UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE CONTABILIDAD Y AUDITORIA

CARRERA DE CONTABILIDAD Y AUDITORIA

VIII SEMINARIO DE INGENIERIA EN CONTABILIDAD Y AUDITORIA CPA.

TRABAJO DE GRADUACION PREVIO A LA OBTENCION DEL TITULO DE INGENIERO EN CONTABILIDAD Y AUDITORIA CPA.

Tema:

"LA AUDITORÍA INFORMÁTICA Y SU INCIDENCIA EN LA DISPONIBILIDAD DE LOS SISTEMAS DE INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO EL SAGRARIO LTDA. EN EL 2010"

Autor: Jaime Ramiro Freire Freire

Tutor: C.P.A. DR. Joselito Ricardo Naranjo Santamaría

AMBATO – ECUADOR

2011

AUTORIA DEL TRABAJO DE INVESTIGACIÓN

Yo, Jaime Ramiro Freire Freire, con C.I. # 1803272119, tengo a bien indicar que los criterios emitidos en el Trabajo de Graduación **"LA AUDITORÍA INFORMÁTICA Y SU INCIDENCIA EN LA DISPONIBILIDAD DE LOS SISTEMAS DE INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO EL SAGRARIO LTDA. EN EL 2010"** es original, auténtico y personal, en tal virtud la responsabilidad del contenido de Investigación, para efectos legales y académicos son de exclusiva responsabilidad del autor y el patrimonio intelectual de la misma a la Universidad Técnica de Ambato; por lo que autorizo a la Biblioteca de la Facultad de Contabilidad y Auditoría para que haga de esta tesis un documento disponible para su lectura y publicación según las Normas de la Universidad.

Ambato, 13 de octubre del 2011

AUTