Datos, Estudio Previo y Plan de Trabajo, Diseño y Carga, Explotación y Mantenimiento, Revisión Post-Implantación, Auditoría de Redes, Auditoría de la Seguridad.

2.3.1.4.2 Técnicas y Herramientas

Para detectar falencias de información como de equipo tecnológico se debe recurrir a la recolección de la información observada y documentada donde se analiza las situaciones de debilidad o fortalezas de los diferentes entornos es por ello que se debe utilizar una técnica para recabar la información relevante que pueden ser: Cuestionario, Entrevista, Checklist".

2.3.1.4.3 Metodologías en Auditoría Informática.

Según PIATTINI, Mario, DEL PESO, Emilio (2001, Auditoría Informática Un Enfoque Práctico, pág. 63) menciona que

"Las metodologías de auditoría informática son de tipo cualitativo/subjetivo. Se puede decir que son subjetivas por excelencia. Están basadas en profesionales de gran nivel de experiencia y formación, capaces de dictar recomendaciones técnicas, operativas y jurídicas, que exigen en gran profesionalidad y formación continua. Solo existen dos tipos de metodologías para la auditoría informática:

Controles Generales.- Son el producto estándar de los auditores profesionales. El objetivo aquí es dar una opinión sobre la fiabilidad de los datos del computador para la auditoría financiera, es resultado es escueto y forma parte del informe de auditoría, en donde se hacen notar las vulnerabilidades encontradas. Están desprestigiadas ya que dependen en gran medida de la experiencia de los profesionales que las usan".

La auditoría informática es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas.

2.3.1.4.3.1 Análisis Comparativo de Metodologías.

2.3.1.4.3.1.1 MAGERIT versión 3.

MAGERIT es una metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Pública. Además consigo trae una herramienta llamada PILAR en la versión 5.2.9.

2.3.1.4.3.1.2 COSO II

COSO es una metodología de control interno, proporcionando un foco más robusto y extenso sobre la identificación, evaluación y gestión integral de riesgo para mejorar la calidad de la información financiera concentrándose en el manejo corporativo, las normas éticas y el control interno.

Cuadro Comparativo de las Metodologías.

Factor	MAGERIT	COSO	Mejor
Tipos de Empresas donde es Aplicable	Empresas o Cooperativas Financieras	Empresas o Cooperativas Financieras	MAGERIT COSO
Área donde se Aplica	Sistemas de Información Financiera	A la Información Financiera	MAGERIT
Estructura	Consta de 3 Fases Planificación del Proyecto Análisis de Riesgos Gestión de Riesgos	Consta de 5 Etapas Ambiente de Control Evaluación de Riesgos Actividades de Control Información y Comunicación Supervisión	MAGERIT
Objetivos	Generar conciencia a los responsables de Sistemas de Información existencias de riesgos y necesidades para solucionarlos a tiempo Ofrecer un método sistemático para analizar riesgos. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos.	Eficacia y Eficiencia de las Operaciones. Confiabilidad de la información Financiera. Cumplimiento de Normas y Leyes Aplicables.	MAGERIT COSO

Objetivos	Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.		MAGERIT COSO
Ventajas	Ofrece un Método Sistematizado para analizar los Riesgos. Ayuda a Identificar y Planificar medidas necesarias para reducir los Riesgos. Brinda Herramientas que ayudan a facilitar el Análisis de Riesgos.	Permite a la dirección de la empresa poseer una visión global del riesgo y accionar los planes para su correcta gestión. Permite dar soporte a las actividades de planificación estratégica y control interno. Fomenta que la gestión de riesgos pase a formar parte de la cultura del grupo.	MAGERIT COSO
Desventajas	Por el contrario, el hecho de tener que traducir de forma directa todas las valoraciones en valores económicos hace que la aplicación de esta metodología sea realmente costosa.	Crea una carga administrativa adicional como parte de los procedimientos de Auditoria Interna. Proceso es algo complicado.	MAGERIT COSO
Software de Apoyo	Pilar 5.2.9 De fácil manejo	Meycor COSO AG De manejo complejo y complicado	MAGERIT

Tabla 1: Cuadro Comparativo Metodología Magerit y Coso

2.3.1.4.3.1.3 Conclusión

De las dos Metodologías explicadas la que se va a tomar en cuenta para realizar la Auditoria Informática es la Metodología MAGERIT version3.0 con su herramienta PILAR 5.2.9 ya que esta metodología se basa en Análisis y Gestión de Riesgos de los Sistemas de Información, específicamente se encarga de Auditar Sistemas que es lo que se necesita en este caso y no como COSO que se basa en Análisis y Gestión de Riesgos pero de la información financiera.

2.3.2.1 Sistema

Según DICCIONARIO DE INFORMÁTICA (Internet, 17/05/2007, 12/03/2013 19:10) menciona que

"Un sistema es un conjunto de partes o elementos organizadas y relacionadas que interactúan entre sí para lograr un objetivo. Los sistemas reciben (entrada) datos, energía o materia del ambiente y proveen (salida) información, energía o materia.

Un sistema puede ser físico o concreto (una computadora, un televisor, un humano) o puede ser abstracto o conceptual (un software).

Cada sistema existe dentro de otro más grande, por lo tanto un sistema puede estar formado por subsistemas y partes, y a la vez puede ser parte de un supersistema.

Además GALLEGO, José (2010, Mantenimiento de Sistemas Microinformáticos, pág. 5) menciona que

"Un sistema informático (SI) es un conjunto de partes que funcionan relacionándose entre sí con un objetivo preciso.

El concepto de sistema informático más simple sería el formado por un equipo con su usuario y el manual de instrucciones. No obstante, un SI puede crecer indefinidamente e incluso abarcar o interactuar con otros sistemas informáticos".

Según el análisis se podría concluir que Sistema Un sistema informático es un conjunto de partes que funcionan relacionándose entre sí con un objetivo preciso. Sus partes son: hardware, software y las personas que lo usan.

2.3.2.2 Sistemas de Información

Según VEGA, Edgar (Internet, 04/06/2005, 12/03/2013 21:53) menciona que

"Un Sistema de Información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio. En un sentido amplio, un sistema de información no necesariamente incluye equipo electrónico (hardware).

Sin embargo en la práctica se utiliza como sinónimo de "sistema de información computarizado".

Los elementos que interactúan entre sí son: el equipo computacional, el recurso humano, los datos o información fuente, programas ejecutados por las computadoras, las telecomunicaciones y los procedimientos de políticas y reglas de operación.

Un Sistema de Información realiza cuatro actividades básicas:

Entrada de información, Almacenamiento de información, Procesamiento de la información, Tipos de sistemas de información".

Según VÁZQUEZ, Anaely (Internet, 02/03/2012, 12/03/2013 22:15) menciona que

"En el sector organizacional se han desarrollado diversas tipologías de Sistemas de Información. Estas surgen básicamente a partir de las propias necesidades del sector a que pertenecen las organizaciones, los procesos fundamentales y las particularidades que se dan en cada organización.

Varios autores como Cohen, Ponjuán y Muñoz Cañavate coinciden en clasificar los Sistemas de Información desarrollados para diferentes propósitos, pero fundamentalmente orientados a la toma de decisiones, como:

a) De Procesamiento de Datos (TPS – Transactional Processing Systems).
b) Sistemas de Información para la Administración o Gerenciales (MIS - Management Information Systems).
c) Sistemas de Soporte a la Toma de Decisiones (DSS – Decision Support Systems).
d) Sistemas de información para ejecutivos (EIS – Executive Information Systems).
e) Sistemas Expertos o sistemas basados en el conocimiento (WKS –Knowledge Working Systems).
f) Sistema de Información de Marketing (S.I.M)
g) Sistemas de Información de Producción (S.I.P).
h) Sistema de Información Financiera (S.I.F).
i) Sistema de Información de Recursos Humanos (S.I.R.H).
j) Sistemas de Dirección para Directivos (S.D.D)".

Un Sistema de Información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio.

2.3.2.3 Sistemas de Información Financiera

Según Globalsoft Technologies Ltda (Internet, 30/05/2006, 28/03/2013 19:40) menciona que

SIF: El SIF es un sistema de información integral que está concebido desde cuatro perspectivas equilibradas que permiten mediar y focalizar el curso de la empresa:

Los aspectos Financieros

Los clientes y proveedores de la empresa

Las personas, tecnologías de la información, formación, aprendizaje y crecimiento

Los procesos internos de la empresa.

Según VÁZQUEZ, Anaely (Internet, 02/03/2012, 28/03/2013 20:24) menciona que

“Sistema de Información Financiera (S.I.F): proporciona a personas y grupos, tanto de dentro como de fuera de la organización, información relacionada con los asuntos financieros de la organización”.

Además FERNÁNDEZ Vicenç (2006, Desarrollo de sistemas de información pág. 24) menciona que

“Los sistemas de información financiera proporcionan a personas y grupos (stakeholders) tanto de dentro como de fuera de la organización información relacionada con los asuntos financieros de la compañía. El sistema de información financiera está formado por tres (sub)sistemas de entrada y tres subsistemas de salida.

Los tres subsistemas de entrada son alimentados mediante información procedente de fuentes del entorno de la empresa. Por otro lado, el sistema de información contable y el subsistema de auditoría interna recopilan información que procede de fuentes internas de la empresa.

Los subsistemas de salida tiene una fuerte influencia sobre la gestión y el flujo financiero de la empresa a través del subsistema de pronóstico, el subsistema de administración de fondos y el subsistema de control”.

El SIF es un sistema de información integral que proporciona información relacionada con los asuntos financieros de la organización y que depende mucho del Sistema de Información Contable.

2.3.2.3.1 Sistema de Información Contable

Según MARTELO, Lizeth (Internet, 23/01/2009, 28/03/2013 21:45) menciona que

“Un sistema de información contable comprende los métodos, procedimientos y recursos utilizados por una entidad para llevar un control de las actividades financieras y resumirlas en forma útil para la toma de decisiones.

2.3.2.3.2 Estructura de un Sistema de Información Contable

Un sistema de información contable sigue un modelo básico y un sistema de información bien diseñado, ofreciendo así control, compatibilidad, flexibilidad y una relación aceptable de costo/beneficio. El sistema contable de cualquier empresa independientemente del sistema contable que utilicé, se deben ejecutar tres pasos básicos utilizando relacionada con las actividades financieras; los datos se deben registrar, clasificar y resumir, sin embargo el proceso contable involucra la comunicación a quienes estén interesados y la interpretación de la información contable para ayudar en la toma de decisiones comerciales.

- Registro de la actividad financiera: en un sistema contable se debe llevar un registro sistemático de la actividad comercial diaria en términos económicos. En una empresa se llevan a cabo todo tipo de transacciones que se pueden expresar en términos monetarios y que se deben registrar en los libros de contabilidad. Una transacción se refiere a una acción terminada más que a una posible acción a futuro. Ciertamente, no todos los eventos comerciales se pueden medir y describir objetivamente en términos monetarios.

- Clasificación de la información: un registro completo de todas las actividades comerciales implica comúnmente un gran volumen de datos, demasiado grande y diverso para que pueda ser útil para las personas encargadas de tomar decisiones. Por tanto, la información de debe clasificar en grupos o categorías. Se deben agrupar aquellas transacciones a través de las cuales se recibe o paga dinero.

- Resumen de la información: para que la información contable utilizada por quienes toman decisiones, esta debe ser resumida. Por ejemplo, una relación completa de las transacciones de venta de una empresa como Mars sería demasiado larga para que cualquier persona se dedicara a leerla. Los empleados responsables de comprar mercancías necesitan la información de las ventas resumidas por producto. Los gerentes de almacén necesitaran la información de ventas resumida por departamento, mientras que la alta gerencia de Mars necesitará la información de ventas resumida por almacén.

Estos tres pasos que se han descrito: registro, clasificación y resumen constituyen los medios que se utilizan para crear la información contable. Sin embargo, el proceso contable incluye algo más que la creación de información, también involucra la comunicación de esta información a quienes estén interesados y la interpretación de la información contable para ayudar en la toma de decisiones comerciales. Un sistema contable debe proporcionar información a los gerentes y también a varios usuarios externos que tienen interés en las actividades financieras de la empresa.

2.3.2.3.3 Características de un Sistema de Información Contable

Un sistema de información bien diseñado ofrece control, compatibilidad, flexibilidad y una relación aceptable de costo/beneficio.

Control: un buen sistema de contabilidad le da a la administración control sobre las operaciones de la empresa.

Los controles internos son los métodos y procedimientos que usa un negocio para autorizar las operaciones, proteger sus activos y asegurar la exactitud de sus registros contables.

Compatibilidad: un sistema de información cumple con la pauta de compatibilidad cuando opera sin problemas con la estructura, el personal, y las características especiales de un negocio en particular.

2.3.2.3.4 Objetivos de un Sistema de Información Contable

La información contable debe servir fundamentalmente para: Conocer y demostrar los recursos controlados por un ente económico, las obligaciones que tenga de transferir recursos a otros entes, los cambios que hubieren experimentado tales recursos y el resultado obtenido en el periodo.

Predecir flujos de efectivo.

Apoyar a los administradores en la planeación, organización y dirección de los negocios.

Tomar decisiones en materia de inversiones y crédito.

Evaluar la gestión de los administradores del ente económico.

Ejercer control sobre las operaciones del ente económico.

Fundamentar la determinación de cargas tributarias, precios y tarifas.

Ayudar a la conformación de la información estadística nacional.

Contribuir a la evaluación del beneficio o impacto social que la actividad económica representa para la comunidad.

2.3.2.3.5 Elementos de Sistemas de Información Contable

El Equipo computacional. Es el hardware necesario para que el sistema de información pueda funcionar.

El Recurso humano. Que interactúa con el sistema, el cual está formado por las personas que utilizan el sistema, alimentándolo con datos o utilizando los resultados que genere.

Los programas (software).que son ejecutados por la computadora y producen diferentes tipos de resultados.

Las telecomunicaciones. Que son básicamente software y hardware, facilitan la transmisión de texto, datos, imágenes y voz en forma electrónica.

Procedimientos que incluyen las Políticas y reglas de operación, tanto en la parte funcional del proceso de negocio, como los mecanismos para hacer trabajar una aplicación en la empresa".

2.3.2.3.6 Clases de Sistema de Información Contable

Según Introducción a la Contabilidad General (Internet, 31/01/2001, 29/03/2013 01:11) menciona que

1) Contabilidad Empresarial

La Contabilidad empresarial, ha ocupado el lugar más destacado, debido al papel que desempeñan las empresas en la actividad económica. El hecho de que estas unidades creen más o menos riqueza repercute en la totalidad de la economía. De ahí que se la considere el núcleo de la contabilidad.

2) Contabilidad Pública

La Contabilidad pública, o contabilidad del sector público, no ha alcanzado el nivel de la contabilidad empresarial porque durante mucho tiempo ha sido concebida como una contabilidad ligada al Presupuesto del Estado, olvidando aspectos como la determinación periódica de la renta y la riqueza. En los últimos años, sin embargo, está superando las anteriores limitaciones.

3) Contabilidad de las entidades sin ánimo de lucro

La Contabilidad de las entidades sin ánimo de lucro es necesaria ya que estas entidades precisan también de una organización contable a través de la cual se llegue

a la información correspondiente, ya que han de rendir cuentas públicamente por representar intereses colectivos

2.4 Hipótesis

Las Auditorías Informáticas incidirían en la funcionalidad del Sistema de Información Financiera de la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU).

2.5 Señalamiento de variables

Variable Independiente

Auditoría Informática

Variable Dependiente

Sistema de Información Financiera

2.6 Análisis e Interpretación de Resultados

La Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU, se ha enfocado en verificar la funcionalidad del Sistema de Información Financiera.

Se realizaron reuniones con el Sr. Gerente y Empleados de la Cooperativa, para obtener información sobre el funcionamiento, procesos, agilidad y documentación del Sistema implantado en la Cooperativa.

En la presente investigación la información fue recopilada utilizando como técnica la Encuesta, la misma que fue aplicada a toda la población de acuerdo al modelo presentado en el *Anexo 1*.

La aplicación de dicha herramienta tuvo como objetivo central conocer el Estado del Sistema de Información Financiera y su Manejo en la Cooperativa de Ahorro y

Crédito Universitaria Limitada COPEU, así como recolectar información sobre sus necesidades y criterios que enriquezcan la propuesta que se pretende plantear.

Cabe indicar que la población colaboró con toda la disposición que ameritaba esta actividad. A continuación se presentan los resultados.

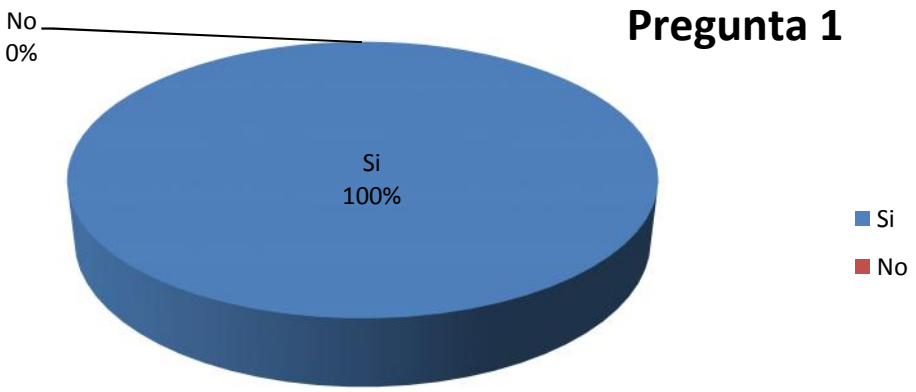
2.6.1 Análisis e Interpretación

ENCUESTA APLICADA A PERSONAL DE LA COOPERATIVA DE AHORRO Y CRÉDITO UNIVERSITARIA LIMITADA.

1. ¿Se han realizado Auditorías Informáticas en la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU)?

N°	Ítems	Valores Numéricos	Valores Porcentuales
1.1	Si	19	100%
1.2	No	0	0%
	Total	19	100%

Tabla 2: Pregunta 1



Autor: Andrés Simbaya
Fuente: Personal COPEU

Figura 5: Pregunta 1

Interpretación:

De acuerdo a la encuesta aplicada al personal de la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU indica que 19 personas que representa el

100% dicen que si se ha realizado Auditorías Informáticas anteriormente en la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU.

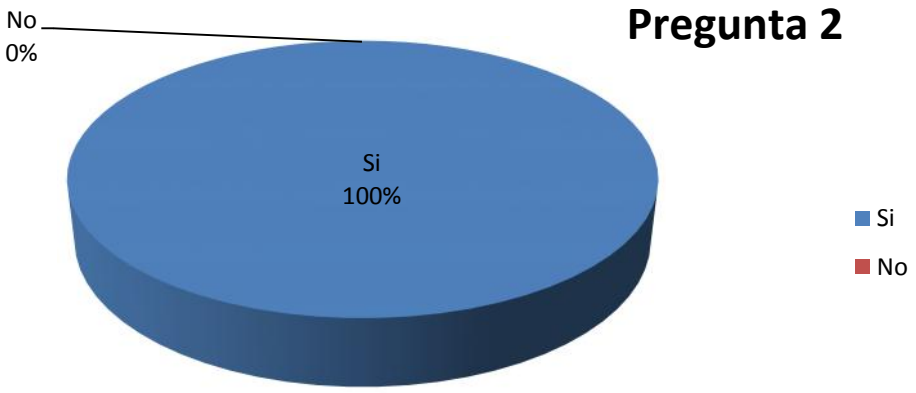
Análisis:

Se evidencia en los resultados de la pregunta que si se han realizado Auditorías Informáticas en la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU.

2. ¿Las Auditorías Informáticas realizadas en la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU) han servido para el progreso y mejor desempeño de la misma?

N°	Ítems	Valores Numéricos	Valores Porcentuales
2.1	Si	19	100%
2.2	No	0	0%
	Total	19	100%

Tabla 3: Pregunta 2



Autor: Andrés Simbaya
Fuente: Personal COPEU

Figura 6: Pregunta 2

Interpretación:

De acuerdo a la encuesta aplicada al personal de la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU indica que 19 personas que representa el 100% dicen que las Auditorías Informáticas que se han realizado en la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU han servido para el progreso y un mejor desempeño de la misma.

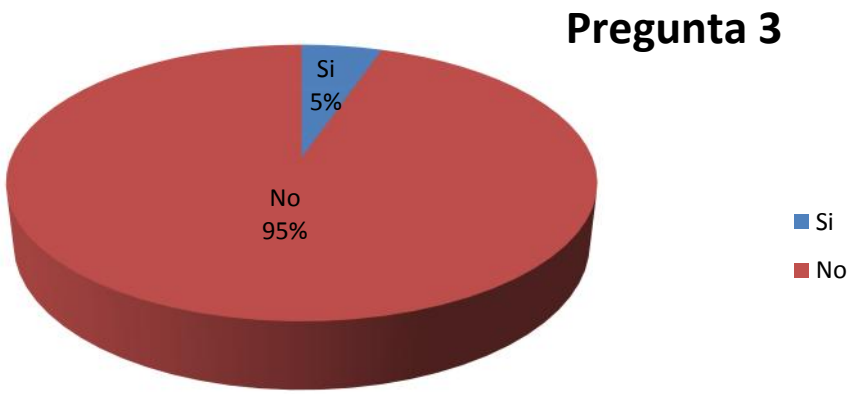
Análisis:

Se evidencia en los resultados de la pregunta que las Auditorías Informáticas realizadas en la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU han servido para el progreso y un mejor desempeño de la misma.

3. ¿Se lleva algún registro y seguimiento de los fallos producidos por el Sistema de Información Financiera?

N°	Ítems	Valores Numéricos	Valores Porcentuales
2.1	Si	1	5%
2.2	No	18	95%
	Total	19	100%

Tabla 4: Pregunta 3



Autor: Andrés Simbaya
Fuente: Personal COPEU

Figura 7: Pregunta 3

Interpretación:

De acuerdo a la encuesta aplicada al personal de la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU indica que 1 persona que representa el 5% dice que se lleva algún registro y seguimiento de los fallos producidos por el Sistema de Información Financiera, mientras que 18 personas que representan el 95% dicen que no se lleva algún registro y seguimiento de los fallos producidos por el Sistema de Información Financiera.

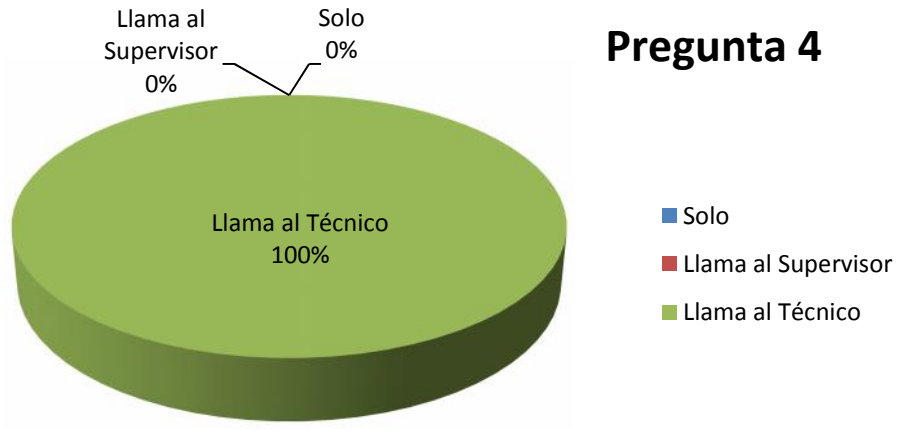
Análisis:

Se evidencia en los resultados de la pregunta que no se lleva algún registro y seguimiento de los fallos producidos por el Sistema de Información Financiera de la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU.

4. ¿Qué tipo de controles tiene implantados el Sistema de Información Financiera?

N°	Ítems	Valores Numéricos	Valores Porcentuales
4.1	Solo	0	0%
4.2	Llama al Supervisor	0	0%
4.3	Llama al Técnico	19	100%
	Total	19	100%

Tabla 5: Pregunta 4



Autor: Andrés Simbaya
Fuente: Personal COPEU

Figura 8: Pregunta 4

Interpretación:

De acuerdo a la encuesta aplicada al personal de la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU indica que 19 personas que representa el 100% dicen que cuándo se produce alguna falla en el Sistema de Información Financiera.

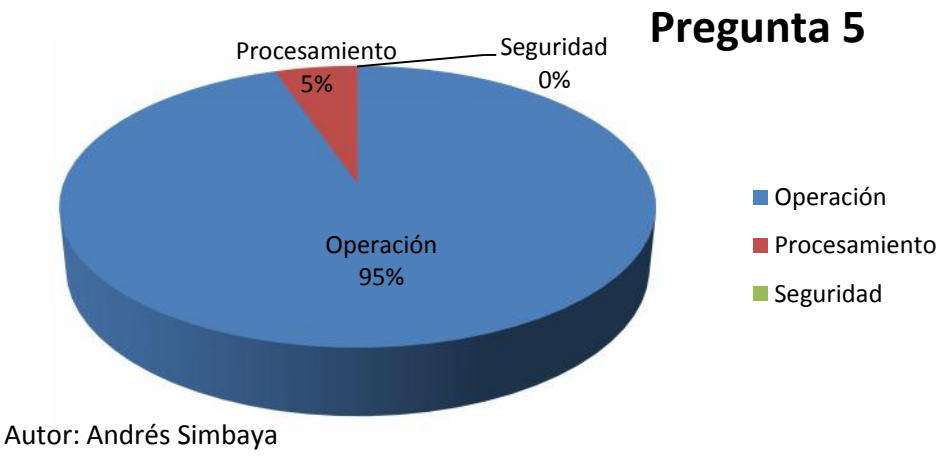
Análisis:

Se evidencia en los resultados de la pregunta que cuándo se produce alguna falla en el Sistema de Información Financiera se Llama al Técnico de la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU.

5. ¿Qué tipo de control de cambios se realiza al Sistema de Información Financiera?

N°	Ítems	Valores Numéricos	Valores Porcentuales
5.1	Operación	18	95%
5.2	Procesamiento	1	5%
5.3	Seguridad	0	0%
	Total	19	100%

Tabla 6: Pregunta 5



Autor: Andrés Simbaya
Fuente: Personal COPEU

Figura 9: Pregunta 5

Interpretación:

De acuerdo a la encuesta aplicada al personal de la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU indica que 18 personas que representan el 95% dicen que el tipo de control de cambios que se realiza al Sistema de Información Financiera es el de Operación, mientras que 1 persona que representa el 5% dicen que el tipo de control de cambios que se realiza al Sistema de Información Financiera es el de Procesamiento.

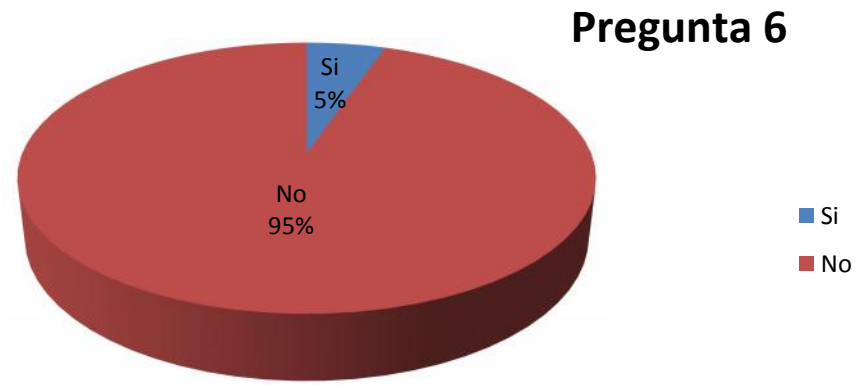
Análisis:

Se evidencia en los resultados de la pregunta que el tipo de control de cambios que se realiza al Sistema de Información Financiera es el de Operación en la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU.

6. ¿Se ha realizado una Auditoría Informática específicamente al Sistema de Información Financiera de la Cooperativa?

N°	Ítems	Valores Numéricos	Valores Porcentuales
6.1	Si	1	5%
6.2	No	18	95%
	Total	19	100%

Tabla 7: Pregunta 6



Autor: Andrés Simbaya
Fuente: Personal COPEU

Figura 10: Pregunta 6

Interpretación:

De acuerdo a la encuesta aplicada al personal de la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU indica que 1 persona que representa el 5% dice que se ha realizado una Auditoría Informática específicamente al Sistema de Información Financiera de la Cooperativa, mientras que 18 personas que representan el 95% dicen que no se ha realizado una Auditoría Informática específicamente al Sistema de Información Financiera de la Cooperativa.

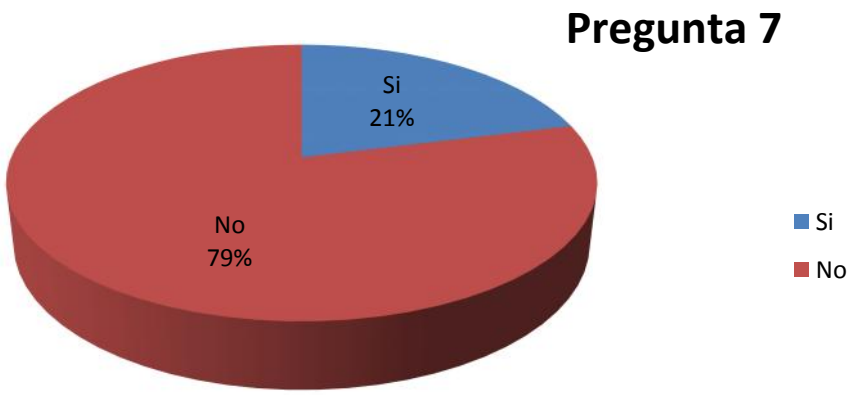
Análisis:

Se evidencia en los resultados de la pregunta que no se ha realizado una Auditoría Informática específicamente al Sistema de Información Financiera de la Cooperativa.

7. ¿Al realizar las actividades diarias, el sistema responde con agilidad en el proceso?

N°	Ítems	Valores Numéricos	Valores Porcentuales
7.1	Si	4	21%
7.2	No	15	79%
	Total	19	100%

Tabla 8: Pregunta 7



Autor: Andrés Simbaya
Fuente: Personal COPEU

Figura11: Pregunta 7

Interpretación:

De acuerdo a la encuesta aplicada al personal de la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU indica que 4 personas que representan el 21% dicen que al realizar las actividades diarias, el sistema responde con agilidad en el proceso, mientras que 15 personas que representan el 79% dicen que al realizar las actividades diarias, el sistema no responde con agilidad en el proceso.

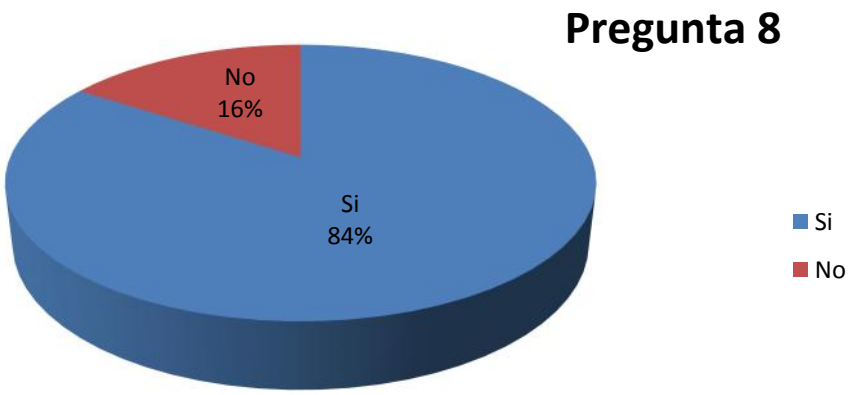
Análisis:

Se evidencia en los resultados de la pregunta que al realizar las actividades diarias, el sistema no responde con agilidad en el proceso en la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU.

8. ¿Tiene conocimiento de todos los procesos del software e información instalados en su computador?

N°	Ítems	Valores Numéricos	Valores Porcentuales
8.1	Si	16	84%
8.2	No	3	16%
	Total	19	100%

Tabla 9: Pregunta 8



Autor: Andrés Simbaya
Fuente: Personal COPEU

Figura 12: Pregunta 8

Interpretación:

De acuerdo a la encuesta aplicada al personal de la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU indica que 16 personas que representan el 84% dicen que tienen conocimiento de todos los procesos del software e información instalados en su computador, mientras que 3 personas que representan el 16% dicen que no tienen conocimiento de todos los procesos del software e información instalados en su computador.

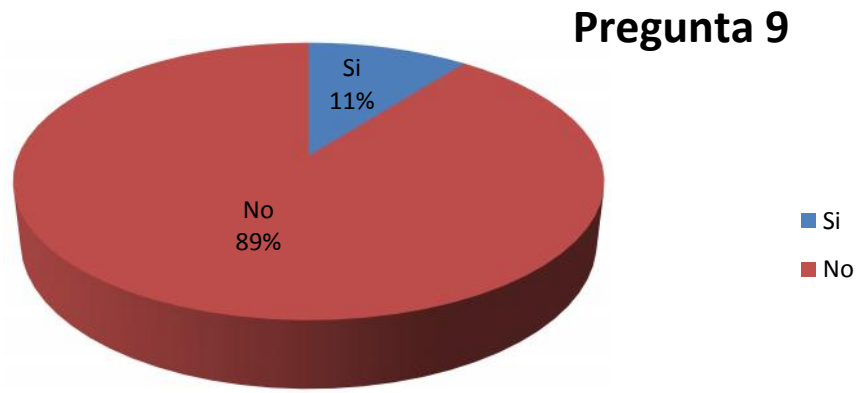
Análisis:

Se evidencia en los resultados de la pregunta que tienen conocimiento de todos los procesos del software e información instalados en su computador en la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU.

9. ¿El Sistema de Información Financiera posee la documentación adecuada?

N°	Ítems	Valores Numéricos	Valores Porcentuales
9.1	Si	2	11%
9.2	No	17	89%
	Total	19	100%

Tabla 10: Pregunta 9



Autor: Andrés Simbaya
Fuente: Personal COPEU

Figura 13: Pregunta 9

Interpretación:

De acuerdo a la encuesta aplicada al personal de la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU indica que 2 personas que representan el 11% dicen que el Sistema de Información Financiera posee la documentación adecuada, mientras que 17 personas que representan el 89% dicen que el Sistema de Información Financiera no posee la documentación adecuada.

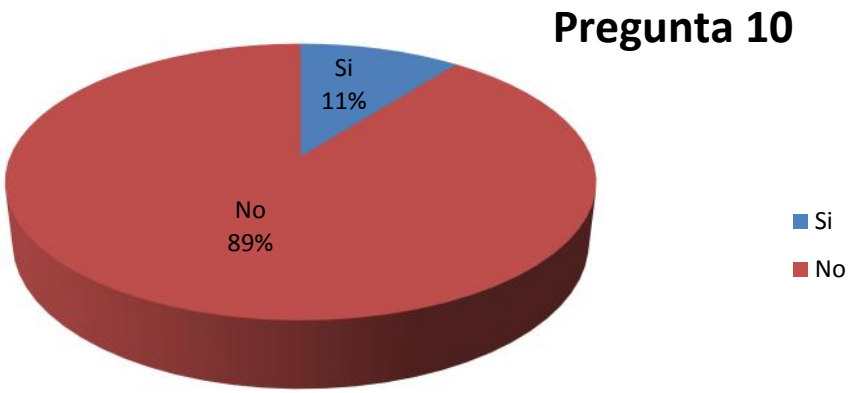
Análisis:

Se evidencia en los resultados de la pregunta que el Sistema de Información Financiera no posee la documentación adecuada en la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU.

10. ¿Se realiza chequeos habituales de mantenimiento al Sistema de Información Financiera en la Institución?

N°	Ítems	Valores Numéricos	Valores Porcentuales
10.1	Si	2	11%
10.2	No	17	89%
	Total	19	100%

Tabla 11: Pregunta 10



Autor: Andrés Simbaya
Fuente: Personal COPEU

Figura 14: Pregunta 10

Interpretación:

De acuerdo a la encuesta aplicada al personal de la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU indica que 2 personas que representan el 11% dicen que se realiza chequeos habituales de mantenimiento al Sistema de Información Financiera en la Institución, mientras que 17 personas que representan el 89% dicen que no se realiza chequeos habituales de mantenimiento al Sistema de Información Financiera en la Institución.

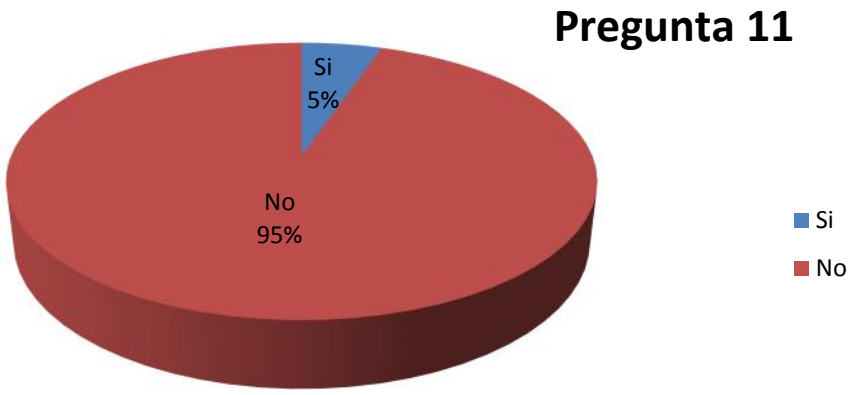
Análisis:

Se evidencia en los resultados de la pregunta que no se realiza chequeos habituales de mantenimiento al Sistema de Información Financiera en la Institución.

11. ¿Se efectúan actualizaciones del sistema periódicamente?

N°	Ítems	Valores Numéricos	Valores Porcentuales
11.1	Si	1	5%
11.2	No	18	95%
	Total	19	100%

Tabla 12: Pregunta 11



Autor: Andrés Simbaya
Fuente: Personal COPEU

Figura 15: Pregunta 11

Interpretación:

De acuerdo a la encuesta aplicada al personal de la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU indica que 1 persona que representa el 5% dice que se efectúan actualizaciones del sistema periódicamente, mientras que 17 personas que representan el 95% dicen que no se efectúan actualizaciones del sistema periódicamente.

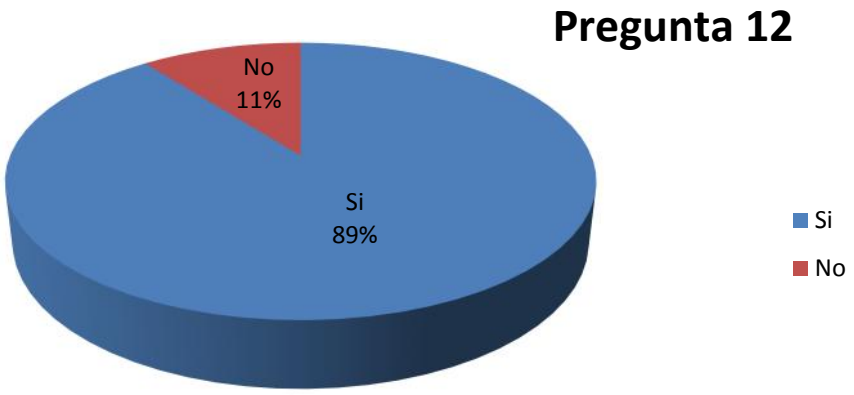
Análisis:

Se evidencia en los resultados de la pregunta que no se efectúan actualizaciones del sistema periódicamente en la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU.

12. ¿Existen procesos en la institución para los que no se usa el sistema?

N°	Ítems	Valores Numéricos	Valores Porcentuales
12.1	Si	17	89%
12.2	No	2	11%
	Total	19	100%

Tabla 13: Pregunta 12



Autor: Andrés Simbaya
Fuente: Personal COPEU

Figura 16: Pregunta 12

Interpretación:

De acuerdo a la encuesta aplicada al personal de la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU indica que 17 personas que representan el 89% dicen que existen procesos en la institución para los que no se usa el sistema, mientras que 2 personas que representan el 11% dicen que no existen procesos en la institución para los que no se usa el sistema.

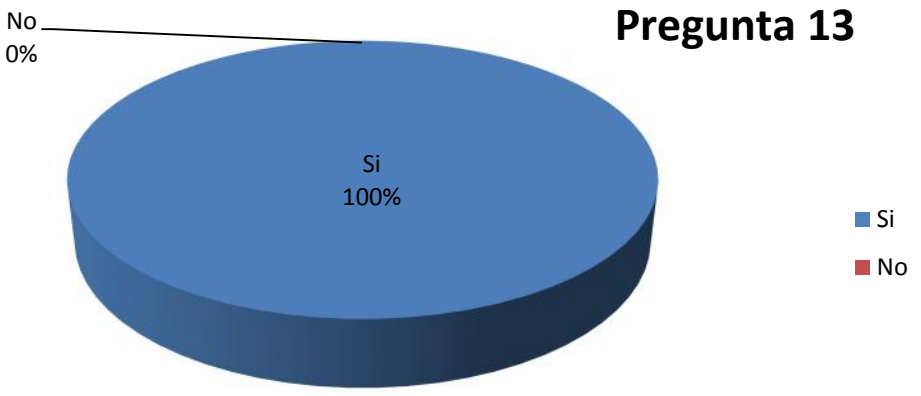
Análisis:

Se evidencia en los resultados de la pregunta que existen procesos en la institución para los que no se usa el sistema en la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU.

13. ¿Cree Ud. Necesario la implementación de un nuevo Sistema de Información Financiera?

N°	Ítems	Valores Numéricos	Valores Porcentuales
13.1	Si	19	100%
13.2	No	0	0%
	Total	19	100%

Tabla 14: Pregunta 13



Autor: Andrés Simbaya
Fuente: Personal COPEU

Figura 17: Pregunta 13

Interpretación:

De acuerdo a la encuesta aplicada al personal de la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU indica que 19 personas que representa el 100% dicen que es necesario la implantación de un nuevo Sistema de Información Financiera.

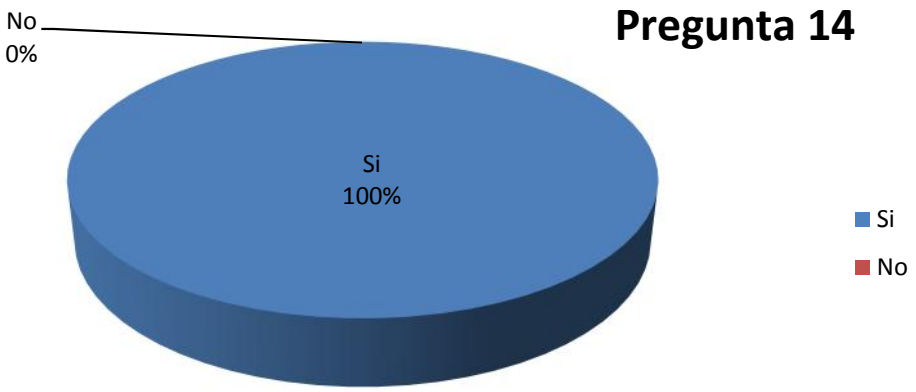
Análisis:

Se evidencia en los resultados de la pregunta que es necesario la implantación de un nuevo Sistema de Información Financiera en la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU.

14. ¿Cree Ud. que un nuevo Sistema de Información Financiera mejoraría el proceso y velocidad en las transacciones?

N°	Ítems	Valores Numéricos	Valores Porcentuales
14.1	Si	19	100%
14.2	No	0	0%
	Total	19	100%

Tabla 15: Pregunta 14



Autor: Andrés Simbaya
Fuente: Personal COPEU

Figura 18: Pregunta 14

Interpretación:

De acuerdo a la encuesta aplicada al personal de la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU indica que 19 personas que representa el 100% dicen que un nuevo Sistema de Información Financiera mejoraría el proceso y velocidad en las transacciones.

Análisis:

Se evidencia en los resultados de la pregunta que un nuevo Sistema de Información Financiera mejoraría el proceso y velocidad en las transacciones en la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU.

Se ha tomado en cuenta las preguntas discriminantes 6, 7 de la encuesta aplicada, con los siguientes resultados.

Pregunta #1. (Pregunta 6) ¿Se ha realizado una Auditoría Informática específicamente al Sistema de Información Financiera de la Cooperativa?

Resumen: El no realizar una Auditoría Informática al Sistema de Información Financiera es motivo de muchos inconvenientes para la Cooperativa, por lo que no se sabe el estado funcional del sistema en cuanto a transacciones y su rendimiento.

Pregunta #2. (Pregunta 7) ¿Al realizar las actividades diarias, el sistema responde con agilidad en el proceso?

Resumen: Si el sistema no responde con agilidad en las actividades cotidianas que realiza la Cooperativa debe ser evaluado para que no cause inconvenientes en los procesos y así no ocasionar pérdidas a la Cooperativa.

2.7 Comprobación Hipótesis

Preguntas	Resultados
(Pregunta 1) ¿Se han realizado Auditorías Informáticas en la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU)?	El 100% del personal manifestó que si se ha realizado Auditorías Informáticas en la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU).
(Pregunta 2) ¿Las Auditorías Informáticas realizadas en la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU) han servido para el progreso y mejor desempeño de la misma?	El 100% del personal manifestó que las Auditorías Informáticas realizadas en la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU) han servido para el progreso y mejor desempeño de la misma.
(Pregunta 6) ¿Se ha realizado una Auditoría Informática específicamente al Sistema de Información Financiera de la Cooperativa?	El 95% del personal manifestó que no se ha realizado una Auditoría Informática específicamente al Sistema de Información Financiera de la Cooperativa.
(Pregunta 7) ¿Al realizar las actividades diarias, el sistema responde con agilidad en el proceso?	El 79% del personal manifestó que no responde con agilidad el sistema en las actividades diarias.

Tabla 16: Cuadro Comprobación Hipótesis

Tomando en cuenta las encuestas realizadas al personal de la Cooperativa de Ahorro y Crédito Universitaria Limitada, se puede evidenciar que se han realizado Auditorías Informáticas que han servido para el progreso y mejor desempeño de la misma, pero no se ha realizado una Auditoría Informática específicamente al Sistema de Información de la Cooperativa, siendo este la herramienta fundamental que facilita las actividades laborales que desempeña a diario el personal de la Cooperativa con lo que se evidencia el descuido al Sistema de Información Financiera por parte de la institución, por lo que se sugiere realizar una Auditoria Informática que permita verificar la funcionalidad del Sistema de Información Financiera para corregir falencias que afronta la institución y dar la mejor solución posible aplicando la Metodología Magerit Versión 3 y la Herramienta Pilar 5.2.9.

CAPÍTULO III

3. MARCO METODOLÓGICO

3.1 Enfoque

El presente trabajo investigativo tomará un enfoque Cuali-Cuantitativo ya que se trabajará con sentido participativo considerando una realidad dinámica pero al mismo tiempo estará orientada a la comprobación de hipótesis y con énfasis en el resultado.

Se desarrollará en entorno natural, considerando la participación de las personas que intervienen dentro del problema, su cultura y creencia. Además es interna porque permite analizar de manera interna el problema, se considera interpretativa porque permite analizar sus resultados.

Además, será normativa porque se generará una norma o herramienta a seguir, se considera nomotética porque llevará a un fin concreto, se considera externa porque se determinará la influencia del problema con relación a la sociedad, se considera explicativa porque permitirá explicar los resultados a obtener.

3.2 Modalidades Básicas de la Investigación

La presente investigación tiene las siguientes modalidades:

Modalidad Bibliográfica o Documentada: Se ha considerado esta modalidad porque se ha tomado información de Internet, Libros virtuales, Tesis, Artículos publicados en la Web, Libros, entre otros.

Modalidad Campo: Se ha considerado esta modalidad ya que el investigador irá a recoger la información primaria directamente de los involucrados a través de encuestas y entrevistas.

3.3 Tipos de Investigación

Se ha realizará la Investigación Exploratoria, ya que permitirá determinar las condiciones actuales del Sistema de Información Financiera.

Se ha considerará la Investigación Descriptiva porque permitirá analizar el problema en sus partes como delimitar en tiempo y en espacio construyendo el Análisis Crítico, la Contextualización y los Antecedentes Investigativos.

Por otro lado se ha tomado la investigación Correlacional ya que se determinará la relación de una variable con otra y la incidencia que tiene en la solución del problema.

3.4 Población y Muestra

La población que se va a considerar en la presente investigación será la totalidad del personal que actualmente labora en la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU).

Población y Muestra COPEU.

POBLACIÓN	TOTAL	FRECUENCIA
DIRECTIVOS	9	47,4%
CONSEJOS *	5	26,3%
EMPLEADOS	5	26,3%
TOTAL	19	100%

*Consejo de Administración, Consejo de Vigilancia.

Tabla 17: Cuadro Población y Muestra

Debido a que la población es pequeña no se definirá una muestra y se trabajará con el total de la población.

3.5 Operacionalización de Variables

Variable Independiente: Auditoría Informática

Concepto	**Categorías**	**Indicadores**	**Ítems**	**Técnicas e instrumentos**
La Auditoría Informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos	Proceso Evidencia Sistema Informatizado Recurso	• Si • No • Si • No • Si • No • Solo • Llama al Supervisor • Llama al Técnico • Operación • Procesamiento • Seguridad • Si • No	¿Se han realizado Auditorías Informáticas en la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU)? ¿Las Auditorías Informáticas realizadas en la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU) han servido para el progreso y mejor desempeño de la misma? ¿Se lleva algún registro y seguimiento de los fallos producidos por el Sistema de Información Financiera? ¿Cuándo se produce alguna falla en el Sistema de Información Financiera usted soluciona el problema? ¿Qué tipo de control de cambios se realiza al Sistema de Información Financiera? ¿Se ha realizado una Auditoría Informática específicamente al Sistema de Información Financiera de la Cooperativa?	Encuesta a través de un cuestionario aplicada al personal de la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU). .

Tabla 18: Operacionalización Variable Independiente

Variable Dependiente: Sistema de Información Financiera.

Concepto	Categorías	Indicadores	Ítems	Técnicas e instrumentos
Los sistemas de información financiera proporcionan a personas y grupos (stakeholders) tanto de dentro como de fuera de la organización información relacionada con los asuntos financieros de la compañía.	Sistema	• Si • No	¿Al realizar las actividades diarias, el sistema responde con agilidad en el proceso?	Encuesta a través de un cuestionario aplicada al personal de la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU).
	Información	• Si • No • Si • No	¿Tiene conocimiento de todos los procesos del software e información instalados en su computador? ¿El Sistema de Información Financiera posee la documentación adecuada?	
	Financiero	• Si • No • Si • No • Si • No	¿Se realiza chequeos habituales de mantenimiento al Sistema de Información Financiera en la Institución? ¿Se efectúan actualizaciones del sistema periódicamente? ¿Existen procesos en la institución para los que no se usa el sistema?	
	Compañía	• Si • No • Si • No	¿Cree Ud. necesario la implementación de un nuevo sistema de información financiera en la Cooperativa? ¿Cree Ud. que usted que un nuevo sistema de información financiera mejoraría el proceso y velocidad en las transacciones?	

Tabla 19: Operacionalización Variable Dependiente

3.6 Recolección y Análisis de la Información

SECUNDARIA	PRIMARIA
• Se recolectó de estudios realizados anteriormente como Tesis de Grado que se han realizado anteriormente. • Se encuentra registrada en documentos y material impreso: libros, revistas especializadas, tesis de grado, etc. • Las fuentes de información son: bibliotecas, archivos, internet.	• Se recolecta directamente a través del contacto directo con el personal de la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU).

Tabla 20: Recolección y Análisis de la Información

Técnicas de Investigación

BIBLIOGRÁFICAS	DE CAMPO
• La información se encuentra registrada en: • Libros, archivos	• La encuesta • Observación

Tabla 21: Técnicas de Investigación

Recolección de la Información

PREGUNTAS	EXPLICACIÓN
1. ¿Para Qué?	Recolectar Información primaria para comprobar y contrastar la Hipótesis
2. ¿A Qué Personas o Sujetos?	La información se tomará al personal que actualmente labora en la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU).
3. ¿Sobre Qué Aspectos?	**V.I.** Auditoria Informática **V.D.** Sistema de Información Financiera

4. ¿Quién?	Carlos Andrés Simbaya Camacho
5. ¿Cuándo?	De acuerdo al cronograma establecido
6. ¿Lugar de Recolección de la Información?	Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU) y su Sucursal.
7. ¿Cuántas veces?	Una sola vez
8. ¿Qué técnicas de recolección?	Encuesta
9. ¿Con Qué?	Cuestionario
10. ¿En Qué Situación?	Situación Normal y Cotidiana

Tabla 22: Recolección de la Información

3.7 Procesamiento y Análisis de la Información

1. Revisión y Codificación de la Información

2. Categorización y Tabulación de la Información

- Tabulación Manual
- Tabulación Computarizada: Programa Microsoft Excel 2010

3. Análisis de los datos

- La presentación de los datos se lo hará a través de cuadros para analizarlos e interpretarlos.

4. Interpretación de los Resultados

- Describir los resultados
- Estudiar cada uno de los resultados por separado
- Redactar una síntesis general de los resultados

CAPÍTULO IV

4. DESARROLLO DE LA PROPUESTA

Inconsistencias de Auditorías Informáticas en la Cooperativa

Auditoría	Áreas Evaluadas	Objetivos	Inconsistencias
Auditoría de la unidad informática de la Cooperativa de Ahorro y Crédito Universitaria Limitada.	-Sistema de Información -Financiera Software Ilegal -Cableado Estructurado -Software Desactualizado	-Evaluar el desempeño del sistema de información, y el uso de los recursos informáticos que posee la Cooperativa de Ahorro y Crédito Universitaria Limitada, utilizando herramientas adecuadas con el fin de comprobar el funcionamiento de los mismos y contribuir con el mejoramiento de la entidad auditada para incrementar la seguridad de la información. -Evaluar el cumplimiento de políticas de seguridad.	-Se ha evaluado al Sistema de Información Financiera, pero solo si es software legal más no su funcionamiento y componentes. -El antivirus no está con licencia y desactualizado.
Auditoria de Control Interno en los Procedimientos para la Colocación de Créditos y su incidencia en la Rentabilidad de la Cooperativa de Ahorro y Crédito Universitaria Limitada.	-Área de Créditos -Área de Cobros	-Elaborar políticas y procedimientos para la colocación y cobranza de créditos enfocada a buscar el desarrollo de la cooperativa y satisfacer la demanda de crédito. -Proporcionar un manual de políticas y procedimientos eficaz que permita el buen funcionamiento del área de Créditos y cobros, a través de mejorar la recuperación de cartera de clientes, obteniendo como resultado una excelencia solvencia, rentabilidad y liquidez.	-Se ha evaluado el área de créditos y Cobros pero no al Sistema de Información Financiera. -Los porcentajes de los Créditos son muy elevados ya que se compara con bancos y la Cooperativa es pequeña ya que recién se encuentra en crecimiento.

En conclusión podemos acotar que se han realizado Auditorías Informáticas que han sido de gran ayuda en algunos puntos para la Cooperativa pero no se auditado específicamente al Sistema de Información Financiera así como también se ha encontrado unas inconsistencias como el antivirus que está sin licencia y desactualizado y los Créditos que están un poco elevados ya que se han comparado con Bancos que son entidades mucho más grandes que la Cooperativa que recién se encuentra en proceso de desarrollo y crecimiento.

4.1 Introducción a Magerit Versión 3

Magerit es el acrónimo de "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Publicas", creado por el Consejo Superior de Administración Electrónica (CSAE). El uso de esta metodología es de carácter público, pertenece al Ministerio de Administraciones Públicas (MAP) de España.

Se elaboró Magerit porque está dirigido a los medios electrónicos, informáticos y telemáticos, ya que su uso en la actualidad es frecuente, lo cual ha dado lugar al origen de ciertos riesgos que se deben de evitar con medidas preventivas para lograr tener confianza en utilizarlos.

4.2 Historia y evolución

En la actualidad se encuentra en la versión 3.0, pero el tiempo ha pasado desde la primera publicación de Magerit en 1997, y su segunda publicación en 2005, donde el análisis de riesgos se ha venido consolidando como eje central para la gestión de la seguridad.

4.3 Objetivos de Magerit

En el libro I de la publicación de Magerit versión 3 persigue los siguientes objetivos:

Directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos:

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

4.4 Metodología Magerit Versión 3

Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina "Proceso de Gestión de los Riesgos", ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos". En otras palabras, Magerit implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados de uso de tecnologías de la información.

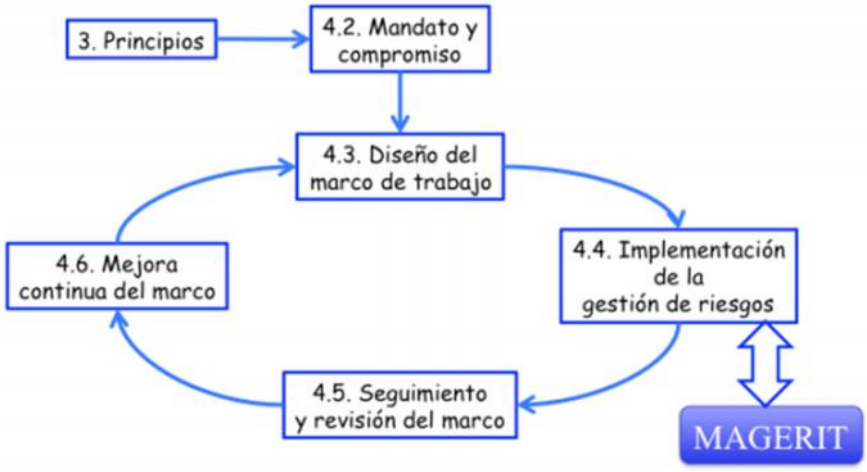


Figura 19: ISO 31000 - Marco de trabajo para la gestión de riesgos
Fuente: Tomado del Libro 1 de Magerit versión 3

Existen varias aproximaciones que sirven para analizar los riesgos que pueden sufrir sistemas y las tecnologías de la información y comunicación: guías formales, aproximaciones metódicas y herramientas de soporte. Todas ellas tienen como finalidad el saber cuan seguros o inseguros son los sistemas. Existen muchos elementos que hay que considerar para lograr tener buenos resultados. Es por ello que Magerit está basado sobre una aproximación metódica que no deja lugar a la improvisación, ni dependa de la arbitrariedad del analista.

4.5 Elementos de Magerit Versión 3

A continuación definimos brevemente los elementos de MAGERIT para el estudio de los Sistemas de Información.

Activos: recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la Dirección.

Amenazas: eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o perdidas inmateriales en sus activos.

Vulnerabilidad de un activo: potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.

Impacto de un activo: consecuencia sobre éste de la materialización de un activo.

Riesgo: posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.

Servicio de salvaguarda: acción que reduce el riesgo.

La siguiente figura muestra los elementos y sus interrelaciones:

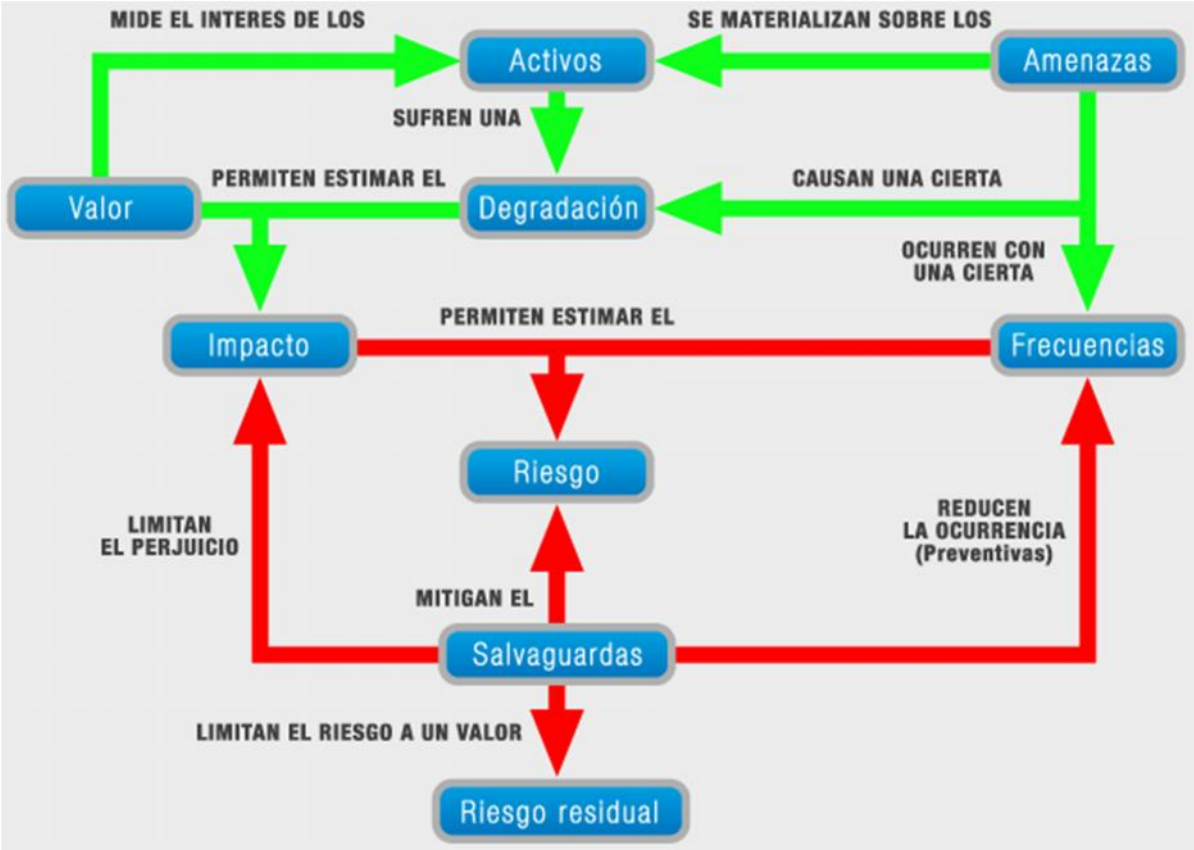


Figura 20: Elementos de Magerit versión 3
Fuente: Tomado de Magerit versión 3

4.6 Herramienta P.I.L.A.R

PILAR, es el acrónimo de "Procedimiento Informático-Lógico para el Análisis de Riesgos" es una herramienta desarrollada por el Centro Nacional de Inteligencia para soportar el Análisis de Riesgos de Sistemas de Información basado en la metodología Magerit.

Esta herramienta se puede hacer todas las actividades que se realizan en el Análisis y Gestión de Riesgos:

- Determinación de Activos: Identificación, dependencias y valoración.
- Determinación de Amenazas
- Estimación de Impactos
- Determinación de los criterios de aceptación del riesgo

- Determinación de las medidas de seguridad necesarias o Salvaguardas.

Este software permite hacer un Análisis de Riesgos sobre las dimensiones de valoración como son: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

Además nos ayuda con el cálculo del impacto y el riesgo, acumulado, repercutido, potencial y residual.

PILAR puede hacer análisis cuantitativo y cualitativo.

Figura 21: Primer Pantallazo de Pilar 5.2.9
Fuente: Herramienta PILAR 5.2.9

Los resultados se presentan en diversos formatos como son: gráficas y tablas donde se pueden incorporar hojas de cálculo.

A continuación vamos a mostrar unos pantallazos de la herramienta.

1 Después de la pantalla principal elegimos el Análisis Cualitativo que es el que vamos aplicar.

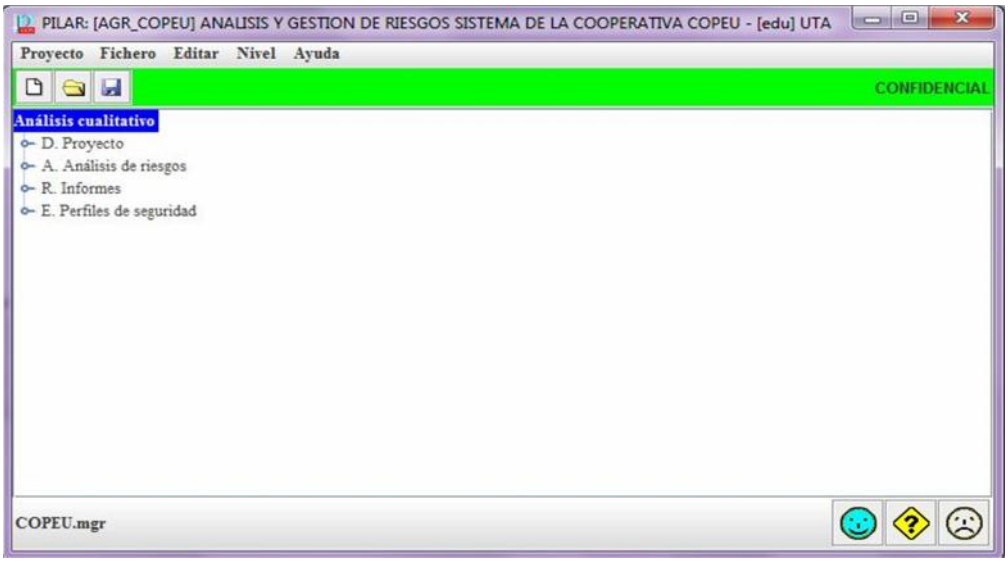


Figura 22: Pantalla Análisis Cualitativo
Fuente: Herramienta PILAR 5.2.9

2 Procedemos a dar click en nuevo para crear un proyecto nuevo.

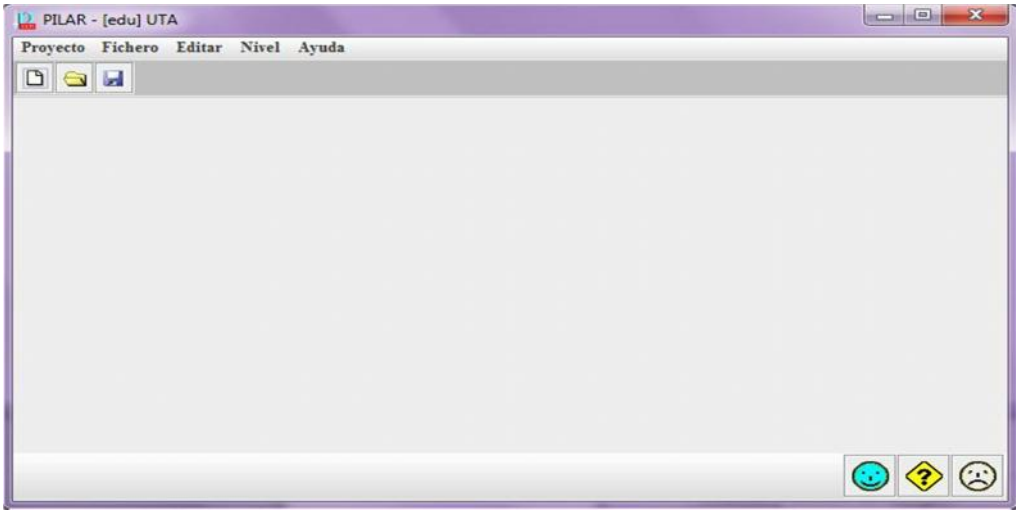


Figura 23: Pantalla Proyecto Nuevo
Fuente: Herramienta PILAR 5.2.9

3 Llenamos los datos requeridos y procedemos a guardar.

Figura 24: Pantalla Llenado de Información
Fuente: Herramienta PILAR 5.2.9

4 Creamos el dominio que se llamara COPEU

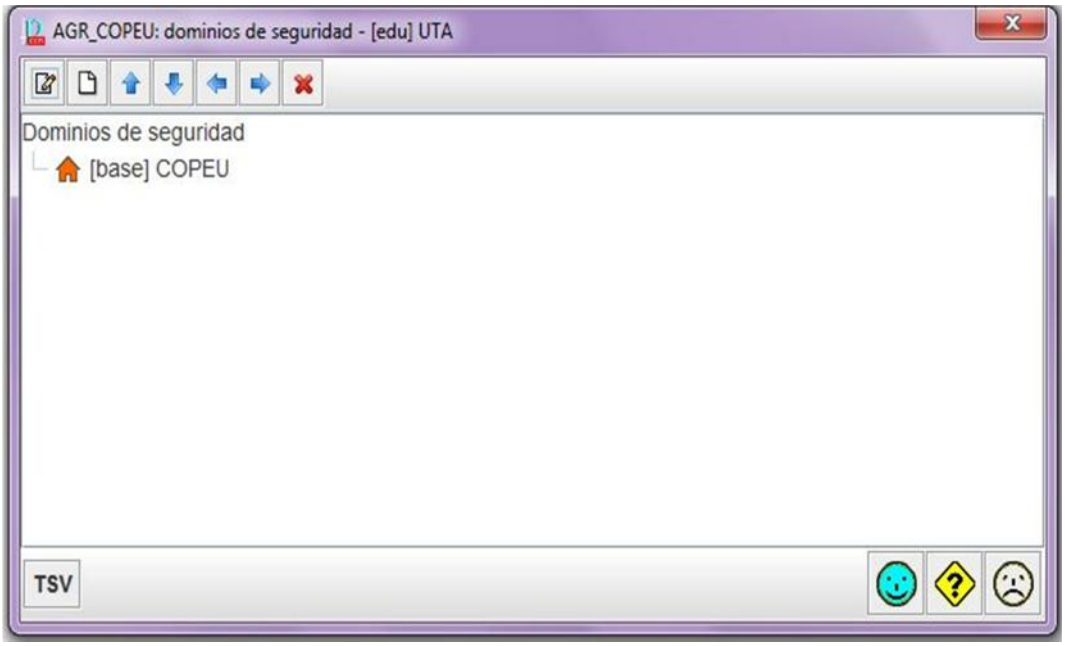


Figura 25: Pantalla Creación del Dominio
Fuente: Herramienta PILAR 5.2.9

5 Las fases del proyecto que serán la situación actual y la situación objetivo.

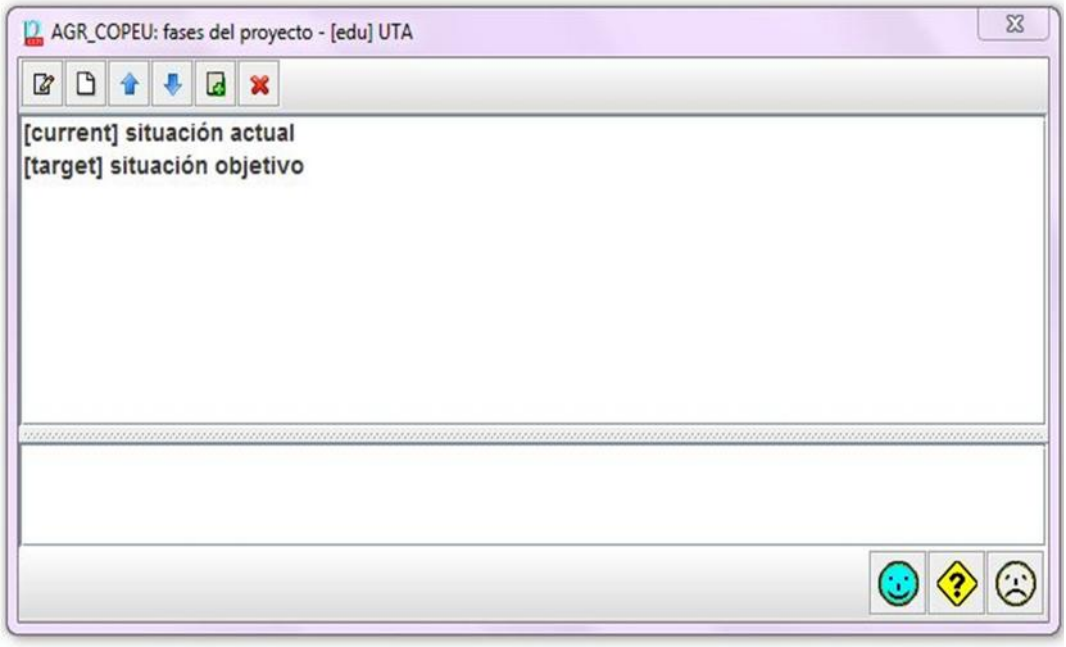


Figura 26: Pantalla Fases del Proyecto
Fuente: Herramienta PILAR 5.2.9

6 Identificación de los activos.

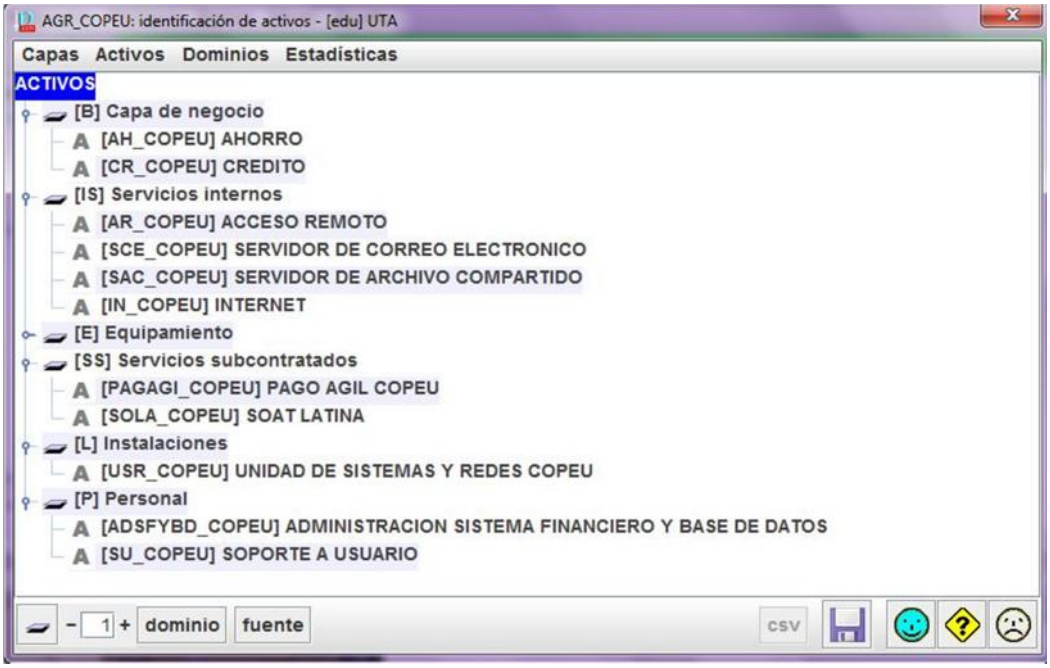


Figura 27: Pantalla Identificación de Los Activos
Fuente: Herramienta PILAR 5.2.9

7 A continuación mostramos una pantalla de todo lo que procederemos hacer para poder aplicar la metodología MAGERIT Versión 3 como son:

Activos: Identificación, Clases de Activos, Dependencias, Valores de los Activos

Amenazas: Factores agravantes/atenuantes, Identificación, Valoración.

Salvaguardas: Identificación, Valoración.

Impacto y Riesgo: Valores Acumulados, Valores Repercutidos.

Informes: Por Patrón, Textuales y Graficas.

Perfiles de Seguridad: Código de buenas prácticas para la Gestión de la Seguridad de la Información.

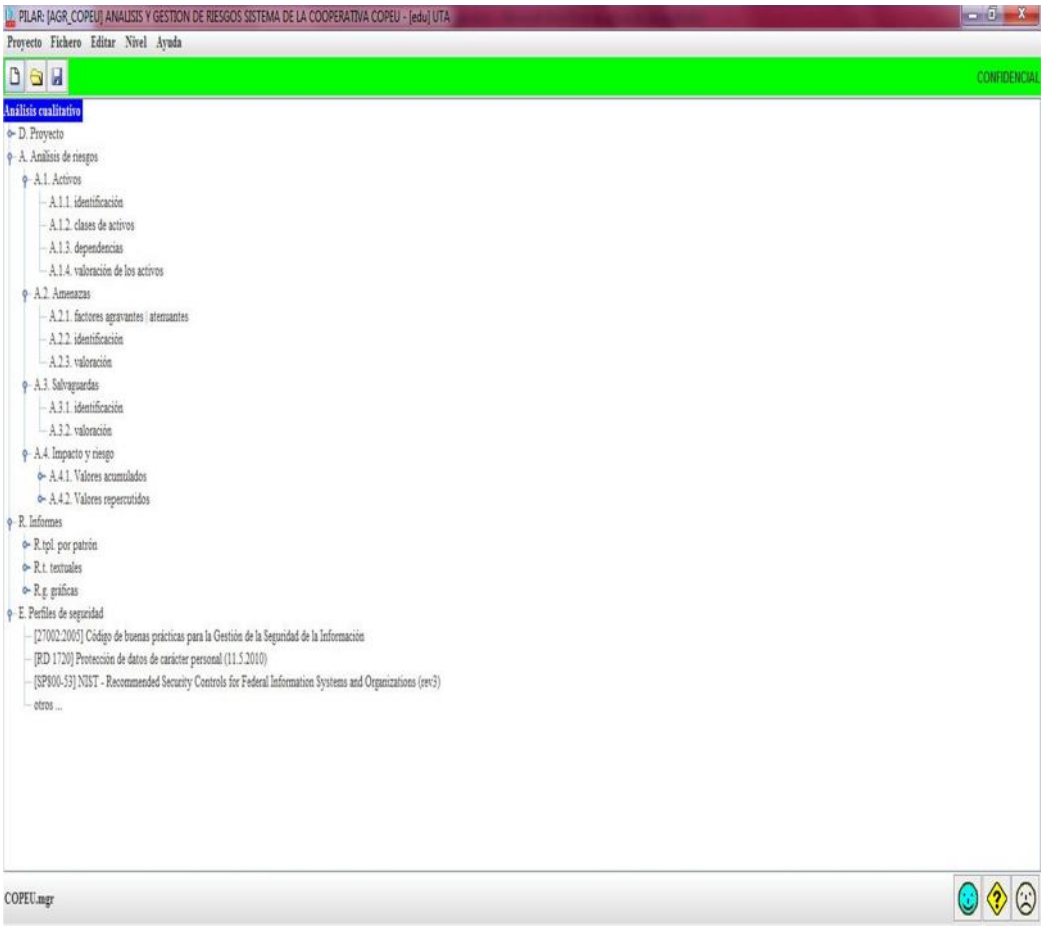


Figura 28: Pantalla Todo los procesos a Realizar EN Pilar 5.2.9
Fuente: Herramienta PILAR 5.2.9

4.7 Fases de Magerit Versión 3

Las fases que contempla el modelo MAGERIT son:

- Planificación del Proyecto.- establece el marco general de referencia para el proyecto
- Análisis de Riesgos.- permite determinar cómo es, cuánto vale y cómo de protegidos se encuentran los activos
- Gestión de Riesgos.- permite la selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados

4.7.1 Planificación del Proyecto

4.7.1.1 Objetivos

Antes de iniciar con el Análisis y Gestión de Riesgos (AGR) de los sistemas de información (S.I) de la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU), es importante que conozcamos la situación que presentan los S.I., lo cual podemos conocer mediante la etapa de Planificación, la misma que tiene como objetivo principal establecer el marco general de referencia para todo el proyecto.

El proyecto de AGR será desarrollado con la metodología MAGERIT versión 3 bajo la aplicación de la herramienta PILAR versión 5.2.9.

Su objetivo principal es:

- Implantar una visión general de referencia para todo el proyecto

Como objetivos complementarios a lograrse en esta etapa podemos identificar los siguientes:

- Motivar y concienciar a la Gerencia de la Organización
- Razonar y validar la oportunidad de realizar un proyecto AGR
- Dar a conocer la voluntad de la Gerencia para la realización del proyecto

- Crear condiciones adecuadas y necesarias para el buen desarrollo del proyecto

Para un trabajo eficiente de la etapa de Planificación, se necesitará la colaboración y participación de todo el personal involucrado con los sistemas de información.

Para el desarrollo del proceso de Planificación de Análisis y Gestión de Riesgos, aplicaremos los siguientes pasos:

- Estudio de oportunidad
- Determinación del alcance del proyecto
- Planificación del proyecto
- Lanzamiento del proyecto

4.7.1.2 Estudio de oportunidad

Esta actividad tiene como objetivo:

- Impulsar el desarrollo del proyecto de Análisis y Gestión de Riesgos en la "Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU)."

En la "Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU)." se han beneficiado de la colaboración que brindan las nuevas tecnologías informáticas y comunicación a su funcionamiento, pero no se han percatado de los problemas de seguridad que estas tecnologías traen.

Mediante entrevistas y encuestas realizadas al Personal de la Cooperativa se ha percibido que se ha generado incidentes significativos relacionados a la seguridad y deterioro del sistema así como su agilidad en el funcionamiento.

Como es la falta de mantenimiento a los soportes de información, donde la información queda vulnerable para los empleados que acceden a ella.

El ambiente inadecuado donde está situado el servidor que almacena la información del sistema “MQR” así como fallos y problemas que presenta el mismo sistema ya por el tiempo que ya está deteriorado.

En cuanto a las contraseñas de cada computadora de escritorio, no son confidenciales, lo que puede provocar robo de información.

Los antivirus que están desactualizados

4.7.1.3 Determinación del alcance del proyecto

Después de haber comprobado la oportunidad de ejecutar el proyecto de Análisis y Gestión de Riesgos, en esta fase se procede a identificar los objetivos que debe cumplir el proyecto y definir su dominio y límites.

Los objetivos se ordenan en tres ciclos

- Definir una programación orientada a la seguridad del sistema de información.
- Analizar el estado actual de la empresa y especificar cuáles son las necesidades de mayor importancia respecto a la seguridad.
- Escoger mecanismos de salvaguarda.

El dominio de proyecto se centra en el Departamento Informático de la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU).

Personal del Departamento que van a estar involucrados en la realización del proyecto:

Ingeniero Francisco Mena – Gerente de la Cooperativa

Ingeniera Cristina Guerra - Persona encargada del manejo del sistema MQR, manejo de la Base de Datos y Digitadora.

Ingeniera Miriam Peñaherrera - Persona encargada del mantenimiento del sistema MQR, así como también encargada del mantenimiento de los equipos informáticos

4.7.1.4 Planificación del proyecto

Esta actividad estima los elementos de Planificación del proyecto, es decir sus cargas de trabajo, el grupo de usuarios, los participantes y su modo de actuación y el plan de trabajo para la realización del proyecto.

En la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU) para la realización de las entrevistas y encuestas en la que se hará una cita a cada entrevistado en un plazo no mayor a 15 días laborables.

Las entrevistas nos ayudaran a determinar por ámbito a los usuarios afectados y a planificar la intervención de ellos en el proyecto.

Y las encuestas arrojarán porcentajes exactos sobre las fallas de seguridad en los sistemas de información y su demás entorno.

El proyecto AGR de los Sistemas de información de la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU) está constituido por los siguientes órganos:

Equipo de investigación: Carlos Andrés Simbaya Camacho estudiante de Ingeniería de Sistemas de la Universidad Politécnica Salesiana sede Cuenca.

Grupo de usuarios: está formado por los utilizadores, actuales del Sistema de Información.

4.7.1.5 Lanzamiento del proyecto

Para la recolección de la información se ha escogido las fichas de captura de datos del Apéndice 2 del libro – Catálogo de Elementos MAGERIT – versión 3, ya que se ajusta a las necesidades de este tipo de proyectos.

Las fichas de captura de datos recogen información específica de cada activo perteneciente a la Cooperativa tomando en cuenta como dimensiones de seguridad y dependencias de activos, que ayudará a identificar correctamente lo que son:

vulnerabilidades, impactos, salvaguardas efectivas. La situación de la seguridad de los sistemas de información de la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU) es el resultado de la incorporación de salvaguardas tomadas para prevenir o reducir riesgos que no han sido debidamente estudiadas de forma sistemática. (Ver Anexo 2. Fichas para la recolección de datos)

Gracias al análisis de riesgos permitirá sistematizar las medidas actuales y mejorarlas con algunas otras que serán suficientes para lograr un nivel de seguridad estable.

La Cooperativa de Ahorro y Crédito Universitaria Limitada dispone de los recursos a utilizarse para el desarrollo del proyecto en disponibilidad de equipos, tiempos planificados, medios materiales- herramientas, envío de documentos y manuales.

Primeramente se estableció la comunicación a las unidades afectadas sobre el lanzamiento del proyecto. Se tuvo comunicación con el Ingeniero Francisco Mena, sobre el proyecto y su contenido, quien nos supo informar que la unidad implicada conoce sobre el proyecto y que estén prestos ayudarnos para el desarrollo del mismo. Además se envió un oficio a la Gerencia en el cual se indicaba el proyecto, la metodología y demás parámetros formales para un buen desempeño del proyecto de Análisis y Gestión de Riesgos.

Indicando lo anterior, se informó que el proyecto está autorizado y listo para su ejecución.

4.7.2 Análisis de Riesgos

Como es de conocimiento general, de toda organización se encuentra expuesta a riesgos; debido a que no existe un entorno 100% seguro, ya que la exposición de riesgos es constante. Por tal motivo toda organización deberá estar alerta a cualquier cambio o situación extraña y que considera que podría afectar negativamente a un activo, a un dominio o a toda su organización.

Esta etapa se constituye en el núcleo central de MAGERIT, y su correcta aplicación de condiciona la validez y utilidad de todo el proyecto.

Mediante del Análisis de Riesgos se deberán alcanzar los siguientes objetivos:

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza

Para la ejecución de esta fase, la recolección de la información será desarrollada mediante encuestas y entrevistas a los usuarios responsables de los sistemas de información de la "Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU).", del mismo modo se consideran las inspecciones físicas.

Mediante el análisis de riesgos se puede saber cuánto vale y como están protegidos los activos evaluándolos de manera metódica para obtener conclusiones con fundamento.

La siguiente figura recoge lo mencionado anteriormente.

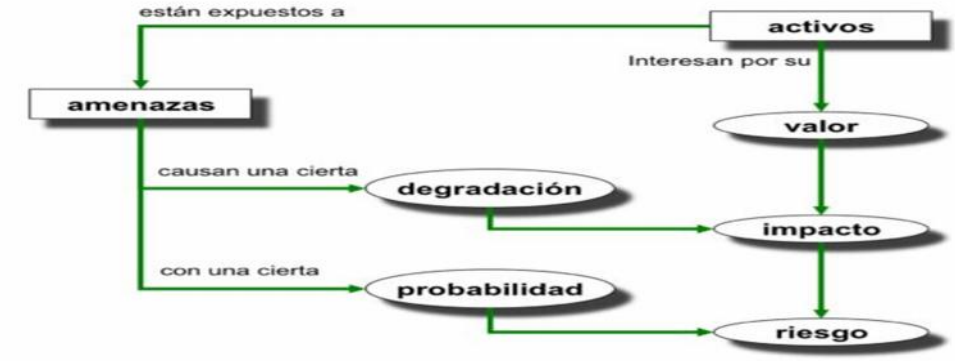


Figura 29: Análisis de Riesgo
Fuente: Magerit Versión 3

4.7.2.1 Caracterización de activos

Esta actividad consta de 3 sub-tareas:

- Identificación de los activos
- Dependencias entre los activos
- Valoración de los activos

El objetivo de estas tareas es reconocer los activos que componen el sistema, definir las dependencias entre ellos, y determinar de parte del valor del sistema se soporta en cada activo. Se puede resumir en la expresión “conócete a ti mismo.

4.7.2.1.1 Identificación de los activos

Esta tarea es crítica por que una, buena identificación permite realizar las siguientes tareas:

- Establecer las dependencias entre los activos
- Permite valorar a los activos con precisión
- Ayuda a identificar y valorar las amenazas
- Escoge que salvaguardas serán necesarias para proteger el sistema

4.7.2.1.1.1 [B] Capa de negocio

La capa de negocio principal de la Cooperativa son el Ahorro y el Crédito.

- [AH_COPEU] AHORRO
- [CR_COPEU] CREDITO

4.7.2.1.1.2 [IS] Servicios internos

Para los empleados, de la organización se presta los siguientes servicios:

- [AR_COPEU] ACCESO REMOTO
- [SCE_COPEU] SERVIDOR DE CORREO ELECTRONICO
- [SAC_COPEU] SERVIDOR DE ARCHIVO COMPARTIDO

- [IN_COPEU] INTERNET

4.7.2.1.1.3 [SW] Aplicaciones

Entre las aplicaciones que ostenta la Cooperativa tenemos los siguientes:

- [SISCO_COPEU] SISTEMA FINANCIERO COPEU
- [OF_COPEU] OFIMATICA
- [AN_COPEU] ANTIVIRUS
- [OTR_COPEU] OTRO SOFTWARE

4.7.2.1.1.4 [HW] Equipos

Dentro de los equipos informáticos que posee la Cooperativa tenemos los siguientes:

- [SBD_COPEU] SERVIDOR DE BASE DE DATOS
- [ROU_COPEU] ROUTER
- [SWI_COPEU] SWITCH
- [FIR_COPEU] FIREWALL
- [COM_COPEU] COMPUTADORAS DE ESCRITORIO
- [COMPO_COPEU] COMPUTADORAS PORTATILES
- [IMPLA_COPEU] IMPRESORA A LASER
- [IMPMA_COPEU] IMPRESORA MATRICIAL

4.7.2.1.1.5 [COM] Comunicaciones

A través de los siguientes medios de transporte de información tenemos:

- [REDLA_COPEU] RED LAN
- [REDWA_COPEU] RED WAN
- [INT_COPEU] INTERNET COPEU

4.7.2.1.1.6 [AUX] Elementos auxiliares

La Cooperativa cuenta con los siguientes equipos auxiliares:

- [CABDAT_COPEU] CABLEADO DE DATOS COPEU
- [EQUAUX_COPEU] EQUIPAMIENTO AUXILIAR

4.7.2.1.1.7 [SS] Servicios subcontratados

La Cooperativa cuenta con dos servicios subcontratados que sirve para el pago de diferentes servicios y el SOAT.

- [PAGAGI_COPEU] PAGO AGIL COPEU
- [SOLA_COPEU] SOAT LATINA

4.7.2.1.1.8 [L] Instalaciones

La infraestructura donde se localiza los sistemas de información y comunicación, está ubicado en Ingahurco El Salvador 05-39 y Av. Colombia, lateral a la UTA.

- [USR_COPEU] UNIDAD DE SISTEMAS Y REDES COPEU

4.7.2.1.1.9 [P] Personal

El personal involucrado en esta investigación esta los siguientes:

- [ADSFYBD_COPEU] ADMINISTRACION SISTEMA FINANCIERO Y BASE DE DATOS
- [SU_COPEU] SOPORTE A USUARIO

4.7.2.1.2 Dependencia entre los activos

Objetivo:

- Reconocer las dependencias entre activos, es decir la medida en que un activo de orden superior se puede ver perjudicado por una amenaza materializada sobre un activo de orden inferior.

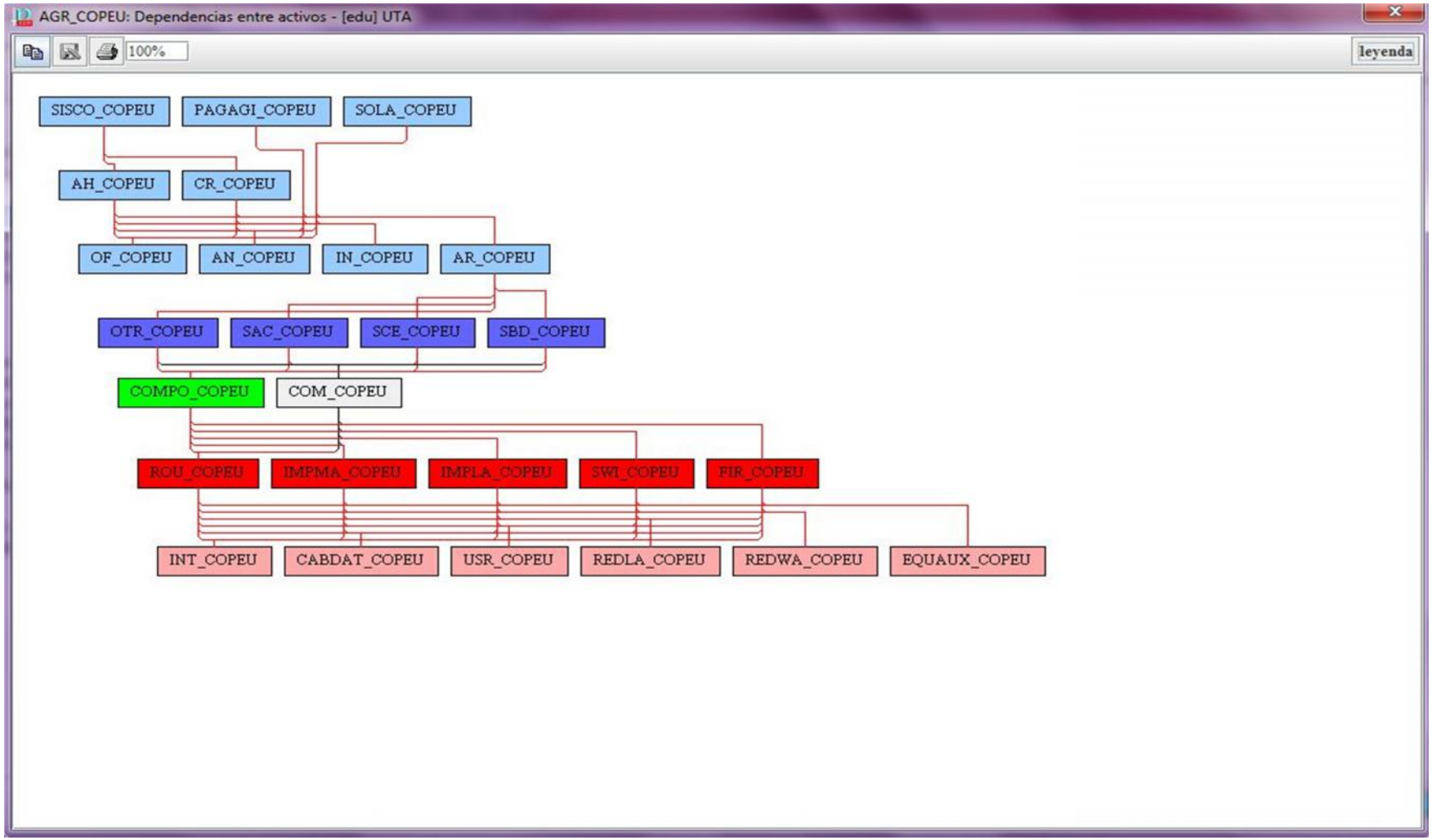


Figura 30. Diagrama de Dependencias entre los activos
Fuente: Realizado en PILAR 5.2.9

Leyenda

azul claro	activos superiores relacionados indirectamente
azul fuerte	activos superiores relacionados directamente
verde	el activo seleccionado
rojo fuerte	activos inferiores relacionados directamente
rojo claro	activos inferiores relacionados indirectamente
gris	sin relación

Figura 31: Código de Colores de Dependencia de Activos
Fuente: PILAR 5.2.9

Se realizó esta dependencia de activos gracias a las entrevistas y encuestas realizadas a los empleados donde se pudo categorizar a los activos como se muestra en la figura 31. El sistema "MQR" y los servicios Subcontratados son fundamentales es sus actividades laborales por eso se encuentra el parte superior.

Los programas que están instalados en los equipos son importantes como el caso del paquete de Microsoft Office ya que pueden hacer reportes e informes.

En el mismo nivel se encuentra el Acceso Remoto, Servidor de Correo Electrónico, Servidor de Archivos Compartido y el Antivirus.

El servidor de Base de Datos está por encima de todos los equipos el motivo es que almacena información por debajo esta las computadoras de escritorio.

En los activos inferiores están el router, los equipos auxiliares, impresora, etc. Los activos de menor jerarquía como son la red WIFI, red LAN y el internet. Todos los activos están dentro de un mismo edificio.

4.7.2.1.3 Valoración de los activos

Para cada valoración conviene tomar en consideración la siguiente información:

- Dimensiones en las que el activo es relevante
- Estimación de la valoración en cada dimensión

Criterios de la valoración

Nivel	Criterio
10	Nivel 10
9	Nivel 9
8	Nivel 8(+)
7	Alto
6	Alto(-)
5	Medio(+)
4	Medio
3	Medio(-)
2	Bajo(+)
1	Bajo
0	Depreciable

Tabla 23: Criterios de Valoración
Fuente: Herramienta PILAR 5.2.9

Dimensiones

[D] disponibilidad

[I] integridad de los datos

[C] confidencialidad de los datos

[A] autenticidad de los usuarios y de la información

[T] trazabilidad del servicio y de los datos

	Dimensiones				
Activos	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Capa de negocio					
[AH_COPEU] AHORRO	[9]	[9]	[9]	[9]	[9]
[CR_COPEU] CREDITO	[9]	[9]	[9]	[9]	[9]
Servicios internos					

[AR_COPEU] ACCESO REMOTO	[3]	[3]	[3]	[3]	[3]
[SCE_COPEU] SERVIDOR DE CORREO ELECTRONICO	[2]	[2]	[2]	[2]	[2]
[SAC_COPEU] SERVIDOR DE ARCHIVO COMPARTIDO	[4]	[4]	[4]	[4]	[4]
[IN_COPEU] INTERNET	[2]	[2]	[2]	[2]	[2]
Equipamiento					
[SW.SISCO_COPEU] SISTEMA FINANCIERO COPEU	[9]	[9]	[9]	[9]	[9]
[SW.OF_COPEU] OFIMATICA	[1]	[1]	[1]	[1]	[1]
[SW.AN_COPEU] ANTIVIRUS	[5]	[5]	[5]	[5]	[5]
[SW.OTR_COPEU] OTRO SOFTWARE	[3]	[3]	[3]	[3]	[3]
[HW.SBD_COPEU] SERVIDOR DE BASE DE DATOS	[5]	[5]	[5]	[5]	[5]
[HW.ROU_COPEU] ROUTER	[1]	[1]	[1]	[1]	[1]
[HW.SWI_COPEU] SWITCH	[1]	[1]	[1]	[1]	[1]
[HW.FIR_COPEU] FIREWALL	[1]	[1]	[1]	[1]	[1]
[HW.COM_COPEU] COMPUTADORAS DE ESCRITORIO	[3]	[3]	[3]	[3]	[3]
[HW.COMPO_COPEU] COMPUTADORAS PORTATILES	[1]	[1]	[1]	[1]	[1]
[HW.IMPLA_COPEU] IMPRESORA A LASER	[1]	[1]	[1]	[1]	[1]
[HW.IMPMA_COPEU] IMPRESORA MATRICIAL	[1]	[1]	[1]	[1]	[1]
[COM.REDLA_COPEU] RED LAN	[2]	[2]	[2]	[2]	[2]
[COM.REDWA_COPEU] RED WAN	[2]	[2]	[2]	[2]	[2]

[COM.INT_COPEU] INTERNET COPEU	[2]	[2]	[2]	[2]	[2]
[AUX.CABDAT_COPEU] CABLEADO DE DATOS COPEU	[2]	[2]	[2]	[2]	[2]
[AUX.EQUAUX_COPEU] EQUIPAMIENTO AUXILIAR	[2]	[2]	[2]	[2]	[2]
Servicios subcontratados					
[PAGAGI_COPEU] PAGO AGIL COPEU	[4]	[4]	[4]	[4]	[4]
[SOLA_COPEU] SOAT LATINA	[4]	[4]	[4]	[4]	[4]
Instalaciones					
[USR_COPEU]UNIDAD DE SISTEMAS Y REDES COPEU	[7]	[7]	[7]	[7]	[7]
Personal					
[ADSFYBD_COPEU] ADMINISTRACION SISTEMA FINANCIERO Y BASE DE DATOS	[4]	[4]	[4]	[4]	[4]
[SU_COPEU] SOPORTE A USUARIO	[4]	[4]	[4]	[4]	[4]

Tabla 24: Valor Propio de los Activos
Fuente: Realizado en PILAR 5.2.9

El resultado de esta primera tarea es el informe de Modelo de Valor (Ver Anexo 3) donde se describe detalladamente cada uno los activos antes mencionados.

4.7.2.2 Caracterización de las amenazas

La herramienta PILAR estandarizada por Magerit. Según la misma, las amenazas están clasificadas en cuatro grupos:

- [N] Desastres Naturales
- [I] De origen industrial
- [E] Errores y fallos no intencionados
- [A] Ataque intencionados

Esta actividad consta de 2 sub-tareas:

- Identificación de las amenazas
- Valoración de la amenazas

4.7.2.2.1 Identificación de las amenazas

Luego de la identificación de los activos se deben de identificar las amenazas que pueden afectar a cada activo, por lo que una amenaza puede desencadenar muchas más.

El objetivo de esta tarea:

- Identificar las amenazas relevantes sobre cada activo

La herramienta PILAR 5.2.9 aplicada, asigna de forma automática las amenazas, su frecuencia de materialización y el impacto que supondría.

Las amenazas que genera la biblioteca de PILAR 5.2.9 no serán tomadas en su totalidad, debido a que consideraremos las amenazas obtenidas de las encuestas realizadas al Personal responsable del sistema de información de la Cooperativa.

Activos	Amenazas
[AH_COPEU] AHORRO	[I.6] Corte del suministro eléctrico [I.8] Fallo de servicios de comunicaciones [E.2] Errores del administrador del sistema / de la seguridad
[CR_COPEU] CREDITO	[I.6] Corte del suministro eléctrico [I.8] Fallo de servicios de comunicaciones [E.2] Errores del administrador del sistema / de la seguridad
[AR_COPEU] ACCESO REMOTO	[E.2] Errores del administrador del sistema / de la seguridad [E.19] Fugas de información [A.5] Suplantación de la identidad del usuario [A.11] Acceso no autorizado [A.18] Destrucción de la información [A.26] Ataque destructivo
[SCE_COPEU] SERVIDOR DE	[I.5] Avería de origen físico o lógico

CORREO ELECTRONICO	[I.6] Corte del suministro eléctrico [I.8] Fallo de servicios de comunicaciones [E.2] Errores del administrador del sistema / de la seguridad [E.14] Fugas de información (> E.19) [E.21] Errores de mantenimiento / actualización de programas (software) [A.5] Suplantación de la identidad del usuario [A.24] Denegación de servicio
[SAC_COPEU] SERVIDOR DE ARCHIVO COMPARTIDO	[N.1] Fuego [I.5] Avería de origen físico o lógico [I.8] Fallo de servicios de comunicaciones [I.9] Interrupción de otros servicios o suministros esenciales [I.10] Degradación de los soportes de almacenamiento de la información [E.14] Fugas de información (> E.19) [E.15] Alteración de la información [E.18] Destrucción de la información [E.21] Errores de mantenimiento / actualización de programas (software) [A.5] Suplantación de la identidad del usuario [A.15] Modificación de la información [A.18] Destrucción de la información [A.24] Denegación de servicio
[IN_COPEU] INTERNET	[I.6] Corte del suministro eléctrico [E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [E.21] Errores de mantenimiento / actualización de programas (software) [A.4] Manipulación de los ficheros de configuración [A.7] Uso no previsto
[SW.SISCO_COPEU] SISTEMA FINANCIERO COPEU	[N.1] Fuego [N.2] Daños por agua [I.5] Avería de origen físico o lógico [I.8] Fallo de servicios de comunicaciones [E.1] Errores de los usuarios [E.4] Errores de configuración [E.15] Alteración de la información [E.20] Vulnerabilidades de los programas (software)

	[E.21] Errores de mantenimiento / actualización de programas (software) [A.5] Suplantación de la identidad del usuario [A.8] Difusión de software dañino [A.11] Acceso no autorizado [A.15] Modificación de la información
[SW.OF_COPEU] OFIMATICA	[I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.10] Degradación de los soportes de almacenamiento de la información [E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.4] Manipulación de los ficheros de configuración
[SW.AN_COPEU] ANTIVIRUS	[I.5] Avería de origen físico o lógico [E.1] Errores de los usuarios [E.4] Errores de configuración [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.8] Difusión de software dañino
[SW.OTR_COPEU] OTRO SOFTWARE	[I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.10] Degradación de los soportes de almacenamiento de la información [E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.4] Manipulación de los ficheros de configuración

	[A.7] Uso no previsto
[HW.SBD_COPEU] SERVIDOR DE BASE DE DATOS	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [I.10] Degradación de los soportes de almacenamiento de la información [E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.11] Acceso no autorizado [A.15] Modificación de la información [A.23] Manipulación del hardware [A.24] Denegación de servicio
[HW.ROU_COPEU] ROUTER	[N.1] Fuego [N.2] Daños por agua [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [E.21] Errores de mantenimiento / actualización de programas (software) [A.4] Manipulación de los ficheros de configuración [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [A.25] Robo de equipos [A.26] Ataque destructivo
[HW.SWI_COPEU] SWITCH	[N.1] Fuego [N.2] Daños por agua [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [E.21] Errores de mantenimiento / actualización de programas (software)

	[A.4] Manipulación de los ficheros de configuración [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [A.25] Robo de equipos [A.26] Ataque destructivo
[HW.FIR_COPEU] FIREWALL	[I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [E.21] Errores de mantenimiento / actualización de programas (software) [A.4] Manipulación de los ficheros de configuración
[HW.COM_COPEU] COMPUTADORAS DE ESCRITORIO	[N.1] Fuego [N.2] Daños por agua [I.*] Desastres industriales [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [E.8] Difusión de software dañino [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] Caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos [A.4] Manipulación de los ficheros de configuración [A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto
[HW.COMPO_COPEU] COMPUTADORAS PORTATILES	[N.1] Fuego [N.2] Daños por agua [I.*] Desastres industriales [I.5] Avería de origen físico o lógico

	[I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [E.8] Difusión de software dañino [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] Caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos [A.4] Manipulación de los ficheros de configuración [A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto
[HW.IMPLA_COPEU] IMPRESORA A LASER	[N.2] Daños por agua [I.5] Avería de origen físico o lógico [I.7] Condiciones inadecuadas de temperatura o humedad [I.9] Interrupción de otros servicios o suministros esenciales [E.1] Errores de los usuarios [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.25] Pérdida de equipos [A.4] Manipulación de los ficheros de configuración [A.11] Acceso no autorizado
[HW.IMPMA_COPEU] IMPRESORA MATRICIAL	[N.1] Fuego [N.2] Daños por agua [I.5] Avería de origen físico o lógico [I.7] Condiciones inadecuadas de temperatura o humedad [I.9] Interrupción de otros servicios o suministros esenciales [E.1] Errores de los usuarios [E.4] Errores de configuración [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.25] Pérdida de equipos

	[A.4] Manipulación de los ficheros de configuración [A.11] Acceso no autorizado
[COM.REDLA_COPEU] RED LAN	[N.2] Daños por agua [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [I.8] Fallo de servicios de comunicaciones [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.21] Errores de mantenimiento / actualización de programas (software) [E.24] Caída del sistema por agotamiento de recursos [E.28] Indisponibilidad del personal [A.4] Manipulación de los ficheros de configuración [A.5] Suplantación de la identidad del usuario [A.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado
[COM.REDWA_COPEU] RED WAN	[N.2] Daños por agua [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [I.8] Fallo de servicios de comunicaciones [I.11] Emanaciones electromagnéticas [E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado

	[A.12] Análisis de tráfico [A.28] Indisponibilidad del personal
[COM.INT_COPEU] INTERNET COPEU	[N.2] Daños por agua [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [I.8] Fallo de servicios de comunicaciones [E.15] Alteración de la información [E.21] Errores de mantenimiento / actualización de programas (software) [E.24] Caída del sistema por agotamiento de recursos [E.28] Indisponibilidad del personal [A.4] Manipulación de los ficheros de configuración
[AUX.CABDAT_COPEU] CABLEADO DE DATOS COPEU	[N.*] Desastres naturales [I.3] Contaminación medioambiental [I.4] Contaminación electromagnética [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [I.8] Fallo de servicios de comunicaciones [I.11] Emanaciones electromagnéticas [E.1] Errores de los usuarios [E.7] Deficiencias en la organización
[AUX.EQUAUX_COPEU] EQUIPAMIENTO AUXILIAR	[N.*] Desastres naturales [I.4] Contaminación electromagnética [I.6] Corte del suministro eléctrico [I.8] Fallo de servicios de comunicaciones [I.11] Emanaciones electromagnéticas [E.1] Errores de los usuarios
[PAGAGI_COPEU] PAGO AGIL COPEU	[N.*] Desastres naturales [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.8] Fallo de servicios de comunicaciones [E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [E.14] Fugas de información (> E.19) [E.19] Fugas de información [E.24] Caída del sistema por agotamiento de recursos [A.5] Suplantación de la identidad del usuario

	[A.11] Acceso no autorizado
[SOLA_COPEU] SOAT LATINA	[N.*] Desastres naturales [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.8] Fallo de servicios de comunicaciones [E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.4] Errores de configuración [E.14] Fugas de información (> E.19) [E.19] Fugas de información [E.24] Caída del sistema por agotamiento de recursos [A.5] Suplantación de la identidad del usuario [A.11] Acceso no autorizado
[USR_COPEU]UNIDAD DE SISTEMAS Y REDES COPEU	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [N.*.4] Terremotos [N.*.10] Tormentas de invierno y frio extremo [N.*.11] Calor extremo [I.*] Desastres industriales [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [E.7] Deficiencias en la organización [A.11] Acceso no autorizado [A.27] Ocupación enemiga
[ADSFYBD_COPEU] ADMINISTRACION SISTEMA FINANCIERO Y BASE DE DATOS	[E.7] Deficiencias en la organización [A.28.1] Enfermedad [A.28.2] Huelga [A.29] Extorsión [A.30] Ingeniería social (picaresca)
[SU_COPEU] SOPORTE A USUARIO	[E.7] Deficiencias en la organización [A.29] Extorsión [A.30] Ingeniería social (picaresca)

Tabla 25: Identificación de Amenazas a cada uno de los activos
Fuente: Realizado en PILAR 5.2.9

4.7.2.2.2 Valoración de las amenazas

Los objetivos planteados en esta tarea son:

Evaluar la probabilidad de ocurrencia de cada amenaza concerniente a cada activo.

Estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse.

B	BAJO
M	MEDIO
A	ALTO
MA	MUY ALTO
T	TOTAL
0	

Tabla 26: Degradación del valor
Fuente: Tomado de PILAR 5.2.9

MR	MUY RARO
PP	POCO POSIBLE
P	POSIBLE
MA	MUY ALTO
CS	CASI SEGURO
0	

Tabla 27: Probabilidad de ocurrencia
Fuente: Tomado de PILAR 5.2.9

Activos	Amenazas	Probabilidad	[D]	[I]	[C]	[A]	[T]
[AH_COPEU] AHORRO	[I.6] Corte del suministro eléctrico	PP	A	A	A	A	A
	[I.8] Fallo de servicios de comunicaciones	PP	A	A	A	A	A
	[E.2] Errores del administrador del sistema / de la seguridad	PP	A	A	A	A	A
[CR_COPEU] CREDITO	[I.6] Corte del suministro eléctrico	PP	A	A	A	A	A
	[I.8] Fallo de servicios de comunicaciones	PP	A	A	A	A	A
	[E.2] Errores del administrador del sistema / de la seguridad	PP	A	A	A	A	A
[AR_COPEU] ACCESO REMOTO	[E.2] Errores del administrador del sistema / de la seguridad	PP	A	A	A	A	A
	[E.19] Fugas de información	PP	M	M	M	M	M
	[A.5] Suplantación de la identidad del usuario	PP	M	M	M	M	M
	[A.11] Acceso no autorizado	PP	M	M	M	M	M
	[A.18] Destrucción de la información	PP	M	M	M	M	M
	[A.26] Ataque destructivo	PP	M	M	M	M	M
[SCE_COPEU] SERVIDOR DE CORREO ELECTRONICO	[I.5] Avería de origen físico o lógico	PP	MA	MA	MA	MA	MA
	[I.6] Corte del suministro eléctrico	PP	A	A	A	A	A
	[I.8] Fallo de servicios de comunicaciones	PP	A	A	A	A	A
	[E.2] Errores del administrador del sistema / de la seguridad	PP	A	A	A	A	A
	[E.14] Fugas de información (> E.19)	PP	M	M	M	M	M
	[E.21] Errores de mantenimiento / actualización de programas (software)	PP	M	M	M	M	M
	[A.5] Suplantación de la identidad del usuario	PP	M	M	M	M	M
	[A.24] Denegación de servicio	PP	M	M	M	M	M
[SAC_COPEU] SERVIDOR DE	[N.1] Fuego	PP	MA	MA	MA	MA	MA

ARCHIVO COMPARTIDO	[I.5] Avería de origen físico o lógico	PP	MA	MA	MA	MA	MA
	[I.8] Fallo de servicios de comunicaciones	PP	A	A	A	A	A
	[I.9] Interrupción de otros servicios o suministros esenciales	PP	M	M	M	M	M
	[I.10] Degradación de los soportes de almacenamiento de la información	PP	M	M	M	M	M
	[E.14] Fugas de información (> E.19)	PP	M	M	M	M	M
	[E.15] Alteración de la información	PP	M	M	M	M	M
	[E.18] Destrucción de la información	PP	M	M	M	M	M
	[E.21] Errores de mantenimiento / actualización de programas (software)	PP	M	M	M	M	M
	[A.5] Suplantación de la identidad del usuario	PP	M	M	M	M	M
	[A.15] Modificación de la información	PP	M	M	M	M	M
	[A.18] Destrucción de la información	PP	M	M	M	M	M
	[A.24] Denegación de servicio	PP	M	M	M	M	M
[IN_COPEU] INTERNET	[I.6] Corte del suministro eléctrico	PP	MA	MA	MA	MA	MA
	[E.1] Errores de los usuarios	PP	A	A	A	A	A
	[E.2] Errores del administrador del sistema / de la seguridad	PP	A	A	A	A	A
	[E.4] Errores de configuración	PP	A	A	A	A	A
	[E.21] Errores de mantenimiento / actualización de programas (software)	PP	A	A	A	A	A
	[A.4] Manipulación de los ficheros de configuración	PP	A	A	A	A	A
	[A.7] Uso no previsto	PP	A	A	A	A	A
[SW.SISCO_COPEU] SISTEMA FINANCIERO COPEU	[N.1] Fuego	PP	T	T	T	T	T
	[N.2] Daños por agua	PP	T	T	T	T	T
	[I.5] Avería de origen físico o lógico	PP	T	T	T	T	T

	[I.8] Fallo de servicios de comunicaciones	PP	T	T	T	T	T
	[E.1] Errores de los usuarios	PP	MA	MA	MA	MA	MA
	[E.4] Errores de configuración	PP	MA	MA	MA	MA	MA
	[E.15] Alteración de la información	PP	MA	MA	MA	MA	MA
	[E.20] Vulnerabilidades de los programas (software)	PP	MA	MA	MA	MA	MA
	[E.21] Errores de mantenimiento / actualización de programas (software)	PP	MA	MA	MA	MA	MA
	[A.5] Suplantación de la identidad del usuario	PP	MA	MA	MA	MA	MA
	[A.8] Difusión de software dañino	PP	MA	MA	MA	MA	MA
	[A.11] Acceso no autorizado	PP	MA	MA	MA	MA	MA
	[A.15] Modificación de la información	PP	MA	MA	MA	MA	MA
[SW.OF_COPEU] OFIMATICA	[I.5] Avería de origen físico o lógico	PP	M	M	M	M	M
	[I.6] Corte del suministro eléctrico	PP	M	M	M	M	M
	[I.10] Degradación de los soportes de almacenamiento de la información	PP	M	M	M	M	M
	[E.1] Errores de los usuarios	PP	M	M	M	M	M
	[E.2] Errores del administrador del sistema / de la seguridad	PP	M	M	M	M	M
	[E.4] Errores de configuración	PP	M	M	M	M	M
	[E.8] Difusión de software dañino	PP	M	M	M	M	M
	[E.20] Vulnerabilidades de los programas (software)	PP	M	M	M	M	M
	[E.21] Errores de mantenimiento / actualización de programas (software)	PP	M	M	M	M	M
	[A.4] Manipulación de los ficheros de configuración	PP	M	M	M	M	M
[SW.AN_COPEU] ANTIVIRUS	[I.5] Avería de origen físico o lógico	PP	A	A	A	A	A

	[E.1] Errores de los usuarios	PP	A	A	A	A	A
	[E.4] Errores de configuración	PP	A	A	A	A	A
	[E.20] Vulnerabilidades de los programas (software)	PP	A	A	A	A	A
	[E.21] Errores de mantenimiento / actualización de programas (software)	PP	A	A	A	A	A
	[A.8] Difusión de software dañino	PP	A	A	A	A	A
[SW.OTR_COPEU] OTRO SOFTWARE	[I.5] Avería de origen físico o lógico	PP	M	M	M	M	M
	[I.6] Corte del suministro eléctrico	PP	M	M	M	M	M
	[I.10] Degradación de los soportes de almacenamiento de la información	PP	M	M	M	M	M
	[E.1] Errores de los usuarios	PP	M	M	M	M	M
	[E.2] Errores del administrador del sistema / de la seguridad	PP	M	M	M	M	M
	[E.4] Errores de configuración	PP	M	M	M	M	M
	[E.8] Difusión de software dañino	PP	M	M	M	M	M
	[E.20] Vulnerabilidades de los programas (software)	PP	M	M	M	M	M
	[E.21] Errores de mantenimiento / actualización de programas (software)	PP	M	M	M	M	M
	[A.4] Manipulación de los ficheros de configuración	PP	M	M	M	M	M
	[A.7] Uso no previsto	PP	M	M	M	M	M
[HW.SBD_COPEU] SERVIDOR DE BASE DE DATOS	[N.1] Fuego	PP	A	A	A	A	A
	[N.2] Daños por agua	PP	A	A	A	A	A
	[N.*] Desastres naturales	PP	A	A	A	A	A
	[I.5] Avería de origen físico o lógico	PP	A	A	A	A	A
	[I.6] Corte del suministro eléctrico	PP	A	A	A	A	A
	[I.7] Condiciones inadecuadas de	PP	MA	MA	MA	MA	MA

	temperatura o humedad						
	[I.10] Degradación de los soportes de almacenamiento de la información	PP	A	A	A	A	A
	[E.1] Errores de los usuarios	PP	A	A	A	A	A
	[E.2] Errores del administrador del sistema / de la seguridad	PP	A	A	A	A	A
	[E.4] Errores de configuración	PP	A	A	A	A	A
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	PP	MA	MA	MA	MA	MA
	[A.6] Abuso de privilegios de acceso	PP	A	A	A	A	A
	[A.7] Uso no previsto	PP	A	A	A	A	A
	[A.11] Acceso no autorizado	PP	A	A	A	A	A
	[A.15] Modificación de la información	PP	A	A	A	A	A
	[A.23] Manipulación del hardware	PP	A	A	A	A	A
	[A.24] Denegación de servicio	PP	A	A	A	A	A
[HW.ROU_COPEU] ROUTER	[N.1] Fuego	PP	M	M	M	M	M
	[N.2] Daños por agua	PP	M	M	M	M	M
	[I.5] Avería de origen físico o lógico	PP	M	M	M	M	M
	[I.6] Corte del suministro eléctrico	PP	M	M	M	M	M
	[I.7] Condiciones inadecuadas de temperatura o humedad	PP	M	M	M	M	M
	[E.21] Errores de mantenimiento / actualización de programas (software)	PP	M	M	M	M	M
	[A.4] Manipulación de los ficheros de configuración	PP	M	M	M	M	M
	[A.6] Abuso de privilegios de acceso	PP	M	M	M	M	M
	[A.11] Acceso no autorizado	PP	M	M	M	M	M
	[A.25] Robo de equipos	PP	M	M	M	M	M
	[A.26] Ataque destructivo	PP	M	M	M	M	M

[HW.SWI_COPEU] SWITCH	[N.1] Fuego	PP	M	M	M	M	M
	[N.2] Daños por agua	PP	M	M	M	M	M
	[I.5] Avería de origen físico o lógico	PP	M	M	M	M	M
	[I.6] Corte del suministro eléctrico	PP	M	M	M	M	M
	[I.7] Condiciones inadecuadas de temperatura o humedad	PP	M	M	M	M	M
	[E.21] Errores de mantenimiento / actualización de programas (software)	PP	M	M	M	M	M
	[A.4] Manipulación de los ficheros de configuración	PP	M	M	M	M	M
	[A.6] Abuso de privilegios de acceso	PP	M	M	M	M	M
	[A.11] Acceso no autorizado	PP	M	M	M	M	M
	[A.25] Robo de equipos	PP	M	M	M	M	M
	[A.26] Ataque destructivo	PP	M	M	M	M	M
[HW.FIR_COPEU] FIREWALL	[I.5] Avería de origen físico o lógico	PP	M	M	M	M	M
	[I.6] Corte del suministro eléctrico	PP	M	M	M	M	M
	[I.7] Condiciones inadecuadas de temperatura o humedad	PP	M	M	M	M	M
	[E.1] Errores de los usuarios	PP	M	M	M	M	M
	[E.2] Errores del administrador del sistema / de la seguridad	PP	M	M	M	M	M
	[E.4] Errores de configuración	PP	M	M	M	M	M
	[E.21] Errores de mantenimiento / actualización de programas (software)	PP	M	M	M	M	M
	[A.4] Manipulación de los ficheros de configuración	PP	M	M	M	M	M
[HW.COM_COPEU] COMPUTADORAS DE ESCRITORIO	[N.1] Fuego	PP	A	A	A	A	A
	[N.2] Daños por agua	PP	A	A	A	A	A
	[I.*] Desastres industriales	PP	A	A	A	A	A

	[I.5] Avería de origen físico o lógico	PP	A	A	A	A	A
	[I.6] Corte del suministro eléctrico	PP	A	A	A	A	A
	[I.7] Condiciones inadecuadas de temperatura o humedad	PP	A	A	A	A	A
	[E.1] Errores de los usuarios	PP	A	A	A	A	A
	[E.2] Errores del administrador del sistema / de la seguridad	PP	A	A	A	A	A
	[E.4] Errores de configuración	PP	A	A	A	A	A
	[E.8] Difusión de software dañino	PP	A	A	A	A	A
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	PP	A	A	A	A	A
	[E.24] Caída del sistema por agotamiento de recursos	PP	A	A	A	A	A
	[E.25] Pérdida de equipos	PP	A	A	A	A	A
	[A.4] Manipulación de los ficheros de configuración	PP	A	A	A	A	A
	[A.5] Suplantación de la identidad del usuario	PP	A	A	A	A	A
	[A.6] Abuso de privilegios de acceso	PP	A	A	A	A	A
	[A.7] Uso no previsto	PP	A	A	A	A	A
[HW.COMPO_COPEU] COMPUTADORAS PORTATILES	[N.1] Fuego	PP	M	M	M	M	M
	[N.2] Daños por agua	PP	M	M	M	M	M
	[I.*] Desastres industriales	PP	M	M	M	M	M
	[I.5] Avería de origen físico o lógico	PP	M	M	M	M	M
	[I.6] Corte del suministro eléctrico	PP	M	M	M	M	M
	[I.7] Condiciones inadecuadas de temperatura o humedad	PP	M	M	M	M	M
	[E.1] Errores de los usuarios	PP	M	M	M	M	M
	[E.2] Errores del administrador del sistema /	PP	M	M	M	M	M

	de la seguridad						
	[E.4] Errores de configuración	PP	M	M	M	M	M
	[E.8] Difusión de software dañino	PP	M	M	M	M	M
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	PP	M	M	M	M	M
	[E.24] Caída del sistema por agotamiento de recursos	PP	M	M	M	M	M
	[E.25] Pérdida de equipos	PP	M	M	M	M	M
	[A.4] Manipulación de los ficheros de configuración	PP	M	M	M	M	M
	[A.5] Suplantación de la identidad del usuario	PP	M	M	M	M	M
	[A.6] Abuso de privilegios de acceso	PP	M	M	M	M	M
	[A.7] Uso no previsto	PP	M	M	M	M	M
[HW.IMPLA_COPEU] IMPRESORA A LASER	[N.2] Daños por agua	PP	B	B	B	B	B
	[I.5] Avería de origen físico o lógico	PP	B	B	B	B	B
	[I.7] Condiciones inadecuadas de temperatura o humedad	PP	B	B	B	B	B
	[I.9] Interrupción de otros servicios o suministros esenciales	PP	B	B	B	B	B
	[E.1] Errores de los usuarios	PP	B	B	B	B	B
	[E.4] Errores de configuración	PP	B	B	B	B	B
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	PP	B	B	B	B	B
	[E.25] Pérdida de equipos	PP	B	B	B	B	B
	[A.4] Manipulación de los ficheros de configuración	PP	B	B	B	B	B
	[A.11] Acceso no autorizado	PP	B	B	B	B	B
[HW.IMPMA_COPEU]	[N.1] Fuego	PP	B	B	B	B	B

IMPRESORA MATRICIAL	[N.2] Daños por agua	PP	B	B	B	B	B
	[I.5] Avería de origen físico o lógico	PP	B	B	B	B	B
	[I.7] Condiciones inadecuadas de temperatura o humedad	PP	B	B	B	B	B
	[I.9] Interrupción de otros servicios o suministros esenciales	PP	B	B	B	B	B
	[E.1] Errores de los usuarios	PP	B	B	B	B	B
	[E.4] Errores de configuración	PP	B	B	B	B	B
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	PP	B	B	B	B	B
	[E.25] Pérdida de equipos	PP	B	B	B	B	B
	[A.4] Manipulación de los ficheros de configuración	PP	B	B	B	B	B
	[A.11] Acceso no autorizado	PP	B	B	B	B	B
[COM.REDLA_COPEU] RED LAN	[N.2] Daños por agua	PP	A	A	A	A	A
	[I.6] Corte del suministro eléctrico	PP	A	A	A	A	A
	[I.7] Condiciones inadecuadas de temperatura o humedad	PP	A	A	A	A	A
	[I.8] Fallo de servicios de comunicaciones	PP	A	A	A	A	A
	[E.9] Errores de [re-]encaminamiento	PP	A	A	A	A	A
	[E.10] Errores de secuencia	PP	A	A	A	A	A
	[E.21] Errores de mantenimiento / actualización de programas (software)	PP	A	A	A	A	A
	[E.24] Caída del sistema por agotamiento de recursos	PP	A	A	A	A	A
	[E.28] Indisponibilidad del personal	PP	A	A	A	A	A
	[A.4] Manipulación de los ficheros de configuración	PP	A	A	A	A	A
	[A.5] Suplantación de la identidad del	PP	A	A	A	A	A

	usuario						
	[A.9] [Re-]encaminamiento de mensajes	PP	A	A	A	A	A
	[A.10] Alteración de secuencia	PP	A	A	A	A	A
	[A.11] Acceso no autorizado	PP	A	A	A	A	A
[COM.REDWA_COPEU] RED WAN	[N.2] Daños por agua	PP	A	A	A	A	A
	[I.5] Avería de origen físico o lógico	PP	A	A	A	A	A
	[I.6] Corte del suministro eléctrico	PP	A	A	A	A	A
	[I.7] Condiciones inadecuadas de temperatura o humedad	PP	A	A	A	A	A
	[I.8] Fallo de servicios de comunicaciones	PP	A	A	A	A	A
	[I.11] Emanaciones electromagnéticas	PP	A	A	A	A	A
	[E.2] Errores del administrador del sistema / de la seguridad	PP	A	A	A	A	A
	[E.4] Errores de configuración	PP	A	A	A	A	A
	[E.9] Errores de [re-]encaminamiento	PP	A	A	A	A	A
	[E.10] Errores de secuencia	PP	A	A	A	A	A
	[E.20] Vulnerabilidades de los programas (software)	PP	A	A	A	A	A
	[E.21] Errores de mantenimiento / actualización de programas (software)	PP	A	A	A	A	A
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	PP	A	A	A	A	A
	[A.6] Abuso de privilegios de acceso	PP	A	A	A	A	A
	[A.7] Uso no previsto	PP	A	A	A	A	A
	[A.9] [Re-]encaminamiento de mensajes	PP	A	A	A	A	A
	[A.10] Alteración de secuencia	PP	A	A	A	A	A
	[A.11] Acceso no autorizado	PP	A	A	A	A	A
	[A.12] Análisis de tráfico	PP	A	A	A	A	A
	[A.28] Indisponibilidad del personal	PP	A	A	A	A	A

[COM.INT_COPEU] INTERNET COPEU	[N.2] Daños por agua	PP	A	A	A	A	A
	[I.6] Corte del suministro eléctrico	PP	A	A	A	A	A
	[I.7] Condiciones inadecuadas de temperatura o humedad	PP	A	A	A	A	A
	[I.8] Fallo de servicios de comunicaciones	PP	A	A	A	A	A
	[E.15] Alteración de la información	PP	A	A	A	A	A
	[E.21] Errores de mantenimiento / actualización de programas (software)	PP	A	A	A	A	A
	[E.24] Caída del sistema por agotamiento de recursos	PP	A	A	A	A	A
	[E.28] Indisponibilidad del personal	PP	A	A	A	A	A
	[A.4] Manipulación de los ficheros de configuración	PP	A	A	A	A	A
[AUX.CABDAT_COPEU] CABLEADO DE DATOS COPEU	[N.*] Desastres naturales	PP	A	A	A	A	A
	[I.3] Contaminación medioambiental	PP	A	A	A	A	A
	[I.4] Contaminación electromagnética	PP	A	A	A	A	A
	[I.6] Corte del suministro eléctrico	PP	A	A	A	A	A
	[I.7] Condiciones inadecuadas de temperatura o humedad	PP	A	A	A	A	A
	[I.8] Fallo de servicios de comunicaciones	PP	A	A	A	A	A
	[I.11] Emanaciones electromagnéticas	PP	A	A	A	A	A
	[E.1] Errores de los usuarios	PP	A	A	A	A	A
	[E.7] Deficiencias en la organización	PP	A	A	A	A	A
[AUX.EQUAUX_COPEU] EQUIPAMIENTO AUXILIAR	[N.*] Desastres naturales	PP	M	M	M	M	M
	[I.4] Contaminación electromagnética	PP	M	M	M	M	M
	[I.6] Corte del suministro eléctrico	PP	M	M	M	M	M
	[I.8] Fallo de servicios de comunicaciones	PP	M	M	M	M	M
	[I.11] Emanaciones electromagnéticas	PP	M	M	M	M	M
	[E.1] Errores de los usuarios	PP	M	M	M	M	M

[PAGAGI_COPEU] PAGO AGIL COPEU	[N.*] Desastres naturales	PP	A	A	A	A	A
	[I.5] Avería de origen físico o lógico	PP	A	A	A	A	A
	[I.6] Corte del suministro eléctrico	PP	A	A	A	A	A
	[I.8] Fallo de servicios de comunicaciones	PP	A	A	A	A	A
	[E.1] Errores de los usuarios	PP	A	A	A	A	A
	[E.2] Errores del administrador del sistema / de la seguridad	PP	A	A	A	A	A
	[E.4] Errores de configuración	PP	A	A	A	A	A
	[E.14] Fugas de información (> E.19)	PP	A	A	A	A	A
	[E.19] Fugas de información	PP	A	A	A	A	A
	[E.24] Caída del sistema por agotamiento de recursos	PP	A	A	A	A	A
	[A.5] Suplantación de la identidad del usuario	PP	A	A	A	A	A
	[A.11] Acceso no autorizado	PP	A	A	A	A	A
[SOLA_COPEU] SOAT LATINA	[N.*] Desastres naturales	PP	A	A	A	A	A
	[I.5] Avería de origen físico o lógico	PP	A	A	A	A	A
	[I.6] Corte del suministro eléctrico	PP	A	A	A	A	A
	[I.8] Fallo de servicios de comunicaciones	PP	A	A	A	A	A
	[E.1] Errores de los usuarios	PP	A	A	A	A	A
	[E.2] Errores del administrador del sistema / de la seguridad	PP	A	A	A	A	A
	[E.4] Errores de configuración	PP	A	A	A	A	A
	[E.14] Fugas de información (> E.19)	PP	A	A	A	A	A
	[E.19] Fugas de información	PP	A	A	A	A	A
	[E.24] Caída del sistema por agotamiento de recursos	PP	A	A	A	A	A
	[A.5] Suplantación de la identidad del usuario	PP	A	A	A	A	A

	[A.11] Acceso no autorizado	PP	A	A	A	A	A
[USR_COPEU] UNIDAD DE SISTEMAS Y REDES COPEU	[N.1] Fuego	PP	A	A	A	A	A
	[N.2] Daños por agua	PP	A	A	A	A	A
	[N.*] Desastres naturales	PP	A	A	A	A	A
	[N.*.4] Terremotos	PP	A	A	A	A	A
	[N.*.10] Tormentas de invierno y frio extremo	PP	A	A	A	A	A
	[N.*.11] Calor extremo	PP	A	A	A	A	A
	[I.*] Desastres industriales	PP	A	A	A	A	A
	[I.6] Corte del suministro eléctrico	PP	A	A	A	A	A
	[I.7] Condiciones inadecuadas de temperatura o humedad	PP	A	A	A	A	A
	[E.7] Deficiencias en la organización	PP	A	A	A	A	A
	[A.11] Acceso no autorizado	PP	A	A	A	A	A
	[A.27] Ocupación enemiga	PP	A	A	A	A	A
[ADSFYBD_COPEU] ADMINISTRACION SISTEMA FINANCIERO Y BASE DE DATOS	[E.7] Deficiencias en la organización	PP	B	B	B	B	B
	[A.28.1] Enfermedad	PP	B	B	B	B	B
	[A.28.2] Huelga	PP	B	B	B	B	B
	[A.29] Extorsión	PP	B	B	B	B	B
	[A.30] Ingeniería social (picaresca)	PP	B	B	B	B	B
[SU_COPEU] SOPORTE A USUARIO	[E.7] Deficiencias en la organización	PP	B	B	B	B	B
	[A.29] Extorsión	PP	B	B	B	B	B
	[A.30] Ingeniería social (picaresca)	PP	B	B	B	B	B

Tabla 28: Valoración de Amenazas a cada uno de los activos
Fuente: Realizado en PILAR 5.2.9

4.7.2.3 Caracterización de las Salvaguardas

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar organizándose adecuadamente, otras requieren elementos técnicos (programas o equipos), otras seguridad física y por último, esta la política de personal.

En esta actividad se identifican las salvaguardas efectivas para la organización junto con la eficacia que tiene cada una de ellas para mitigar el riesgo. Dentro de esta metodología se pueden definir varias etapas de estudio que pueden abarcar lapsos de tiempo corto o largos incluso de un año, pero nuestro caso de estudio tomaremos tres fases:

Primera etapa llamada POTENCIAL(Potential)

Segunda etapa llamada SITUACIÓN ACTUAL (Current)

Tercera etapa llamada OBJETIVO (Target) Esta actividad consta de de dos sub-tareas:

Identificación de las salvaguardas pertinentes

Valoración de las salvaguardas

4.7.2.3.1 Identificación de las salvaguardas

Su objetivo principal es:

Identificar las salvaguardas convenientes para proteger el sistema

En esta tarea contaremos con la ayuda de la herramienta PILAR 5.2.9 que nos ayuda a la elección de salvaguardas de cada activo para contrarrestar las amenazas identificadas.

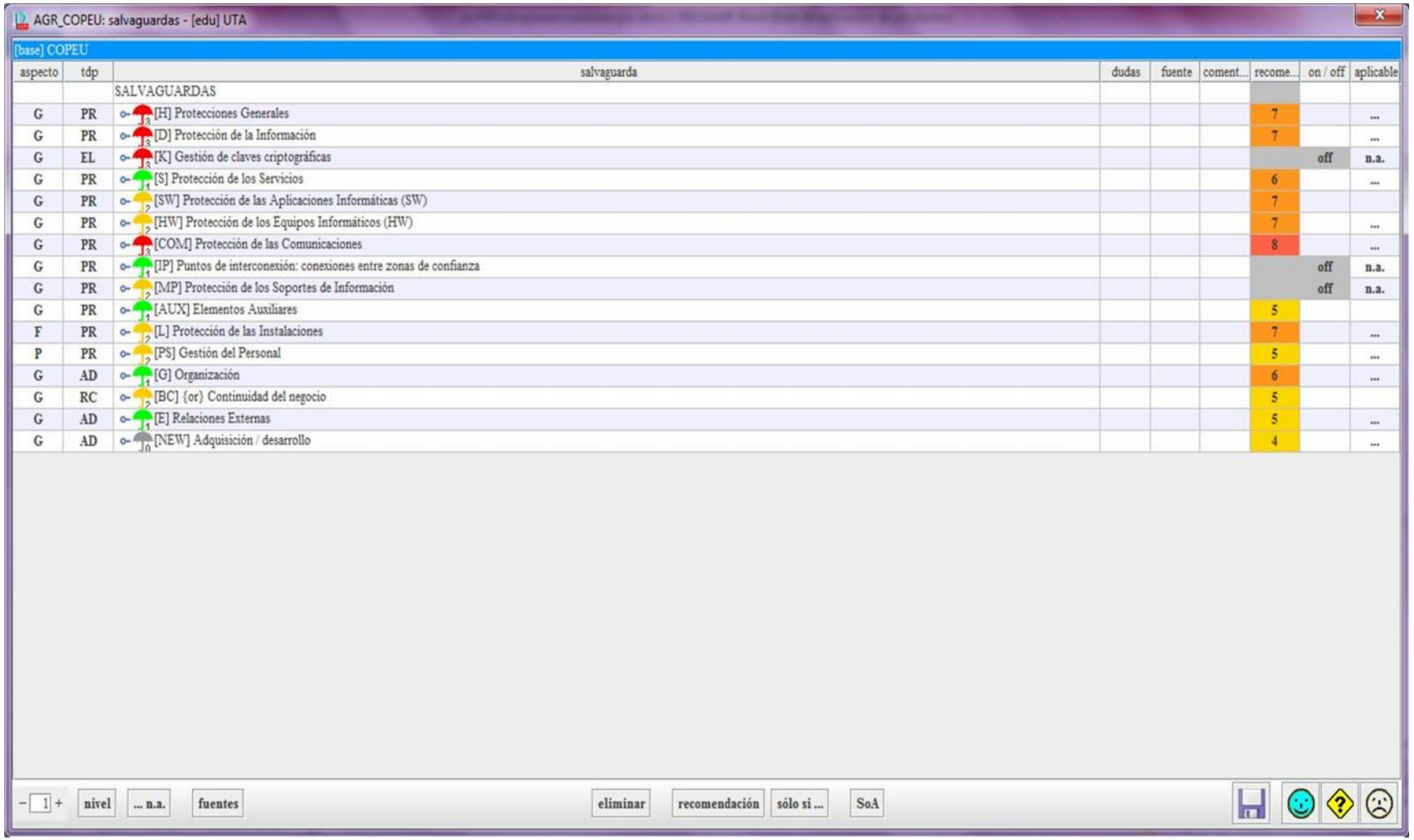


Figura 32: Identificación de las Salvaguardas
Fuente: PILAR 5.2.9

Protecciones Generales: A continuación las salvaguardas que fueran escogidas: Se requiere autorización previa: Pertenece al grupo de Restricción de acceso a la información que a su vez pertenece al Control de Acceso Lógico. La razón se escogió esta salvaguarda ya que cualquier persona puede acceder a los activos inclusive los más importantes. La misma por que hace frente a las amenazas a las que están expuestos los activos. Y esta pueda ser aplicada a estas clases de activos: Datos/ Información, Servicios, Aplicaciones (software), Equipamiento informático (hardware), Redes de comunicaciones y Soportes de información Protege a las siguientes dimensiones de seguridad: Integridad, Confidencialidad y Autenticidad.

Hace frente a las siguientes amenazas: Errores de los usuarios, Errores del administrador del sistema/ de la seguridad, Difusión de software dañino, Errores de [re]-encaminamiento, Errores de secuencia, Alteración de la información, Fugas de información, Vulnerabilidad de los programas (software), Errores de mantenimiento /actualización de programas (software), Suplantación de la identidad del usuario, Abuso de privilegios de acceso, Uso no previsto, [Re-]encaminamiento de mensajes, Alteración de secuencia, Acceso no autorizado, Modificación de la información, Revelación de información y Manipulación de hardware

Por eso se escogió las siguientes salvaguardas:

- El programa se actualiza regularmente
- La base de datos de virus se actualiza regularmente
- Se revisan los programas y servicios de arranque del sistema

Protecciones de las Aplicaciones Informáticas: Se seleccionó las siguientes salvaguardas ya que la Cooperativa no posee estas normas de seguridad como son:

- Se dispone de normativa sobre el uso autorizado de las aplicaciones
- Se dispone de normativa relativa al cumplimiento de los derechos
- Se controla la instalación de software autorizado y productos con licencia
- Se dispone de procedimientos para realizar copias de seguridad

- Se aplican perfiles de seguridad: esta salvaguarda se encuentra a medias porque solo existe cuentas de usuario lo que es suficiente para acceder a cualquier parte del sistema pero gracias a esta salvaguarda podemos hacer frente a estas amenazas : Errores de los usuarios, Difusión de software dañino, Vulnerabilidad de los programas (software), Errores de mantenimiento/actualización de programas (software) y Uso no previsto

Se debería tratar de cumplir con lo siguiente:

- Seguridad de los ficheros de datos de la aplicación
- Se protegen los ficheros de configuración
- Seguridad de los mecanismos de comunicación entre procesos

Donde se asegura las dimensiones de seguridad como confidencialidad e integridad

- Además de que se debe de llevar un Control de versión de toda actualización de software, ayuda a saber que cualquier software que posea la Cooperativa esté libre de errores y hacer frente amenazas como son: Vulnerabilidades de los programas (software) y Errores de mantenimiento/actualización de programas (software).

Protección de los Equipos Informáticos (HW): A continuación las salvaguardas adecuadas para la protección de los equipos.

- Se dispone de normativa sobre el uso correcto de los equipos
- Se dispone de procedimientos de uso de equipamiento
- Se aplican perfiles de seguridad: si se implementa esta salvaguarda en la Cooperativa minimiza amenazas como son: Errores del administrados del sistema / de la seguridad, Uso no previsto y Acceso no autorizado, además de asegurar las dimensiones: integridad y confidencialidad.

Además se debe de tener en cuenta con estas salvaguardas al momento de utilizar los equipos como son:

- Protección física de los equipos: son mecanismos que la Cooperativa no ha tomado en cuenta para proteger la información principalmente sobre un activo que es el Servidor de Datos
- Para evitar accesos innecesarios
- Para evitar acceso no autorizados
- Seguridad del equipamiento de oficina

Después de evaluar las salvaguardas antes mencionadas se debe implantar las siguientes salvaguardas:

- Se evalúa el impacto en la confidencialidad de los datos
- Se evalúa el impacto en la integridad de los datos

Ninguna de estas salvaguardas posee la Cooperativa como son:

- Se priorizan las actuaciones encaminadas corregir riesgos elevados
- Se mantiene en todo momento la regla de “seguridad por defecto”
- Se debe de controlar: Reproducción de documentos

Protección de las comunicaciones: Se han escogido las siguientes salvaguardas para minimizar riesgos:

Se deben de aplicar perfiles de seguridad : para garantizar la comunicación en la Cooperativa y para hacer frente amenazas como: Errores de [re] – encaminamiento, Errores de secuencia, Alteración de la información, Uso no previsto, [Re-]encaminamiento de mensajes, Alteración de secuencia y Acceso no autorizado, además proteger las dimensiones de seguridad : integridad, confidencialidad y autenticidad.

- La Cooperativa no posee dispone de normativa de uso de los servicios de red.
- Así mismo no dispone de un Control de filtrado

- Ni siquiera de mecanismos como son :
- Comprobación de origen y destino
- Mecanismos de control
- No tiene ninguna: Seguridad de los servicios de red

Todas las salvaguardas anteriormente desplegadas hacen frente a la amenaza de Acceso no autorizado

Para garantizar las comunicaciones cuando están utilizando el internet es necesario emplear siguiente salvaguardas:

- Herramienta de control de contenidos con filtros actualizados
- Se controla la configuración de los navegadores
- Se registra la descarga
- Se han instalado herramientas anti spyware
- Se deshabilitan las “cookies” en los navegadores
- Se registra la navegación web
- Se dispone de normativa sobre el uso de los servicios Internet
- Herramienta de monitorización del trafico
- Se toman medidas frente a la inyección de información espuria
- S aplica la regla de “seguridad por defecto”
- Se requiere autorización para que medios y dispositivos que tengan acceso a redes y servicios

Elementos Auxiliares: Se han escogido las siguientes salvaguardas para minimizar riesgos:

Se asegura la disponibilidad como:

- Siguiendo las recomendaciones del fabricante o proveedor

- Continuidad de operaciones: para asegurar las disponibilidad de los equipos auxiliares además para contrarrestar la amenaza de contaminación medioambiental
- Climatización: La adecuada climatización de cada equipo ayuda a enfrentar la amenaza que tiene la mayoría de estos componentes que es: Condiciones inadecuadas de temperatura o humedad.

Protección de las Instalaciones: Se han escogido las siguientes salvaguardas para minimizar riesgos:

Se dispone de normativa de seguridad para la seguridad de las instalaciones.

Se dispone de áreas específicas para equipos informáticos, para protegerlos de la Ocupación enemiga

Gestión del Personal: Se deben de crear las siguientes normas de seguridad

- Se dispone de normativa relativa a la gestión de personal(materia de seguridad)
- Se dispone de procedimientos para la gestión de personal(materia de seguridad)
- Creación de normas del personal: Propio y Subcontratado
- Se dispone de normativa de obligado cumplimiento en el desempeño del puesto de trabajo
- Se establecen normas para la contratación de personal, para garantizar la confidencialidad de los datos , frente ataques de cómo Extorsión y Ataque desde el interior
- Procedimientos relevantes de seguridad: Emergencias, incidencias.

Después de haber realizado esta tarea tendremos la Declaratoria de Aplicabilidad que es documento formal donde constan las salvaguardas necesarias para proteger al sistema (Ver Anexo 4 Declaratoria de Aplicabilidad).

4.7.2.3.2 Valoración de las salvaguardas

Objetivo:

- Determinar la eficacia de las salvaguardas pertinentes

Eficacia	Nivel	Madurez	Estado
0%	L0	inexistente	inexistente
10%	L1	inicial/ad hoc	iniciado
50%	L2	reproducible, pero intuitivo	parcialmente realizado
90%	L3	proceso definido	en funcionamiento
95%	L4	gestionado y medible	monitorizado
100%	L5	optimizado	mejora continua

Tabla 29: Niveles de Madurez
Fuente: Herramienta PILAR 5.2.9

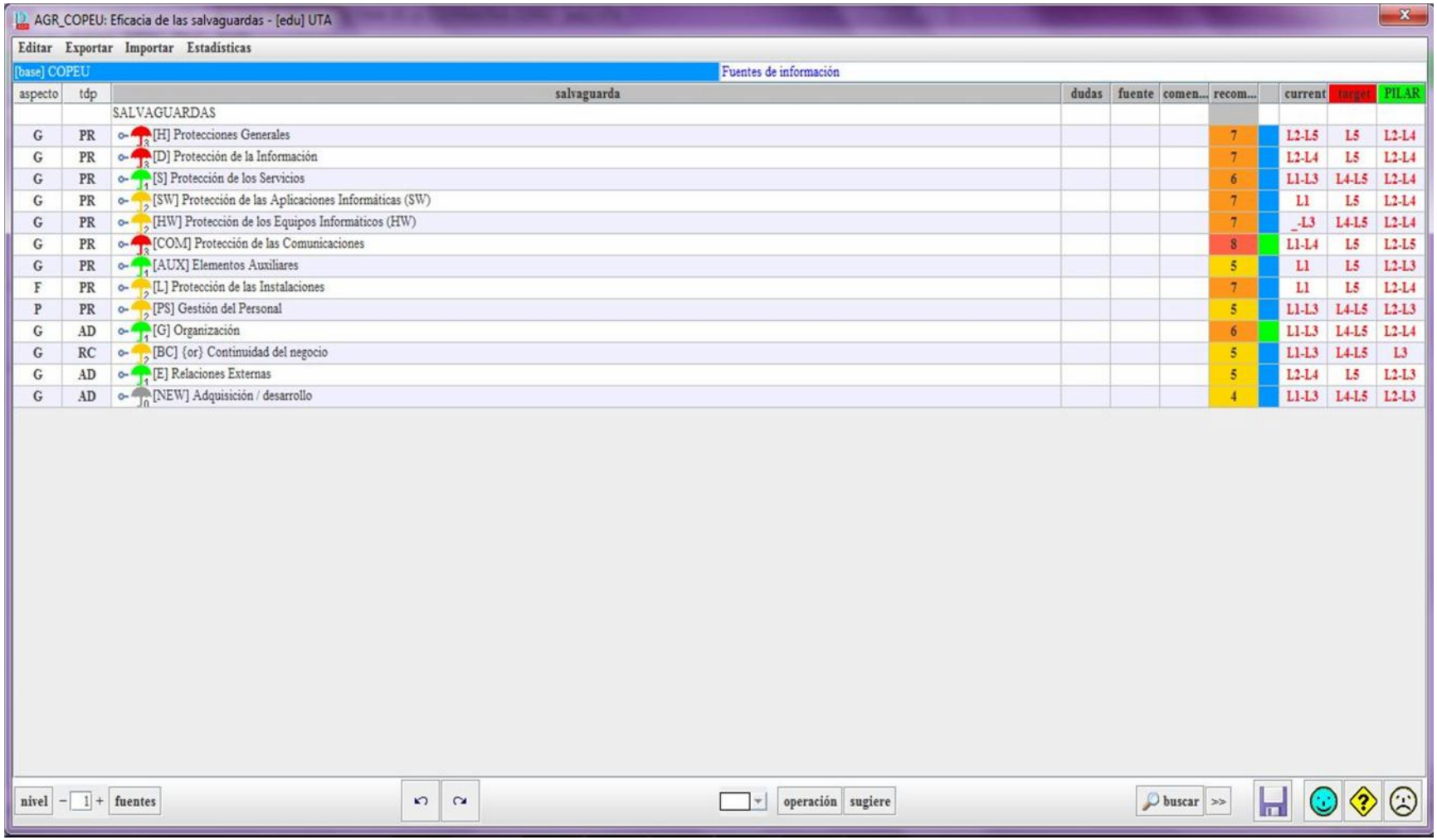


Figura 33: Tarea de Valoración de Salvaguardas
Fuente: PILAR 5.2.9

4.7.2.4 Identificación de Vulnerabilidades

Una vez identificado las amenazas y las salvaguardas existentes de los activos, la siguiente actividad es la identificación de vulnerabilidades.

Vulnerabilidad es la potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.

En la Gestión de Vulnerabilidades que genera la herramienta PILAR 5.2.9, se podrá definir qué criterios pueden influir sobre un dominio (y por lo tanto sobre todos los activos que se encuentran en dicho dominio)

Las Vulnerabilidades identificadas por medio de las encuestas, (Ver Anexo 5 Vulnerabilidad de los Dominios), que podrían generar que una amenaza se materialice son las siguientes:

Identificación del Atacante
Público en General
Competidor Comercial
Criminales/Terroristas
Personal Interno
Bandas Criminales
Motivación del Atacante
Económica (Beneficios en Dinero)
Beneficios Comerciales
Con ánimo destructivo
Con ánimo de causar daño
Beneficios del Atacante
Muy interesado
Motivación del Personal Interno
Con problemas de conciencia
Permisos de los Usuarios (derechos)
Se permite la ejecución de programas sin autorización previa
Se permite la instalación de programas sin autorización
Conectividad del Sistema de Información
Conectado a un amplio colectivo de redes
Ubicación del Sistema de Información
Dentro de una zona segura (“en casa”)

Tabla 30: Tarea de Valoración de Salvaguardas
Fuente: PILAR 5.2.9

4.7.2.5 Estimación del Estado de Riesgo

En esta tarea se procesa e interpreta los resultados obtenidos de las actividades anteriores para detallar en un informe del estado de riesgo de la empresa.

Y consta de dos tareas:

- Estimación del impacto
- Estimación del riesgo

El objetivo de esta tarea es:

- Disponer de una estimación fundada de lo que puede ocurrir (impacto) y de lo que probablemente ocurra (riesgo)

4.7.2.5.1 Estimación del Impacto

Su objetivo es:

- Establecer el impacto potencial al que está sometido el sistema
- Establecer el impacto residual al que está sometido el sistema

En esta tarea se estima al que están expuestos los activos del sistema:

- El impacto potencial, al que está expuesta el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas.
- El impacto residual, al que está expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas.

4.7.2.5.1.1 Impacto Potencial

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias

dimensiones) y la degradación que causan las amenazas, es directo el impacto que estas tendrían sobre el sistema.

Activos	[D]	[I]	[C]	[A]	[T]
Capa de negocio					
[AH_COPEU] AHORRO	[8]	[8]	[8]	[8]	[8]
[CR_COPEU] CREDITO	[8]	[8]	[8]	[8]	[8]
Servicios internos					
[AR_COPEU] ACCESO REMOTO	[8]	[8]	[8]	[8]	[8]
[SCE_COPEU] SERVIDOR DE CORREO ELECTRONICO	[9]	[9]	[9]	[9]	[9]
[SAC_COPEU] SERVIDOR DE ARCHIVO COMPARTIDO	[9]	[9]	[9]	[9]	[9]
[IN_COPEU] INTERNET	[9]	[9]	[9]	[9]	[9]
Equipamiento					
[SW.SISCO_COPEU] SISTEMA FINANCIERO COPEU	[9]	[9]	[9]	[9]	[9]
[SW.OF_COPEU] OFIMATICA	[6]	[6]	[6]	[6]	[6]
[SW.AN_COPEU] ANTIVIRUS	[8]	[8]	[8]	[8]	[8]
[SW.OTR_COPEU] OTRO SOFTWARE	[6]	[6]	[6]	[6]	[6]
[HW.SBD_COPEU] SERVIDOR DE BASE DE DATOS	[9]	[9]	[9]	[9]	[9]
[HW.ROU_COPEU] ROUTER	[6]	[6]	[6]	[6]	[6]
[HW.SWI_COPEU] SWITCH	[6]	[6]	[6]	[6]	[6]

[HW.FIR_COPEU] FIREWALL	[6]	[6]	[6]	[6]	[6]
[HW.COM_COPEU] COMPUTADORAS DE ESCRITORIO	[8]	[8]	[8]	[8]	[8]
[HW.COMPO_COPEU] COMPUTADORAS PORTATILES	[6]	[6]	[6]	[6]	[6]
[HW.IMPLA_COPEU] IMPRESORA A LASER	[3]	[3]	[3]	[3]	[3]
[HW.IMPMA_COPEU] IMPRESORA MATRICIAL	[3]	[3]	[3]	[3]	[3]
[COM.REDLA_COPEU] RED LAN	[8]	[8]	[8]	[8]	[8]
[COM.REDWA_COPEU] RED WAN	[8]	[8]	[8]	[8]	[8]
[COM.INT_COPEU] INTERNET COPEU	[8]	[8]	[8]	[8]	[8]
[AUX.CABDAT_COPEU] CABLEADO DE DATOS COPEU	[8]	[8]	[8]	[8]	[8]
[AUX.EQUAUX_COPEU] EQUIPAMIENTO AUXILIAR	[6]	[6]	[6]	[6]	[6]
Servicios subcontratados					
[PAGAGI_COPEU] PAGO AGIL COPEU	[3]	[3]	[3]	[3]	[3]
[SOLA_COPEU] SOAT LATINA	[3]	[3]	[3]	[3]	[3]
Instalaciones					
[USR_COPEU]UNIDAD DE SISTEMAS Y REDES COPEU	[8]	[8]	[8]	[8]	[8]
Personal					
[ADSFYBD_COPEU] ADMINISTRACION SISTEMA FINANCIERO Y BASE DE DATOS	[0]	[0]	[0]	[0]	[0]
[SU_COPEU] SOPORTE A USUARIO	[0]	[0]	[0]	[0]	[0]

Tabla 31: Impacto Potencial sobre cada uno de los activos
Fuente: Realizado en PILAR 5.2.9

Los impactos que se muestran con la siguiente escala de colores según su valor:

10	Critico
9	Muy Alto
8	Muy Alto
7	Alto
6	Alto
5	Medio
4	Medio
3	Bajo
2	Bajo
1	Despreciable
0	Despreciable

Tabla 32: Impacto Escala de Colores según su Valor
Fuente: Realizado en PILAR 5.2.9

4.7.2.5.1.2 Impacto Residual Acumulado

El impacto acumulado se calcula con los datos de impacto acumulado sobre un activo y salvaguardas apropiadas para las amenazas sobre dicho activo.

Activos	[D]	[I]	[C]	[A]	[T]
Capa de negocio					
[AH_COPEU] AHORRO	[9]	[9]	[9]	[9]	[9]
[CR_COPEU] CREDITO	[9]	[9]	[9]	[9]	[9]
Servicios internos					
[AR_COPEU] ACCESO REMOTO	[3]	[3]	[3]	[3]	[3]
[SCE_COPEU] SERVIDOR DE CORREO ELECTRONICO	[2]	[2]	[2]	[2]	[2]
[SAC_COPEU] SERVIDOR DE ARCHIVO COMPARTIDO	[4]	[4]	[4]	[4]	[4]
[IN_COPEU] INTERNET	[2]	[2]	[2]	[2]	[2]

Equipamiento					
[SW.SISCO_COPEU] SISTEMA FINANCIERO COPEU	[9]	[9]	[9]	[9]	[9]
[SW.OF_COPEU] OFIMATICA	[1]	[1]	[1]	[1]	[1]
[SW.AN_COPEU] ANTIVIRUS	[5]	[5]	[5]	[5]	[5]
[SW.OTR_COPEU] OTRO SOFTWARE	[2]	[2]	[2]	[2]	[2]
[HW.SBD_COPEU] SERVIDOR DE BASE DE DATOS	[5]	[5]	[5]	[5]	[5]
[HW.ROU_COPEU] ROUTER	[0]	[0]	[0]	[0]	[0]
[HW.SWI_COPEU] SWITCH	[0]	[0]	[0]	[0]	[0]
[HW.FIR_COPEU] FIREWALL	[0]	[0]	[0]	[0]	[0]
[HW.COM_COPEU] COMPUTADORAS DE ESCRITORIO	[2]	[2]	[2]	[2]	[2]
[HW.COMPO_COPEU] COMPUTADORAS PORTATILES	[0]	[0]	[0]	[0]	[0]
[HW.IMPLA_COPEU] IMPRESORA A LASER	[0]	[0]	[0]	[0]	[0]
[HW.IMPMA_COPEU] IMPRESORA MATRICIAL	[0]	[0]	[0]	[0]	[0]
[COM.REDLA_COPEU] RED LAN	[1]	[1]	[1]	[1]	[1]
[COM.REDWA_COPEU] RED WAN	[1]	[1]	[1]	[1]	[1]
[COM.INT_COPEU] INTERNET COPEU	[1]	[1]	[1]	[1]	[1]
[AUX.CABDAT_COPEU] CABLEADO DE DATOS COPEU	[1]	[1]	[1]	[1]	[1]
[AUX.EQUAUX_COPEU] EQUIPAMIENTO AUXILIAR	[0]	[0]	[0]	[0]	[0]
Servicios subcontratados					

[PAGAGI_COPEU] PAGO AGIL COPEU	[4]	[4]	[4]	[4]	[4]
[SOLA_COPEU] SOAT LATINA	[4]	[4]	[4]	[4]	[4]
Instalaciones					
[USR_COPEU]UNIDAD DE SISTEMAS Y REDES COPEU	[6]	[6]	[6]	[6]	[6]
Personal					
[ADSFYBD_COPEU] ADMINISTRACION SISTEMA FINANCIERO Y BASE DE DATOS	[0]	[0]	[0]	[0]	[0]
[SU_COPEU] SOPORTE A USUARIO	[0]	[0]	[0]	[0]	[0]

Tabla 33: Impacto Residual sobre cada uno de los activos
Fuente: Realizado en PILAR 5.2.9

4.7.2.5.2 Estimación del Riesgo

Sus objetivos son:

- Determinar el riesgo potencial al que está sometido el sistema
- Determinar el riesgo residual al que está sometido el sistema

En esta tarea se estima el riesgo al o que están sometidos los activos del sistema:

- El riesgo potencial, al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas.
- El riego residual , al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como eficacia de las salvaguardas actualmente desplegadas.

4.7.2.5.2.1 Riesgo Potencial

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener la probabilidad de ocurrencia.

Activos	[D]	[I]	[C]	[A]	[T]
Capa de negocio					
[AH_COPEU] AHORRO	[4,8]	[4,8]	[4,8]	[4,8]	[4,8]
[CR_COPEU] CREDITO	[4,8]	[4,8]	[4,8]	[4,8]	[4,8]
Servicios internos					
[AR_COPEU] ACCESO REMOTO	[4,8]	[4,8]	[4,8]	[4,8]	[4,8]
[SCE_COPEU] SERVIDOR DE CORREO ELECTRONICO	[5,3]	[5,3]	[5,3]	[5,3]	[5,3]
[SAC_COPEU] SERVIDOR DE ARCHIVO COMPARTIDO	[5,3]	[5,3]	[5,3]	[5,3]	[5,3]
[IN_COPEU] INTERNET	[5,3]	[5,3]	[5,3]	[5,3]	[5,3]
Equipamiento					
[SW.SISCO_COPEU] SISTEMA FINANCIERO COPEU	[5,4]	[5,4]	[5,4]	[5,4]	[5,4]
[SW.OF_COPEU] OFIMATICA	[3,6]	[3,6]	[3,6]	[3,6]	[3,6]
[SW.AN_COPEU] ANTIVIRUS	[4,8]	[4,8]	[4,8]	[4,8]	[4,8]
[SW.OTR_COPEU] OTRO SOFTWARE	[3,6]	[3,6]	[3,6]	[3,6]	[3,6]
[HW.SBD_COPEU] SERVIDOR DE BASE DE DATOS	[5,3]	[5,3]	[5,3]	[5,3]	[5,3]
[HW.ROU_COPEU] ROUTER	[3,6]	[3,6]	[3,6]	[3,6]	[3,6]
[HW.SWI_COPEU] SWITCH	[3,6]	[3,6]	[3,6]	[3,6]	[3,6]

[HW.FIR_COPEU] FIREWALL	[3,6]	[3,6]	[3,6]	[3,6]	[3,6]
[HW.COM_COPEU] COMPUTADORAS DE ESCRITORIO	[4,8]	[4,8]	[4,8]	[4,8]	[4,8]
[HW.COMPO_COPEU] COMPUTADORAS PORTATILES	[3,6]	[3,6]	[3,6]	[3,6]	[3,6]
[HW.IMPLA_COPEU] IMPRESORA A LASER	[1,8]	[1,8]	[1,8]	[1,8]	[1,8]
[HW.IMPMA_COPEU] IMPRESORA MATRICIAL	[1,8]	[1,8]	[1,8]	[1,8]	[1,8]
[COM.REDLA_COPEU] RED LAN	[4,8]	[4,8]	[4,8]	[4,8]	[4,8]
[COM.REDWA_COPEU] RED WAN	[4,8]	[4,8]	[4,8]	[4,8]	[4,8]
[COM.INT_COPEU] INTERNET COPEU	[4,8]	[4,8]	[4,8]	[4,8]	[4,8]
[AUX.CABDAT_COPEU] CABLEADO DE DATOS COPEU	[4,8]	[4,8]	[4,8]	[4,8]	[4,8]
[AUX.EQUAUX_COPEU] EQUIPAMIENTO AUXILIAR	[3,6]	[3,6]	[3,6]	[3,6]	[3,6]
Servicios subcontratados					
[PAGAGI_COPEU] PAGO AGIL COPEU	[1,9]	[1,9]	[1,9]	[1,9]	[1,9]
[SOLA_COPEU] SOAT LATINA	[1,9]	[1,9]	[1,9]	[1,9]	[1,9]
Instalaciones					
[USR_COPEU]UNIDAD DE SISTEMAS Y REDES COPEU	[4,8]	[4,8]	[4,8]	[4,8]	[4,8]
Personal					
[ADSFYBD_COPEU] ADMINISTRACION SISTEMA FINANCIERO Y BASE DE DATOS	[0,57]	[0,57]	[0,57]	[0,57]	[0,57]
[SU_COPEU] SOPORTE A USUARIO	[0,57]	[0,57]	[0,57]	[0,57]	[0,57]

Tabla 34: Riesgo Potencial sobre cada uno de los activos
Fuente: Realizado en PILAR 5.2.9

Los riesgos se muestran con la siguiente escala de colores según su valor:

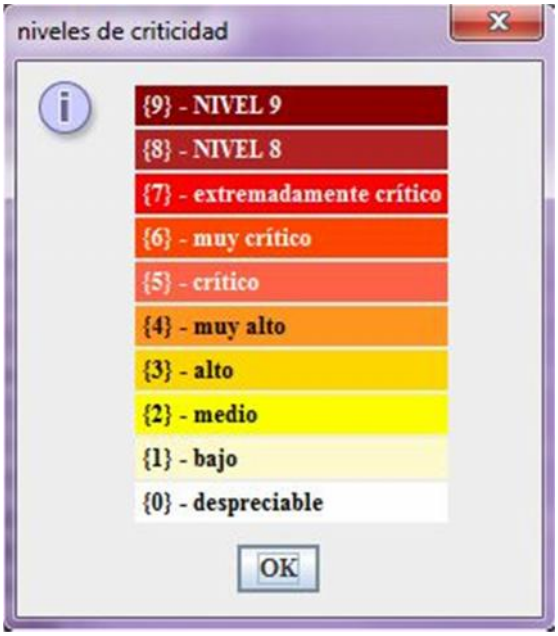


Figura 34: Riesgo Escala de Colores según su Valor
Fuente: Realizado en PILAR 5.2.9

4.7.2.5.2.2 Riesgo Residual

4.7.2.5.2.2.1 Riesgo Residual Acumulado

La estimación de riesgo residual acumulado nos indica la medida que las amenazas que afectan a los activos de orden superior que dependen de dicho activo.

Activos	[D]	[I]	[C]	[A]	[T]
Capa de negocio					
[AH_COPEU] AHORRO	[5,3]	[5,3]	[5,3]	[5,3]	[5,3]
[CR_COPEU] CREDITO	[5,3]	[5,3]	[5,3]	[5,3]	[5,3]
Servicios internos					
[AR_COPEU] ACCESO REMOTO	[1,7]	[1,7]	[1,7]	[1,7]	[1,7]

[SCE_COPEU] SERVIDOR DE CORREO ELECTRONICO	[1,2]	[1,2]	[1,2]	[1,2]	[1,2]
[SAC_COPEU] SERVIDOR DE ARCHIVO COMPARTIDO	[2,3]	[2,3]	[2,3]	[2,3]	[2,3]
[IN_COPEU] INTERNET	[1,2]	[1,2]	[1,2]	[1,2]	[1,2]
Equipamiento					
[SW.SISCO_COPEU] SISTEMA FINANCIERO COPEU	[5,4]	[5,4]	[5,4]	[5,4]	[5,4]
[SW.OF_COPEU] OFIMATICA	[0,91]	[0,91]	[0,91]	[0,91]	[0,91]
[SW.AN_COPEU] ANTIVIRUS	[2,9]	[2,9]	[2,9]	[2,9]	[2,9]
[SW.OTR_COPEU] OTRO SOFTWARE	[1,3]	[1,3]	[1,3]	[1,3]	[1,3]
[HW.SBD_COPEU] SERVIDOR DE BASE DE DATOS	[2,9]	[2,9]	[2,9]	[2,9]	[2,9]
[HW.ROU_COPEU] ROUTER	[0,82]	[0,82]	[0,82]	[0,82]	[0,82]
[HW.SWI_COPEU] SWITCH	[0,82]	[0,82]	[0,82]	[0,82]	[0,82]
[HW.FIR_COPEU] FIREWALL	[0,82]	[0,82]	[0,82]	[0,82]	[0,82]
[HW.COM_COPEU] COMPUTADORAS DE ESCRITORIO	[1,3]	[1,3]	[1,3]	[1,3]	[1,3]
[HW.COMPO_COPEU] COMPUTADORAS PORTATILES	[0,82]	[0,82]	[0,82]	[0,82]	[0,82]
[HW.IMPLA_COPEU] IMPRESORA A LASER	[0,82]	[0,82]	[0,82]	[0,82]	[0,82]
[HW.IMPMA_COPEU] IMPRESORA MATRICIAL	[0,82]	[0,82]	[0,82]	[0,82]	[0,82]
[COM.REDLA_COPEU] RED LAN	[0,94]	[0,94]	[0,94]	[0,94]	[0,94]
[COM.REDWA_COPEU] RED WAN	[0,94]	[0,94]	[0,94]	[0,94]	[0,94]
[COM.INT_COPEU] INTERNET COPEU	[0,94]	[0,94]	[0,94]	[0,94]	[0,94]

[AUX.CABDAT_COPEU] CABLEADO DE DATOS COPEU	[0,94]	[0,94]	[0,94]	[0,94]	[0,94]
[AUX.EQUAUX_COPEU] EQUIPAMIENTO AUXILIAR	[0,69]	[0,69]	[0,69]	[0,69]	[0,69]
Servicios subcontratados					
[PAGAGI_COPEU] PAGO AGIL COPEU	[2,3]	[2,3]	[2,3]	[2,3]	[2,3]
[SOLA_COPEU] SOAT LATINA	[2,3]	[2,3]	[2,3]	[2,3]	[2,3]
Instalaciones					
[USR_COPEU]UNIDAD DE SISTEMAS Y REDES COPEU	[3,6]	[3,6]	[3,6]	[3,6]	[3,6]
Personal					
[ADSFYBD_COPEU] ADMINISTRACION SISTEMA FINANCIERO Y BASE DE DATOS	[0,57]	[0,57]	[0,57]	[0,57]	[0,57]
[SU_COPEU] SOPORTE A USUARIO	[0,57]	[0,57]	[0,57]	[0,57]	[0,57]

Tabla 35: Riesgo Residual sobre cada uno de los activos
Fuente: Realizado en PILAR 5.2.9

4.7.2.5.2.3 Interpretación de los resultados

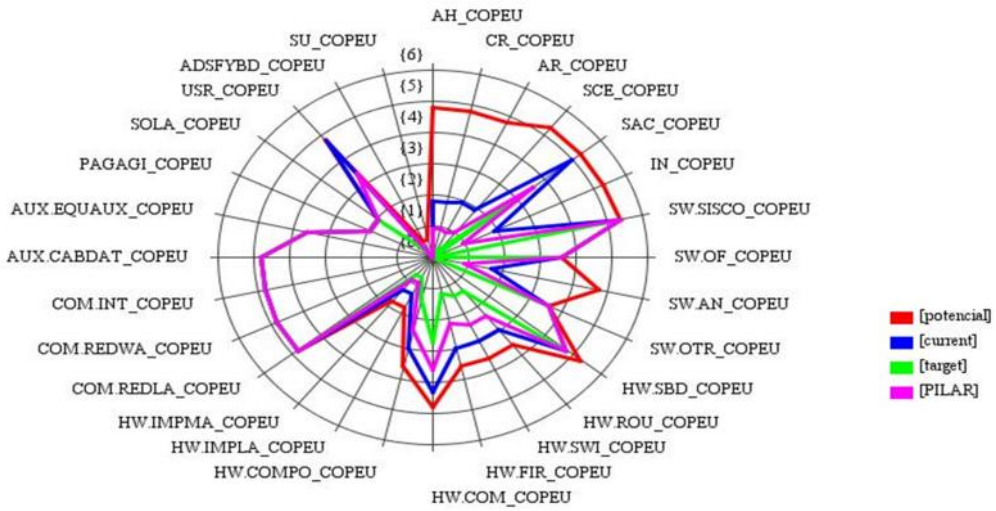


Figura 35: Identificación de Riesgos
Fuente: PILAR 5.2.9

Como se puede observar en la Figura 35 Esto es el resultado de todos los pasos del Análisis de Riesgos ya que se hace fácil saber cuáles son los activos que tiene un nivel alto de riesgos, para mitigarlos en la siguiente fase que es la Gestión de Riesgos

4.7.3 Gestión de Riesgos

Después de haber realizado el Análisis de Riesgos queda a la vista los impactos y los riesgos que están expuesto la empresa.

Lo que ha llegado a una calificación de cada riesgo significativo, determinándose si

- Es crítico en el sentido de que requiere atención urgente
- Es grave en el sentido de que requiere atención
- Es apreciable en el sentido d que pueda ser objeto de estudio para su tratamiento
- Es asumible en el sentido de que no se van a tomar acciones para atajarlo

El resultado del análisis es solo un análisis. A partir de que disponemos de información para tomar decisiones conociendo lo que queremos proteger (activos valorados =, de que lo queremos proteger (amenazas valoradas)) y que hemos por protegerlo (salvaguardas valoradas). Todo ello sintetizado en los valores de impacto y riesgo.

4.7.3.1 Toma de Decisiones

4.7.3.1.1 Identificación de Riesgos Críticos

En toda organización los activos están expuestos a riegos, pero lo importante es conocer cuáles de los activos poseen mayor nivel de riesgo con el fin de implementar salvaguardas para evitar que las amenazas se materialicen.

Una vez evaluado los activos y conocido el riesgo a los que están expuestos los mismos, hemos seleccionado los activos que poseen un nivel de riesgo. A continuación se mostramos la siguiente tabla.

Activos	[D]	[I]	[C]	[A]	[T]
Capa de negocio					
[AH_COPEU] AHORRO	[4,8]	[5]	[5]	[5]	[5]
[CR_COPEU] CREDITO	[4,8]	[5]	[5]	[5]	[5]
Servicios internos					
[SAC_COPEU] SERVIDOR DE ARCHIVO COMPARTIDO	[1,9]	[2,1]	[2,1]	[2,1]	[2,1]
Equipamiento					
[SW.SISCO_COPEU] SISTEMA FINANCIERO COPEU	[4,8]	[5,4]	[5,4]	[5,4]	[5,4]
[SW.AN_COPEU] ANTIVIRUS	[2,5]	[2,7]	[2,7]	[2,7]	[2,7]
[HW.SBD_COPEU] SERVIDOR DE BASE DE DATOS	[2,5]	[2,5]	[2,5]	[2,5]	[2,5]
Servicios subcontratados					
[PAGAGI_COPEU] PAGO AGIL COPEU	[1,9]	[2,1]	[2,1]	[2,1]	[2,1]
[SOLA_COPEU] SOAT LATINA	[1,9]	[2,1]	[2,1]	[2,1]	[2,1]
Instalaciones					
[USR_COPEU]UNIDAD DE SISTEMAS Y REDES COPEU	[3,1]	[3,5]	[3,5]	[3,5]	[3,5]

Tabla 36: Identificación de Riesgos Críticos (current)
Fuente: Realizado en PILAR 5.2.9

Los riesgos se muestran con la siguiente escala de colores según su valor:

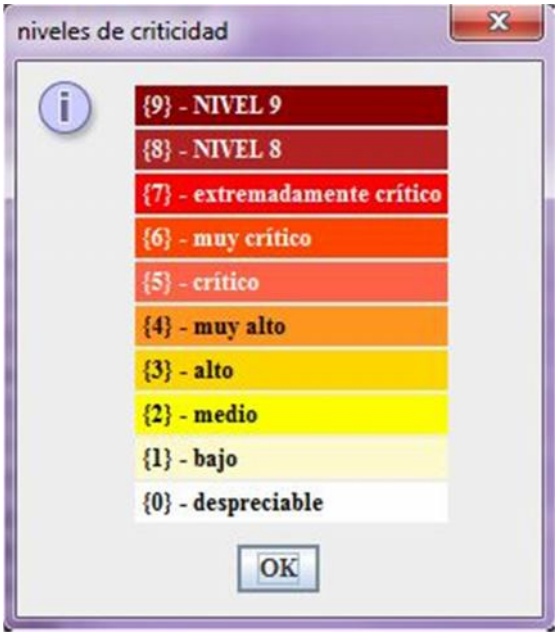


Figura 36: Riesgo Escala de Colores según su Valor
Fuente: Realizado en PILAR 5.2.9

4.7.3.1.2 Calificación del Riesgo

A continuación se gestionan los activos con riesgos críticos:

Ahorro: Este activo pertenece a la capa de Negocio, una vez encontrado amenazas y de haber escogidos las salvaguardas antes mencionadas se han obtenido los siguientes resultados.

La amenaza de mayor relevancia que posee es fallo de servicios de comunicaciones que afecta en la disponibilidad (4,8) y en la integridad, confidencialidad, autenticidad, trazabilidad (5) si se llega a materializar esta amenaza no podrían ejecutar tareas diarias como es las transacciones que es el negocio fundamental de la Cooperativa.

Las medidas para reducir el riesgo actual (current) de este activo, son las siguientes:

La medida que se debe de tomar es de realizar mantenimientos regulares del estado de la red y del sistema para que no exista fallos y problemas al momento de realizar las transacciones que maneja diariamente la Cooperativa y respondan ágilmente.

Crédito: Este activo pertenece a la capa de Negocio, una vez encontrado amenazas y de haber escogidos las salvaguardas antes mencionadas se han obtenido los siguientes resultados.

La amenaza de mayor relevancia que posee es fallo de servicios de comunicaciones que afecta en la disponibilidad (4,8) y en la integridad, confidencialidad, autenticidad, trazabilidad (5) si se llega a materializar esta amenaza no podrían ejecutar tareas diarias como es las transacciones que es el negocio fundamental de la Cooperativa.

Las medidas para reducir el riesgo actual (current) de este activo, son las siguientes:

La medida que se debe de tomar es de realizar mantenimientos regulares del estado de la red y del sistema para que no exista fallos y problemas al momento de realizar las transacciones que maneja diariamente la Cooperativa y respondan ágilmente.

Servidor de Archivo Compartido: Este activo pertenece a la capa de Servicios Internos, una vez encontrado amenazas y de haber escogidos las salvaguardas antes mencionadas se han obtenido los siguientes resultados.

La amenaza de mayor relevancia que posee es la degradación de los soportes de almacenamiento de información así como también la modificación y destrucción de la información que afecta en la disponibilidad (1,9) y en la integridad, confidencialidad, autenticidad, trazabilidad (2,1) si se llega a materializar esta amenaza no podrían realizar el compartimiento de información y archivos dentro de la Cooperativa.

Las medidas para reducir el riesgo actual (current) de este activo, son las siguientes:

La medida que se debe de tomar es de realizar mantenimientos al Servidor de Archivo Compartido así como también crear claves al momento de acceder a la

información compartida y en seguridad configurar para que los que accedan no puedan borrar o modificar la información.

Sistema Financiero COPEU: Este activo pertenece a la capa de Aplicaciones, una vez encontrado amenazas y de haber escogidos las salvaguardas antes mencionadas se han obtenido los siguientes resultados.

La amenaza de mayor relevancia que posee es Avería de Origen Físico o Lógico, Fallo de Servicios de Comunicación y el Acceso no Autorizado que afecta en la disponibilidad (4,8) y en la integridad, confidencialidad, autenticidad, trazabilidad (5,4) si se llega a materializar estas amenazas no podrían ejecutar tareas diarias como es las transacciones de Ahorro y Crédito que es el negocio fundamental de la Cooperativa.

Las medidas para reducir el riesgo actual (current) de este activo, son las siguientes:

La medida que se debe de tomar es de realizar mantenimientos regulares del estado de la red y del sistema para que no exista fallos y problemas al momento de realizar las transacciones que maneja diariamente la Cooperativa y respondan ágilmente.

Mejorar las medidas de control de acceso para aumentar la seguridad de la información, como el control mediante firewall.

Implementar un registro de errores no intencionales.

Antivirus: Este activo pertenece a la capa de Aplicaciones, una vez encontrado amenazas y de haber escogidos las salvaguardas antes mencionadas se han obtenido los siguientes resultados.

La amenaza de mayor relevancia que posee este activo es la Difusión de software dañino que afecta en la disponibilidad (2,5) y en la integridad, confidencialidad, autenticidad, trazabilidad (2,7). Una de las principales razones es que la mayoría de veces cuando hacen uso de dispositivos externos como memory flash no la hacen

analizar por el antivirus provocando la propagación de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.

Las medidas para reducir el riesgo actual (current) de este activo, son las siguientes:

La medida que se debe tomar es la adquisición de software óptimo para evitar la propagación de virus.

También actualizar el antivirus para que pueda contra restar cualquier software dañino.

O que en lo posible de colocar dispositivos externos en las máquinas para así evitar que pueda ser infectadas.

Cambiar por otro antivirus que se mejor y licenciado.

Servidor de Base de Datos: este activo pertenece a la capa de Equipos, una vez encontrado amenazas y de haber escogidos las salvaguardas antes mencionadas se han obtenido los siguientes resultados.

Las amenazas de mayor relevancia que posee este activo son Condición Inadecuada de temperatura o humedad, denegación del servicio y manipulación de hardware que afecta en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad (2,5). Si la primera amenaza llegase a materializarse el servidor de base de datos trasladaría la información demasiado tarde a quien lo requiera, debido a la deficiencia de adaptación del local donde se encuentra, por exceso de calor, frio o humedad. La amenaza denegación de servicio provoca que el sistema caiga debido a una carencia de recursos suficientes. Por último la amenaza manipulación de hardware es producida por que no existe un lugar adecuado donde solo ingrese el personal autorizado permitiendo que cualquier empleado pueda hacer mal uso de este equipo quedando totalmente inseguro. Si estas amenazas se materializan podrían causar graves daños para la Cooperativa ya que se encuentra almacenada información importante y no hay redundancia.

La medida para reducir el riesgo actual (current) de este activo, es la siguiente

Es de trasladar el servidor hacia un cuarto donde se toman todas las medidas de seguridad necesarias como es el control de accesos y en el espacio adecuado para evitar calor, frio o humedad.

Resguardar la seguridad física para ser frente amenazas como desastres naturales.

Pago Ágil COPEU: Este activo pertenece a la capa de Servicios Subcontratados, una vez encontrado las amenazas y de haber escogido las salvaguardas antes mencionadas se han obtenido los siguientes resultados:

Las amenazas de mayor relevancia que posee este activo son Caída del Sistema por Agotamiento de Recursos, Acceso no Autorizado y la Suplantación de la Identidad del Usuario que afecta en la disponibilidad (1,9) y en la integridad, confidencialidad, autenticidad, trazabilidad (2,1). Si la primera amenaza llegase a materializarse provocarían que los usuarios no puedan realizar el pago de alguno de los servicios que presta la Cooperativa. La amenaza de acceso no autorizado si se materializa provocaría que el atacante acceda al sistema burlando su autenticidad haciendo que el sistema funcione con fallas o simplemente no funcione. Si la tercera amenaza llegase a materializarse provocaría que el atacante disfrute de los privilegios para sus fines o propios o para terceros.

La medida para reducir el riesgo actual (current) de este activo, es la siguiente

Implementar controles de monitorización y verificación del rendimiento.

Implementar acuerdos para informar, notificar, investigar las incidencias y fallos de seguridad.

Implementar medidas de control de acceso para aumentar la seguridad de los servicios en línea como: protección de acceso controlado donde se limite los intentos fallidos de acceso.

SOAT Latina: Este activo pertenece a la capa de Servicios Subcontratados, una vez encontrado las amenazas y de haber escogido las salvaguardas antes mencionadas se han obtenido los siguientes resultados:

Las amenazas de mayor relevancia que posee este activo son Caída del Sistema por Agotamiento de Recursos, Acceso no Autorizado y la Suplantación de la Identidad del Usuario que afecta en la disponibilidad (1,9) y en la integridad, confidencialidad, autenticidad, trazabilidad (2,1). Si la primera amenaza llegase a materializarse provocarían que los usuarios no puedan realizar el pago del SOAT que es el seguro obligatorio de accidentes de tránsito que presta la Cooperativa. La amenaza de acceso no autorizado si se materializa provocaría que el atacante acceda al sistema burlando su autenticidad haciendo que el sistema funcione con fallas o simplemente no funcione. Si la tercera amenaza llegase a materializarse provocaría que el atacante disfrute de los privilegios para sus fines o propios o para terceros.

La medida para reducir el riesgo actual (current) de este activo, es la siguiente

Implementar controles de monitorización y verificación del rendimiento.

Implementar acuerdos para informar, notificar, investigar las incidencias y fallos de seguridad.

Implementar medidas de control de acceso para aumentar la seguridad de los servicios en línea como: protección de acceso controlado donde se limite los intentos fallidos de acceso.

Unidad de Sistemas y Redes COPEU: Este activo que pertenece a la capa de Instalaciones, una vez encontrado las amenazas y de haber escogido las salvaguardas antes mencionadas se han obtenido los siguientes resultados:

Las amenazas de mayor relevancia que posee este activo son Desastres Naturales, Deficiencias en la Organización y Acceso no Autorizado que afecta en la disponibilidad (3,1) y en la integridad, confidencialidad, autenticidad, trazabilidad (3,5). Si las dos primeras amenazas llegasen a materializarse el nivel de impacto sería

alto, causando daños físicos y económicos así como impediría que el personal disponga de las instalaciones para poder ejecutar sus actividades diarias. La amenaza de acceso no autorizado si llegase a materializarse el atacante puede ser el causante de producir daños irreversibles como son físicos y económicos.

La medida para reducir el riesgo actual (current) de este activo, es la siguiente:

Supervisar la norma de conducta (prohibición de fumar, beber, comer, etc).

Implementar un plan de Protección frente a desastres así como también implementar una separación de áreas de seguridad y de acceso público.

4.7.3.2 Plan de seguridad

Es una actividad con el objetivo de ordenar en un lapso de tiempo los programas de seguridad considerando la criticidad, gravedad de los impactos y/o riesgos que se van a mitigar, con una prioridad relevante a los activos en situaciones críticas, como también la disponibilidad del personal para la implementación de las actividades del plan.

Los planes pueden llevarse en un plazo de tiempo, ya sea a corto o a largo plazo, dependiendo de la perspectiva y objetivos específicos en los que se materialicen los programas de seguridad.

Un control de seguridad que la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU) debe implementar es la norma ISO/IEC 27002:2005 Código de buenas prácticas para la Gestión de la Seguridad de la Información. La herramienta PILAR 5.2.9 nos genera un reporte de dicha norma. (Ver Anexo 6. Código de buenas prácticas para la Gestión de la Seguridad de la Información)

En esta fase del proyecto se trata de cómo llevar a cabo planes de seguridad, atendiendo por tales proyectos para materializar las decisiones adoptadas para el tratamiento de los riesgos.

Aquí se identifican 3 tareas

- Identificación de proyectos de seguridad
- Plan Ejecución
- Ejecución

4.7.3.2.1 Identificación de proyectos de Seguridad

El objetivo de esta tarea es:

- Elaborar un conjunto integral de programas de seguridad

Un programa seguridad es una agrupación de tareas. La agrupación se realiza por conveniencia, porque se trata de tareas que en singular carecerían de eficacia, bien porque se trata de tareas con objetivo en común, bien porque se trata de tareas que competen a una única unidad acción."

Esta tarea se va a realizar 3 actividades:

- Normativas de Seguridad
- Eliminar fallos de seguridad evidentes
- Clasificación del inventario (SW, HW, Soportes de Información, Elementos auxiliares)

4.7.3.2.1.1 Normativas de Seguridad

Documentación del uso autorizado de las aplicaciones

- Se considerara una falta grave el que los empleados instalen cualquier tipo de programa (Software) en sus computadoras, que sea para fines personales o de recreación.
- Para prevenir infecciones por virus informáticos, los empleados deberán evitar hacer uso de cualquier clase de software proporcionado por la empresa.
- Los empleados están obligados a verificar que la información y que los medios de almacenamiento, considerando memorias USB estén libres de

cualquier tipo de software dañino, para ello deben ejecutar el software antivirus.

Documentación del uso correcto de equipos de equipos informáticos

- A cada empleado se le asigna un equipo asiéndolo responsable.
- Los empleados no deberán mover o reubicar los equipos de cómputo, instalar o desinstalar dispositivos. Solo el personal adecuado podrá realizarlo.
- Mientras se utilizan los equipos de cómputo, no se podrá consumir alimentas o ingerir líquidos, solo si son botellas de plástico.
- Evitar colocar objeto encima del equipo o cubrir los orificios de ventilación.
- Mantener el equipo informático en un entorno limpio y sin humedad.
- Solo el personal apropiado podrá llevar a cabo los servicios y reparaciones al equipo informático.
- En caso de que existe descompostura por maltrato por descuido o negligencia por parte del empleado, estará obligado a cubrir el valor de la reparación o reposición del equipo o accesorio afectado.

Documentación del resguardo y protección de la información

- El uso de CDs es exclusivo para respaldos de información. El empleado es el responsable de su resguardo.
- Los empleados deberán respaldar de manera periódica la información sensible y critica que se encuentren en sus computadoras.

Documentación del uso de servicios de internet

- Para el uso del correo electrónico los empleados no debe de usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros.

- Los empleados deben tratar los mensajes de correo electrónico y archivos adjuntos como información que es de propiedad de la “Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU)”.
- Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.
- El acceso a internet es exclusivamente para actividades relacionadas con las necesidades del puesto y función que desempeña.

Documentación de protección de las instalaciones

- Establecer normas de conducta cuando estén cerca del servidor, lugares de trabajo, etc. además de cumplir todas las normas de sanidad y seguridad existentes para las instalaciones de la Cooperativa.

Documentación de la gestión del personal

- En cada contrato de trabajo se deberá cláusulas de confidencialidad para asegurar información de la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU).
- Todo empleado que utilice los bienes y servicios informáticos se compromete a conducirse bajo los principios de confidencialidad de la información.
- Que cada empleado deberá cumplir con un horario de trabajo.
- Establecer normas de conducta de los empleados para formar un ambiente laboral adecuado y respetuoso entre todos.

Con la estudio de salvaguardas en el nivel de riesgo actual (current), a la aplicación de salvaguardas al nivel de riesgo objetivo (target), los riesgos disminuyen considerablemente como se puede observar en la siguiente tabla.

Activos	[D]	[I]	[C]	[A]	[T]
Capa de negocio					
[AH_COPEU] AHORRO	[4,8]	[4,8]	[4,8]	[4,8]	[4,8]
[CR_COPEU] CREDITO	[4,8]	[4,8]	[4,8]	[4,8]	[4,8]
Servicios internos					
[SAC_COPEU] SERVIDOR DE ARCHIVO COMPARTIDO	[1,9]	[1,9]	[1,9]	[1,9]	[1,9]
Equipamiento					
[SW.SISCO_COPEU] SISTEMA FINANCIERO COPEU	[4,8]	[5,4]	[5,4]	[5,4]	[5,4]
[SW.AN_COPEU] ANTIVIRUS	[2,5]	[2,5]	[2,5]	[2,5]	[2,5]
[HW.SBD_COPEU] SERVIDOR DE BASE DE DATOS	[2,5]	[2,5]	[2,5]	[2,5]	[2,5]
Servicios subcontratados					
[PAGAGI_COPEU] PAGO AGIL COPEU	[1,9]	[1,9]	[1,9]	[1,9]	[1,9]
[SOLA_COPEU] SOAT LATINA	[1,9]	[1,9]	[1,9]	[1,9]	[1,9]
Instalaciones					
[USR_COPEU]UNIDAD DE SISTEMAS Y REDES COPEU	[0,01]	[0,01]	[0,01]	[0,01]	[0,01]

Tabla 37: Resultados de Riesgos Residuales (target)
Fuente: Realizado en PILAR 5.2.9

Los riesgos se muestran con la siguiente escala de colores según su valor:

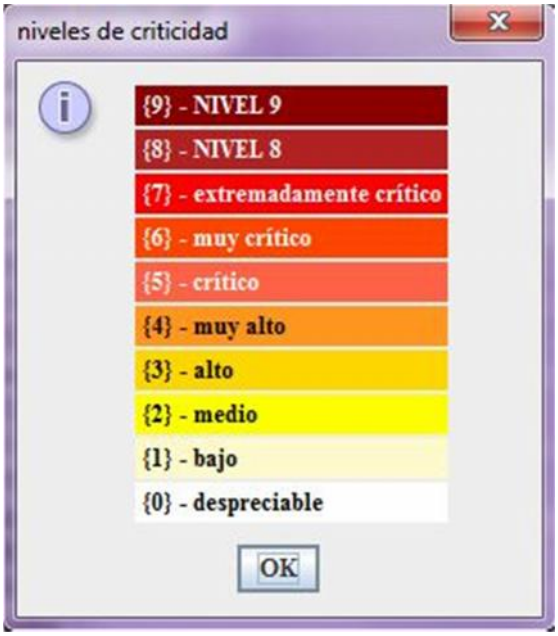


Figura 37: Riesgo Escala de Colores según su Valor
Fuente: Realizado en PILAR 5.2.9

4.7.3.2.1.2 Eliminar fallos de seguridad evidentes

4.7.3.2.1.2.1 Sistema Financiero y su capa del negocio Ahorro y Crédito.

Por lo que podemos sacar de conclusión es que el sistema actual de la Cooperativa ya es muy antiguo y anda deteriorado es decir cumplió su vida útil realiza los procesos y transacciones pero no con agilidad e igual existen caídas del sistema y agotamiento en el tiempo de respuesta por lo que hemos procedido a plantear la propuesta de un nuevo Sistema Financiero actual para mejorar el funcionamiento y desempeño de las actividades diarias que realiza la Cooperativa y así no realizar perdidas económicas y la Cooperativa pueda seguir creciendo.

PROPUESTA PARA LA IMPLANTACIÓN DE LA SOLUCIÓN

FINANCIAL BUSINESS SYSTEM 2.0 BASIC EDITION

EN LA COOPERATIVA DE AHORRO Y CRÉDITO UNIVERSITARIA LIMITADA (COPEU).

4.7.3.2.1.2.1.1 Antecedentes

En los tiempos actuales la tecnología de información juega un papel fundamental como medio y soporte para alcanzar los niveles de eficiencia operativa y administrativa requeridos para la consecución de los objetivos estratégicos de las empresas modernas.

Por lo cual la presente propuesta de implantación de la solución **FINANCIAL BUSINESS SYSTEM 2.0 BASIC EDITION**, responde a las exigencias actuales y las metas que la entidad se plantea hacia futuro.

4.7.3.2.1.2.1.2 Propuesta de Bienes y Servicios Tecnológicos

Mediante la presente propuesta se pone a consideración de la Cooperativa de Ahorro y Crédito Universitaria Limitada los siguientes bienes y servicios tecnológicos:

- FBS 2.0 Basic Edition

    - Licencia de Uso Ilimitado módulos básicos, de negocio y de cumplimiento
    - Licencia de Uso Ilimitado módulos adicionales que la Cooperativa escoja

- Servicios de Adaptación, Implantación, Estabilización y Puesta en producción de la solución ofertada

4.7.3.2.1.2.1.3 FBS 2.0 Basic Edition - Aspectos Tecnológicos

4.7.3.2.1.2.1.3.1 Tecnologías Utilizadas, Arquitectura y Base de Datos

A continuación mostramos todas las Tecnologías Utilizadas, Arquitectura y Base de Datos a las que se puede acoplar el Sistema que proponemos implantar como es el FINANCIAL BUSINESS SYSTEM 2.0 BASIC EDITION.

Tecnologías Utilizadas.

Desarrollo:

Microsoft Visual Studio 2010

Silverlight

Microsoft Expression

Windows Presentation Foundation

Windows Communication Foundation

Enterprise Libra

Arquitectura

SOA

Web Services

Smart Client

Base de Datos

Oracle 10g / 11g

SQL Server 2005 / 2008

IBM DB2

Sybase

Informix

Figura 38: Gráficos de Tecnologías, Arquitectura y Base de Datos

Características Tecnológicas Relevantes

- ✓ Desarrollado en Visual Studio .NET 2010, la más moderna herramienta de desarrollo liberada por Microsoft
- ✓ Sistema Multi-capas, garantizando una total escalabilidad.
- ✓ Código Fuente C# (Sharp), el lenguaje de desarrollo de mayor difusión y versatilidad en la actualidad.
- ✓ Multi – Plataforma Base De Datos, Oracle 10g / 11g, SQL Server 2008 / 2012, IBM DB2, IBM Informix, Sybase.
- ✓ Arquitectura Orientada a Servicios (SOA), alta cohesión, escalabilidad y acoplamiento.
- ✓ Tecnología Smart Client, Front End Windows (Interacción con el Usuario de Gran Calidad) y Back End basado en Web Services XML (Máximo Rendimiento y Escalabilidad)
- ✓ Fácil Integración con tecnologías y canales de acceso de terceros
- ✓ Encriptamiento y Compresión de mensajes proporcionando total seguridad y alto rendimiento.
- ✓ Estaciones de Trabajo Windows XP, 2000, Vista, 7, 8.
- ✓ Autogeneración de código, simplificando el trabajo de los desarrolladores y minimizando los errores de sintaxis y estandarización.
- ✓ Entrega de programas fuentes y capacitación técnica para su uso

Arquitectura Orientada a Servicios (SOA), infraestructura de alto nivel basada en *best practices* y patrones para crear soluciones basadas en servicios, de alta cohesión y bajo acoplamiento.

El concepto de orientación a servicios representa a nivel global lo último en cuanto a Arquitectura de Sistemas se refiere, deja atrás el uso de páginas web para sistemas con altos requerimientos de operatividad, rendimiento y transaccionalidad. Si bien la orientación a servicios se basa en el uso de las comunicaciones vía Internet, mejora ostensiblemente el rendimiento de las aplicaciones y sobre todo la concepción escalable y modular de sistemas.

Figura 39: Estructura y Procesamiento
Fuente: Financial Business System 2.0 Basic Edition

Tecnología Smart Client, proporciona al usuario un interfaz Rica para acceder a un sistema basado en servicios web, pero que mantiene las ventajas de los clientes web tradicionales, como la ausencia de instalación en la máquina cliente, el funcionamiento a través de Internet y la actualización automática.

Figura 40: Interfaz y Ejecución
Fuente: Financial Business System 2.0 Basic Edition

Sistema Multi-capas, Financial 2.0 está diseñado en una arquitectura con tecnología abierta, formada por múltiples capas lógicas e independientes entre sí, esto permite tener una arquitectura completamente versátil sobre la cual se puede incluir en cualquier momento sistemas avanzados de ejecución entre capas, como por ejemplo: sistemas de lectura y reconocimiento de huellas dactilares, sistemas de seguridad, capas de filtrado de información, acceso a bases de datos distribuidas, etc.

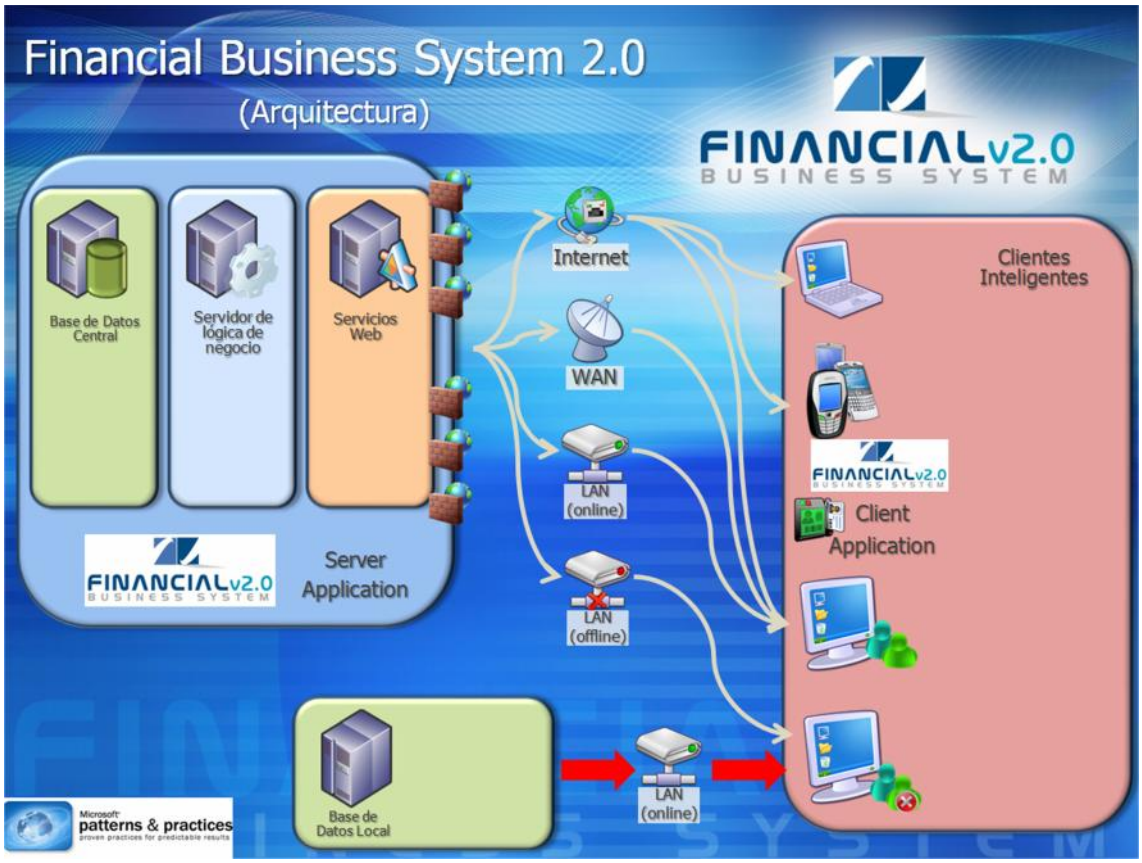


Figura 41: Arquitectura
Fuente: Financial Business System 2.0 Basic Edition

Herramientas de última tecnología, Financial 2.0 está desarrollado completamente con herramientas de última tecnología, cuidando siempre que la aplicación se mantenga actualizada en cuanto a las mejoras que las versiones de cada herramienta de desarrollo utilizada presenta con el tiempo, es así como FBS 2.0 en el tiempo de vida que tiene ha sido adecuado y compilado en 3 del versiones del kit de desarrollo (Visual Studio 2005; Visual Studio 2008 y Visual Studio 2010). Esta vigencia y actualización tecnológica permite que Financial se conecte con cualquier Base de Datos existente en el mercado y haga uso de todos los canales de atención y comunicación modernos.

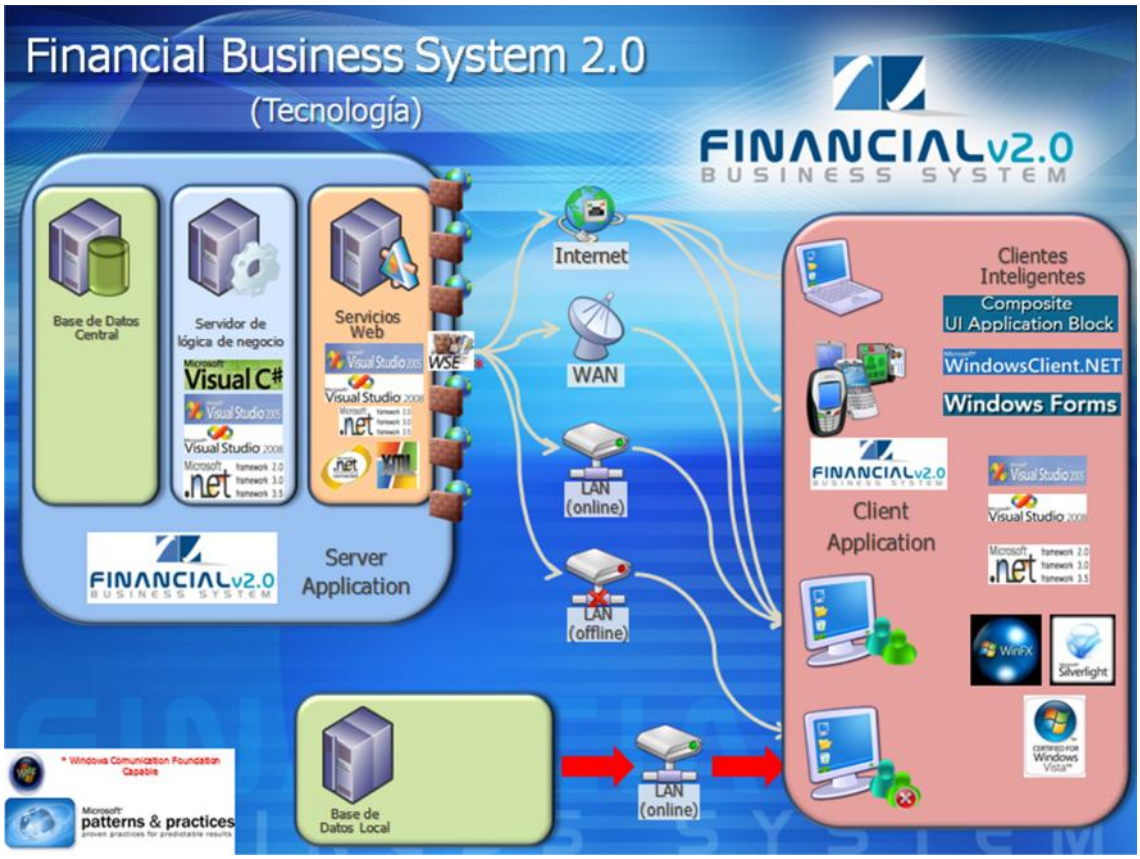


Figura 42: Tecnología
Fuente: Financial Business System 2.0 Basic Edition

Características Funcionales Relevantes

- ✓ Sistema Centralizado altamente transaccional, cuyo núcleo principal es el Cliente
- ✓ Sistema completamente modular con total integración entre módulos mediante Servicios Web
- ✓ Multi-Empresa
- ✓ Multi-Moneda
- ✓ Contabilidad Integrada y completamente automática
- ✓ Workflow integrado
- ✓ Seguridad Propia Basada en Usuarios, Roles y Accesos
- ✓ Almacenamiento integral de pistas de Auditoria
- ✓ Completamente Paramétrico
- ✓ Reportes exportables a diferentes formatos: Excel, pdf, etc.
- ✓ Crecimiento ilimitado
- ✓ Licenciamiento de uso ilimitado

Figura 43: Estructura General de Módulos
Fuente: Financial Business System 2.0 Basic Edition

4.7.3.2.1.2.1.3.2 Módulos Propuestos - Descripción y Características

La solución **FINANCIAL Basic Edition** para esta oferta, se compone de los siguientes módulos:

Módulos Básicos

a. FBS Seguridad

Provee la seguridad propia de Financial 2.0 para evitar accesos no formales a la aplicación, es importante señalar que la autenticación de ingreso se la hace tanto a las Funcionalidades del Front End como a los Servicios Web del Servidor, obteniendo un esquema de seguridad completo, robusto y confiable.

- Roles y Perfiles
- Accesos por menús y funcionalidades.
- Asignación de usuarios a oficinas
- Manejo de claves de acuerdo a los requerimientos de la SBS - SEPS.
- FINANCIAL se basa en un modelo de Funcionalidades, Roles y Usuarios, en donde se crean Funcionalidades de acuerdo a las aplicaciones que Financial 2.0 implementa, se asignan estas Funcionalidades para su acceso a los Roles existentes y se establecen los Usuarios que pertenecen a cada Rol.

b. FBS Administración

FINANCIAL mantiene en su estructura un conjunto de opciones de usuario que permiten parametrizar y configurar las diferentes opciones que el sistema presenta, FBS Administración se encarga de gestionar dichas actividades en una interfaz amigable e intuitiva para facilidad de uso de los usuarios con los accesos correspondientes.

c. FBS Contabilidad

La consolidación contable de las operaciones realizadas por los módulos de negocio de Financial 2.0 está a cargo de Financial/Contabilidad. Para que esto sea posible todas las operaciones de negocio generan la información necesaria para que en un momento determinado Financial/Contabilidad realice las Contabilizaciones en lote o en línea que permitan obtener los resultados del periodo de operaciones, es importante señalar que todas las operaciones financieras generan su registro contable automáticamente, por lo que el ingreso de comprobantes contables de manera manual está reservado para operaciones excepcionales que no pueden ser generadas automáticamente o que no están soportadas por los módulos adquiridos por la Cooperativa.

FBSl/Contabilidad entre su Funcionalidad principal presenta:

- Administración: Plan de cuentas paramétrico (cuentas y auxiliares), causales, condiciones de transferencia entre oficinas, perfiles contables de transacciones.
- Contabilización Automática de todas las operaciones financieras
- Tipos de comprobantes paramétricos
- Perfiles contables por transacción o grupo de transacciones
- Comprobantes Manuales con afectación a anexo transaccional (SRI) y workflow
- Impresión de documentos de comprobantes de egreso: cheques, etc.
- Impresión de documentos de comprobantes de egreso: cheques, etc.
- Emisión de Libros Diarios, Mayores, Balances y Estados Financieros
- Conciliación Bancaria automática y manual
- Procesos de generación de comprobantes automáticos, Mayorización y Cierre independientes de fecha sistema (financiera)

d. FBS Personas – Clientes

Financial 2.0 basa su operación en el Cliente como entidad fundamental de ejecución; De esto se ocupa FINANCIAL/Clientes la aplicación que otorga la Funcionalidad para la administración óptima de información de personas y clientes, entre sus principales habilidades tenemos:

- Personas - Ingreso y Mantenimiento
- Clientes - Ingreso y Mantenimiento
- Cambio de Oficina
- Cambio de Identificación y Tipo de Identificación
- Bitácora de Comentarios de Clientes

Módulos de Negocio

e. FBS Cajas

La Funcionalidad de Financial 2.0 garantiza la rápida, confiable y segura operación de Transacciones. Financial/Transacciones es el subsistema de Gestión de Operaciones, tanto de Caja como Internas, que permite realizar estas operaciones, considerando que el ingreso y recepción de valores son parte fundamental del Negocio Financiero este módulo se encarga de almacenar toda la información necesaria para que cada una de las acciones que realicen los Usuarios asignados a este tipo de operaciones sean ejecutadas de la manera correcta y permita realizar un análisis exhaustivo en lo posterior, Dentro de la Funcionalidad que Financial/Transacciones maneja tenemos:

- Administración de Bóvedas y movimientos de fondeo
- Administración de Ventanillas y movimientos de dotación
- Transacciones de Caja (Efectivo)
- Transacciones Internas (entre productos y con causales)
- Manejo de denominación en bóvedas y ventanillas
- Impresión de recibos, certificaciones de papeletas y/o libretas
- Cuadres de Ventanilla en totales y denominaciones en cualquier momento
- Cierres Temporales
- Reapertura de cajas
- Cierres de caja
- Reversos con niveles de aprobación

- Órdenes de Pago o Ingreso

f. FBS Captaciones Plazo Fijo

Gestiona la captación de dinero a plazo fijo, permitiendo las múltiples variantes que el manejo de Certificados de Depósito o Depósitos a Plazo Fijo presentan. Captaciones en efectivo, cheque, valores depositados en cuenta y cualquier otro que se pueda presentar son solventemente manejados en una misma operación lo que permiten agilidad en los procesos y satisfacción de las necesidades del cliente.

Dentro de las principales Funcionalidades de Financial/DPFs tenemos:

- Completamente Parametrizable: Multi-producto, Multi-moneda, Multi-componente
- Creación de Depósitos a Plazo Fijo, con orígenes de recursos distintos: Cuenta, Causal, Efectivo
- Certificados Provisionales y Definitivos
- Multi-Titulares y Multi-beneficiarios
- Reimpresión de Certificados
- Pre-cancelaciones anticipadas (con o sin castigo de tasa)
- Formas de Pago configurables: cuenta, caja, renovación.
- Pago de intereses: al inicio, periódicos o al final.
- Anulaciones y Reversos
- Transferencia / Cesión de Depósitos a Plazo Fijo
- Cancelación de Depósitos a Plazo Fijo
- Renovación de Depósitos a Plazo Fijo
- Generación e impresión de retenciones (rendimientos financieros)
- Intereses y Provisiones

g. FBS Captaciones Vista - Cuentas de Ahorros

Suministra una plataforma versátil y flexible para el manejo de las operaciones de los Productos o Servicios Financieros de Captaciones a la Vista, permitiendo la creación de productos de acuerdo a las características del negocio, necesidades de los clientes y el mercado objetivo hacia donde se orientan los mismos.

Su diseño permite el manejo de cuentas de ahorro, aportaciones de socios, ahorros programados, fondos acumulativos, etc. Y proporciona planes flexibles para cálculo,

acumulación y acreditación de intereses. Sus principales características se detallan a continuación:

- Completamente Parametrizable: Multi-producto, Multi-componente
- Creación de Cuentas
- Cuentas Conjuntas e Indistintas
- Cuentas con múltiples registros de firmas
- Manejo de Bloqueos / Des-bloqueos: automáticos, manuales en demanda y contratados
- Manejo de Encajes
- Remesas y Depósitos en Tránsito
- Control de rutas banco - oficina digitales para efectivización automática de cheques
- Acreditación Manual y Protesto de Cheques
- Cierre de Cuentas
- Activación de Cuentas
- Posteo de libretas
- Intereses y Provisiones automáticos
- Movimientos en Lote: Manuales y Con Archivo formateado

h. FBS Crédito - FBS Cartera – FBS Cobranzas

Financial 2.0 presenta una poderosa herramienta para la administración del proceso crediticio de una institución financiera, Financial/Préstamos se subdivide en tres sub-aplicaciones: Crédito, Cartera y Cobranzas, lo que permite hacer un seguimiento exhaustivo de una operación crediticia desde que el cliente se acerca a solicitarla hasta cuando termina su pago.

Módulo de Crédito

- Completamente Parametrizable: Multi-producto, Multi-Segmento, Multi-componente, Parámetros BCE
- Workflow de Solicitudes configurable, almacenamiento de ruta digital
- Solicitudes de Crédito personal o empresarial
- Parámetros de Solicitud: Cliente (s), Producto, Tipo de Préstamo, Segmento Interno (Destino + Calificación Contable), Sub-calificación Contable (BCE), Tipo de Tabla de pagos, monto, plazo (número de cuotas y frecuencia), día de pago, datos BCE, garantías personales, garantías hipotecarias, garantías prendarias, componentes manuales, encajes.

- Control de tasas nominales o efectivas
- Scoring de Crédito Configurable y Paramétrico: Multi-plantilla, Multi-Categoría, Multi-Ítem, Ítems con calificación manual y automática.
- Desembolso automático a las Cuentas
- Impresión integral de documentación desde el sistema: solicitudes, pagarés, anexo 2, autorizaciones, tablas, liquidaciones, scoring, etc.
- Tablas presuntivas
- Administración de Garantías: Personales, Hipotecarias, Prendarias

Módulo de Cartera

- Consultas y Administración de Préstamos
- Consultas de Encajes
- Consultas de Garantías: Personales, Hipotecarias, Prendarias,
- Consultas de Movimientos
- Consultas de Tablas de Amortización y Rubros por pagar
- Reimpresión de documentos
- Clasificación y Devengado automáticos
- Calificación de Riesgo Automática
- Ingreso/Mantenimiento de Rubros Manuales
- Préstamos Vinculados
- Reportes Especializados para seguimiento y control: vencimientos, próximos vencimientos, morosidad, adjudicaciones, estado de cartera, cancelaciones, recuperación, clasificación y devengado

Módulo de Cobranzas

- Préstamos Judiciales
  - ✓ Asignación de abogados y porcentajes de honorarios
  - ✓ Generación de valores en línea para pago de abogados
- Prestamos Castigados
- Generación de Notificaciones
- Reportes Especializados para cobranzas: cuadros de morosidad ampliados, cumplimiento de compromisos, gestiones por oficial, próximos vencimientos ampliado, etc.

Módulos de Cumplimiento (Obligatorio)

i. FBS Estructuras Organismos de Control

- SBS – SEPS
- SRI
- BCE.

- COSEDE.
- UIF.

Otros Módulos Adicionales Disponibles

j. FBS Activos Fijos

- Mantenimiento de Activos
- Depreciación en línea recta
- Reportes y consultas
- Traslado de activos
- Contabilización automática.

k. FBS Control Presupuestario

- Ingreso y Mantenimiento de Registros de Presupuestos
- Control presupuestario
- Reportes y consultas

l. FBS Lavado de Activos

Es exigencia de la Unidad de Inteligencia Financiera Ecuatoriana el prevenir, detectar, sancionar y erradicar el Lavado de activos en todas sus formas, en este aspecto las Instituciones Financieras juegan un papel determinante y es así como existen requerimientos explícitos y de alta exigencia para el cumplimiento de incorporación de un sistema de control de lavado de activos, FBS Lavado de Activos es el módulo que le permitirá a la Institución detectar y gestionar de manera eficiente posibles intentos o incidencias de lavado de activos dentro de su cartera de clientes.

Las principales características de este módulo son:

- Completamente configurable
- Administración de Perfiles de Clientes
  - ✓ Tipo de cliente
  - ✓ Actividad Económica
  - ✓ Profesión
  - ✓ Edad
  - ✓ Ubicación Geográfica
  - ✓ Oficina
  - ✓ Productos asignados
  - ✓ Servicios utilizados

- Segmentación del Mercado de perfil de lavado de activos por cliente, oficina y consolidado
- Control de umbral por transacción o grupo de ellas, de manera que se puedan determinar umbrales individuales y que trabajen por separado para organismos de control y control interno
- Interacción automática y en línea con la base de datos transaccional del core para una gestión adecuada, dinámica y alineada con las políticas de riesgos
- Control y auditoria de acceso de usuarios a la información del módulo de lavado de activos sustentada en el módulo de FBS Seguridad
  - ✓ Reportes para el organismo de control (UIF):
  - ✓ Reporte de operaciones y transacciones económicas inusuales e injustificadas
  - ✓ Reporte de no existencia de operaciones y transacciones económicas inusuales e injustificadas
  - ✓ Reporte de tentativa de operaciones y transacciones económicas inusuales e injustificadas
  - ✓ Reporte de operaciones y transacciones que igualen o superen el umbral individuales y múltiples
  - ✓ Reporte de no existencia de operaciones y transacciones que igualen o superen el umbral
- Reportes y Consultas:
  - ✓ Perfil de cliente
  - ✓ Operaciones de cliente
  - ✓ Alertas: consolidado, oficina, usuario y cliente
  - ✓ Gráficos Estadísticos de alertas, por: cliente, usuario, oficina y consolidado
  - ✓ Información completamente extraíble a Excel y pdf

m. FBS Nómina – RRHH

FBS Nomina es la aplicación que gestiona de extremo a extremo el recurso humano de la Institución Financiera, ocupándose de los procesos de Enrolamiento, Recursos Humanos, Talento Humano, Control Horario y Rol de Pagos. Esta aplicación integral permite mantener un adecuado registro de todas las operaciones que realizan los colaboradores de la Institución incluso interconectándose con módulos de negocio: Contabilidad, Captaciones a la Vista, etc.

- Administración de empleados
- Ingreso / Mantenimiento
  - ✓ Datos generales
  - ✓ Instrucción formal
  - ✓ Capacitación

  - ✓ Cargas familiares
  - ✓ Horarios
  - ✓ Sueldo, cargos y descuentos (multi-componente)
  - ✓ Baja de empleados
- Control horario
  - ✓ Registro de entrada
    - ID / Clave
    - Huella Digital (módulo adicional requerido)
  - ✓ Registro de receso y almuerzos
  - ✓ Registro de salidas
- Gestión de permisos
  - ✓ Asignación
  - ✓ Aprobación
  - ✓ Registro
- Acciones de personal (vacaciones, reemplazos, ajuste de sueldos, subrogaciones, etc.)
  - ✓ Ingreso
  - ✓ Aprobación
  - ✓ Activación y desactivación automática
- Rol de pagos
  - ✓ Multi-Rol
  - ✓ Rol Masivo Previo -> Definitivo
  - ✓ Rol individual
  - ✓ Acreditaciones a cuentas de ahorros en Lote
- Talento Humano
- Contabilizaciones automáticas
- Reportes Operativos y de control

n. FBS Presupuestos Proyectados

- Generación de Presupuestos estadísticos
- Manejo de Varios Presupuestos
- Reportes y Consultas
- Conectividad con Módulos de Control Presupuestario

o. FBS Obligaciones Financieras

- Multi-Producto, Multi-Moneda, Multi-Componente
- Parametrizaciones: Fondeadores, Líneas de Crédito, Tasas Base, Tasas de Cambio, etc.
- Ingreso de Obligaciones Financieras: Datos Generales del Crédito, Generación Automática
- Carga de Tablas de amortización desde Archivo, Manejo de tasas base y diferenciales.

- Pagos de obligaciones financieras.
- Modificación de tablas de amortización manual o con subida de archivo.
- Contabilizaciones automáticas: Provisiones, Maduración en base a rangos de tiempo, pagos.
- Reportes operativos y de gestión

p. FBS Huellas Dactilares

El tema de seguridad ha tomado especial preponderancia en todos los procesos de automatización y con mayor razón incluso dentro de la actividad financiera, el poder asegurarse que quien realiza las operaciones es siempre el cliente es un reto para la mayoría de áreas de operaciones y control. FBS Huellas Dactilares asegura que las operaciones con clientes y usuarios se realicen con total seguridad garantizándose su presencia por medio del uso del control biométrico de su huella digital

- Totalmente integrado, control biométrico de acceso de huella digital de usuarios o clientes en:
  - ✓ Transacciones
  - ✓ Procesos
  - ✓ Ingreso / Salida de usuarios
- Multi – Huella por cliente / usuario
- Altas, Bajas, Cambios

q. FBS Riesgo de Liquidez y Mercado

Permite el análisis, control y administración de los riesgos de liquidez, tasa de interés y tipo de cambio, de tal forma que el proceso de toma de decisiones en la Institución cuente con el soporte necesario de la información, organizada en modelos especializados que facilitarán su análisis y utilización. Las principales características de este módulo son:

- Completamente parametrizable
- Basado en un modelo estadístico / matemático desarrollado para el mercado financiero regional y contemplando la normativa actual
- Escenarios:
  - ✓ Contractual.- se basa en los vencimientos ciertos de las operaciones expresados en sus documentos o contratos
  - ✓ Esperado.- escenario contractual afectado por parámetros reales tales como morosidad histórica, renovaciones, pre-cancelaciones, etc.

  - ✓ Dinámico.- ajustando por tasas de crecimiento, presupuestos y supuestos.
- Distribución de activos y pasivos en bandas de tiempo tipo de producto y vencimiento
- Cálculo de la volatilidad
- Cálculo de la brecha marginal y la brecha de liquidez acumulada
- Incluye metodología estadística para la distribución de productos de vencimiento incierto
- Generación de escenarios contractuales, esperados, y dinámicos de liquidez
- Cálculo de Valor Presente y Duración a nivel de flujos individuales
- Cálculo de Valor Patrimonial en Riesgo y Margen Financiero en Riesgo
- Reportes para organismos de control: R36, R41, R42, R45

r. FBS Interfaz con Cajeros Automáticos (ATM's) y Ventanillas Compartidas

El uso de medios electrónicos que resultaba en épocas anteriores un factor diferenciador entre las Instituciones financieras, en la actualidad se ha convertido en un requisito indispensable para la atención a los socios y clientes. La conexión con las diversas redes de ATM's del país es imprescindible para captar y mantener adecuados estándares de atención y servicio.

- Web services de conexión con las principales redes de cajeros del país (Coonecta, Multiservices, Banco del Austro, Banco Internacional, MegaRed, BanRed etc.)
- Seguridad integrada con autentificación de usuario para conexión diferenciada entre cajeros propios y de la red
- Log de transacciones
- Capacidad funcional para las siguientes transacciones:
  - ✓ Retiros
  - ✓ Consultas de Saldos
  - ✓ Reversos
- Manejo de códigos de error y ejecución de operaciones derivadas de dichos códigos
- Registro y contabilización automática de transacciones de ATM
- Reportes de cuadres y afectaciones contables por movimientos
- Reposición de fondo de dinero
- Conciliación automática de mallas

s. FBS Adición de Componentes (Add-in EXCEL)

La tecnología smart client proporciona la facilidad para integrar a FBS 2.0 con utilitarios de diversa índole, dentro de ellos al que se le da más uso desde la parte administrativa financiera es Microsoft Excel, FBS 2.0 presenta un Add-in que será el aliado ideal para el proceso de toma de decisiones, con la posibilidad de extraer datos directamente desde la Base de Datos a cualquier hoja de cálculo (en EXCEL) mediante el uso de fórmulas el usuario de este utilitario podrá combinar todo tipo de información para obtener hojas de cálculo tan especializadas como se requiera:

- Add-in para Excel para la instalación de fórmulas de extracción directa de datos
- Set de fórmulas (20) para uso en Excel
- Visualización de información en línea
- Actualización de información cada vez que se abra el archivo de Excel o se ejecute la fórmula
- Total seguridad

t. FBS E-Banking - Banca Móvil

Comprende aquellas herramientas que se pueden ofrecer a los clientes de la Institución de manera que sea posible realizar sus operaciones bancarias a través de un computador utilizando una conexión a la red Internet. La banca por Internet es un nuevo tipo de sistema de información que utiliza los recursos de Internet y la World Wide Web (WWW) para permitir a los consumidores efectuar operaciones financieras en el espacio virtual con total seguridad y eficiencia.

- Transaccionalidad en línea, en donde los movimientos realizados en la banca virtual se reflejan inmediatamente para todos los usuarios internos y/o externos
- Capacidad funcional para las siguientes transacciones:
  - ✓ Consultas de saldos y estados de cuentas de ahorros
  - ✓ Consultas de movimientos de cuentas de ahorro
  - ✓ Transferencias entre cuentas de ahorros de la Institución.
  - ✓ Pago de préstamos con débito a cuentas de ahorros propias de la Institución.
  - ✓ Asignación y Administración de pines y claves de seguridad
- Afectación en línea de operaciones

- Contabilización automática y en línea de operaciones

u. FBS ORM / Riesgo Operativo / Seguimiento

FBS-ORM / Riesgo Operativo constituye la aplicación para la administración, control y gestión de eventos de riesgo operativo, integrado con FBS-ORM / Seguimiento complementa su trabajo con un administrador de proyectos tendientes a la reducción de la incidencia de los eventos de riesgo operativo detectados. De esta manera la institución puede mantener una Base de Datos de los proyectos emprendidos y el seguimiento de las tareas que de cada uno de ellos se desprendan

- Parámetros de Administración de Riesgo: Tipos de Procesos, Impacto, Probabilidad, Definición de tamaño y características de la matriz de riesgo, Zonas de Riesgo, Niveles de Riesgo, Tipos de Evento, Respuesta, Tipos de Análisis de Eventos, Tipos de Control, Frecuencia de Control, Categorías de Control, Tiempo de implantación de controles, Tiempo de ejecutantes de controles, Tiempo de ejecutantes de actividades, Tipos de incidentes, Campos Adicionales que se definen en forma automática para ser solicitados en la creación de un evento sea descriptivo o tabular, Efectividad del Control, Tipo de Ejecución, Efectividad de Diseño, Tipo de Objetivos, Indicadores de Riesgo: Factor, Unidad de Tiempo, Unidad de medida, Calificación del Indicador
- Parámetros de Seguimiento: Tipo de Entregables asociados a la Tarea, Tipo de Ejecutantes asociados a la Tarea, Tipo de Riesgo, Periodicidad
- Entre las principales habilidades de FBS-ORM/Riesgo Operativo tenemos:

Creación/Mantenimiento de Macro-Procesos – Líneas de Negocio

Creación/Mantenimiento de Procesos por Líneas de Negocio (Macro-Procesos)

Tipo de Proceso (Configurables).

Procesos Críticos.

Asignación de Procesos a Usuarios y Entidades Externas (Clientes Externos).

Base de Datos de Objetivos de Proceso.

Subprocesos

Afectación Organizacional

Almacenamiento (Histórico) de Análisis de Eventos de Riesgo.

Tipos de Análisis (Configurables): Inherente, Residual, etc.

Ubicación en Zonas de Riesgo dependiendo de su Probabilidad e Impacto, con identificación visual de colores.

Respuestas al Riesgo (Configurables): Aceptar, Compartir, Evitar, Transferir, etc.

Posibilidad de que varios usuarios puedan emitir su criterio de análisis (ubicación en la matriz de riesgo del evento), lo que le permite al sistema hacer un análisis combinatorio en base a pesos de estos criterios y emitir un análisis sugerido en la matriz de riesgos.

Ingreso/Mantenimiento de Controles existentes por Evento de Riesgo.

Categorías de Control (Configurables): Interna, Externa, etc.

Tipos de Control (Configurables): Preventivo, Correctivo, etc.

Frecuencias de Control (Configurables): Diaria, Mensual, etc.

Tipos de Implementación de Control (Configurables): Implementado, No Implementado, Parcialmente Implementado, etc.

Identificación de Controles Manuales y Automáticos.

Identificación de Controles Documentados y No Documentados.

Identificación de Controles con Diseño Deficiente.

Identificación de Usuarios y Entidades Externas (Clientes Externos) asociados al control.

Cálculo de exposición: evaluación periódica de los riesgos y los controles utilizados para mitigarlos a fin de calcular el riesgo residual

Informes de registro del riesgo: describen los riesgos y los controles para los gestores del riesgo de forma proactiva y en tiempo real

Ingreso/Mantenimiento de Actividades para Implementación, Mejora o Reemplazo de Controles no Efectivos.

Asociación de actividades a proyectos del módulo de Seguimiento (FBS-ORM/Seguimiento) lo que nos permite efectuar un análisis del progreso de la implementación de la actividad basándonos en el progreso del proyecto vinculado a la misma.

Base de Datos de Indicadores de Gestión.

Indicadores de Probabilidad e Impacto.

Indicadores de diferente naturaleza

Unidades de medida paramétricas: eventos por mes, dólares por año, promedio de eventos por semana, etc.

Ingreso de valores de Indicadores manual o captura automática del valor por fecha desde otro sistema mediante la exposición de estos valores en un Servicio Web.

Mantenimiento del Histórico de Indicadores con la posibilidad de definir rangos de alerta para mostrar el comportamiento de un indicador en el trascurso del tiempo.

Asignación de Indicadores de Impacto y Probabilidad a un Evento de Riesgo lo que posibilita la definición cuantitativa de la ubicación en la Matriz de Riesgo de acuerdo al comportamiento histórico de los Indicadores asociados.

Reportes:

Matrices de riesgo muti-filtro

Matrices de priorización de riesgos

Árbol de procesos

Pre-eventos

- Entre las principales habilidades de FBS-ORM/Seguimiento tenemos: Creación de Proyectos Asignación de Responsables a Proyectos Creación/Mantenimiento de Tareas del Proyecto. Fecha Inicio. Fecha Fin. Porcentajes de Proyecto y de Cumplimientos. Usuarios Asignados. Porcentajes de Tarea y Cumplimiento. Clientes Externos Asignados. Porcentajes de Tarea y Cumplimiento. Carga y Visualización de Archivos entregables de Tarea:

Diagrama de interacción de módulos

Todos los módulos en Financial que se comunican entre sí lo hacen a través de Servicios Web, es más cada módulo representa física y lógicamente una carpeta virtual de un sitio web, dentro de la misma se encuentra un servicio web por cada entidad de negocio que está presto a atender las solicitudes de otros servicios web de su mismo módulo, de otro módulo o de una aplicación cliente. Siempre conservando los principios de seguridad, encriptamiento y compresión configurados.

Por diseño los módulos de Financial mantienen las siguientes líneas de comunicación:

Figura 44: Línea de Comunicación de los Módulos
Fuente: Financial Business System 2.0 Basic Edition

Características de infraestructura tecnológica

Servidores requeridos con características recomendadas

Evaluando el tamaño actual de la Cooperativa y sus proyecciones normales de crecimiento en los próximos años consideramos que las características mínimas del equipo servidor de aplicación requerido son: Doble Procesador Xeon, 6 GB en RAM, Disco Duro de 120 Gb.

Sistemas operativos recomendados

Servidor de Aplicaciones: Windows Server 2003 / 2008

Servidor de Base de Datos: Windows, Linux o el que la Institución determine dependiendo de su motor de base de datos requiera.

Características mínimas de las estaciones de trabajo recomendadas

Las características mínimas de los equipos clientes de aplicación requeridas son: Procesador Pentium IV, 256 Mb en RAM, Disco Duro de 16 Gb.

4.7.3.2.1.2.1.3.3 Costos, Plazos y Forma de Pago

Costos

Los costos de los bienes y servicios detallados se expresan en el siguiente cuadro:

Módulos Básicos y De Negocio y opcionales solicitados

ÍTEM	VALOR (USD)
Licencia de Uso Ilimitado Módulos Básicos y de Negocio FBS Seguridad FBS Administración FBS Contabilidad FBS Personas – Clientes FBS Cajas FBS Captaciones Plazo Fijo FBS Captaciones Vista - Cuentas de Ahorros	**40.000,00**

FBS Crédito - FBS Cartera – FBS Cobranzas FBS Estructuras Organismos de Control	
Servicios de Adaptación, Implantación , Estabilización, Migración de datos y Puesta en producción Módulos Básicos y de Negocio (6 meses)	**15.000,00**
TOTAL (Módulos Básicos y de Negocio)	**55.000,00**

Tabla 38: Costo del Sistema y los Módulos que consta
Fuente: Financial Business System 2.0 Basic Edition

Es importante entender que la Cooperativa se encuentra en un proceso de franco crecimiento y sobre todo que con el tiempo el organismo de control va a hacer una serie de ajustes a la Normatividad que rige al mercado de las Instituciones Financieras Populares, por lo tanto las Instituciones deben buscar herramientas PROBADAS que además de cubrir sus necesidades básicas actuales les permitan pensar que en el futuro deberán incrementar estas herramientas para mejorar sus operaciones y cumplir con los estándares que el organismo de control y el mercado exigen, por esta razón ofrecemos además, una serie de módulos adicionales que pueden optar su compra en cualquier momento:

Módulos Opcionales

ÍTEM	VALOR (USD)
FBS Activos Fijos	4.000,00
FBS Control Presupuestario	4.000,00
FBS Lavado de Activos	11.000,00
FBS Obligaciones Financieras	6.000,00
FBS Huellas Dactilares	3.000,00
FBS Riesgo de Liquidez Y Mercado	12.000,00
FBS ATM’s y Ventanillas Compartidas	6.000,00
FBS Adición de Componentes (Add-in EXCEL)	3.000,00
FBS E-Banking - Banca Móvil	9.500,00
FBS Riesgo Operativo / Seguimiento	15.000,00

Tabla 39: Costo de Módulos adicionales del Sistema
Fuente: Financial Business System 2.0 Basic Edition

Programas Fuentes

La Institución además puede optar por la compra del derecho de uso de los programas fuentes de la versión instalada y la capacitación al personal técnico para su mantenimiento (máximo 2 personas), con el siguiente costo:

ITEM	VALOR (USD)
Programas Fuentes y Capacitación Técnica	20.000,00

Tabla 40: Programas Fuentes y Capacitación Técnica
Fuente: Financial Business System 2.0 Basic Edition

Impuestos

Los valores de la presente oferta NO INCLUYEN IVA

Plazos

El plazo de entrega de los bienes, servicios y competencias para la propuesta detallada anteriormente es de 6 meses, lo que incluye los Módulos Básicos, de Negocio y de Cumplimiento ofertados.

Forma de Pago

La forma de pago propuesta es:

El 40% a la firma del contrato y el valor restante en 12 cuotas mensuales equivalentes al 5% del valor del contrato cada una.

De requerir un financiamiento mayor, se incrementará un 10% del valor de la oferta por cada año adicional de plazo o fracción, siendo el máximo plazo posible, 36 meses. El valor adicional se prorrateará al plazo escogido e incrementará cada una de las cuotas proporcionales.

La Empresa dueña del sistema se llama SIFIZSOFT S.A. la cual es muy conocida a nivel nacional e internacional y tienes muchas Cooperativas que han adquirido su

sistema a continuación mostramos una breve historia de la empresa y su Cartera de Clientes.

Historia

SifizSoft S.A. es una empresa ecuatoriana fundada en el 2004, resultado de la fusión de un grupo de especialistas que independientemente ofrecían servicios a Instituciones Financieras del mercado local. Durante los 9 años de existencia de la empresa nos sentimos orgullosos de haber liderado más de 50 proyectos exitosos de instalación de software en Cooperativas, Financieras, Fondos y ONG's dentro y fuera del país obteniendo un amplio acoge por las Cooperativas y que hoy por hoy garantiza resultados óptimos en tiempos inmejorables.

Nuestra Cartera de Clientes en la actualidad comprenden más de 50 instituciones de todo tamaño quienes entre otras son:

Figura 45: Cartera de Clientes que usan este Sistema
Fuente: Financial Business System 2.0 Basic Edition

Instituciones Financieras Controladas (SBS): 13

Cooperativa de Ahorro y Crédito "Jardín Azuayo", Oscus Ltda. (Desarrollo - SifizOS), San Francisco Ltda. (Financial 1.0), Sagrario Ltda. (Financial 2.0), Santa Ana Ltda. (Financial 2.0), Cámara de Comercio de Ambato Ltda. (Financial 1.0), CACPECO Ltda. (Financial 2.0), CTH (Financial 2.0 – instalándose), Vazcorp (Financial 1.0), CODESARROLLO Ltda., 9 DE OCTUBRE Ltda. (Financial 2.0). Cooperativa COMERCIO Ltda. , (Financial 2.0 – en proceso). Andalucía Ltda. (Financial 2.0 – ORM).

Cooperativas No Controladas (SBS): 26

Cacspmec Ltda., Magisterio Manabita Ltda., Marqués de Selva Alegre Ltda., Cacpe Yantzaza Ltda., Cacpe Gualaquiza Ltda., Cacpe Zamora Ltda., Puéllaro Ltda., Nueva Jerusalén Ltda., Unión Popular Ltda., Unión El Ejido Ltda., Cooperare Ltda., Alfonso Jaramillo Ltda., 14 de Marzo Ltda., Ilaló Ltda., La Merced Ltda. Cuenca, Corpucoop Ltda. (en proceso) (Financial 1.0); Lucha Campesina Ltda., Futuro Lamanense Ltda., Cacpe Urocal Ltda., Pedro Moncayo Ltda., La Merced Ltda. Ambato, Visandes Ltda., Cooperart, Cooperarte, Kullki Wasi Ltda., PISA Ltda., COAC CAAP Ltda, (Financial 2.0).

Administradoras de Fondos y ONG's: 13

Asoprep (Financial 1.0), Contactar (Financial 2.0 - Colombia), FODEMI, INSOTEC, Corfocesantía, Fundación Alternativas para el Desarrollo, Vision Fund International (6 Instituciones – 6 Países) (Financial 2.0).

A continuación algunos pantallazos del Sistema

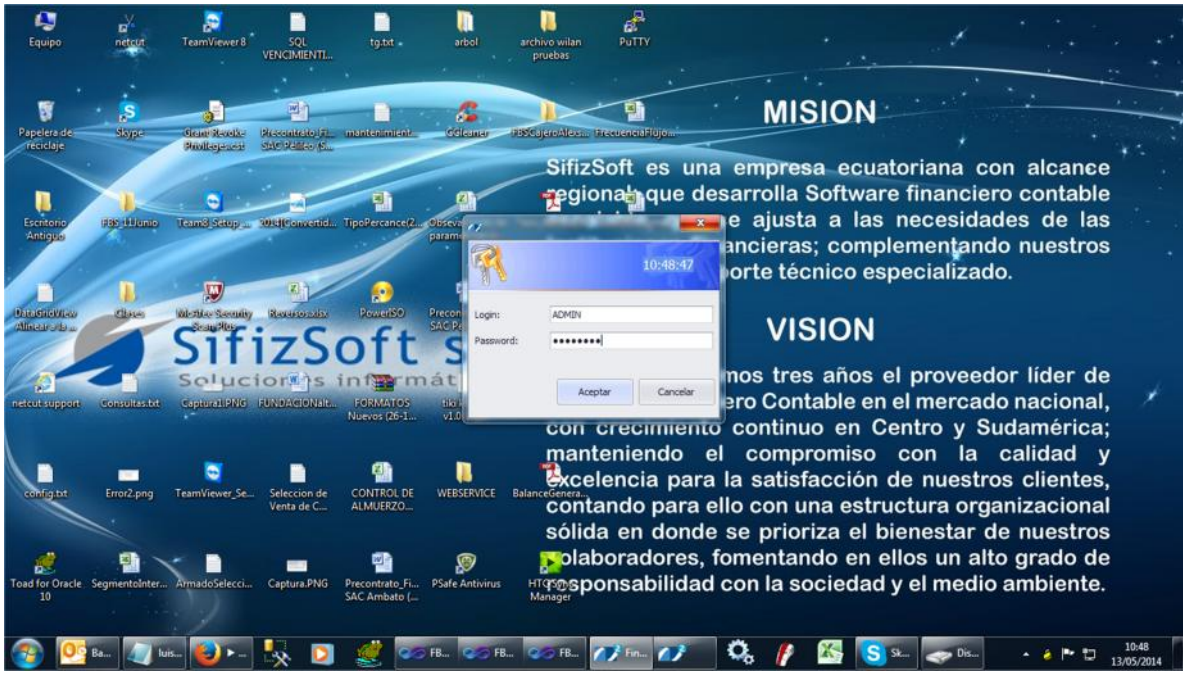


Figura 46: Pantalla Ingreso al Sistema
Fuente: Financial Business System 2.0 Basic Edition

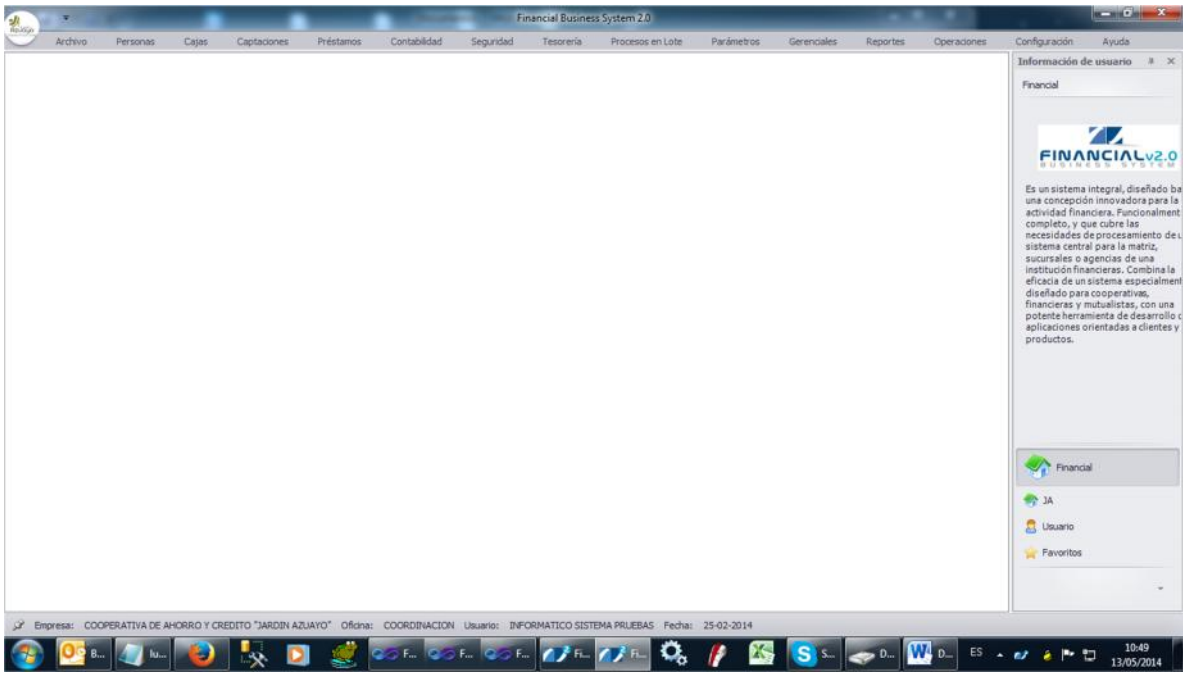


Figura 47: Pantalla General de Ingreso al Sistema
Fuente: Financial Business System 2.0 Basic Edition

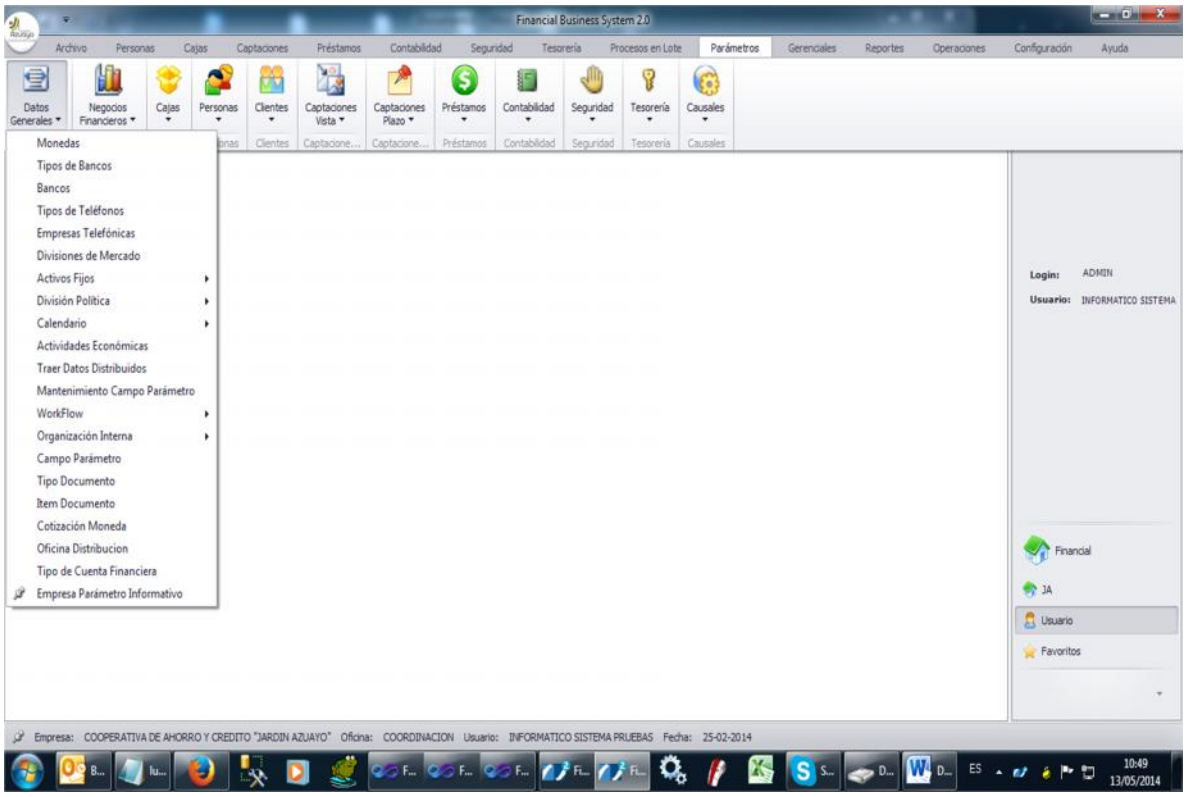


Figura 48: Pantalla Lista de Módulos
Fuente: Financial Business System 2.0 Basic Edition

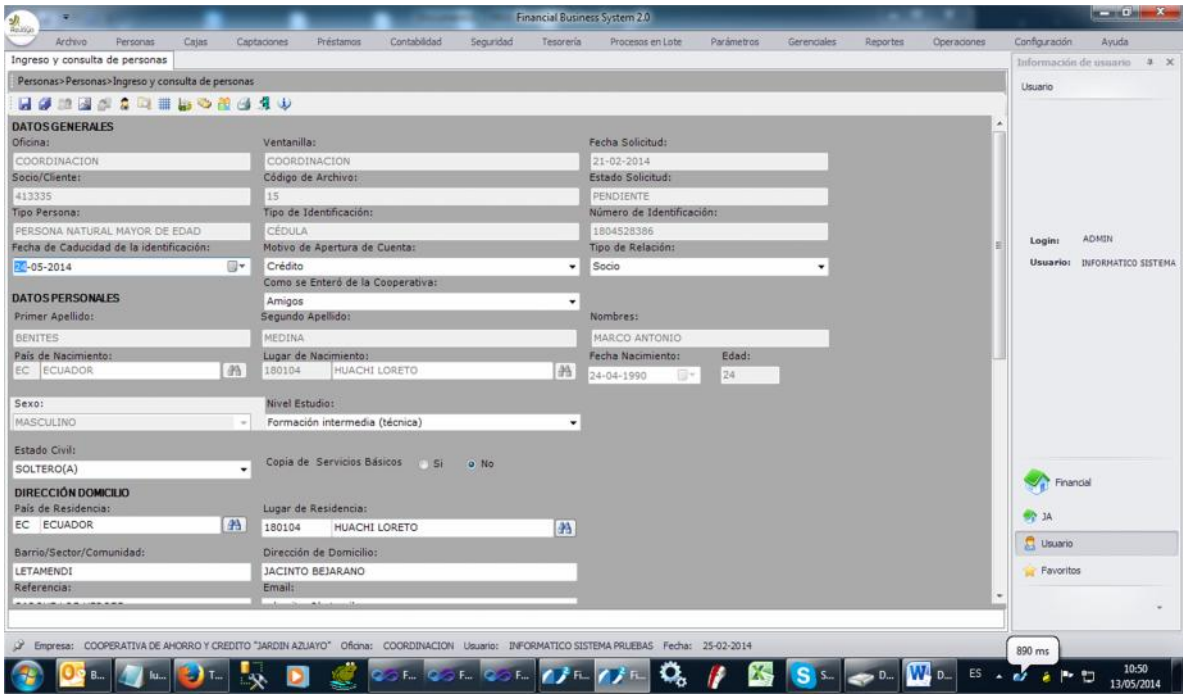


Figura 49: Pantalla Ingreso y Consulta de Personas
Fuente: Financial Business System 2.0 Basic Edition

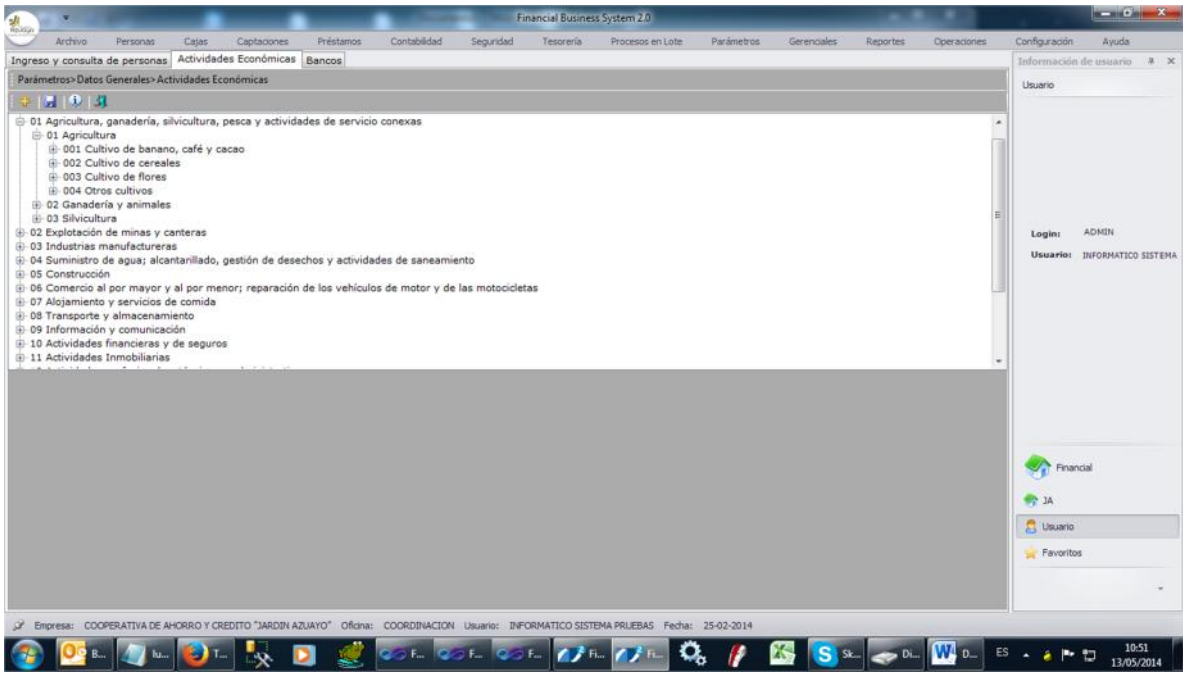


Figura 50: Pantalla Actividades Económicas
Fuente: Financial Business System 2.0 Basic Edition

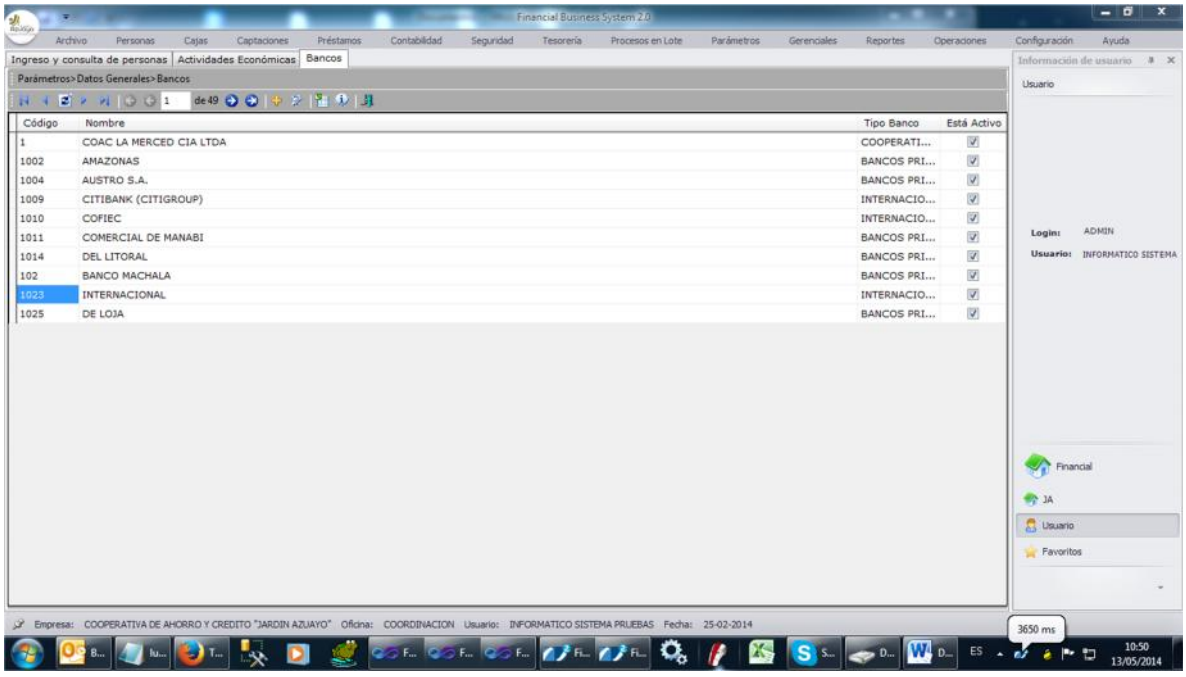


Figura 51: Pantalla Bancos
Fuente: Financial Business System 2.0 Basic Edition

4.7.3.2.1.2.2 Base de Datos

El lugar donde se encuentra el servidor de base de datos no cuenta con una instalación adecuada ya que no han seguido ninguna estándar de seguridad por lo que se puedo observar, así mismo que se encuentra ubicado en una oficina que está a la vista de todos pudiendo cualquier persona manipular el equipo.

Las contraseñas que son empleadas para el uso de los computadores no son secretas cada empleado sabe la contraseña de su compañero existe una amenaza evidente que es la ingeniería social pudiendo afectar el trabajo de su compañero. Lo ideal sería que las contraseñas fueran secretas o que tuvieran que ser cambiadas dentro de un periodo determinado.

4.7.3.2.1.2.3 Antivirus

En cuanto a la actualización antivirus tienen serios problemas porque algunos equipos no tienen acceso a internet, los mismos que se ve afectado y desprotegidos. Asimismo pasa con los equipos que si tienen acceso a internet ya que el antivirus ya caduco. Lo correcto sería que cada cierto tiempo existe un mantenimiento del Antivirus y no esperar que el equipo deje de funcionar o que peor aún la información se pierda para tomar estas acciones de seguridad y si se observa que el antivirus que actualmente posee la Cooperativa ya no protege tratar de cambiar por otro y con su respectivo licenciamiento.

4.7.3.2.1.3 Clasificación del inventario (SW,HW, Soportes de Información, Elementos auxiliares)

La Cooperativa no contaba con un inventario donde se clasificaba a cada uno de sus activos de una manera más detallada como se lo ha realizado en este proyecto, ya que para ellos todos eran equipos informáticos, pero en cuanto aplicación no tiene ningún inventario registrado y lo que son soportes de información solo poseen CDs donde resguardan su información diaria.

4.7.3.2.2 Plan de Ejecución

Objetivo

- Ordenar temporalmente los programas de seguridad

Para llegar un plan de seguridad optimo se ha llegado a lo siguiente orden de los programas de seguridad.

- Eliminar fallos de seguridad evidentes
- Clasificación del inventario(SW,HW, Soportes de Información, Elementos auxiliares)
- Normativas de Seguridad

4.7.3.2.3 Ejecución del plan

Esta actividad recoge la serie de proyectos que materializan el plan de seguridad y que se van realizando según dicho plan de acuerdo a lo analizado.

La aplicación de las salvaguardas implica recurrir en costos, los cuales estarán en función de los materiales a emplearse, del recurso humano a disponer tanto interno como externo, y del tiempo que se extienda en la aplicación de dichas salvaguardas.

Se deberá tomar en cuenta antes de la aplicación de la salvaguarda, la variable costo-beneficio, con el fin de poder controlar que el costo de la aplicación de la salvaguarda no supere al costo de la amenaza en caso de que se materialice.

La Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU) a su criterio analizará la factibilidad de la aplicación de las salvaguardas y el beneficio que éstas aportarán con el fin de disminuir el riesgo; así también, a su libre criterio seleccionarán los recursos convenientes a utilizarse para la aplicación de las salvaguardas, con sus costos respectivos y el tiempo que estimen prudente.

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- El presente trabajo sirve como una aplicación de la metodología MAGERIT Versión 3 basada en su herramienta PILAR 5.2.9, para la ejecución del Análisis y Gestión de Riesgos, extendida hacia cualquier institución pública o privada que posea activos.

- La herramienta PILAR 5.2.9, fue de vital importancia para comprender que los Sistemas de Información están expuestos a amenazas que pueden causar daños significativos a las operaciones de la organización, el mismo que tiene un interfaz amigable de aplicación para el usuario.

- La "Cooperativa de Ahorro y Crédito Universitaria Limita (COPEU)" no tiene medidas de seguridad guiados y documentados, por lo cual este estudio será de gran beneficio para minimizar riesgos en el futuro.

- El personal de la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU no lleva registro y seguimiento de fallos del Sistema de Información Financiera para poder dar soluciones adecuadas.

- El Sistema de Información Financiera no responde con agilidad en el proceso por lo que provoca malestar en el personal y en los clientes.

- Al Sistema de Información Financiera no se le realiza mantenimiento lo que provoca bajo funcionamiento en los procesos que realiza la Cooperativa diariamente generando malestar en los usuarios y pérdidas a la misma.

- Después de haber realizado este proyecto, la Cooperativa obtendrá un documento encaminado a la seguridad que será punto de partida para la creación de normativas de seguridad para los recursos informáticos y para los empleados que laboran en la Cooperativa.

5.2 Recomendaciones

- Se recomienda utilizar la Metodología MAGERIT Versión 3, en el Análisis y Gestión de Riesgos, complementando con la herramienta PILAR 5.2.9, que es una herramienta propia automatizada y basada en la metodología, que permite trabajar con varios activos, amenazas y salvaguardas.

- Se recomienda que la administración tome en cuenta estándares como: ISO/IEC 27002:2005 Código de buenas prácticas para la Gestión de la Seguridad de la Información, COBIT e ITIL (mejores prácticas de prestación de servicios TI y auditoría) y CISCO (estándares internacionales de redes y telecomunicaciones).

- Se recomienda al Técnico de la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU realizar mantenimiento al Sistema de Información Financiera para mejorar el desenvolvimiento y funcionamiento del sistema sin retrasos en sus transacciones.

- Se recomienda la implementación de un nuevo Sistema de Información Financiera que satisfaga las necesidades tanto de la Cooperativa como de sus clientes evitando causar molestias o pérdidas de tiempo a los mismos y generando mayores ingresos a la Cooperativa.

BIBLIOGRAFÍA.

- FERNÁNDEZ, Vicenç, (2006). Desarrollo de sistemas de información. Una metodología basada en el modelado. Edicions UPC. España.
- GALLEGO, José, (2010). Mantenimiento de Sistemas Microinformáticos. Informática y Comunicaciones. Editex. España.
- PIATTINI, Mario, DEL PESO, Emilio, (2001). Auditoria Informática Un Enfoque Práctico. 2da Edición Ampliada y Revisada. RA-MA. España.
- RIVAS, Gonzalo, (1998). Auditoria Informática. Díaz de Santos. España.
- AMUTIO, Miguel, CANDAU, Javier, (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. Ministerio de Hacienda y Administraciones Pública. España.
- AMUTIO, Miguel, CANDAU, Javier, (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II – Catalogo de Elementos. Ministerio de Hacienda y Administraciones Pública. España.
- AMUTIO, Miguel, CANDAU, Javier, (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III – Guía de Técnicas. Ministerio de Hacienda y Administraciones Pública. España.
- MÉNDEZ, Andrés, MAÑAS, José Antonio, (2012), Manual de Usuario Pilar 5.2.9. Ministerio de Hacienda y Administraciones Pública. España.

- SÁNCHEZ, Verónica. (2011). Sobre Conceptos Informática. Extraído el 11 de Marzo del 2013 de http://sobreconceptos.com/informatica

- TORRES, Alcides. (2012). Informática. Concepto. Clasificación. Extraído el 11 de Marzo del 2013 de http://www.educa.una.py/politecnica/mod/page/view.php?id=2734

- HURTADO, Pablo. (2005). Concepto de Auditoría. Extraído el 11 de Marzo del 2013 de http://www.emagister.com/curso-elemental-auditoria/concepto-auditoria

- AUDITORÍA DE INFORMÁTICA. (2010). Conceptos Generales de Auditoría. Extraído el 11 de Marzo del 2013 de http://auditoriadeinformatica.blogspot.es/

- ARANGUIZ, Giselle, CABELLO, Nadia, RIQUELME, Eduardo, RIVAS, Carla, RODRÍGUEZ, Jenny, SILVA, Romina. (2010). Importancia de las TIC'S en la Auditoría. Extraído el 12 de Marzo del 2013 de Archivo: importanciadelasticsenlaauditoria-100620210930-phpapp02.doc

- NORMAS DE AUDITORÍA GUBERNAMENTAL NAG 270 Y CORRELATIVA. (2006). Auditoria de Tecnologías de la Información y Comunicación. Extraído el 12 de Marzo del 2013 de http://www.contraloria.gob.bo/portal/Auditoria/AuditoriasOperativas/Auditor%C3%ADasTIC.aspx

- NORMAS DE AUDITORÍA INFORMÁTICA. (2009). Procedimientos de Auditoría Informática. Extraído el 12 de Marzo del 2013 de http://www.elregistroycontrol.com.ar/portal/index.php?option=com_content&view=article&id=49:normas-de-auditoria-informatica&catid=9:articulos&Itemid=61

- ECONOMÍA AIDA. (2009). Estándares de Auditoría Informática. Extraído el 12 de Marzo del 2013 de Archivo: standaresauditoria-111118074827-phpapp02.pdf

- DICCIONARIO DE INFORMÁTICA. (2007). Definición de Sistema. Extraído el 12 de Marzo del 2013 de http://www.alegsa.com.ar/Dic/sistema.php

- VEGA, Edgar. (2005). Los Sistemas de Información y su importancia para las organizaciones y empresas. Extraído el 12 de Marzo del 2013 de http://www.gestiopolis.com/Canales4/mkt/simparalas.htm

- VÁZQUEZ, Anaely. (2012). Tipos de Sistema de Información. Extraído el 12 de Marzo del 2013 de http://www.eumed.net/libros-gratis/2012a/1169/tipos_de_sistema_de_informacion.html

- GLOBALSOFT TECHNOLOGIES LTDA. (2006). Sistema de Información Integral SIF. Extraído el 28 de Marzo del 2013 de http://colombia.acambiode.com/producto/sistema-de-informacin-integral-sif_118662

- MARTELO, Lizeth. (2009). Sistema de Información Contable. Extraído el 28 de Marzo del 2013 de Archivo: sistema-informacion-contable.doc

- INTRODUCCIÓN A LA CONTABILIDAD GENERAL. (2001). Clases de Sistemas de la Información Contable. Extraído el 29 de Marzo del 2013 de http://ciberconta.unizar.es/leccion/cf001/410.HTM

GLOSARIO DE TÉRMINOS

Ataque: Amenaza de origen intencionado

Impacto: Resultado sobre un activo ante la materialización de una amenaza

Incidente: Cualquier evento no esperado o no deseado que pueda comprometer la seguridad del sistema

Normativa de Seguridad: Conjunto de documentos que desarrollan la política de seguridad.

Salvaguarda: Son acciones que protegen a un activo de forma física o lógica.

Seguridad: Capacidad de resistir, con un determinado nivel de confianza, los incidentes que puedan causar daño.

Valor: Estimación de la unidad de una determinada activo de información para la organización teniendo en cuenta los diferentes requerimientos

Abuso de privilegios de acceso: Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

Acceso no autorizado: El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

Acreditación: Acción de facultar a un sistema o red de información para que procese datos sensibles, determinando el grado en el que el diseño y la materialización de dicho sistema cumple los requerimientos de seguridad técnica preestablecidos.

Activo: Recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y a alcance los objetivos propuestos por su dirección.

Alteración de la información: Es la alteración accidental de la información.

Amenaza: Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Análisis: La acción y el efecto de separar un todo en los elementos que lo componen con el objeto de estudiar su naturaleza, función o significado.

Análisis de Riesgos: Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

Autenticidad: Aseguramiento de la identidad u origen.

Avería de origen físico o lógico: Son los fallos en los equipos y/o fallos en los programas. Puede ser debido a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

Caída del sistema por agotamiento físico de recursos: La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

Condiciones inadecuadas de temperatura o humedad: Son las deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frio, exceso de humedad.

Confidencialidad: Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.

Deficiencias en la organización: Es cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión.

Degradación: Mide el daño causado por un incidente en el supuesto de que ocurriera.

Denegación de servicio: Es la carencia de recursos suficientes que provoca la caída del sistema cuando la carga de trabajo es desmesurada.

Disponibilidad: Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

Dominio: Conjunto de activos sometidos a un tratamiento homogéneo, bajo una cierta política de seguridad común.

Gestión de Riesgos: Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

Impacto: Consecuencia que sobre un activo tiene la materialización de una amenaza.

Impacto residual: Impacto remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad.

Integridad: Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.

ISO/IEC 27002:2005 Código de buenas prácticas para la Gestión de la Seguridad de la Información: Establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información en una organización.

ISO / IEC 27002:2005 contiene las mejores prácticas de los objetivos de control y los controles en las siguientes áreas de gestión de seguridad de la información:

- Política de seguridad;
- Organización de seguridad de la información;
- De gestión de activos;
- Recursos de la seguridad humana;
- Seguridad física y ambiental;
- Las comunicaciones y la gestión de las operaciones;
- Control de acceso;
- La adquisición de sistemas de información, desarrollo y mantenimiento;
- Seguridad de la información de gestión de incidentes;
- Gestión de la continuidad;
- Cumplimiento.

Modelo de Valor: Informe: Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.

Riesgo: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

Riesgo residual: Riesgo remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información.

Sistemas de Información: Son los ordenadores y redes de comunicaciones electrónicas, así como los datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento.

Suplantación de la identidad del usuario: Es cuando un atacante consigue hacerse pasar por un usuario autorizado, disfrutando de los privilegios de este para sus fines propios.

Trazabilidad.- Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.

ANEXOS

ANEXO 1

ENCUESTA

COOPERATIVA DE AHORRO Y CRÉDITO UNIVERSITARIA LIMITADA

OBJETIVO: Conocer la situación actual de la Cooperativa y del funcionamiento del Sistema de Información Financiera.

INSTRUCTIVO

Señale con una X una de las alternativas que usted considere conveniente

CUESTIONARIO

1. ¿Se han realizado Auditorías Informáticas en la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU)?

   SI ☐ NO ☐

2. ¿Las Auditorías Informáticas realizadas en la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU) han servido para el progreso y mejor desempeño de la misma?

   SI ☐ NO ☐

3. ¿Se lleva algún registro y seguimiento de los fallos producidos por el Sistema de Información Financiera?

   SI ☐ NO ☐

4. ¿Cuándo se produce alguna falla en el Sistema de Información Financiera usted soluciona el problema?

   SOLO ☐ LLAMA AL SUPERVISOR ☐ LLAMA AL TÉCNICO ☐

5. ¿Qué tipo de control de cambios se realiza al Sistema de Información Financiera?

   OPERACIÓN ☐ PROCESAMIENTO ☐ SEGURIDAD ☐

6. ¿Se ha realizado una Auditoría Informática específicamente al Sistema de Información Financiera de la Cooperativa?

   SI ☐ NO ☐

7. ¿Al realizar las actividades diarias, el sistema responde con agilidad en el proceso?

   SI ☐ NO ☐

8. ¿Tiene conocimiento de todos los procesos del software e información instalados en su computador?

   SI ☐ NO ☐

9. ¿El Sistema de Información Financiera posee la documentación adecuada?

   SI ☐ NO ☐

10. ¿Se realiza chequeos habituales de mantenimiento al Sistema de Información Financiera en la Institución?

SI ☐ NO ☐

11. ¿Se efectúan actualizaciones del sistema periódicamente?

SI ☐ NO ☐

12. ¿Existen procesos en la institución para los que no se usa el sistema?

SI ☐ NO ☐

13. ¿Cree Ud. necesario la implementación de un nuevo sistema de información financiera en la Cooperativa?

SI ☐ NO ☐

14. ¿Cree Ud. que usted que un nuevo sistema de información financiera mejoraría el proceso y velocidad en las transacciones?

SI ☐ NO ☐

ANEXO 2
FICHAS PARA LA RECOPILACIÓN DE DATOS

[S] SERVICIOS	
NOMBRE:	
DESCRIPCIÓN: …… ……	
RESPONSABLE:	
Tipo (marque todos los adjetivos que procedan): ( ) [anon] anónimo (sin requerir identificación del usuario) ( ) [pub] al público en general (sin relación contractual) ( ) [ext] a usuarios externos (bajo una relación contractual) ( ) [int] interno (usuarios y medios de la propia organización) ( ) [www] world wide web ( ) [telnet] acceso remoto a cuenta local ( ) [email] correo electrónico ( ) [voip] voz sobre ip ( ) [file] almacenamiento de ficheros ( ) [print] servicio de impresión ( ) [ftp] transferencia de ficheros ( ) [backup] servicio de copias de respaldo (backup) ( ) [edi] intercambio electrónico de datos ( ) [dir] servicio de directorio ( ) [dns] servidor de nombres de dominio ( ) [idm] gestión de identidades ( ) [ipm] gestión de privilegios ( ) [crypto] servicios criptográficos ( ) [key_gen] generación de claves ( ) [integrity] protección de la integridad ( ) [encryption] cifrado ( ) [auth] autenticación ( ) [sign] firma electrónica ( ) [time] fechado electrónico ( ) [pki] PKI - infraestructura de clave pública ( ) [ca] autoridad de certificación ( ) [ra] autoridad de registro ( ) [ba] autoridad de validación ( ) [tsa] autoridad de fechado electrónico ( ) [aa] autoridad de atributos ( ) [other] otros…	**CARACTERÍSTICAS:** …… …… …… …….. …… …… …… …… …… …… …… …… …… …… …….. …… …….. …… …….. …… …….. …… ……

AMENAZAS:

[N] Desastres Naturales

[N.1] Fuego

[N.2] Daños por agua

[N.*]Desastres naturales

[I] De origen industrial

[I.1] Fuego

[I.2] Daños por agua

[I.*] Desastres industriales

[I.3] Contaminación medioambiental

[I.4] Contaminación electromagnética

[I.5] Avería de origen físico o lógico

[I.6] Corte del suministro eléctrico

[I.7] Condiciones inadecuadas de temperatura o humedad

[I.8] Fallo de servicios de comunicaciones

[I.9] Interrupción de otros servicios o suministros esenciales

[I.10] Degradación de los soportes de almacenamiento de la información

[I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados

[E.1] Errores de los usuarios [E.2] Errores del administrador [E.3] Errores de monitorización (log)

[E.4] Errores de configuración

[E.7] Deficiencias en la organización

[E.8] Difusión de software dañino

[E.9] Errores de (re-)encaminamiento

[E.10] Errores de secuencia

[E.14] Fugas de información

[E.15] Alteración de la información

[E.18] Destrucción de la información

[E.19] Fugas de información

[E.20] Vulnerabilidad de los programas (software)

[E.21] Errores de mantenimiento / actualización de programas (software)

[E.23] Errores de mantenimiento / actualización de equipos (hardware)

[E.24] Caída del sistema por agotamiento de recursos

[E.25] Perdidas de equipos

[E.28] Indisponibilidad del personal

[A] Ataques deliberados

[A.3] Manipulación de los registros de actividad

[A.4] Manipulación de los ficheros de configuración

[A.5] Suplantación de la identidad del usuario

[A.6] Abuso de privilegios de acceso

[A.7] Uso no previsto

[A.8] Difusión de software dañino

[A.9] (Re-) encaminamiento de mensajes

[A.10] Alteración de secuencia

[A.11] Acceso no autorizado

[A.12] Análisis de trafico

[A.13] Repudio

[A.14] Interceptación de información (escucha)

[A.15] Modificación de información

[A.18] Destrucción de la información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.23] Manipulación de hardware
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

[SW] APLICACIONES (Software)

NOMBRE:

DESCRIPCIÓN:
……
……

CARACTERÍSTICAS:
……
……
…..……..

RESPONSABLE:

Tipo (marque todos los adjetivos que procedan):
( ) [prp] desarrollo propio (in house)
( ) [sub] desarrollo a medida (subcontratado)
( ) [std] estándar (off the shelf)
- ( ) [browser] navegador web
- ( ) [www] servidor de presentación
- ( ) [app] servidor de aplicaciones
- ( ) [email_client] cliente de correo electrónico
- ( ) [email_server] servidor de correo electrónico
- ( ) [directory] servidor de directorio
- ( ) [file] servidor de ficheros
- ( ) [dbms] sistema de gestión de bases de datos
- ( ) [tm] monitor transaccional
- ( ) [office] ofimática
- ( ) [av] anti virus
- ( ) [os] sistema operativo
  - ( ) [windows] Windows
  - ( ) [solaris] Solaris
  - ( ) [linux] linux
  - ( ) [other] otros…
- ( ) [ts] servidor de terminales
- ( ) [backup] sistema de backup
- ( ) [other] otros…

AMENAZAS:

[N] Desastres Naturales

[N.1] Fuego
[N.2] Daños por agua
[N.*]Desastres naturales

[I] De origen industrial

[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación medioambiental
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios o suministros esenciales
[I.10] Degradación de los soportes de almacenamiento de la información
[I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados

[E.1] Errores de los usuarios [E.2] Errores del administrador [E.3] Errores de monitorización (log)
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de (re-)encaminamiento
[E.10] Errores de secuencia
[E.14] Fugas de información
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.20] Vulnerabilidad de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Perdidas de equipos
[E.28] Indisponibilidad del personal

[A] Ataques deliberados

[A.3] Manipulación de los registros de actividad
[A.4] Manipulación de los ficheros de configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] (Re-) encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de trafico
[A.13] Repudio
[A.14] Interceptación de información (escucha)
[A.15] Modificación de información

[A.18] Destrucción de la información
[A.19] Revelación de información
[A.22] Manipulación de programas
[A.23] Manipulación de hardware
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

[HW] EQUIPAMIENTO INFORMÁTICO (Hardware)

NOMBRE:

DESCRIPCIÓN:

……
……

CARACTERÍSTICAS:

MARCA:…….. VERSIÓN:……..
MODELO:……. AÑO:…….

RESPONSABLE:

Tipo (marque todos los adjetivos que procedan):

( ) [host] grandes equipos (host)
( ) [mid] equipos medios
( ) [pc]informática personal
( ) [vhost]equipos virtuales
( ) [cluster] cluster
( ) [mobile] informática móvil
( ) [pda]agendas electrónicas
( ) [easy]fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
  ( ) [print] medios de impresión
  ( ) [scan] escáner
  ( ) [crypto] dispositivo criptográfico
  ( ) [other] otros…
( ) [bd] dispositivo de frontera
( ) [network] soporte de la red
  ( ) [modem] módem
  ( ) [hub] concentrador
  ( ) [switch] conmutador
  ( ) [router] encaminador
  ( ) [bridge]puente
  ( ) [gtwy] pasarela
  ( ) [firewall] cortafuegos
  ( ) [wap] punto de acceso wireless
  ( ) [other] otros…
( ) [pabx]centralita telefónica
( ) [other] otros…

AMENAZAS:

[N] Desastres Naturales

[N.1] Fuego
[N.2] Daños por agua
[N.*]Desastres naturales

[I] De origen industrial

[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación medioambiental
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios o suministros esenciales
[I.10] Degradación de los soportes de almacenamiento de la información
[I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados

[E.1] Errores de los usuarios [E.2] Errores del administrador [E.3] Errores de monitorización (log)
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de (re-)encaminamiento
[E.10] Errores de secuencia
[E.14] Fugas de información
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.20] Vulnerabilidad de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Perdidas de equipos
[E.28] Indisponibilidad del personal

[A] Ataques deliberados

[A.3] Manipulación de los registros de actividad
[A.4] Manipulación de los ficheros de configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] (Re-) encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de trafico
[A.13] Repudio
[A.14] Interceptación de información (escucha)
[A.15] Modificación de información
[A.18] Destrucción de la información

[A.19] Revelación de información
[A.22] Manipulación de programas
[A.23] Manipulación de hardware
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

[COM] COMUNICACIONES
NOMBRE:
DESCRIPCIÓN: …… ……
CARACTERÍSTICAS: MARCA:…….. CANTIDAD:…….. MODELO:…… …….. …….
RESPONSABLE:
Tipo (marque todos los adjetivos que procedan): ( ) [PSTN] red telefónica ( ) [ISDN] RDSI (red digital) ( ) [X25] X25 (red de datos) ( ) [ADSL] ADSL ( ) [pp] punto a punto ( ) [radio] red inalámbrica ( ) [wifi]Wifi ( ) [mobile] telefonía movil ( ) [sat] por satélite ( ) [LAN] red local ( ) [VLAN] LAN irtual ( ) [MAN] red metropolitana ( ) [WAN] red de área amplia ( ) [Internet] Internet ( ) [vpn] red privada virtual ( ) [other] otros…

AMENAZAS:

[N] Desastres Naturales

[N.1] Fuego
[N.2] Daños por agua
[N.*]Desastres naturales

[I] De origen industrial

[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación medioambiental
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios o suministros esenciales
[I.10] Degradación de los soportes de almacenamiento de la información
[I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados

[E.1] Errores de los usuarios [E.2] Errores del administrador [E.3] Errores de monitorización (log)
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de (re-)encaminamiento
[E.10] Errores de secuencia
[E.14] Fugas de información
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.20] Vulnerabilidad de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Perdidas de equipos
[E.28] Indisponibilidad del personal

[A] Ataques deliberados

[A.3] Manipulación de los registros de actividad
[A.4] Manipulación de los ficheros de configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] (Re-) encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de trafico
[A.13] Repudio
[A.14] Interceptación de información (escucha)
[A.15] Modificación de información

[A.18] Destrucción de la información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.23] Manipulación de hardware
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

[SI] SOPORTES DE INFORMACIÓN

NOMBRE:

DESCRIPCIÓN:
……
……

CARACTERÍSTICAS:
MARCA:…..……
……
CAPACIDAD:……
……..…
CANTIDAD:……
……..
……

RESPONSABLE:

Tipo (marque todos los adjetivos que procedan):

( ) [electronic] electrónicos
- ( ) [disk] discos
- ( ) [vdisk] discos virtuales
- ( ) [san] almacenamiento en red
- ( ) [disquette] disquetes
- ( ) [cd] cederrón (CD-ROM)
- ( ) [usb] dispositivos USB
- ( ) [dvd] DVD
- ( ) [tape] cinta magnética
- ( ) [mc] tarjetas de memoria
- ( ) [ic] tarjetas inteligentes
- ( ) [other] otros…

( ) [non_electronic] no electrónicos
- ( ) [printed] material impreso
- ( ) [tape] cinta de papel
- ( ) [film] microfilm
- ( ) [cards] tarjetas perforadas
- ( ) [other] otros…

AMENAZAS:

[N] Desastres Naturales

[N.1] Fuego
[N.2] Daños por agua
[N.*]Desastres naturales

[I] De origen industrial

[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación medioambiental
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios o suministros esenciales
[I.10] Degradación de los soportes de almacenamiento de la información
[I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados

[E.1] Errores de los usuarios [E.2] Errores del administrador [E.3] Errores de monitorización (log)
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de (re-)encaminamiento
[E.10] Errores de secuencia
[E.14] Fugas de información
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.20] Vulnerabilidad de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Perdidas de equipos
[E.28] Indisponibilidad del personal

[A] Ataques deliberados

[A.3] Manipulación de los registros de actividad
[A.4] Manipulación de los ficheros de configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] (Re-) encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de trafico
[A.13] Repudio
[A.14] Interceptación de información (escucha)
[A.15] Modificación de información
[A.18] Destrucción de la información

[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.23] Manipulación de hardware
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

[AUX] EQUIPAMIENTO AUXILIAR

NOMBRE:

DESCRIPCIÓN:
……
……

CARACTERÍSTICAS:
MARCA:……
TIPO:……..
….……..……
……..……..

RESPONSABLE:

Tipo (marque todos los adjetivos que procedan):
( ) [power] fuentes de alimentación
( ) [ups] sai - sistemas de alimentación ininterrumpida
( ) [gen] generadores eléctricos
( ) [ac] equipos de climatización
( ) [cabling] cableado
  ( ) [wire] cable eléctrico
  ( ) [fiber] fibra óptica
( ) [robot] robots
  ( ) [tape] ... de cintas
  ( ) [disk] ... de discos
( ) [supply] suministros esenciales
( ) [destroy] equipos de destrucción de soportes de información
( ) [furniture] mobiliario: armarios, etc
( ) [safe] cajas Fuertes
( ) [other] otros…

AMENAZAS:

[N] Desastres Naturales

[N.1] Fuego
[N.2] Daños por agua
[N.*]Desastres naturales

[I] De origen industrial

[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación medioambiental
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios o suministros esenciales
[I.10] Degradación de los soportes de almacenamiento de la información
[I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados

[E.1] Errores de los usuarios [E.2] Errores del administrador [E.3] Errores de monitorización (log)
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de (re-)encaminamiento
[E.10] Errores de secuencia
[E.14] Fugas de información
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.20] Vulnerabilidad de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento/actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Perdidas de equipos
[E.28] Indisponibilidad del personal

[A] Ataques deliberados

[A.3] Manipulación de los registros de actividad
[A.4] Manipulación de los ficheros de configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] (Re-) encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de trafico
[A.13] Repudio
[A.14] Interceptación de información (escucha)
[A.15] Modificación de información

[A.18] Destrucción de la información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.23] Manipulación de hardware
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

[SS] SERVICIOS SUBCONTRATADOS

NOMBRE:

DESCRIPCIÓN:
……
……

CARACTERÍSTICAS:
SERVICIO:…..……

RESPONSABLE:

Tipo (marque todos los adjetivos que procedan):
( ) [anon] anónimo (sin requerir identificación del usuario)
( ) [pub] al público en general (sin relación contractual)
( ) [ext] a usuarios externos (bajo una relación contractual)
( ) [int] interno (usuarios y medios de la propia organización)
( ) [cont] contratado a terceros (se presta con medios ajenos)

( ) [www] world wide web
( ) [telnet] acceso remoto a cuenta local
( ) [email] correo electrónico
( ) [voip] voz sobre ip
( ) [file] almacenamiento de ficheros
( ) [print] servicio de impresión
( ) [ftp] transferencia de ficheros
( ) [backup] servicio de copias de respaldo (backup)
( ) [edi] intercambio electrónico de datos

( ) [dir] servicio de directorio
( ) [dns] servidor de nombres de dominio
( ) [idm] gestión de identidades
( ) [ipm] gestión de privilegios
( ) [crypto] servicios criptográficos
  ( ) [key_gen] generación de claves
  ( ) [integrity] protección de la integridad
  ( ) [encryption] cifrado
  ( ) [auth] autenticación
  ( ) [sign] firma electrónica
  ( ) [time] fechado electrónico

AMENAZAS:

[N] Desastres Naturales

[N.1] Fuego

[N.2] Daños por agua

[N.*]Desastres naturales

[I] De origen industrial

[I.1] Fuego

[I.2] Daños por agua

[I.*] Desastres industriales

[I.3] Contaminación medioambiental

[I.4] Contaminación electromagnética

[I.5] Avería de origen físico o lógico

[I.6] Corte del suministro eléctrico

[I.7] Condiciones inadecuadas de temperatura o humedad

[I.8] Fallo de servicios de comunicaciones

[I.9] Interrupción de otros servicios o suministros esenciales

[I.10] Degradación de los soportes de almacenamiento de la información

[I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados

[E.1] Errores de los usuarios [E.2] Errores del administrador [E.3] Errores de monitorización (log)

[E.4] Errores de configuración

[E.7] Deficiencias en la organización

[E.8] Difusión de software dañino

[E.9] Errores de (re-)encaminamiento

[E.10] Errores de secuencia

[E.14] Fugas de información

[E.15] Alteración de la información

[E.18] Destrucción de la información

[E.19] Fugas de información

[E.20] Vulnerabilidad de los programas (software)

[E.21] Errores de mantenimiento / actualización de programas (software)

[E.23] Errores de mantenimiento/actualización de equipos (hardware)

[E.24] Caída del sistema por agotamiento de recursos

[E.25] Perdidas de equipos

[E.28] Indisponibilidad del personal

[A] Ataques deliberados

[A.3] Manipulación de los registros de actividad

[A.4] Manipulación de los ficheros de configuración

[A.5] Suplantación de la identidad del usuario

[A.6] Abuso de privilegios de acceso

[A.7] Uso no previsto

[A.8] Difusión de software dañino

[A.9] (Re-) encaminamiento de mensajes

[A.10] Alteración de secuencia

[A.11] Acceso no autorizado

[A.12] Análisis de trafico

[A.13] Repudio

[A.14] Interceptación de información (escucha)

[A.15] Modificación de información

[A.18] Destrucción de la información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.23] Manipulación de hardware
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

[L] INSTALACIONES
NOMBRE:
DESCRIPCIÓN: …… …… ……
CARACTERÍSTICAS: TIPO:…….. DIRECCIÓN:……. TELÉFONOS:…… ……. ……. …….
RESPONSABLE:
Tipo (marque todos los adjetivos que procedan): ( ) [site] emplazamiento ( ) [building] edificio ( ) [local] local ( ) [mobile] plataformas móviles ( ) [car] vehículo terrestre: coche, camión, etc. ( ) [plane] vehículo aéreo: avión, etc. ( ) [ship] vehículo marítimo: buque, lancha, etc. ( ) [shelter] contenedores ( ) [channel] canalización ( ) [other] otros…

AMENAZAS:

[N] Desastres Naturales

[N.1] Fuego
[N.2] Daños por agua
[N.*]Desastres naturales

[I] De origen industrial

[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación medioambiental
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios o suministros esenciales
[I.10] Degradación de los soportes de almacenamiento de la información
[I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados

[E.1] Errores de los usuarios [E.2] Errores del administrador [E.3] Errores de monitorización (log)
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de (re-)encaminamiento
[E.10] Errores de secuencia
[E.14] Fugas de información
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.20] Vulnerabilidad de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Perdidas de equipos
[E.28] Indisponibilidad del personal

[A] Ataques deliberados

[A.3] Manipulación de los registros de actividad
[A.4] Manipulación de los ficheros de configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] (Re-) encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de trafico
[A.13] Repudio
[A.14] Interceptación de información (escucha)
[A.15] Modificación de información
[A.18] Destrucción de la información

[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.23] Manipulación de hardware
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

[P] PERSONAL
NOMBRE:
DESCRIPCIÓN: …… ……
CARACTERÍSTICAS: RESPONSABLES:…… ……
RESPONSABLE:
Tipo (marque todos los adjetivos que procedan): ( ) [ue] usuarios externos ( ) [ui] usuarios internos ( ) [op] operadores ( ) [adm] administradores de sistemas ( ) [com] administradores de comunicaciones ( ) [dba] administradores de BBDD ( ) [sec] administradores de seguridad ( ) [des] desarrolladores/programadores ( ) [sub] subcontratas ( ) [prov] proveedores ( ) [other] otros…

AMENAZAS:

[N] Desastres Naturales
- [N.1] Fuego
- [N.2] Daños por agua
- [N.*]Desastres naturales

[I] De origen industrial
- [I.1] Fuego
- [I.2] Daños por agua
- [I.*] Desastres industriales
- [I.3] Contaminación medioambiental

[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios o suministros esenciales
[I.10] Degradación de los soportes de almacenamiento de la información
[I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados

[E.1] Errores de los usuarios [E.2] Errores del administrador [E.3] Errores de monitorización (log)
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de (re-)encaminamiento
[E.10] Errores de secuencia
[E.14] Fugas de información
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.20] Vulnerabilidad de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Perdidas de equipos
[E.28] Indisponibilidad del personal

[A] Ataques deliberados

[A.3] Manipulación de los registros de actividad
[A.4] Manipulación de los ficheros de configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] (Re-) encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de trafico
[A.13] Repudio
[A.14] Interceptación de información (escucha)
[A.15] Modificación de información
[A.18] Destrucción de la información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.23] Manipulación de hardware
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

Dependencias de activos inferiores (hijos) [S] SERVICIOS	
activo:	**grado:**
¿por qué?	

activo:	**grado:**
¿por qué?	

activo:	**grado:**
¿por qué?	

Dependencias de activos inferiores (hijos) [SW] APLICACIONES (Software)	
activo:	**grado:**
¿por qué?	

activo:	**grado:**
¿por qué?	

activo:	**grado:**
¿por qué?	

Dependencias de activos inferiores (hijos) [HW] EQUIPAMIENTO INFORMÁTICO (Hardware)	
activo:	**grado:**
¿por qué?	

activo:	**grado:**
¿por qué?	

activo:	**grado:**
¿por qué?	

Dependencias de activos inferiores (hijos) [COM] COMUNICACIONES	
activo:	**grado:**
¿por qué?	

activo:	**grado:**
¿por qué?	

activo:	**grado:**
¿por qué?	

Dependencias de activos inferiores (hijos) [SI] SOPORTES DE INFORMACIÓN	
activo:	**grado:**
¿por qué?	

activo:	**grado:**
¿por qué?	

activo:	**grado:**
¿por qué?	

Dependencias de activos inferiores (hijos) [AUX] EQUIPAMIENTO AUXILIAR	
activo:	**grado:**
¿por qué?	

activo:	**grado:**
¿por qué?	

activo:	**grado:**
¿por qué?	

Dependencias de activos inferiores (hijos) [SS] SERVICIOS SUBCONTRATADOS	
activo:	**grado:**
¿por qué?	

activo:	**grado:**
¿por qué?	

activo:	**grado:**
¿por qué?	

Dependencias de activos inferiores (hijos) [L] INSTALACIONES	
activo:	**grado:**
¿por qué?	

activo:	**grado:**
¿por qué?	

activo:	**grado:**
¿por qué?	

ANEXO 3

MODELO DE VALOR

proyecto: [AGR_COPEU] ANÁLISIS Y GESTIÓN DE RIESGOS SISTEMA DE LA COOPERATIVA COPEU

1. Datos del proyecto

AGR_COPEU	ANÁLISIS Y GESTIÓN DE RIESGOS SISTEMA DE LA COOPERATIVA COPEU
Descripción	Análisis al Sistema
Responsable	Carlos Andrés Simbaya Camacho
Organización	Cooperativa de Ahorro y Crédito Universitaria Limitada
Versión	5.2.9
Fecha	07-10-2013
Biblioteca	[std] Biblioteca INFOSEC (28.8.2012)

Descripción

El presente trabajo es realizado para un proyecto de tesis en la Universidad Técnica de Ambato que se realizó en la Cooperativa de Ahorro y Crédito Universitaria Limitada.

Licencia

[edu] UTA
Universidad Técnica de Ambato
Facultad de Ingeniería en Sistemas, Electrónica e Industrial
[... 31.12.2014]

2. Dimensiones

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos

3. Dominios de seguridad

- [base] COPEU

4. Activos

4.1. Capa - [B] Capa de negocio

[AH_COPEU] AHORRO
[CR_COPEU] CREDITO

4.2. Capa - [IS] Servicios internos

[AR_COPEU] ACCESO REMOTO
[SCE_COPEU] SERVIDOR DE CORREO ELECTRONICO
[SAC_COPEU] SERVIDOR DE ARCHIVO COMPARTIDO
[IN_COPEU] INTERNET

4.3. Capa - [E] Equipamiento

[SW] Aplicaciones
[SISCO_COPEU] SISTEMA FINANCIERO COPEU
[OF_COPEU] OFIMATICA
[AN_COPEU] ANTIVIRUS
[OTR_COPEU] OTRO SOFTWARE
[HW] Equipos
[SBD_COPEU] SERVIDOR DE BASE DE DATOS
[ROU_COPEU] ROUTER
[SWI_COPEU] SWITCH
[FIR_COPEU] FIREWALL
[COM_COPEU] COMPUTADORAS DE ESCRITORIO
[COMPO_COPEU] COMPUTADORAS PORTATILES
[IMPLA_COPEU] IMPRESORA A LASER
[IMPMA_COPEU] IMPRESORA MATRICIAL
[COM] Comunicaciones
[REDLA_COPEU] RED LAN
[REDWA_COPEU] RED WAN
[INT_COPEU] INTERNET COPEU
[AUX] Elementos auxiliares
[CABDAT_COPEU] CABLEADO DE DATOS COPEU
[EQUAUX_COPEU] EQUIPAMIENTO AUXILIAR

4.4. Capa - [SS] Servicios subcontratados

[PAGAGI_COPEU] PAGO AGIL COPEU
[SOLA_COPEU] SOAT LATINA

4.5. Capa - [L] Instalaciones

[USR_COPEU] UNIDAD DE SISTEMAS Y REDES COPEU

4.6. Capa - [P] Personal

[ADSFYBD_COPEU] ADMINISTRACION SISTEMA FINANCIERO Y BASE DE DATOS
[SU_COPEU] SOPORTE A USUARIO

5. Activos

5.1. [AH_COPEU] AHORRO

- [S] Servicios
- [S.pub] al público en general (sin relación contractual)
- [S.ext] a usuarios externos (bajo una relación contractual)

Dominio de seguridad

- [base] COPEU

Datos

A LA VISTA	Interés Semestral del 2%; Cualquier cantidad gana interés; no se cobra mantenimiento de cuenta
CERTIFICADO DE DEPOSITO A PLAZO (Póliza)	Monto de 100 a 2000 Plazo de 30 a 60 días se gana 6%, de 61 a 120 días se gana 7%, de 121 a 180 días se gana 8%, de 181 a 360 días se gana 9%. Monto de 2001 a 5000 Plazo de 30 a 60 días se gana 6,50%, de 61 a 120 días se gana 7,50%, de 121 a 180 días se gana 8,50%, de 181 a 360 días se gana 9,50%. Monto de 5001 a 10000 Plazo de 30 a 60 días se gana 7%, de 61 a 120 días se gana 8%, de 121 a 180 días se gana 9%, de 181 a 360 días se gana 10%. Monto de 10001 a 20000 Plazo de 30 a 60 días se gana 7,50%, de 61 a 120 días se gana 8,50%, de 121 a 180 días se gana 9,50%, de 181 a 360 días se gana 10,50%. Monto más de 20000 Plazo de 30 a 60 días se gana 8%, de 61 a 120 días se gana 9%, de 121 a 180 días se gana 10%, de 181 a 360 días se gana 11%.

Descripción

Para realizar los depósitos usted debe presentar:
-libreta de ahorros.
-la papeleta de depósito (color azul), si su depósito incluye cheques, deberá llenar el detalle de los mismos en el reverso de la papeleta.

Para realizar los retiros usted necesita:
-cedula de identidad
-libreta de ahorros
-papeleta de retiro color (naranja)

(En cada oficina se tienen montos máximos de un retiro que es de 500 dólares si es más se realiza con cheque, solo si hay exceso de fondo de cambio se entregan en dinero el retiro superior al valor mencionado anteriormente.

Superiores (activos que dependen de este)

- [SW.SISCO_COPEU] SISTEMA FINANCIERO COPEU

Inferiores (activos de los que depende este)

- [AR_COPEU] ACCESO REMOTO
- [IN_COPEU] INTERNET
- [SW.OF_COPEU] OFIMATICA
- [SW.AN_COPEU] ANTIVIRUS

Valor

Dimensión	***valor***	***valores acumulados***
[D] disponibilidad	[9]	[9]
[I] integridad de los datos	[9]	[9]
[C] confidencialidad de los datos	[9]	[9]

[A] autenticidad de los usuarios y de la información	[9]	[9]
[T] trazabilidad del servicio y de los datos	[9]	[9]

5.2. [CR_COPEU] CREDITO

- o [S] Servicios
- o [S.pub] al público en general (sin relación contractual)
- o [S.ext] a usuarios externos (bajo una relación contractual)

Dominio de seguridad

- o [base] COPEU

Datos

TIPO DE CRÉDITO	**MONTOS**	**TASAS**
CONSUMO	DE 300 HASTA 8000	15,10%
MICROCRÉDITO MINORISTA	DE 300 HASTA 3000	24,00%
MICROCRÉDITO ACUM. SIMPLE	DE 3001 HASTA 8000	23,00%

Descripción

Son créditos que la Cooperativa de Ahorro y Crédito Universitaria Limitada otorga a sus socios.

Superiores (activos que dependen de este)

- o [SW.SISCO_COPEU] SISTEMA FINANCIERO COPEU

Inferiores (activos de los que depende este)

- o [AR_COPEU] ACCESO REMOTO
- o [IN_COPEU] INTERNET
- o [SW.OF_COPEU] OFIMATICA
- o [SW.AN_COPEU] ANTIVIRUS

Valor

Dimensión	***valor***	***valores acumulados***
[D] disponibilidad	[9]	[9]
[I] integridad de los datos	[9]	[9]
[C] confidencialidad de los datos	[9]	[9]
[A] autenticidad de los usuarios y de la información	[9]	[9]
[T] trazabilidad del servicio y de los datos	[9]	[9]

5.3. [AR_COPEU] ACCESO REMOTO

- o [S] Servicios
- o [S.int] interno (usuarios y medios de la propia organización)
- o [S.telnet] acceso remoto a cuenta local

Dominio de seguridad

- [base] COPEU

Datos

SISTEMA OPERATIVO	Windows Server 2003
FUNCIÓN	Protocolo cliente / servicio

Descripción

Sirve para dar soporte remotamente usando claves fijas, también se usa para acceder a equipos como activos de red.

Superiores (activos que dependen de este)

- [AH_COPEU] AHORRO
- [CR_COPEU] CREDITO
- [PAGAGI_COPEU] PAGO AGIL COPEU
- [SOLA_COPEU] SOAT LATINA

Inferiores (activos de los que depende este)

- [SCE_COPEU] SERVIDOR DE CORREO ELECTRONICO
- [SAC_COPEU] SERVIDOR DE ARCHIVO COMPARTIDO
- [SW.OTR_COPEU] OTRO SOFTWARE
- [HW.SBD_COPEU] SERVIDOR DE BASE DE DATOS

Valor

Dimensión	***valor***	***valores acumulados***
[D] disponibilidad	[3]	[9]
[I] integridad de los datos	[3]	[9]
[C] confidencialidad de los datos	[3]	[9]
[A] autenticidad de los usuarios y de la información	[3]	[9]
[T] trazabilidad del servicio y de los datos	[3]	[9]

5.4. [SCE_COPEU] SERVIDOR DE CORREO ELECTRONICO

- [S] Servicios
- [S.int] interno (usuarios y medios de la propia organización)
- [S.email] correo electrónico

Dominio de seguridad

- [base] COPEU

Datos

SISTEMA OPERATIVO	Windows, Linux
PROPIETARIO	COPEU
CANTIDAD	1

Descripción

El servidor presta funcionalidades de servidor de envío y recepción de correo electrónico.

Superiores (activos que dependen de este)

- [AR_COPEU] ACCESO REMOTO
- [IN_COPEU] INTERNET
- [SW.OF_COPEU] OFIMATICA
- [SW.AN_COPEU] ANTIVIRUS

Inferiores (activos de los que depende este)

- [HW.COM_COPEU] COMPUTADORAS DE ESCRITORIO
- [HW.COMPO_COPEU] COMPUTADORAS PORTATILES

Valor

Dimensión	***valor***	***valores acumulados***
[D] disponibilidad	[2]	[9]
[I] integridad de los datos	[2]	[9]
[C] confidencialidad de los datos	[2]	[9]
[A] autenticidad de los usuarios y de la información	[2]	[9]
[T] trazabilidad del servicio y de los datos	[2]	[9]

5.5. [SAC_COPEU] SERVIDOR DE ARCHIVO COMPARTIDO

- [S] Servicios
- [S.int] interno (usuarios y medios de la propia organización)
- [S.file] almacenamiento de ficheros

Dominio de seguridad

- [base] COPEU

Datos

SERVIDOR DE ARCHIVOS	Windows Server 2003
PROPIETARIO	COPEU
CANTIDAD	1

Descripción

Servicio de archivos compartidos compatible con Windows y Linux.

Superiores (activos que dependen de este)

- [AR_COPEU] ACCESO REMOTO
- [IN_COPEU] INTERNET
- [SW.OF_COPEU] OFIMATICA
- [SW.AN_COPEU] ANTIVIRUS

Inferiores (activos de los que depende este)

- [HW.COM_COPEU] COMPUTADORAS DE ESCRITORIO
- [HW.COMPO_COPEU] COMPUTADORAS PORTATILES

Valor

Dimensión	*valor*	*valores acumulados*
[D] disponibilidad	[4]	[9]
[I] integridad de los datos	[4]	[9]
[C] confidencialidad de los datos	[4]	[9]
[A] autenticidad de los usuarios y de la información	[4]	[9]
[T] trazabilidad del servicio y de los datos	[4]	[9]

5.6. [IN_COPEU] INTERNET

- [SW] Aplicaciones (software)
- [SW.std] estándar (off the shelf)
- [SW.std.browser] navegador web
- [SW.std.os] sistema operativo
- [SW.std.os.windows] windows

Dominio de seguridad

- [base] COPEU

Datos

DISEÑO	HTML, CSSS, XML
INTERFAZ DE USUARIO	FTP
PROTOCOLO	HTTP, FTP
SISTEMA OPERATIVO	Windows

Descripción

Navegación internet, browser para acceso a Pago Ágil y Soat Latina y configuración de router.

Superiores (activos que dependen de este)

- [AH_COPEU] AHORRO
- [CR_COPEU] CREDITO
- [PAGAGI_COPEU] PAGO AGIL COPEU
- [SOLA_COPEU] SOAT LATINA

Inferiores (activos de los que depende este)

- [SCE_COPEU] SERVIDOR DE CORREO ELECTRONICO
- [SAC_COPEU] SERVIDOR DE ARCHIVO COMPARTIDO
- [SW.OTR_COPEU] OTRO SOFTWARE
- [HW.SBD_COPEU] SERVIDOR DE BASE DE DATOS

Valor

Dimensión	*valor*	*valores acumulados*
[D] disponibilidad	[2]	[9]
[I] integridad de los datos	[2]	[9]
[C] confidencialidad de los datos	[2]	[9]
[A] autenticidad de los usuarios y de la información	[2]	[9]
[T] trazabilidad del servicio y de los datos	[2]	[9]

5.7. [SW.SISCO_COPEU] SISTEMA FINANCIERO COPEU

- [essential] Activos esenciales
- [D] Datos / Información
- [D.conf] datos de configuración
- [D.int] datos de gestión interna
- [D.auth] datos de validación de credenciales
- [D.log] registro de actividad (log)
- [SW] Aplicaciones (software)
- [SW.sub] desarrollo a medida (subcontratado)
- [SW.std] estándar (off the shelf)
- [SW.std.browser] navegador web
- [SW.std.app] servidor de aplicaciones
- [SW.std.dbms] sistema de gestión de bases de datos
- [SW.std.os] sistema operativo
- [SW.std.os.windows] windows
- [SW.std.os.linux] linux

Dominio de seguridad

- [base] COPEU

Datos

NOMENCLATURA	SISCO MQR
CREACIÓN	1995
LENGUAJE DE PROGRAMACIÓN	Microsoft Visual Fox
PLATAFORMA	Windows, Linux

Descripción

Controla y automatiza las tareas de Ahorro y Crédito, control de equipos y usuarios de la Institución.

Inferiores (activos de los que depende este)

- [AH_COPEU] AHORRO
- [CR_COPEU] CREDITO

Valor

Dimensión	*valor*	*valores acumulados*
[D] disponibilidad	[9]	[9]
[I] integridad de los datos	[9]	[9]
[C] confidencialidad de los datos	[9]	[9]
[A] autenticidad de los usuarios y de la información	[9]	[9]
[T] trazabilidad del servicio y de los datos	[9]	[9]

5.8. [SW.OF_COPEU] OFIMATICA

- [SW] Aplicaciones (software)
- [SW.std] estándar (off the shelf)
- [SW.std.office] ofimática
- [SW.std.os] sistema operativo
- [SW.std.os.windows] windows
- [SW.std.os.linux] linux

Dominio de seguridad

- [base] COPEU

Datos

BAJO WINDOWS	Microsoft Office 2007

Descripción

Sirven para trabajos de oficina: procesamiento de texto, hojas de cálculo, presentaciones electrónicas etc.

Superiores (activos que dependen de este)

- [AH_COPEU] AHORRO
- [CR_COPEU] CREDITO
- [PAGAGI_COPEU] PAGO AGIL COPEU
- [SOLA_COPEU] SOAT LATINA

Inferiores (activos de los que depende este)

- [SCE_COPEU] SERVIDOR DE CORREO ELECTRONICO
- [SAC_COPEU] SERVIDOR DE ARCHIVO COMPARTIDO
- [SW.OTR_COPEU] OTRO SOFTWARE
- [HW.SBD_COPEU] SERVIDOR DE BASE DE DATOS

Valor

Dimensión	*valor*	*valores acumulados*
[D] disponibilidad	[1]	[9]
[I] integridad de los datos	[1]	[9]

[C] confidencialidad de los datos	[1]	[9]
[A] autenticidad de los usuarios y de la información	[1]	[9]
[T] trazabilidad del servicio y de los datos	[1]	[9]

5.9. [SW.AN_COPEU] ANTIVIRUS

- [D] Datos / Información
- [D.conf] datos de configuración
- [D.other] otros ...
- [SW] Aplicaciones (software)
- [SW.std] estándar (off the shelf)
- [SW.std.av] anti virus
- [SW.std.os] sistema operativo
- [SW.std.os.windows] windows
- [SW.std.os.linux] linux

Dominio de seguridad

- [base] COPEU

Datos

SOFTWARE	Avira Antivirus

Descripción

Programa cuya función es detectar y eliminar virus informáticos y otros programas maliciosos.

Superiores (activos que dependen de este)

- [AH_COPEU] AHORRO
- [CR_COPEU] CREDITO
- [PAGAGI_COPEU] PAGO AGIL COPEU
- [SOLA_COPEU] SOAT LATINA

Inferiores (activos de los que depende este)

- [SCE_COPEU] SERVIDOR DE CORREO ELECTRONICO
- [SAC_COPEU] SERVIDOR DE ARCHIVO COMPARTIDO
- [SW.OTR_COPEU] OTRO SOFTWARE
- [HW.SBD_COPEU] SERVIDOR DE BASE DE DATOS

Valor

Dimensión	***valor***	***valores acumulados***
[D] disponibilidad	[5]	[9]
[I] integridad de los datos	[5]	[9]
[C] confidencialidad de los datos	[5]	[9]
[A] autenticidad de los usuarios y de la información	[5]	[9]

[T] trazabilidad del servicio y de los datos	[5]	[9]

5.10. [SW.OTR_COPEU] OTRO SOFTWARE

- [D] Datos / Información
- [D.conf] datos de configuración
- [D.acl] datos de control de acceso
- [D.other] otros ...
- [SW] Aplicaciones (software)
- [SW.std] estándar (off the shelf)
- [SW.std.os] sistema operativo
- [SW.std.os.windows] windows
- [SW.std.os.linux] linux
- [SW.std.other] otros ...

Dominio de seguridad

- [base] COPEU

Datos

SOFTWARE 1	Adobe Reader
SOFTWARE 2	My SQL
SOFTWARE 3	Project

Descripción

Estos programas son utilizados por la Cooperativa a menudo.

Superiores (activos que dependen de este)

- [AR_COPEU] ACCESO REMOTO
- [IN_COPEU] INTERNET
- [SW.OF_COPEU] OFIMATICA
- [SW.AN_COPEU] ANTIVIRUS

Inferiores (activos de los que depende este)

- [HW.COM_COPEU] COMPUTADORAS DE ESCRITORIO
- [HW.COMPO_COPEU] COMPUTADORAS PORTATILES

Valor

Dimensión	***valor***	***valores acumulados***
[D] disponibilidad	[3]	[9]
[I] integridad de los datos	[3]	[9]
[C] confidencialidad de los datos	[3]	[9]
[A] autenticidad de los usuarios y de la información	[3]	[9]
[T] trazabilidad del servicio y de los datos	[3]	[9]

5.11. [HW.SBD_COPEU] SERVIDOR DE BASE DE DATOS

- [HW] Equipamiento informático (hardware)
- [HW.host] grandes equipos (host)
- [HW.data] que almacena datos

Dominio de seguridad

- [base] COPEU

Datos

NOMBRE	SQL-SERVER

Descripción

La base de datos contiene la información de los sistemas de caja, directivos, operaciones, etc.

Superiores (activos que dependen de este)

- [AR_COPEU] ACCESO REMOTO
- [IN_COPEU] INTERNET
- [SW.OF_COPEU] OFIMATICA
- [SW.AN_COPEU] ANTIVIRUS

Inferiores (activos de los que depende este)

- [HW.COM_COPEU] COMPUTADORAS DE ESCRITORIO
- [HW.COMPO_COPEU] COMPUTADORAS PORTATILES

Valor

Dimensión	***valor***	***valores acumulados***
[D] disponibilidad	[5]	[9]
[I] integridad de los datos	[5]	[9]
[C] confidencialidad de los datos	[5]	[9]
[A] autenticidad de los usuarios y de la información	[5]	[9]
[T] trazabilidad del servicio y de los datos	[5]	[9]

5.12. [HW.ROU_COPEU] ROUTER

- [HW] Equipamiento informático (hardware)
- [HW.network] soporte de la red
- [HW.network.router] encaminador
- [HW.network.gtwy] pasarela
- [HW.network.wap] punto de acceso wireless

Dominio de seguridad

- [base] COPEU

Datos

MARCA	D-Link
PROPIETARIO	COPEU
CANTIDAD	2

Descripción

Un Router es el hardware que sirve para rutear direcciones, dar salida a internet a un switch o directamente a una PC así como también permiten interconectar tanto redes de área local como redes de área extensa.

Superiores (activos que dependen de este)

- [HW.COM_COPEU] COMPUTADORAS DE ESCRITORIO
- [HW.COMPO_COPEU] COMPUTADORAS PORTATILES

Inferiores (activos de los que depende este)

- [COM.REDLA_COPEU] RED LAN
- [COM.REDWA_COPEU] RED WAN
- [COM.INT_COPEU] INTERNET COPEU
- [AUX.CABDAT_COPEU] CABLEADO DE DATOS COPEU
- [AUX.EQUAUX_COPEU] EQUIPAMIENTO AUXILIAR
- [USR_COPEU] UNIDAD DE SISTEMAS Y REDES COPEU

Valor

Dimensión	***valor***	***valores acumulados***
[D] disponibilidad	[1]	[9]
[I] integridad de los datos	[1]	[9]
[C] confidencialidad de los datos	[1]	[9]
[A] autenticidad de los usuarios y de la información	[1]	[9]
[T] trazabilidad del servicio y de los datos	[1]	[9]

5.13. [HW.SWI_COPEU] SWITCH

- [HW] Equipamiento informático (hardware)
- [HW.network] soporte de la red
- [HW.network.switch] conmutador

Dominio de seguridad

- [base] COPEU

Datos

MARCA	D-Link
PROPIETARIO	COPEU
CANTIDAD	4

Descripción

Un Switch es el hardware que sirve para conectar dos o más computadoras para compartir recursos.

Superiores (activos que dependen de este)

- [HW.COM_COPEU] COMPUTADORAS DE ESCRITORIO
- [HW.COMPO_COPEU] COMPUTADORAS PORTATILES

Inferiores (activos de los que depende este)

- [COM.REDLA_COPEU] RED LAN
- [COM.REDWA_COPEU] RED WAN
- [COM.INT_COPEU] INTERNET COPEU
- [AUX.CABDAT_COPEU] CABLEADO DE DATOS COPEU
- [AUX.EQUAUX_COPEU] EQUIPAMIENTO AUXILIAR
- [USR_COPEU] UNIDAD DE SISTEMAS Y REDES COPEU

Valor

Dimensión	***valor***	***valores acumulados***
[D] disponibilidad	[1]	[9]
[I] integridad de los datos	[1]	[9]
[C] confidencialidad de los datos	[1]	[9]
[A] autenticidad de los usuarios y de la información	[1]	[9]
[T] trazabilidad del servicio y de los datos	[1]	[9]

5.14. [HW.FIR_COPEU] FIREWALL

- [HW] Equipamiento informático (hardware)
- [HW.network] soporte de la red
- [HW.network.firewall] cortafuegos

Dominio de seguridad

- [base] COPEU

Datos

SISTEMA OPERATIVO	Windows Server 2003
PROPIETARIO	COPEU
CANTIDAD	1

Descripción

Un cortafuegos (o firewall en inglés) es una parte de un sistema o una red que está diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Superiores (activos que dependen de este)

- [HW.COM_COPEU] COMPUTADORAS DE ESCRITORIO
- [HW.COMPO_COPEU] COMPUTADORAS PORTATILES

Inferiores (activos de los que depende este)

- [COM.REDLA_COPEU] RED LAN
- [COM.REDWA_COPEU] RED WAN
- [COM.INT_COPEU] INTERNET COPEU
- [AUX.CABDAT_COPEU] CABLEADO DE DATOS COPEU
- [AUX.EQUAUX_COPEU] EQUIPAMIENTO AUXILIAR
- [USR_COPEU] UNIDAD DE SISTEMAS Y REDES COPEU

Valor

Dimensión	***valor***	***valores acumulados***
[D] disponibilidad	[1]	[9]
[I] integridad de los datos	[1]	[9]
[C] confidencialidad de los datos	[1]	[9]
[A] autenticidad de los usuarios y de la información	[1]	[9]
[T] trazabilidad del servicio y de los datos	[1]	[9]

5.15. [HW.COM_COPEU] COMPUTADORAS DE ESCRITORIO

- [HW] Equipamiento informático (hardware)
- [HW.mid] equipos medios
- [HW.pc] informática personal

Dominio de seguridad

- [base] COPEU

Datos

MARCA	Intel
PROCESADOR	Intel Core Duo
MEMORIA RAM	1.99GB RAM
DISCO DURO	320GB
SISTEMA OPERATIVO	Windows XP Profesional Service Pack 3

Descripción

Son computadoras de escritorio para instalar Windows o Linux que se utilizan para ejecutar las operaciones diarias de la Cooperativa por lo general son Intel puros.

Superiores (activos que dependen de este)

- [SCE_COPEU] SERVIDOR DE CORREO ELECTRONICO
- [SAC_COPEU] SERVIDOR DE ARCHIVO COMPARTIDO
- [SW.OTR_COPEU] OTRO SOFTWARE
- [HW.SBD_COPEU] SERVIDOR DE BASE DE DATOS

Inferiores (activos de los que depende este)

- [HW.ROU_COPEU] ROUTER
- [HW.SWI_COPEU] SWITCH
- [HW.FIR_COPEU] FIREWALL
- [HW.IMPLA_COPEU] IMPRESORA A LASER
- [HW.IMPMA_COPEU] IMPRESORA MATRICIAL

Valor

Dimensión	***valor***	***valores acumulados***
[D] disponibilidad	[4]	[9]
[I] integridad de los datos	[4]	[9]
[C] confidencialidad de los datos	[4]	[9]
[A] autenticidad de los usuarios y de la información	[4]	[9]
[T] trazabilidad del servicio y de los datos	[4]	[9]

5.16. [HW.COMPO_COPEU] COMPUTADORAS PORTATILES

- [HW] Equipamiento informático (hardware)
- [HW.pc] informática personal
- [HW.mobile] informática móvil

Dominio de seguridad

- [base] COPEU

Datos

MARCA	Toshiba – Hacer
PROCESADOR	Intel Core Duo
MEMORIA RAM	1.99GB RAM
DISCO DURO	320GB
SISTEMA OPERATIVO	Windows 7 Enterprise Edition

Descripción

Sirven para realizar trabajos diarios aplicativo – Institucional.

Superiores (activos que dependen de este)

- [SCE_COPEU] SERVIDOR DE CORREO ELECTRONICO
- [SAC_COPEU] SERVIDOR DE ARCHIVO COMPARTIDO
- [SW.OTR_COPEU] OTRO SOFTWARE
- [HW.SBD_COPEU] SERVIDOR DE BASE DE DATOS

Inferiores (activos de los que depende este)

- [HW.ROU_COPEU] ROUTER
- [HW.SWI_COPEU] SWITCH
- [HW.FIR_COPEU] FIREWALL
- [HW.IMPLA_COPEU] IMPRESORA A LASER
- [HW.IMPMA_COPEU] IMPRESORA MATRICIAL

Valor

Dimensión	*valor*	*valores acumulados*
[D] disponibilidad	[1]	[9]
[I] integridad de los datos	[1]	[9]
[C] confidencialidad de los datos	[1]	[9]
[A] autenticidad de los usuarios y de la información	[1]	[9]
[T] trazabilidad del servicio y de los datos	[1]	[9]

5.17. [HW.IMPLA_COPEU] IMPRESORA A LASER

- [HW] Equipamiento informático (hardware)
- [HW.mid] equipos medios
- [HW.mobile] informática móvil
- [HW.peripheral] periféricos
- [HW.peripheral.print] medios de impresión

Dominio de seguridad

- [base] COPEU

Datos

MARCA	Samsung
MODELO	ML1665
CANTIDAD	6

Descripción

Son impresoras que sirven para reportes del módulo crédito, SOAT, Pago Agil.

Superiores (activos que dependen de este)

- [HW.COM_COPEU] COMPUTADORAS DE ESCRITORIO
- [HW.COMPO_COPEU] COMPUTADORAS PORTATILES

Inferiores (activos de los que depende este)

- [COM.REDLA_COPEU] RED LAN
- [COM.REDWA_COPEU] RED WAN
- [COM.INT_COPEU] INTERNET COPEU
- [AUX.CABDAT_COPEU] CABLEADO DE DATOS COPEU
- [AUX.EQUAUX_COPEU] EQUIPAMIENTO AUXILIAR
- [USR_COPEU] UNIDAD DE SISTEMAS Y REDES COPEU

Valor

Dimensión	*valor*	*valores acumulados*
[D] disponibilidad	[1]	[9]
[I] integridad de los datos	[1]	[9]

[C] confidencialidad de los datos	[1]	[9]
[A] autenticidad de los usuarios y de la información	[1]	[9]
[T] trazabilidad del servicio y de los datos	[1]	[9]

5.18. [HW.IMPMA_COPEU] IMPRESORA MATRICIAL

- [HW] Equipamiento informático (hardware)
- [HW.mid] equipos medios
- [HW.peripheral] periféricos
- [HW.peripheral.print] medios de impresión
- [HW.peripheral.scan] escáner

Dominio de seguridad

- [base] COPEU

Datos

MARCA	Epson
MODELO	LX300
CANTIDAD	4

Descripción

Estas son utilizadas en las oficinas ya que soporta un gran volumen de impresión diaria.

Superiores (activos que dependen de este)

- [HW.COM_COPEU] COMPUTADORAS DE ESCRITORIO
- [HW.COMPO_COPEU] COMPUTADORAS PORTATILES

Inferiores (activos de los que depende este)

- [COM.REDLA_COPEU] RED LAN
- [COM.REDWA_COPEU] RED WAN
- [COM.INT_COPEU] INTERNET COPEU
- [AUX.CABDAT_COPEU] CABLEADO DE DATOS COPEU
- [AUX.EQUAUX_COPEU] EQUIPAMIENTO AUXILIAR
- [USR_COPEU] UNIDAD DE SISTEMAS Y REDES COPEU

Valor

Dimensión	***valor***	***valores acumulados***
[D] disponibilidad	[1]	[9]
[I] integridad de los datos	[1]	[9]
[C] confidencialidad de los datos	[1]	[9]
[A] autenticidad de los usuarios y de la información	[1]	[9]
[T] trazabilidad del servicio y de los datos	[1]	[9]

5.19. [COM.REDLA_COPEU] RED LAN

- [COM] Redes de comunicaciones
- [COM.LAN] red local

Dominio de seguridad

- [base] COPEU

Datos

INTERCONEXIÓN	Computadoras y Periféricos
DISTANCIA	100 metros

Descripción

Permite conectar los equipos y compartir información.

Superiores (activos que dependen de este)

- [HW.ROU_COPEU] ROUTER
- [HW.SWI_COPEU] SWITCH
- [HW.FIR_COPEU] FIREWALL
- [HW.IMPLA_COPEU] IMPRESORA A LASER
- [HW.IMPMA_COPEU] IMPRESORA MATRICIAL

Valor

Dimensión	***valor***	***valores acumulados***
[D] disponibilidad	[2]	[9]
[I] integridad de los datos	[2]	[9]
[C] confidencialidad de los datos	[2]	[9]
[A] autenticidad de los usuarios y de la información	[2]	[9]
[T] trazabilidad del servicio y de los datos	[2]	[9]

5.20. [COM.REDWA_COPEU] RED WAN

- [COM] Redes de comunicaciones
- [COM.WAN] red de área amplia

Dominio de seguridad

- [base] COPEU

Datos

INTERCONEXIÓN	Sucursal
Distancia	100 a 1000 kilómetros

Descripción

Permite conectarse con la sucursal de la Castillo desde la Principal en Ingahurco.

Superiores (activos que dependen de este)

- [HW.ROU_COPEU] ROUTER
- [HW.SWI_COPEU] SWITCH
- [HW.FIR_COPEU] FIREWALL
- [HW.IMPLA_COPEU] IMPRESORA A LASER
- [HW.IMPMA_COPEU] IMPRESORA MATRICIAL

Valor

Dimensión	***valor***	***valores acumulados***
[D] disponibilidad	[2]	[9]
[I] integridad de los datos	[2]	[9]
[C] confidencialidad de los datos	[2]	[9]
[A] autenticidad de los usuarios y de la información	[2]	[9]
[T] trazabilidad del servicio y de los datos	[2]	[9]

5.21. [COM.INT_COPEU] INTERNET COPEU

- [COM] Redes de comunicaciones
- [COM.Internet] Internet
- [COM.vpn] red privada virtual

Dominio de seguridad

- [base] COPEU

Datos

TIPO	Inalámbrico
MODELO	1 en 1 sin compresión
CANTIDAD	1
ISP INTERNET SERVICE PROVIDE	CNT, Telconet

Descripción

Sirve para acceso transaccional transferencia de archivos y navegación por la Web.

Superiores (activos que dependen de este)

- [HW.ROU_COPEU] ROUTER
- [HW.SWI_COPEU] SWITCH
- [HW.FIR_COPEU] FIREWALL
- [HW.IMPLA_COPEU] IMPRESORA A LASER
- [HW.IMPMA_COPEU] IMPRESORA MATRICIAL

Valor

Dimensión	***valor***	***valores acumulados***
[D] disponibilidad	[2]	[9]
[I] integridad de los datos	[2]	[9]

[C] confidencialidad de los datos	[2]	[9]
[A] autenticidad de los usuarios y de la información	[2]	[9]
[T] trazabilidad del servicio y de los datos	[2]	[9]

5.22. [AUX.CABDAT_COPEU] CABLEADO DE DATOS COPEU

- [AUX] Equipamiento auxiliar
- [AUX.cabling] cableado de datos
- [AUX.cabling.wire] cable eléctrico
- [AUX.cabling.fiber] fibra óptica

Dominio de seguridad

- [base] COPEU

Datos

MARCA	Panduit
CATEGORÍA	6A

Descripción

El cableado de datos es fundamental para la trasferencia de archivos y por ende para el funcionamiento de la Cooperativa.

Superiores (activos que dependen de este)

- [HW.ROU_COPEU] ROUTER
- [HW.SWI_COPEU] SWITCH
- [HW.FIR_COPEU] FIREWALL
- [HW.IMPLA_COPEU] IMPRESORA A LASER
- [HW.IMPMA_COPEU] IMPRESORA MATRICIAL

Valor

Dimensión	***valor***	***valores acumulados***
[D] disponibilidad	[2]	[9]
[I] integridad de los datos	[2]	[9]
[C] confidencialidad de los datos	[2]	[9]
[A] autenticidad de los usuarios y de la información	[2]	[9]
[T] trazabilidad del servicio y de los datos	[2]	[9]

5.23. [AUX.EQUAUX_COPEU] EQUIPAMIENTO AUXILIAR

- [AUX] Equipamiento auxiliar
- [AUX.other] otros ...

Dominio de seguridad

- [base] COPEU

Datos

EQUIPO	Cámaras de Vigilancia
EQUIPO	Extintores
EQUIPO	Botiquines de Primeros Auxilios

Descripción

Los equipos auxiliares con los que cuenta la Cooperativa son los mencionados anteriormente.

Superiores (activos que dependen de este)

- [HW.ROU_COPEU] ROUTER
- [HW.SWI_COPEU] SWITCH
- [HW.FIR_COPEU] FIREWALL
- [HW.IMPLA_COPEU] IMPRESORA A LASER
- [HW.IMPMA_COPEU] IMPRESORA MATRICIAL

Valor

Dimensión	***valor***	***valores acumulados***
[D] disponibilidad	[2]	[9]
[I] integridad de los datos	[2]	[9]
[C] confidencialidad de los datos	[2]	[9]
[A] autenticidad de los usuarios y de la información	[2]	[9]
[T] trazabilidad del servicio y de los datos	[2]	[9]

5.24. [PAGAGI_COPEU] PAGO AGIL COPEU

- [S] Servicios
- [S.pub] al público en general (sin relación contractual)
- [S.www] world wide web

Dominio de seguridad

- [base] COPEU

Datos

ENLACE	Web
SERVICIO	Pago de SRI, IESS, Servipagos, CNT, Yanbal, Bono de Desarrollo Humano, Produbanco, RISE, Avon, TV CABLE, Movistar, Claro, Alegro, Matriculación Vehicular, Empresa Eléctrica.
INGRESO AL SISTEMA	Vía web mediante claves de acceso

Descripción

Este es un servicio muy utilizado ya que podemos realizar el pago de cualquiera de los servicios que mencionamos anteriormente.

Inferiores (activos de los que depende este)

- [AR_COPEU] ACCESO REMOTO
- [IN_COPEU] INTERNET
- [SW.OF_COPEU] OFIMATICA
- [SW.AN_COPEU] ANTIVIRUS

Valor

Dimensión	***valor***	***valores acumulados***
[D] disponibilidad	[4]	[4]
[I] integridad de los datos	[4]	[4]
[C] confidencialidad de los datos	[4]	[4]
[A] autenticidad de los usuarios y de la información	[4]	[4]
[T] trazabilidad del servicio y de los datos	[4]	[4]

5.25. [SOLA_COPEU] SOAT LATINA

- [S] Servicios
- [S.pub] al público en general (sin relación contractual)
- [S.www] world wide web

Dominio de seguridad

- [base] COPEU

Datos

ENLACE	Web
SERVICIO	SOAT
INGRESO AL SISTEMA	Vía web usando claves de acceso para ingresar al sistema

Descripción

Es una empresa dedicada a la venta de seguros de vehículos SOAT (Seguro Obligatorio de Accidentes de Tránsito).

Inferiores (activos de los que depende este)

- [AR_COPEU] ACCESO REMOTO
- [IN_COPEU] INTERNET
- [SW.OF_COPEU] OFIMATICA
- [SW.AN_COPEU] ANTIVIRUS

Valor

Dimensión	***valor***	***valores acumulados***
[D] disponibilidad	[4]	[4]
[I] integridad de los datos	[4]	[4]

[C] confidencialidad de los datos	[4]	[4]
[A] autenticidad de los usuarios y de la información	[4]	[4]
[T] trazabilidad del servicio y de los datos	[4]	[4]

5.26. [USR_COPEU] UNIDAD DE SISTEMAS Y REDES COPEU

- [L] Instalaciones
- [L.local] cuarto

Dominio de seguridad

- [base] COPEU

Datos

TIPO	Edifico adecuado
DIRECCIÓN	Ingahurco El Salvador 05-39 y Av. Colombia, lateral a la UTA
TELÉFONO	032520861

Descripción

En esta unidad se encuentra todo lo que es material, elementos y equipos informáticos de la Cooperativa además igual es la Matriz donde también atienden al público en general.

Superiores (activos que dependen de este)

- [HW.ROU_COPEU] ROUTER
- [HW.SWI_COPEU] SWITCH
- [HW.FIR_COPEU] FIREWALL
- [HW.IMPLA_COPEU] IMPRESORA A LASER
- [HW.IMPMA_COPEU] IMPRESORA MATRICIAL

Valor

Dimensión	***valor***	***valores acumulados***
[D] disponibilidad	[7]	[9]
[I] integridad de los datos	[7]	[9]
[C] confidencialidad de los datos	[7]	[9]
[A] autenticidad de los usuarios y de la información	[7]	[9]
[T] trazabilidad del servicio y de los datos	[7]	[9]

5.27. [ADSFYBD_COPEU] ADMINISTRACION SISTEMA FINANCIERO Y BASE DE DATOS

- [P] Personal
- [P.adm] administradores de sistemas
- [P.com] administradores de comunicaciones
- [P.dba] administradores de BBDD

Dominio de seguridad

- [base] COPEU

Datos

RESPONSABLE	Ing. Francisco Mena
RESPONSABLE	Ing. Cristina Guerra

Descripción

Son los encargados de manejar El Sistema y Base de Datos de la Cooperativa.

Valor

Dimensión	***valor***	***valores acumulados***
[D] disponibilidad	[4]	[4]
[I] integridad de los datos	[4]	[4]
[C] confidencialidad de los datos	[4]	[4]
[A] autenticidad de los usuarios y de la información	[4]	[4]
[T] trazabilidad del servicio y de los datos	[4]	[4]

5.28. [SU_COPEU] SOPORTE A USUARIO

- [P] Personal
- [P.ui] usuarios internos

Dominio de seguridad

- [base] COPEU

Datos

RESPONSABLE	Ing. Miriam Peñaherrera

Descripción

Es la encargada de dar soporte a problemas o fallos que puede tener tanto la base de datos como el sistema mismo.

Valor

Dimensión	***valor***	***valores acumulados***
[D] disponibilidad	[4]	[4]
[I] integridad de los datos	[4]	[4]
[C] confidencialidad de los datos	[4]	[4]
[A] autenticidad de los usuarios y de la información	[4]	[4]
[T] trazabilidad del servicio y de los datos	[4]	[4]

ANEXO 4

Declaración de Aplicabilidad

proyecto: [AGR_COPEU] ANALISIS Y GESTION DE RIESGOS SISTEMA DE LA COOPERATIVA COPEU

1. Datos del proyecto

AGR_COPEU	ANALISIS Y GESTION DE RIESGOS SISTEMA DE LA COOPERATIVA COPEU
Descripción	Analisis al Sistema
Responsable	Carlos Andres Simbaya Camacho
Organización	Cooperativa de Ahorro y Credito Universitaria Limitada
Versión	5.2.9
Fecha	07-10-2013
Biblioteca	[std] Biblioteca INFOSEC (28.8.2012)

Licencia

[edu] UTA
Universidad Técnica de Ambato
Facultad de Ingeniería en Sistemas, Electrónica e Industrial
[... 31.12.2014]

2. Dominios de seguridad

- [base] COPEU

3. Dominio de seguridad: [base] COPEU

código	***Salvaguarda***
H	Protecciones Generales
H.IA	Identificación y autenticación
H.IA.1	Se dispone de normativa de identificación y autenticación
H.IA.2	Se dispone de procedimientos para las tareas de identificación y autenticación
H.IA.3	Identificación de los usuarios
H.IA.4	Cuentas especiales (administración)
H.IA.5	Gestión de la identificación y autenticación de usuario
H.IA.5.1	Se mantiene un registro de todos los usuarios con su identificador
H.IA.5.2	Alta, activación, modificación y baja de las cuentas de usuario
H.IA.5.3	Se comprueba la identidad de los usuarios y los privilegios requeridos antes de entregar el autenticador
H.IA.5.4	Se limita el número de autenticadores necesarios por usuario
H.IA.5.5	Los autenticadores se distribuyen de forma segura
H.IA.5.6	El usuario se compromete por escrito a mantener la confidencialidad del autenticador
H.IA.5.7	El usuario confirma la recepción del autenticador
H.IA.5.8	El usuario se hace cargo personalmente del control del autenticador
H.IA.5.9	Existen canales para la comunicación de incidentes que afecten a los autenticadores (pérdida, vulneración, etc.)
H.IA.5.a	Las cuentas se suspenden al ser comprometidas o existir sospecha de ello
H.IA.6	{xor} Factores de autenticación que se requieren:
H.IA.6.1	Algo que se tiene (ej. tarjeta)

H.IA.6.2	Algo que se conoce (ej. contraseña)
H.IA.6.3	2 factores: algo que se tiene + algo que se sabe
H.IA.6.4	Algo que se es (ej. huella dactilar)
H.IA.6.5	2 factores: algo que se sabe + algo que se es
H.IA.6.6	2 factores: algo que se tiene + algo que se es
H.IA.6.7	3 factores: algo que se sabe + algo que se tiene + algo que se es
H.IA.7	{or} Mecanismo de autenticación
H.IA.7.1	Contraseñas
H.IA.7.1.1	El usuario elige su propia contraseña
H.IA.7.1.2	Se seleccionan contraseñas fáciles de recordar pero de difícil conjetura
H.IA.7.1.3	Los usuarios se responsabilizan de la confidencialidad de las contraseñas
H.IA.7.1.4	Se dispone de un mecanismo para la comprobación de la robustez de las contraseñas
H.IA.7.1.5	La misma contraseña no se utiliza en diferentes sitios
H.IA.7.1.6	No se reciclan contraseñas usadas con anterioridad
H.IA.7.1.7	Se emplean diferentes contraseñas para uso privado y para desarrollar las funciones en la organización
H.IA.7.1.8	{xor} Las contraseñas tienen una duración limitada
H.IA.7.1.9	Las contraseñas de usuarios administradores se cambian con mayor frecuencia
H.IA.7.1.a	Las contraseñas se modifican al ser comprometidas o existir sospecha de ello
H.IA.7.1.b	Contraseñas iniciales
H.IA.7.1.c	La información de verificación está protegida
H.IA.7.1.d	Las contraseñas de administración se custodian en cajas de seguridad
H.IA.7.2	{xor} Contraseñas de un sólo uso (OTP: one time password)
H.IA.7.3	{xor} Certificados (criptografía de clave pública)
H.IA.7.4	Biometría
H.AC	Control de acceso lógico
H.AC.1	Se dispone de normativa para el control de accesos
H.AC.2	Se dispone de procedimientos para las tareas de control de accesos
H.AC.3	Se definen y documentan las autorizaciones de acceso
H.AC.4	Restricción de acceso a la información
H.AC.5	Se restringe el uso de las utilidades del sistema
H.AC.6	Se restringe el acceso a la configuración del sistema
H.AC.7	Se controla el trabajo fuera del horario normal
H.AC.8	Gestión de privilegios
H.AC.8.1	Se identifican los perfiles de acceso y sus privilegios asociados
H.AC.8.2	En la asignación de privilegios se tiene en cuenta el principio de 'privilegio mínimo necesario para realizar las tareas asignadas'
H.AC.8.3	En la asignación de privilegios se tiene en cuenta el principio de 'necesidad de conocer'
H.AC.8.4	Los derechos de acceso son aprobados por el propietario del servicio o de la información
H.AC.8.5	La comunicación de sus derechos a los usuarios consta por escrito
H.AC.8.6	Los usuarios reconocen por escrito que conocen y aceptan sus derechos
H.AC.8.7	Se separan las responsabilidades de administración y operación
H.AC.8.8	Se mantiene un registro de los privilegios de acceso
H.AC.8.9	El sistema mantiene los privilegios asociados a cada usuario

H.AC.8.a	Los privilegios se anulan cuando termina la autorización
H.AC.8.b	Los privilegios se revisan cuando el usuario cambia de responsabilidades o de función
H.AC.8.c	Los privilegios se anulan cuando el usuario abandona la organización
H.AC.9	Revisión de los derechos de acceso de los usuarios
H.AC.a	{xor} Modelo de control de acceso
H.AC.a.1	Control de acceso discrecional (DAC)
H.AC.a.2	Control de acceso obligatorio (MAC)
H.AC.a.3	Control de acceso por rol (RBAC)
H.AC.b	Canal seguro de autenticación
H.AC.c	Conexión en terminales (logon)
H.AC.c.1	Se restringen usuarios y grupos de usuarios a ciertas estaciones
H.AC.c.2	Tras un intento fallido existe un retardo hasta que el siguiente intento sea posible
H.AC.c.3	Se bloquea la cuenta tras un número limitado de intentos fallidos
H.AC.c.4	Se requiere autorización para restablecer una cuenta bloqueada
H.AC.c.5	Se limita el tiempo permitido para efectuar el proceso de conexión
H.AC.c.6	Sólo se presenta la mínima información imprescindible durante el proceso de conexión
H.AC.c.7	Sólo se solicita la mínima información imprescindible para conectarse
H.AC.c.8	No se ofrecen mensajes de ayuda durante la conexión
H.AC.c.9	No se muestra identificación alguna del sistema o aplicación hasta que termina el proceso de conexión
H.AC.c.a	Se valida la información de conexión sólo tras rellenar todos los datos de entrada
H.AC.c.b	Se presenta un mensaje indicando el uso debido del sistema
H.AC.c.c	Se presenta un mensaje indicando que queda prohibido todo uso no autorizado
H.AC.c.d	Se presenta un mensaje indicando que toda la actividad podrá ser supervisada
H.AC.c.e	Tras la conexión, se muestra la fecha y hora de la anterior conexión realizada con éxito
H.AC.c.f	Tras la conexión, se muestran los intentos fallidos
H.AC.c.g	Las contraseñas no pueden ser almacenadas en ningún proceso automático (macros, teclas de función, etc.)
H.AC.d	Se limita el tiempo de conexión
H.AC.e	Se limita el número de sesiones concurrentes de un usuario
H.AC.f	Equipo informático de usuario desatendido
H.AC.f.1	Concienciación de los usuarios
H.AC.f.2	Bloqueo de la pantalla al dejar desatendido el equipo
H.AC.f.3	Cancelación o bloqueo de sesiones al dejar desatendido el equipo
H.AC.f.4	Los equipos se desconectan y se apagan al finalizar las actividades
H.AC.g	Los terminales se desconectan automáticamente
H.ST	Segregación de tareas
H.ST.1	Todos los procesos críticos requieren al menos 2 personas
H.ST.2	Se definen roles con autorización exclusiva para realizar tareas
H.ST.3	Se controla la efectividad de la estructura de segregación
H.IR	Gestión de incidencias
H.IR.1	Se dispone de normativa de actuación para la gestión de incidencias
H.IR.2	Se dispone de procedimientos para la gestión de incidencias

H.IR.2.1	Actuación frente a código dañino
H.IR.2.2	Actuación frente a ataques de denegación de servicio (DoS)
H.IR.2.3	Actuación ante fallos del sistema e interrupciones del servicio
H.IR.2.4	Actuación ante errores que resulten de datos del negocio inexactos o incompletos
H.IR.2.5	Actuación frente a violaciones de la confidencialidad
H.IR.2.6	Actuación frente a otros incidentes
H.IR.3	El fallo del sistema deja a este en un estado controlado
H.IR.4	Ayuda a los afectados
H.IR.5	Gestión de la incidencia
H.IR.5.1	Se suspenden cautelarmente los trabajos en el sistema afectado
H.IR.5.2	Se identifica y analiza la causa
H.IR.5.3	Se analiza el impacto del incidente
H.IR.5.4	Se planifica la implantación de medidas correctoras
H.IR.5.5	Hay comunicación con los afectados por la incidencia
H.IR.5.6	Hay comunicación con los implicados en la recuperación de la incidencia
H.IR.5.7	Se informa de las acciones a la autoridad respectiva de la organización
H.IR.5.8	Evidencias
H.IR.6	Comunicación de las incidencias de seguridad
H.IR.7	Comunicación de las deficiencias de seguridad
H.IR.8	Comunicación de los fallos del software
H.IR.9	Se dispone de un registro de incidencias
H.IR.a	Los fallos y las medidas correctoras se registran y se revisan
H.IR.b	Control formal del proceso de recuperación ante el incidente
H.IR.c	Concienciación en la detección y reporte de incidentes
H.IR.d	Formación del personal en detección y gestión de incidentes
H.IR.e	Se prueban regularmente los procedimientos de gestión de incidentes
H.IR.f	Se aprende de los incidentes
H.IR.g	Se toman medidas para prevenir la repetición
H.tools	Herramientas de seguridad
H.tools.AV	Herramienta contra código dañino
H.tools.AV.1	El programa se actualiza regularmente
H.tools.AV.2	La base de datos de virus se actualiza regularmente
H.tools.AV.3	Se revisan los programas y servicios de arranque del sistema
H.tools.AV.4	Se revisa cada aplicación cuando arranca
H.tools.AV.5	Se revisan los anexos al correo electrónico
H.tools.AV.6	Se revisa el contenido de las páginas web que se visitan
H.tools.AV.7	Se revisan todos los ficheros descargados
H.tools.AV.8	Se revisan los ficheros recibidos en un medio removible
H.tools.AV.9	Se revisan medios removibles cuando se conectan al sistema de información
H.tools.AV.a	Comprobación de virus desde diferentes puntos de la red
H.tools.AV.b	Se emplea un producto certificado o acreditado
H.tools.IDS	IDS/IPS: Herramienta de detección / prevención de intrusión
H.tools.CC	Herramienta de chequeo de configuración
H.tools.VA	Herramienta de análisis de vulnerabilidades
H.tools.TM	Herramienta de monitorización de tráfico
H.tools.LA	Herramienta para análisis de logs
H.tools.HP	Honey net / honey pot
H.tools.SFV	Verificación de las funciones de seguridad

H.VM	Gestión de vulnerabilidades
H.VM.1	Se dispone de personas dedicadas a la gestión de vulnerabilidades
H.VM.2	Se han previsto mecanismos para estar informados de vulnerabilidades ...
H.VM.3	Se realizan regularmente tests de penetración para calibrar la posibilidad de explotar las vulnerabilidades
H.VM.4	Se analiza el impacto potencial (estimación de riesgos)
H.VM.5	Se dispone de procedimientos de reacción
H.VM.6	Actuaciones
H.VM.6.1	Se reparan urgentemente las vulnerabilidades que implican un alto riesgo
H.VM.6.2	Se reparan con diligencia las vulnerabilidades que implican un cierto riesgo
H.VM.6.3	Se planifica la reparación de las vulnerabilidades que implican un riesgo bajo
H.AU	Registro y auditoría
H.AU.1	Se dispone de normativa acerca del registro y la auditoría
H.AU.2	Se dispone de procedimientos para las tareas de auditoría y registro de actividad
H.AU.3	Gestión de las actividades de registro y auditoría
H.AU.4	Protección de las herramientas de auditoría de sistemas
H.AU.5	Prevención del mal uso de los mecanismos de registro de actividad
H.AU.6	Se dispone de un registro de actividad
H.AU.7	Se monitoriza el uso de los sistemas
H.AU.8	Diarios de operación
H.AU.9	Sincronización de relojes
H.AU.a	Consolidación y reporte
H.AU.b	Protección de los registros
H.AU.c	Destrucción de los registros

código	***Salvaguarda***
D	Protección de la Información
D.1	Se dispone de un inventario de activos de información
D.2	Se clasifica la información
D.3	Security attributes
D.3.1	The information system supports and maintains the binding of security attributes to information in storage, in process, and in transmission
D.3.2	The information system associates security attributes with information exchanged between information systems
D.4	IPR: Se protegen los derechos de propiedad intelectual de la información
D.5	Se dispone de normativa de retención de datos
D.A	Copias de seguridad de los datos (backup)
D.A.1	Se dispone de normativa relativa a copias de seguridad (backup)
D.A.2	Se dispone de procedimientos para las tareas de realización de copias de seguridad (backup), su protección y su conservación
D.A.3	Gestión de las copias de seguridad de los datos (backup)
D.A.3.1	Se hacen copias de la información en consonancia con sus requisitos de disponibilidad
D.A.3.2	Se hacen copias de las claves para descifrar
D.A.3.3	Se hacen copias de la información de verificación de firmas
D.A.3.4	Las copias de seguridad, y los procedimientos, se almacenan en lugares

	diferentes de tal forma que los datos originales y las copias no se vean afectados simultáneamente por un incidente
D.A.3.5	Las copias de seguridad se protegen de acuerdo a la información que contienen
D.A.3.6	Se cifran las copias de seguridad
D.A.3.7	El acceso a las copias de seguridad requiere autorización previa
D.A.3.8	Periódicamente, se verifican las copias de seguridad
D.A.3.9	Periódicamente, se prueban los procedimientos de restauración
D.A.4	{xor} Mecanismo de backup
D.I	Aseguramiento de la integridad
D.8	Limpieza de documentos publicados
D.C	Cifrado de la información
D.C.1	Se dispone de normativa relativa al uso de cifra
D.C.2	Se dispone de procedimientos relativos al cifrado de información
D.C.3	Se han designado responsables
D.C.4	{xor} Mecanismo de cifrado
D.DS	Uso de firmas electrónicas
D.DS.1	Se dispone de normativa sobre firma electrónica
D.DS.2	Se dispone de procedimientos para las trareas relacionadas con el empleo de firmas electrónicas
D.DS.3	Se han designado responsables
D.DS.4	Se garantiza la eficacia probatoria de la firma
D.DS.5	{xor} Certificados electrónicos
D.DS.6	{xor} Implantación de los algoritmos
D.DS.7	{xor} Mecanismo de firma electrónica

código	***Salvaguarda***
S	Protección de los Servicios
S.1	Se dispone de normativa relativa al uso de los servicios
S.2	Se dispone de un inventario de servicios
S.A	Aseguramiento de la disponibilidad
S.A.1	Se han previsto protecciones frente a ataques de denegación de servicio (DoS)
S.A.2	Los recursos se priorizan en base a la prioridad del servicio afectado
S.A.3	Continuidad de operaciones
S.A.3.1	Se analizan las implicaciones para la continuidad del negocio
S.A.3.2	Se establece un protocolo de actuación en caso de contingencia
S.A.3.3	Se dispone de medios alternativos
S.A.3.4	Los medios alternativos están sujetos a las mismas garantías de protección que los medios habituales
S.start	Aceptación y puesta en operación
S.SC	Se aplican perfiles de seguridad
S.op	Explotación
S.op.1	Prevención del repudio
S.op.2	El personal recibe formación específica en configuración de servicios
S.CM	Gestión de cambios (mejoras y sustituciones)
S.CM.1	Se dispone de normativa de control de cambios
S.CM.2	Se designan responsables

S.CM.3	Se dispone de procedimientos para ejecutar cambios
S.CM.4	Se hace un seguimiento permanente (servicios externos)
S.CM.5	Evaluación del impacto potencial del cambio
S.CM.6	Se mantiene en todo momento la regla de 'funcionalidad mínima'
S.CM.7	Se mantiene en todo momento la regla de 'seguridad por defecto'
S.CM.8	Se verifica que el cambio no inhabilita los mecanismos de detección, monitorización y registro
S.CM.9	Se planifica el cambio de forma que minimice la interrupción del servicio
S.CM.a	Se realiza por personal debidamente autorizado
S.CM.b	Se realizan pruebas de regresión
S.CM.c	Se registran las actualizaciones de servicios
S.CM.d	Documentación
S.CM.e	Se actualizan todos los procedimientos de producción afectados
S.CM.f	Se actualizan todos los procedimientos de recuperación afectados
S.end	Terminación
S.www	Protección de servicios y aplicaciones web
S.www.1	Se dispone de normativa de uso
S.www.2	Se ha designado al responsable del servicio
S.www.3	Se detectan casos de uso inaceptable
S.www.4	Se verifica regularmente que se cumple la política
S.www.5	Publicación electrónica de información
S.www.6	Se controla el acceso a la información
S.www.6.1	Se bloquea el acceso por otros protocolos
S.www.6.2	Se prevén ataques de manipulación de URLs
S.www.6.3	Se prevén ataques de inyección de código (scripting)
S.www.6.4	Se prevén ataques de consultas a bases de datos (sql-scripting)
S.www.6.5	Se prevén ataques en el cliente (por ejemplo, manipulación de 'cookies')
S.www.6.6	Se prevén ataques de escalado de privilegios
S.www.6.7	Se prevén ataques de "cross-site scripting"
S.www.6.8	Se prevén ataques en servidores "proxy"
S.www.6.9	Se prevén ataques en las "cachés"
S.www.7	Protección de la configuración
S.www.8	Se registra el uso del servicio
S.www.9	{or} Se asegura la disponibilidad del servicio según política
S.email	Protección del correo electrónico
S.email.1	Se dispone de normativa de uso
S.email.2	Se establece el responsable de la administración del servicio
S.email.3	Se detectan casos de uso inaceptable
S.email.4	Se verifica regularmente que se cumple la política
S.email.5	Se forma a los usuarios en el uso de los servicios
S.email.6	Se dispone de un procedimiento de actuación en caso de incumplimiento
S.email.7	Se aplican medidas disciplinarias en caso de incumplimiento
S.email.8	Se registra el uso del servicio
S.email.9	Protección de la información
S.email.9.1	Se protege la información en el cuerpo del mensaje
S.email.9.2	Se protege la información adjunta al mensaje
S.email.a	Protección de la configuración
S.email.b	Medidas anti-spam
S.email.c	Medidas frente a código dañino

S.email.c.1	En el servidor de correo
S.email.c.2	En los clientes de correo
S.email.d	Servicios de no repudio
S.email.e	{or} Se asegura la disponibilidad del servicio según política
S.b	Seguridad del comercio electrónico
S.b.1	Se tienen en cuenta los requisitos
S.b.2	Redacción y aprobación de un documento que consigne los términos acordados entre las partes
S.b.3	Controles sobre el desarrollo del proceso (fijación de precios, contratación, etc.)
S.b.4	Implantación de mecanismos de autenticación de las partes
S.b.5	Establecimiento de mecanismos de autorización del proceso
S.b.6	Se dispone de un registro de actividades
S.TW	Teletrabajo
S.TW.1	Se ha designado al responsable de la administración del servicio
S.TW.2	Se dispone de normativa de uso
S.TW.3	Se forma a los usuarios en el uso de los servicios
S.TW.4	Se detectan casos de uso inaceptable
S.TW.5	Se verifica regularmente que se cumple la política
S.TW.6	Se dispone de procedimientos para gestión del teletrabajo
S.TW.7	Se aplican medidas disciplinarias en caso de incumplimiento
S.TW.8	Se requiere autorización previa
S.TW.9	Estudio de las características específicas del emplazamiento
S.TW.9.1	Se analiza la seguridad física
S.TW.9.2	Se analiza el entorno
S.TW.9.3	Se previene el uso del puesto por otras personas (acceso no autorizado)
S.TW.9.4	Seguridad del puesto de usuario
S.TW.9.5	Instalación de software por parte de los usuarios
S.TW.9.6	Seguridad de las comunicaciones
S.TW.9.7	Conexión a redes particulares por parte de los usuarios

código	***Salvaguarda***
SW	Protección de las Aplicaciones Informáticas (SW)
SW.1	Se dispone de un inventario de aplicaciones (SW)
SW.2	Se dispone de normativa relativa a las aplicaciones (SW)
SW.3	Se dispone de procedimientos de uso de las aplicaciones
SW.4	IPR: Se protegen los derechos de propiedad intelectual de las aplicaciones (SW)
SW.A	Copias de seguridad (backup) (SW)
SW.start	Puesta en producción
SW.SC	Se aplican perfiles de seguridad
SW.op	Explotación / Producción
SW.op.1	Se dispone de normativa relativa al software en producción
SW.op.2	Los sistemas de producción no contienen herramientas de desarrollo
SW.op.3	{or} Se controla la integridad del código ejecutable
SW.op.4	El sistema emplea diferentes tecnologías de componentes para evitar puntos únicos de fallo tecnológico
SW.op.5	Aislamiento de sistemas que manejen asuntos delicados

SW.op.6	Seguridad de las aplicaciones
SW.op.6.1	Validación de los datos de entrada
SW.op.6.2	Se verifica la consistencia interna de los datos
SW.op.6.3	Validación de los datos de salida
SW.op.7	Seguridad de los ficheros de datos de la aplicación
SW.op.8	Se protegen los ficheros de configuración
SW.op.9	Se protegen los ficheros del sistema
SW.op.a	Se controla la ejecución de código móvil (ej. 'applets')
SW.op.b	Ejecución de programas colaborativos (ej. teleconferencia)
SW.op.c	Seguridad de los mecanismos de comunicación entre procesos
SW.op.d	Regularmente se realiza un análisis de vulnerabilidades, y se actúa en consecuencia
SW.op.e	Formación del personal en configuración de aplicaciones
SW.CM	Cambios (actualizaciones y mantenimiento)
SW.CM.1	Se dispone de una política
SW.CM.2	Se dispone de procedimientos para ejecutar cambios
SW.CM.3	Se hace un seguimiento permanente de actualizaciones y parches
SW.CM.4	Evaluación del impacto y riesgo residual tras el cambio
SW.CM.5	Se priorizan las actuaciones encaminadas a corregir riesgos elevados
SW.CM.6	Se mantiene en todo momento la regla de 'funcionalidad mínima'
SW.CM.7	Se mantiene en todo momento la regla de 'seguridad por defecto'
SW.CM.8	Se verifica que el cambio no inhabilita los mecanismos de detección, monitorización y registro
SW.CM.9	Se planifica el cambio de forma que minimice la interrupción del servicio
SW.CM.a	Control de versiones de toda actualización del software
SW.CM.b	Realización por personal debidamente autorizado
SW.CM.c	Se retienen copias de las versiones anteriores de software como medida de precaución para contingencias
SW.CM.d	Se retienen copias de las versiones anteriores de configuración
SW.CM.e	Se prueba previamente en un equipo que no esté en producción
SW.CM.f	Pruebas de regresión
SW.CM.g	Se registra toda actualización de SW
SW.CM.h	Documentación
SW.CM.i	Se actualizan todos los procedimientos de producción afectados
SW.CM.j	Se actualizan todos los procedimientos de recuperación afectados
SW.end	Terminación

código	***Salvaguarda***
HW	Protección de los Equipos Informáticos (HW)
HW.1	Se dispone de un inventario de equipos (HW)
HW.2	Se dispone de normativa sobre el uso correcto de los equipos
HW.3	Se dispone de procedimientos de uso del equipamiento
HW.start	Puesta en producción
HW.SC	Se aplican perfiles de seguridad
HW.A	Aseguramiento de la disponibilidad
HW.A.1	Se dimensiona holgadamente y se planifica la adquisición de repuestos
HW.A.2	El mantenimiento periódico se ajusta a las especificaciones de los fabricantes

HW.A.3	El mantenimiento lo realiza personal debidamente autorizado
HW.A.4	Se ejecutan regularmente las rutinas de diagnóstico
HW.A.5	Se monitorizan fallos e incidencias
HW.A.6	Se registran los fallos, reales o sospechados y de mantenimiento preventivo y correctivo
HW.A.7	Se hacen copias de seguridad de la configuración
HW.A.8	Se hacen copias de seguridad de las claves de descifrado
HW.A.9	{xor} Redundancia
HW.A.a	Las medios alternativos están sujetos a las mismas garantías de protección que los habituales
HW.A.b	Se establece un tiempo máximo para que los equipos alternativos entren en funcionamiento
HW.7	Contenedores criptográficos (HW, HW virtual)
HW.9	Instalación
HW.op	Operación
HW.op.1	Proceso de autorización de recursos para el tratamiento de la información
HW.op.2	El sistema emplea diferentes tecnologías de componentes para evitar puntos únicos de fallo tecnológico
HW.op.3	Protección física de los equipos
HW.op.4	Seguridad del equipamiento de oficina
HW.op.5	Seguridad de los equipos fuera de las instalaciones
HW.op.6	Protección de los dispositivos de red
HW.op.8	Formación del personal en configuración de equipos
HW.CM	Cambios (actualizaciones y mantenimiento)
HW.CM.1	Se dispone de una política
HW.CM.2	Se dispone de procedimientos para ejecutar cambios
HW.CM.3	Se siguen las recomendaciones del fabricante o proveedor
HW.CM.4	Se hace un seguimiento permanente de actualizaciones
HW.CM.5	Evaluación del impacto potencial del cambio
HW.CM.6	Se priorizan las actuaciones encaminadas a corregir riesgos elevados
HW.CM.7	Se mantiene en todo momento la regla de 'funcionalidad mínima'
HW.CM.8	Se mantiene en todo momento la regla de 'seguridad por defecto'
HW.CM.9	Se verifica que el cambio no inhabilita los mecanismos de detección, monitorización y registro
HW.CM.a	Se planifica el cambio de forma que minimice la interrupción del servicio
HW.CM.b	Realización por personal debidamente autorizado
HW.CM.c	Se retienen copias de las versiones anteriores de configuración
HW.CM.d	Se prueba previamente en un entorno que no esté en producción
HW.CM.e	Pruebas de regresión
HW.CM.f	Todos los cambios quedan registrados
HW.CM.g	Documentación
HW.CM.h	Control de versiones de todo cambio de hw
HW.CM.i	Se actualizan todos los procedimientos de producción afectados
HW.CM.j	Se actualizan todos los procedimientos de recuperación afectados
HW.end	Terminación
HW.PCD	Informática móvil
HW.PCD.1	Se mantiene un inventario de equipos móviles con identificación del responsable de cada uno
HW.PCD.2	Se requiere autorización previa antes de poder usarlos
HW.PCD.3	Cada equipo se marca con el nivel máximo de información que puede

	almacenar o procesar
HW.PCD.4	Se han identificado los riesgos correspondientes
HW.PCD.5	Se han determinado las medidas y precauciones a tomar
HW.PCD.6	Se sigue un plan de concienciación sobre los riesgos y las medidas pertinentes
HW.PCD.7	Se sigue un plan de formación sobre las medidas pertinentes
HW.PCD.8	Controles aplicables
HW.PCD.8.1	Se han determinado las medidas para la protección física del dispositivo
HW.PCD.8.2	Se instalan detectores de violación
HW.PCD.8.3	Se han establecido los requisitos sobre control de acceso
HW.PCD.8.4	Se utiliza un sistema de defensa perimetral (cortafuegos)
HW.PCD.8.5	Se han establecido los requisitos de cifrado
HW.PCD.8.6	Se han establecido los requisitos sobre copias de seguridad (backups)
HW.PCD.8.7	Se instala software antivirus y se mantiene actualizado
HW.PCD.9	Guías para los usuarios
HW.PCD.a	Gestión de incidencias en informática móvil
HW.print	Reproducción de documentos
HW.print.1	Control de los dispositivos de reproducción (fotocopiadoras, fax, etc.)
HW.print.2	Asignación de cuentas de usuario
HW.print.3	Destrucción ó borrado seguro de las partes de los dispositivos de reproducción que puedan contener información previamente a su sustitución
HW.print.4	Se requiere autorización previa para realizar copias, y numeración de las mismas
HW.print.5	Se registra y se revisa la actividad de los dispositivos de reproducción (número de copias, usuarios que las han realizado, etc.)
HW.h	Voz, facsímil y video
HW.h.1	Está prohibido establecer de conversaciones confidenciales en lugares públicos o sin adecuadas medidas de protección
HW.h.2	Está prohibido dejar mensajes confidenciales en contestadores automáticos
HW.h.3	Formación y concienciación en el uso seguro de los sistemas y recursoslos usuarios están concienciados y reciben formación sobre el uso seguro de los sistemas y recursos disponibles
HW.h.4	Se controla el acceso a la memoria interna del equipo de fax
HW.h.5	Se prohíbe la programación no autorizada del equipo de fax
HW.h.6	Se previene el envío de documentos a números equivocados

código	***Salvaguarda***
COM	Protección de las Comunicaciones
COM.1	Se dispone de un inventario de servicios de comunicación
COM.2	Se dispone de normativa sobre el uso correcto de las comunicaciones
COM.3	Se dispone de procedimientos de uso de las comunicaciones
COM.start	Entrada en servicio
COM.SC	Se aplican perfiles de seguridad
COM.A	Aseguramiento de la disponibilidad
COM.A.1	Se identifican y evitan "puntos únicos de fallo" (SPF-Single Point of Failure)
COM.A.2	Se dimensiona holgadamente y se planifica la adquisición de repuestos
COM.A.3	El mantenimiento periódico se ajusta a las especificaciones de los fabricantes

COM.A.4	Se monitorizan enlaces y dispositivos de red
COM.A.5	Se registran los fallos detectados, sean reales o sospechados
COM.A.6	Se registran las actuaciones de mantenimiento preventivo y correctivo
COM.A.7	Se realizan copias de seguridad de la configuración (backup)
COM.A.8	Se hacen copias de seguridad de las claves de autenticación
COM.A.9	Se hacen copias de seguridad de las claves de descifrado
COM.A.a	{xor} Redundancia
COM.A.b	Las medios alternativos están sujetos a las mismas garantías de protección que los habituales
COM.A.c	Se establece un tiempo máximo para que los equipos alternativos entren en funcionamiento
COM.aut	Autenticación del canal
COM.aut.1	Se requiere autorización previa
COM.aut.2	Se verifica la identidad del usuario antes de entregarle el mecanismo de autenticación
COM.aut.3	Se autentica el origen de la conexión
COM.aut.4	{or} Mecanismo de autenticación
COM.aut.4.1	Contraseñas
COM.aut.4.2	{xor} Contraseñas de un sólo uso (OTP: one time password)
COM.aut.4.3	{xor} Certificados (criptografía de clave pública)
COM.aut.5	{xor} Canal de autenticación
COM.aut.6	Se toman medidas para impedir el secuestro de sesiones establecidas
COM.I	{xor} Protección de la integridad de los datos intercambiados
COM.9	Se toman medidas frente a la inyección de información espuria
COM.C	Protección criptográfica de la confidencialidad de los datos intercambiados
COM.C.1	Se dispone de normativa relativa al uso de controles criptográficos
COM.C.2	Se han designado responsables
COM.C.3	{xor} Implantación de los algoritmos
COM.C.4	{xor} Mecanismo de cifrado (secreto compartido o cifra simétrica)
COM.op	Operación
COM.op.1	Control de acceso a la red
COM.op.1.1	Se dispone de normativa de uso de los servicios de red
COM.op.1.2	Se requiere autorización para que medios y dispositivos tengan acceso a redes y servicios
COM.op.1.3	Acceso remoto
COM.op.1.4	{xor} Protección de los puertos de diagnóstico remoto
COM.op.1.5	Autenticación de nodos de la red
COM.op.1.6	Control del encaminamiento
COM.op.2	Seguridad de los servicios de red
COM.op.2.1	Se monitorizan los servicios de red
COM.op.2.2	Revisiones periódicas de la seguridad
COM.op.3	Se prevé protección frente a análisis del tráfico
COM.op.4	Formación del personal en configuración de las comunicaciones
COM.CM	Cambios (actualizaciones y mantenimiento)
COM.CM.1	Se dispone de una política
COM.CM.2	Se dispone de procedimientos para ejecutar cambios
COM.CM.3	Se hace un seguimiento permanente de actualizaciones
COM.CM.4	Evaluación del impacto y riesgo residual tras el cambio
COM.CM.5	Se priorizan las actuaciones encaminadas a corregir riesgos elevados

COM.CM.6	Se mantiene en todo momento la regla de 'funcionalidad mínima'
COM.CM.7	Se mantiene en todo momento la regla de 'seguridad por defecto'
COM.CM.8	Se verifica que el cambio no inhabilita los mecanismos de detección, monitorización y registro
COM.CM.9	Se planifica el cambio de forma que minimice la interrupción del servicio
COM.CM.a	Realización por personal debidamente autorizado
COM.CM.b	Se retienen copias de las versiones anteriores de configuración
COM.CM.c	Se prueba previamente en un entorno que no esté en producción
COM.CM.d	Pruebas de regresión
COM.CM.e	Todas las actuaciones quedan registradas
COM.CM.f	Documentación
COM.CM.g	Se actualizan todos los procedimientos de producción afectados
COM.CM.h	Se actualizan todos los procedimientos de recuperación afectados
COM.end	Terminación
COM.internet	Internet: uso de ó acceso a
COM.internet.1	Se dispone de normativa sobre el uso de los servicios Internet
COM.internet.2	Compromiso escrito de cumplimiento de las normas por parte del usuario
COM.internet.3	Herramienta de monitorización del tráfico
COM.internet.4	Herramienta de control de contenidos con filtros actualizados
COM.internet.5	Se registra la navegación web
COM.internet.6	Control de descargas
COM.internet.7	Se han instalado herramientas anti spyware
COM.internet.8	Se deshabilitan las 'cookies' en los navegadores
COM.internet.9	Se controla la ejecución de código móvil (ej. 'applets')
COM.DS	Segregación de las redes en dominios

código	***Salvaguarda***
AUX	Elementos Auxiliares
AUX.1	Se dispone de un inventario de equipamiento auxiliar
AUX.A	Aseguramiento de la disponibilidad
AUX.A.1	Se siguen las recomendaciones del fabricante o proveedor
AUX.A.2	Continuidad de operaciones
AUX.start	Instalación
AUX.power	Suministro eléctrico
AUX.power.1	Se dimensiona el sistema considerando necesidades futuras
AUX.power.2	Instalación de acuerdo a la normativa vigente
AUX.power.3	Protección de las líneas de alimentación del sistema frente a fluctuaciones y sobrecargas
AUX.power.4	Interruptor general de la alimentación del sistema situado en la entrada de cada área
AUX.power.5	Interruptores etiquetados y protegidos frente a activaciones accidentales
AUX.power.6	Alimentación de respaldo
AUX.AC	Climatización
AUX.wires	Protección del cableado
AUX.7	{or} Contenedores de seguridad
AUX.8	Se prevén medidas frente a todos los problemas graves identificados en el

	análisis de riesgos

código	*Salvaguarda*
L	Protección de las Instalaciones
L.1	Se dispone de normativa de seguridad
L.2	Se dispone de un inventario de instalaciones
L.3	Entrada en servicio
L.3.1	Se dispone de normativa de entrada en servicio
L.3.2	Se requiere autorización previa
L.3.3	Se han determinado las acreditaciones o certificaciones pertinentes
L.3.4	Se requiere haber pasado las inspecciones o acreditaciones establecidas
L.3.5	Plan de Protección
L.3.5.1	Se dispone de un Plan de Acondicionamiento
L.3.5.2	Se dispone de un Plan de Seguridad
L.3.5.3	Plan de Emergencia
L.3.5.3.1	Plan de Evacuación
L.3.5.3.2	Plan de Comunicación
L.3.5.3.3	Acceso físico a las instalaciones en caso de emergencia
L.design	Diseño
L.design.1	El diseño atiende a las reglas y normas relevantes sobre salud y sanidad
L.design.2	El número de entradas se reduce al mínimo necesario
L.design.3	{xor} Puertas de acceso
L.design.4	Ventanas
L.design.5	Se dispone de protección en los conductos y aberturas (falso techo, conductos de aire, etc.)
L.design.6	Aislamiento acústico de las zonas en las que se hable de información confidencial
L.design.7	Hay una separación entre áreas de seguridad y de acceso público
L.design.8	Los equipos sensibles se instalan en áreas separadas
L.design.9	Se encuentran separadas las áreas gestionadas por otros
L.design.a	Se encuentran separadas las áreas dónde se llevan a cabo actividades peligrosas (cuartos de basura, depósitos de combustible, etc.)
L.design.b	Se encuentran separados los accesos para personas y vehículos
L.design.c	Carga / descarga
L.design.d	Las instalaciones son discretas minimizando indicaciones sobre su propósito
L.depth	Defensa en profundidad
L.depth.1	El perímetro exterior previene el acceso no autorizado
L.depth.2	Los siguientes niveles detectan accesos no autorizados
L.depth.3	Los diferentes niveles retardan el ataque
L.depth.4	El tiempo de reacción a un ataque es inferior al tiempo requerido por el atacante
L.AC	Control de los accesos físicos
L.AC.1	El acceso tiene que ser a través de un área de recepción
L.AC.2	Control de los accesos
L.AC.2.1	Se dispone de normativa de control de accesos
L.AC.2.2	Se dispone de procedimientos para el control de accesos
L.AC.2.3	{or} Mecanismo de autenticación
L.AC.2.3.1	Clave (PIN)

L.AC.2.3.2	{xor} Token
L.AC.2.3.3	{xor} Biometría
L.AC.2.4	La autorización para acceder se verifica antes de conceder el acceso
L.AC.2.5	Se mantiene un registro de los accesos
L.AC.2.6	El registro de accesos se revisa periódicamente
L.AC.2.7	Se investiga cualquier sospecha o intento de acceso físico no autorizado
L.AC.2.8	Los admitidos están acompañados permanentemente (escoltas) según política
L.AC.2.9	Se realiza un registro (examen minucioso) a la entrada
L.AC.2.a	Se realiza un registro (examen minucioso) a la salida
L.AC.2.b	Sistema automático de control de accesos
L.AC.2.c	Se dispone de un sistema de cámaras de vigilancia
L.AC.2.d	Los procedimientos de emergencia garantizan que solo el personal autorizado pueda acceder a las instalaciones
L.AC.3	Control de las visitas
L.AC.4	Pases o identificadores
L.AC.5	Los accesos permanecen cerrados fuera de las horas de trabajo
L.AC.6	Las áreas de trabajo se cierran y controlan periódicamente cuando están vacías
L.AC.7	Se evita que el acceso físico para operación y mantenimiento abra el acceso a otros activos
L.AC.8	Las salidas de emergencia garantizan que solo el personal autorizado pueda acceder a las instalaciones
L.AC.9	Se exige que los puestos de trabajo están despejados
L.AC.a	Se evita el trabajo no supervisado
L.AC.b	Se prohíben equipos de registro (fotografía, video, audio, telefonía, etc.) salvo autorización especial
L.AC.c	Control de llaves, combinaciones o dispositivos de seguridad
L.AC.c.1	Se dispone de un inventario
L.AC.c.2	Las áreas de seguridad disponen de algún tipo de llave, combinación o dispositivo de seguridad para acceder a las mismas
L.AC.c.3	Solamente el personal autorizado puede usarlos
L.AC.c.4	Se custodian de forma segura, incluidos los duplicados
L.AC.c.5	Las llaves se cambian cuando se hayan comprometido o exista sospecha de ello
L.AC.c.6	Las combinaciones se cambian o modifican cuando han sido comprometidas o exista sospecha de ello
L.AC.c.7	Las combinaciones se cambian o modifican cuando haya cambios de personal que haya tenido acceso a las mismas
L.AC.c.8	Las combinaciones se cambian o modifican al menos cada seis meses
L.AC.c.9	Periódicamente, se realiza un auditoría
L.7	Protección del perímetro
L.7.1	El perímetro está claramente definido con una valla, muro o similar
L.7.2	{or} La construcción es resitente frente a ataques de fuerza bruta
L.7.3	Se dispone de un sistema de detección de intrusión perimetral
L.7.4	{or} Se dispone de cámaras de vídeo de vigilancia
L.8	Vigilancia
L.9	Iluminación de seguridad
L.a	Protección frente a desastres
L.a.1	La iluminación de emergencia cubre todas las áreas necesarias para

	garantizar la continuidad de las misiones críticas
L.a.2	Protección frente a incendios
L.a.3	Protección frente a inundaciones
L.a.4	Protección frente a accidentes naturales e industriales
L.a.7	Protección frente a explosivos
L.a.8	Seguros
L.A	Continuidad de operaciones
L.A.1	Se analizan las implicaciones para la continuidad del negocio
L.A.2	Se establece un protocolo de actuación en caso de contingencia
L.A.3	Se dispone de instalaciones alternativas
L.A.4	Las instalaciones alternativas están sujetas a las mismas garantías de protección que las habituales
L.end	Terminación
L.d	La seguridad de la instalación no es responsabilidad de un único guarda

código	***Salvaguarda***
PS	Gestión del Personal
PS.1	Se dispone de normativa relativa a la gestión de personal (en materia de seguridad)
PS.2	Se dispone de procedimientos para la gestión de personal (en materia de seguridad)
PS.3	Relación de personal
PS.4	Puestos de trabajo
PS.4.1	Se dispone de un inventario de puestos de trabajo
PS.4.2	Se especifican las funciones de los puestos de trabajo
PS.4.3	Se han determinado las responsabilidades en materia de seguridad de los puestos de trabajo
PS.4.4	Se tienen en cuenta los requisitos de seguridad de los puestos de trabajo
PS.4.5	Se dispone de normativa de obligado cumplimiento en el desempeño del puesto de trabajo
PS.4.6	Se revisa periódicamente
PS.5	Cambio de puesto de trabajo
PS.6	Contratación
PS.6.1	Se dispone de normativa para la contratación de personal
PS.6.2	Se dispone de procedimientos para la contratación de personal
PS.6.3	Selección de personal
PS.6.4	Términos y condiciones de la relación laboral
PS.6.4.1	Inclusión del ámbito, el alcance y el periodo de las responsabilidades en materia de seguridad
PS.6.4.2	Inclusión de obligaciones y derechos legales de ambas partes
PS.6.4.3	Compromiso escrito de cumplimiento de la política y la normativa correspondiente
PS.6.4.4	Acuerdos de confidencialidad
PS.6.4.5	Procedimiento disciplinario
PS.6.5	Finalización de la relación laboral
PS.AT	Formación y concienciación
PS.AT.1	La Política de Seguridad contempla los aspectos de formación y concienciación
PS.AT.2	Se dispone de normativa relativa a las actividades de formación y concienciación

PS.AT.3	Se dispone de procedimientos relativos a las tareas de formación y concienciación
PS.AT.4	Plan de formación y concienciación
PS.AT.5	Concienciación
PS.AT.6	Formación
PS.AT.7	Procedimientos relevantes de seguridad: emergencias, incidencias, ...
PS.8	Protección del usuario frente a coacciones
PS.A	Aseguramiento de la disponibilidad
PS.A.1	Se prevé suficiente holgura en el dimensionamiento de los equipos de trabajo
PS.A.2	Se monitorizan continuamente las incidencias de disponibilidad de personal
PS.A.3	{or} Redundancia
PS.A.4	El personal alternativo está sujeto a las mismas garantías de seguridad que el habitual

código	***Salvaguarda***
G	Organización
G.1	Organización interna
G.1.1	Enterprise Architecture
G.1.2	Comité de seguridad de la información
G.1.3	Coordinación interna
G.1.4	Roles identificados
G.1.5	Asignación de responsabilidades para la seguridad de la información
G.1.6	Cooperación con otras organizaciones
G.1.7	Se dispone de asesoramiento especializado en seguridad
G.RM	Gestión de riesgos
G.RM.1	Se dispone de normativa en materia de gestión de riesgos
G.RM.2	Se han designado responsables
G.RM.3	Se dispone de procedimientos para llevar a cabo las tareas de análisis y gestión de riesgos
G.RM.4	Activos
G.RM.5	Amenazas
G.RM.6	Salvaguardas
G.RM.7	Evaluación de riesgos
G.RM.8	Se revisa periódicamente
G.3	Documentación técnica (componentes)
G.3.1	Documentación de los componentes del sistema
G.3.1.1	Documentación de las instalaciones
G.3.1.2	Documentación de las comunicaciones
G.3.1.3	Puntos de interconexión (entre zonas de confianza)
G.3.1.4	Documentación de los puntos de acceso lógico al sistema
G.3.1.5	Documentación del control de acceso
G.3.2	Criterios de aceptación para versiones o sistemas nuevos
G.3.3	Seguridad de la documentación del sistema
G.4	Documentación organizativa (normas y procedimientos)
G.4.1	Marco de referencia
G.4.2	Política de Seguridad de la Organización
G.4.3	Normas de seguridad
G.4.4	Procedimientos operativos de seguridad (POS)

G.4.5	Se revisa periódicamente el cumplimiento por parte del personal
G.plan	Planificación de la seguridad
G.plan.1	Se dispone de normativa de planificación (de seguridad)
G.plan.2	Procedimientos de planificación (de seguridad)
G.plan.3	Planificación de capacidades
G.plan.4	Componentes críticos: carentes de suministradores alternativos
G.plan.5	Planificación de actividades de seguridad
G.plan.6	Allocation of Resources
G.plan.7	Configuration Management Plan
G.exam	Inspecciones de seguridad

código	***Salvaguarda***
BC	{or} Continuidad del negocio
BC.1	Se lleva a cabo informalmente
BC.2	Se lleva a cabo formalmente
BC.2.1	Se dispone de normativa relativa a la continuidad del negocio
BC.2.2	El inventario se actualiza regularmente
BC.BIA	Se ha realizado un análisis de impacto (BIA)
BC.2.4	Actividades preparatorias
BC.2.5	Reacción (gestión de crisis)
BC.DRP	Plan de Recuperación de Desastres (DRP)
BC.DRP.1	Se han designado responsables
BC.DRP.2	Todas las áreas de la organización están coordinadas
BC.DRP.3	Documentación
BC.DRP.4	Notificación y activación
BC.DRP.5	Se dispone de un plan de recuperación
BC.DRP.5.1	Están detalladas las actividades de recuperación
BC.DRP.5.2	Están detallados los procedimientos de recuperación
BC.DRP.5.3	Se han previsto los recursos necesarios
BC.DRP.5.4	Están previstas instalaciones alternativas
BC.DRP.5.5	Las copias de seguridad (backup) se realizan con la frecuencia acordada
BC.DRP.5.6	Están previstos los medios alternativos de almacenamiento de la información
BC.DRP.5.7	Están previstos los medios alternativos de procesamiento de la información
BC.DRP.5.8	Están previstos medios alternativos de comunicación
BC.DRP.5.9	Está previsto personal alternativo
BC.DRP.5.a	Están previstos los lugares alternativos de trabajo
BC.DRP.6	Se ejecuta un plan de formación
BC.DRP.7	Los planes se prueban regularmente
BC.2.7	Restitución (retorno a condiciones normales de trabajo)

código	***Salvaguarda***
E	Relaciones Externas
E.1	Acuerdos para intercambio de información y software
E.2	Acceso externo
E.3	Servicios proporcionados por otras organizaciones

E.3.1	Se requiere aprobación previa para el uso de servicios externos
E.3.2	Se identifican las aplicaciones sensibles o críticas que debe retener la Organización
E.3.3	Se identifican los riesgos derivados de depender de un proveedor externo
E.3.4	Contratos de prestación de servicios
E.3.4.1	Se define la política aplicable sobre seguridad de la información
E.3.4.2	Constan las obligaciones de todas las partes
E.3.4.3	Se incluyen los requisitos de seguridad
E.3.4.4	Se define, y se incorpora al contrato el procedimiento para medir el cumplimiento de las medidas de seguridad
E.3.4.5	IPR: Se contemplan los temas relativos a propiedad intelectual
E.3.4.6	Se contempla la protección de la información de carácter personal
E.3.4.7	Se establecen los términos para la implicación de terceros (subcontratistas)
E.3.4.8	Se describen los servicios disponibles
E.3.4.9	Se definen las responsabilidades sobre instalación y mantenimiento de HW y SW
E.3.4.a	Se definen las responsabilidades en la supervisión del cumplimiento del contrato
E.3.5	Operación
E.3.6	Gestión de cambios
E.3.7	Continuidad de operaciones
E.5	Se revisa regularmente el cumplimiento de acuerdos y contratos

código	***Salvaguarda***
NEW	Adquisición / desarrollo
NEW.S	Servicios: Adquisición o desarrollo
NEW.S.1	Se asignan recursos suficientes
NEW.S.2	Se establecen previamente los requisitos funcionales
NEW.S.3	Se identifican los requisitos de seguridad de acuerdo a los condicionantes del negocio
NEW.S.4	Se identifican los requisitos técnicos de seguridad
NEW.SW	Aplicaciones: Adquisición o desarrollo
NEW.SW.1	Se establecen previamente los requisitos funcionales
NEW.SW.2	Se identifican los requisitos de seguridad de acuerdo a los condicionantes del negocio
NEW.SW.3	Se identifican los requisitos técnicos de seguridad
NEW.SW.4	Adquisición de aplicaciones SW
NEW.SW.5	Desarrollo
NEW.SW.5.1	Metodología de desarrollo
NEW.SW.5.1.1	Se tiene en cuenta la seguridad durante todo el ciclo de desarrollo
NEW.SW.5.1.2	Se tratan específicamente los datos de prueba
NEW.SW.5.1.3	Se contempla la posibilidad de inspeccionar el código fuente
NEW.SW.5.2	Los desarrolladores cambian regularmente de asignaciones
NEW.SW.5.3	Código fuente
NEW.SW.5.4	Entorno de desarrollo
NEW.SW.5.4.1	{xor} El entorno de desarrollo está separado del de producción
NEW.SW.5.4.2	Hay una separación de funciones entre el personal que desarrolla y el personal encargado de producción
NEW.SW.5.4.3	Las herramientas de desarrollo no son accesibles al personal de

	producción
NEW.SW.5.4.4	Se controla el acceso a las herramientas de desarrollo
NEW.SW.5.5	Entorno de pruebas (pre-producción)
NEW.SW.5.5.1	{xor} El entorno de pre-producción está separado del de producción
NEW.SW.5.5.2	El entorno de pruebas simula realísticamente el entorno de producción
NEW.SW.5.5.3	Se emplean cuentas de usuario diferentes: pruebas y producción
NEW.SW.5.5.4	Se revisa la corrección y completitud de la documentación
NEW.SW.5.5.5	Se verifica el funcionamiento de los controles de seguridad
NEW.SW.5.5.6	Se verifica que el nuevo sistema no afecta negativamente a las otras funciones del sistema en el que va a operar
NEW.SW.5.6	{or} Protección de los datos de prueba del sistema
NEW.SW.5.6.1	Las pruebas no usan datos reales
NEW.SW.5.6.2	Las pruebas usan datos reales tratados para ser irreconocibles
NEW.SW.5.6.3	Las pruebas usan datos reales
NEW.SW.5.6.3.1	Se requiere autorización previa
NEW.SW.5.6.3.2	Se aplica el mismo control de accesos que al sistema en producción
NEW.SW.5.6.3.3	Cuando termina una campaña de pruebas, la información de producción se elimina del sistema de pruebas
NEW.SW.5.6.3.4	Se registra el uso a efectos de auditoría
NEW.SW.5.7	Contratos de desarrollo SW
NEW.SW.5.8	Documentación del SW
NEW.SW.5.9	Inspección del código fuente
NEW.SW.6	Se prefieren aplicaciones que funcionan sobre varios sistemas operativos
NEW.HW	Equipos: Adquisición o desarrollo
NEW.HW.1	Se establecen previamente los requisitos funcionales
NEW.HW.2	Se identifican los requisitos de seguridad de acuerdo a los condicionantes del negocio
NEW.HW.3	Se identifican los requisitos técnicos de seguridad
NEW.HW.4	Adquisición de HW
NEW.HW.5	Desarrollo de HW
NEW.HW.5.1	Metodología de desarrollo
NEW.HW.5.2	Protocolo de pruebas
NEW.HW.5.3	{or} Desarrollo
NEW.HW.6	Se tienen en cuenta las necesidades de formación
NEW.HW.7	Se tienen en cuenta las necesidades de repuestos
NEW.HW.8	Documentación del HW
NEW.HW.9	Se disponen derechos de acceso para auditar la calidad y exactitud del trabajo realizado
NEW.HW.a	La calidad y exactitud del trabajo realizado se certifica según los estándares requeridos
NEW.HW.b	Entorno de pruebas
NEW.COM	Comunicaciones: Adquisición o contratación
NEW.COM.1	Se establecen previamente los requisitos funcionales
NEW.COM.2	Se identifica el tipo de conexión a establecer
NEW.COM.3	Se revisan las características de la solución propuesta (sobre red pública o privada, de datos, de voz y datos, etc.)

NEW.COM.4	Se identifican los requisitos de seguridad de acuerdo a los condicionantes del negocio
NEW.COM.5	Se identifican los requisitos técnicos de seguridad
NEW.COM.6	Se revisa la arquitectura de la red de la organización
NEW.COM.7	Se identifican los riesgos de la solución propuesta, y las salvaguardas necesarias
NEW.COM.8	La solución propuesta está completamente documentada
NEW.C	Productos certificados o acreditados
NEW.C.1	Se verifica la idoneidad para la misión encomendada
NEW.C.2	Se verifica la vigencia del certificado
NEW.C.3	Se satisfacen las presunciones del producto respecto del entorno

ANEXO 5

VULNERABILIDAD DE LOS DOMINIOS

Vulnerabilidad.- los activos, por su propia naturaleza, se ven influidos por una serie de amenazas. La probabilidad de que se materialice una de dichas amenazas y la degradación que le supone a un activo es lo que se conoce como vulnerabilidad.

En la Gestión de Vulnerabilidades descritas posteriormente, se podrá definir qué criterios pueden influir sobre un dominio (y por lo tanto sobre todos los activos que se encuentran en dicho dominio)

Responsable de la encuesta:
……

(Subrayar los criterios pertinentes)

[101] Identificación del atacante – quienes son los atacantes a los activos
- [101.a] público en general
- [101.b] competidor comercial
- [101.c] proveedor de servicios
- [101.d] grupos de presión política / activistas / extremistas
- [101.e] periodistas
- [101.f] criminales / terroristas
- [101.g] personal interno [101.h]
- bandas criminales [101.i]
- grupos terroristas
- [101.j] servicios de inteligencia

[102] Motivación del atacante
- [102.a] económica (beneficios en dinero)
- [102.b] beneficios comerciales
- [102.c] personal propio con problemas de conciencia
- [102.d] personal propio con conflictos de interés
- [102.e] personal propio con pertenencia a un grupo extremista
- [102.f] con ánimo destructivo [102.g] con
- ánimo de causar daño [102.h] con ánimo de
- provocar pérdidas

[103] Beneficio del atacante
- [103.a] moderadamente interesado
- [103.b] muy interesado
- [103.c] extremadamente interesado

[104] Motivación del personal interno

[104.a] todo el personal está fuertemente motivado [104.b]
baja calificación profesional / escasa información [104.c]
sobrecargos de trabajo
[104.d] con problemas de conciencia
[104.e] con conflictos de intereses
[104.f] personal asociado a grupos extremistas

[105] Permisos de los usuarios (derechos) [105.a]
se permite el acceso a internet
[105.b] se permite la ejecución de programas sin autorización previa [105.c]
se permite la instalación de programas sin autorización previa [105.d] se
permite la conexión de dispositivos móviles

[111] Conectividad del sistema de información
[111.a] sistema aislado
[111.b] conectado a un conjunto reducido y controlado de redes
[111.c] conectado a un amplio colectivo de redes conocidas [111.d]
conectado a internet

[112] Ubicación del sistema de información
[112.a] dentro de una zona segura (“en casa”)
[112.b] en un área de acceso abierto
[112.c] en un entorno hostil

ANEXO 6

Código de buenas prácticas para la Gestión de la Seguridad de la Información [27002:2005]

proyecto: [AGR_COPEU] ANALISIS Y GESTION DE RIESGOS SISTEMA DE LA COOPERATIVA COPEU

1. Datos del proyecto

AGR_COPEU	ANALISIS Y GESTION DE RIESGOS SISTEMA DE LA COOPERATIVA COPEU
Descripcion	Analisis al Sistema
Responsable	Carlos Andres Simbaya Camacho
Organización	Cooperativa de Ahorro y Credito Universitaria Limitada
Version	5.2.9
Fecha	07-10-2013
Biblioteca	[std] Biblioteca INFOSEC (28.8.2012)

Licencia

[edu] UTA
Universidad Técnica de Ambato
Facultad de Ingeniería en Sistemas, Electrónica e Industrial
[... 31.12.2014]

2. Dominios de seguridad

- [base] COPEU

3. Fases del proyecto

- [current] situación actual
- [target] situación objetivo
- [PILAR] recomendación

4. Dominio de seguridad: [base] COPEU

4.1. [5] Política de seguridad

Control	[current]	[target]	[PILAR]
[5] Política de seguridad	60%	100%	60%
[5.1] Política de seguridad de la información	60%	100%	60%
[5.1.1] Documento de política de seguridad de la información	70%	100%	70%
[5.1.2] Revisión de la política de seguridad de la información	50%	100%	50%

4.2. [6] Aspectos organizativos de la seguridad de la información

Control	[current]	[target]	[PILAR]
[6] Aspectos organizativos de la seguridad de la información	49%	92%	62%
[6.1] Organización interna	44%	100%	58%
[6.1.1] Compromiso de la Dirección con la seguridad de la información	50%	100%	50%
[6.1.2] Coordinación de la seguridad de la información	50%	100%	50%

[6.1.3] Asignación de responsabilidades relativas a la seguridad de la información	60%	100%	60%
[6.1.4] Proceso de autorización de recursos para el tratamiento de la información	10%	100%	52%
[6.1.4.hw] equipamiento (HW)	10%	100%	60%
[6.1.4.net] conexión a la red	10%	100%	50%
[6.1.4.comms] comunicaciones	10%	100%	50%
[6.1.4.facilities] instalaciones	10%	100%	50%
[6.1.5] Acuerdos de confidencialidad	10%	100%	80%
[6.1.6] Contacto con las autoridades	50%	100%	50%
[6.1.7] Contacto con grupos de especial interés	50%	100%	50%
[6.1.8] Revisión independiente de la seguridad de la información	70%	100%	70%
[6.2] Terceros	55%	83%	67%
[6.2.1] Identificación de los riesgos derivados del acceso de terceros	50%	100%	50%
[6.2.2] Tratamiento de la seguridad en la relación con los clientes	35%	50%	80%
[Q.6.2.2] Especificación del servicio prestado	0%	0%	90%
[Q.6.2.2.a] descripción del servicio proporcionado			L3
[Q.6.2.2.b] requisitos para el acceso de los usuarios			L3
[Q.6.2.2.c] restricciónes en el uso de la información: copias y divulgación			L3
[Q.6.2.2.d] requisitos de nivel de servicio: objetivo y mínimos inaceptables			L3
[Q.6.2.2.e] responsabilidades respectivas de la organización y del cliente			L3
[Q.6.2.2.f] responsabilidad en asuntos legales			L3
[Q.6.2.2.g] protección de la propiedad intelectual y asignación de derechos de copyright			L3
[Q.6.2.2.h] protección de los trabajos en colaboración			L3
[6.2.3] Tratamiento de la seguridad en contratos con terceros	80%	100%	70%

4.3. [7] Gestión de activos

Control	[current]	[target]	[PILAR]
[7] Gestión de activos	48%	100%	72%
[7.1] Responsabilidad sobre los activos	17%	100%	64%
[7.1.1] Inventario de activos	20%	100%	68%
[7.1.2] Propiedad de los activos	20%	100%	65%
[7.1.3] Uso aceptable de los activos	10%	100%	60%
[7.2] Clasificación de la información	80%	100%	80%
[7.2.1] Directrices de clasificación	70%	100%	70%
[7.2.2] Etiquetado y manipulado de la información	90%	100%	90%

4.4. [8] Seguridad ligada a los recursos humanos

Control	[current]	[target]	[PILAR]
[8] Seguridad ligada a los recursos humanos	19%	100%	73%
[8.1] Antes del empleo	10%	100%	72%
[8.1.1] Funciones y responsabilidades	10%	100%	66%

[8.1.2] Investigación de antecedentes	10%	100%	80%
[8.1.3] Términos y condiciones de contratación	10%	100%	70%
[8.2] Durante el empleo	10%	100%	63%
[8.2.1] Responsabilidades de la Dirección	10%	100%	50%
[8.2.2] Concienciación, formación y capacitación en seguridad de la información	10%	100%	70%
[8.2.3] Proceso disciplinario	10%	100%	70%
[8.3] Cese del empleo o cambio de puesto de trabajo	37%	100%	83%
[8.3.1] Responsabilidad del cese o cambio	10%	100%	70%
[8.3.2] Devolución de activos	10%	100%	90%
[8.3.3] Retirada de los derechos de acceso	90%	100%	90%

4.5. [9] Seguridad física y del entorno

Control	[current]	[target]	[PILAR]
[9] Seguridad física y del entorno	10%	100%	82%
[9.1] Áreas seguras	10%	100%	86%
[9.1.1] Perímetro de seguridad física	10%	100%	90%
[9.1.2] Controles físicos de entrada	10%	100%	73%
[9.1.3] Seguridad de oficinas, despachos e instalaciones	10%	100%	94%
[9.1.4] Protección contra las amenazas externas y de origen ambiental	10%	100%	91%
[9.1.5] Trabajo en áreas seguras	10%	100%	77%
[9.1.6] Áreas de acceso público y de carga y descarga	10%	100%	93%
[9.2] Seguridad de los equipos	10%	100%	78%
[9.2.1] Emplazamiento y protección de equipos	10%	100%	90%
[9.2.2] Instalaciones de suministro	10%	100%	85%
[9.2.3] Seguridad del cableado	10%	100%	70%
[9.2.4] Mantenimiento de los equipos	10%	100%	70%
[9.2.5] Seguridad de los equipos fuera de las instalaciones	10%	100%	70%
[9.2.6] Reutilización o retirada segura de equipos	10%	100%	90%
[9.2.7] Retirada de materiales propiedad de la empresa	10%	100%	70%

4.6. [10] Gestión de comunicaciones y operaciones

Control	[current]	[target]	[PILAR]
[10] Gestión de comunicaciones y operaciones	49%	100%	74%
[10.1] Responsabilidades y procedimientos de operación	47%	100%	72%
[10.1.1] Documentación de los procedimientos de operación	25%	100%	65%
[10.1.1.q1] Soportes de información	n.a.	n.a.	n.a.
[10.1.2] Gestión de cambios	10%	100%	70%
[10.1.3] Segregación de tareas	70%	100%	70%
[10.1.4] Separación de los recursos de desarrollo, prueba y operación	83%	100%	83%
[10.2] Gestión de la provisión de servicios por terceros	60%	100%	59%
[10.2.1] Provisión de servicios	70%	100%	70%
[10.2.2] Supervisión y revisión de los servicios prestados por terceros	59%	100%	58%
[10.2.3] Gestión del cambio en los servicios prestados por terceros	50%	100%	50%
[10.3] Planificación y aceptación del sistema	40%	100%	70%

[10.3.1] Gestión de capacidades	70%	100%	70%
[10.3.2] Aceptación del sistema	10%	100%	70%
[10.4] Protección contra el código malicioso y descargable	51%	100%	81%
[10.4.1] Controles contra el código malicioso	91%	100%	91%
[10.4.2] Controles contra el código descargado en el cliente	10%	100%	70%
[10.5] Copias de seguridad	64%	100%	84%
[10.5.1] Copias de seguridad de la información	64%	100%	84%
[10.6] Gestión de la seguridad de las redes	20%	100%	78%
[10.6.1] Controles de red	30%	100%	74%
[10.6.2] Seguridad de los servicios de red	10%	100%	82%
[10.7] Manipulación de los soportes	70%	100%	70%
[10.7.1] Gestión de soportes extraíbles	n.a.	n.a.	n.a.
[10.7.2] Retirada de soportes	n.a.	n.a.	n.a.
[10.7.3] Procedimientos de manipulación de la información	n.a.	n.a.	n.a.
[10.7.4] Seguridad de la documentación del sistema	70%	100%	70%
[10.8] Intercambio de información	37%	100%	83%
[10.8.1] Políticas y procedimientos de intercambio de información	10%	100%	90%
[10.8.2] Acuerdos de intercambio	90%	100%	90%
[10.8.3] Soportes físicos en tránsito	n.a.	n.a.	n.a.
[10.8.4] Mensajería electrónica	10%	100%	70%
[10.8.5] Sistemas de información empresariales	n.a.	n.a.	n.a.
[10.9] Servicios de comercio electrónico	28%	100%	70%
[10.9.1] Comercio electrónico	10%	100%	70%
[10.9.2] Transacciones en línea	64%	100%	91%
[10.9.3] Información públicamente disponible	10%	100%	50%
[10.10] Supervisión	77%	100%	77%
[10.10.1] Registros de auditoría	50%	100%	50%
[10.10.2] Supervisión del uso del sistema	90%	100%	90%
[10.10.3] Protección de la información de los registros	90%	100%	90%
[10.10.4] Registros de administración y operación	70%	100%	70%
[10.10.5] Registro de fallos	70%	100%	70%
[10.10.6] Sincronización del reloj	92%	100%	92%

4.7. [11] Control de acceso

Control	[current]	[target]	[PILAR]
[11] Control de acceso	55%	100%	84%
[11.1] Requisitos de negocio para el control de acceso	83%	100%	83%
[11.1.1] Política de control de acceso	83%	100%	83%
[11.2] Gestión de acceso de usuario	79%	100%	86%
[11.2.1] Registro de usuario	91%	100%	91%
[11.2.2] Gestión de privilegios	70%	100%	70%
[11.2.3] Gestión de contraseñas de usuario	63%	100%	91%
[11.2.3.services] contraseñas de acceso a los servicios	10%	100%	92%
[11.2.3.sw] contraseñas de acceso a las aplicaciones	10%	100%	92%
[11.2.3.comms] contraseñas de acceso a los servicios de comunicaciones	10%	100%	95%
[11.2.4] Revisión de derechos de acceso de usuario	92%	100%	92%

[11.3] Responsabilidades de usuario	65%	100%	91%
[11.3.1] Uso de contraseñas	90%	100%	90%
[11.3.2] Equipo de usuario desatendido	95%	100%	92%
[11.3.3] Política de puesto de trabajo despejado y pantalla limpia	10%	100%	90%
[11.4] Control de acceso a la red	10%	100%	81%
[11.4.1] Política de uso de los servicios en red	10%	100%	50%
[11.4.2] Autenticación de usuario para conexiones externas	10%	100%	90%
[11.4.3] Identificación de los equipos en las redes	10%	100%	90%
[11.4.4] Diagnóstico remoto y protección de los puertos de configuración	10%	100%	90%
[11.4.5] Segregación de las redes	10%	100%	90%
[11.4.6] Control de la conexión a la red	10%	100%	70%
[11.4.7] Control de encaminamiento (routing) de red	10%	100%	90%
[11.5] Control de acceso al sistema operativo	93%	100%	91%
[11.5.1] Procedimientos seguros de inicio de sesión	92%	100%	92%
[11.5.2] Identificación y autenticación de usuario	91%	100%	90%
[11.5.3] Sistema de gestión de contraseñas	91%	100%	90%
[11.5.4] Uso de los recursos del sistema	92%	100%	90%
[11.5.5] Desconexión automática de sesión	100%	100%	95%
[11.5.6] Limitación del tiempo de conexión	90%	100%	90%
[11.6] Control de acceso a las aplicaciones y a la información	45%	100%	87%
[11.6.1] Restricción del acceso a la información	81%	100%	81%
[11.6.2] Aislamiento de sistemas sensibles	10%	100%	92%
[11.7] Ordenadores portátiles y teletrabajo	10%	100%	70%
[11.7.1] Ordenadores portátiles y comunicaciones móviles	10%	100%	70%
[11.7.2] Teletrabajo	10%	100%	70%

4.8. [12] Adquisición, desarrollo y mantenimiento de los sistemas de información

Control	[current]	[target]	[PILAR]
[12] Adquisición, desarrollo y mantenimiento de los sistemas de información	51%	100%	76%
[12.1] Requisitos de seguridad de los sistemas de información	58%	100%	52%
[12.1.1] Análisis y especificación de los requisitos de seguridad	58%	100%	52%
[12.1.1.s] servicios	60%	100%	50%
[12.1.1.sw] aplicaciones (SW)	60%	100%	60%
[12.1.1.hw] equipamiento (HW)	60%	100%	50%
[12.1.1.comms] servicios de comunicaciones	50%	100%	50%
[12.2] Tratamiento correcto de las aplicaciones	10%	100%	80%
[12.2.1] Validación de los datos de entrada	10%	100%	90%
[12.2.2] Control del procesamiento interno	10%	100%	70%
[12.2.3] Integridad de los mensajes	10%	100%	90%
[12.2.4] Validación de los datos de salida	10%	100%	70%
[12.3] Controles criptográficos	90%	100%	90%
[12.3.1] Política de uso de los controles criptográficos	90%	100%	90%
[12.3.2] Gestión de claves	n.a.	n.a.	n.a.

[12.4] Seguridad de los archivos del sistema	57%	100%	77%
[12.4.1] Control del software en explotación	10%	100%	71%
[12.4.2] Protección de los datos de prueba del sistema	90%	100%	90%
[12.4.3] Control de acceso al código fuente de los programas	70%	100%	70%
[12.5] Seguridad en los procesos de desarrollo y soporte	37%	100%	72%
[12.5.1] Procedimientos de control de cambios	10%	100%	70%
[12.5.2] Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	10%	100%	75%
[12.5.3] Restricciones a los cambios en los paquetes de software	10%	100%	63%
[12.5.4] Fugas de información	85%	100%	83%
[12.5.4.dlp] monitorización de contenidos	n.a.	n.a.	n.a.
[12.5.4.mon] monitorización del tráfico	70%	100%	70%
[12.5.4.media] soportes de información	95%	100%	90%
[12.5.5] Externalización del desarrollo de software	70%	100%	70%
[12.6] Gestión de la vulnerabilidad técnica	57%	100%	84%
[12.6.1] Control de las vulnerabilidades técnicas	57%	100%	84%

4.9. [13] Gestión de incidentes de seguridad de la información

Control	[current]	[target]	[PILAR]
[13] Gestión de incidentes de seguridad de la información	85%	100%	85%
[13.1] Notificación de eventos y puntos débiles de seguridad de la información	90%	100%	90%
[13.1.1] Notificación de eventos de seguridad de la información	90%	100%	90%
[13.1.2] Notificación de puntos débiles de seguridad	90%	100%	90%
[13.2] Gestión de incidentes de seguridad de la información y mejoras	80%	100%	80%
[13.2.1] Responsabilidades y procedimientos	70%	100%	70%
[13.2.2] Aprendizaje de los incidentes de seguridad de la información	80%	100%	80%
[13.2.3] Recopilación de evidencias	90%	100%	90%

4.10. [14] Gestión de la continuidad del negocio

Control	[current]	[target]	[PILAR]
[14] Gestión de la continuidad del negocio	73%	100%	73%
[14.1] Aspectos de seguridad de la información en la gestión de la continuidad del negocio	73%	100%	73%
[14.1.1] Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	80%	100%	80%
[14.1.2] Continuidad del negocio y evaluación de riesgos	70%	100%	70%
[14.1.3] Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información	70%	100%	70%
[14.1.4] Marco de referencia para la planificación de la continuidad del negocio	53%	100%	53%
[14.1.5] Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	90%	100%	90%

4.11. [15] Cumplimiento

Control	[current]	[target]	[PILAR]
[15] Cumplimiento	68%	100%	73%
[15.1] Cumplimiento de los requisitos legales	54%	100%	68%
[15.1.1] Identificación de legislación aplicable	50%	100%	50%
[15.1.2] Derechos de propiedad intelectual (IPR)	50%	100%	65%
[15.1.2.info] de la información manejada	90%	100%	80%
[15.1.2.sw_exp] de las aplicaciones usadas	50%	100%	80%
[15.1.2.sub] de los desarrollos subcontratados	50%	100%	50%
[15.1.3] Protección de los documentos de la organización	n.a.	n.a.	n.a.
[15.1.4] Protección de datos y privacidad de la información de carácter personal	70%	100%	70%
[15.1.5] Prevención del uso indebido de los recursos de tratamiento de la información	38%	100%	68%
[15.1.6] Regulación de los controles criptográficos	63%	100%	90%
[15.2] Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico	66%	100%	66%
[15.2.1] Cumplimiento de las políticas y normas de seguridad	50%	100%	50%
[15.2.2] Comprobación del cumplimiento técnico	81%	100%	81%
[15.3] Consideraciones sobre la auditoría de los sistemas de información	85%	100%	85%
[15.3.1] Controles de auditoría de los sistemas de información	80%	100%	80%
[15.3.2] Protección de las herramientas de auditoría de los sistemas de información	90%	100%	90%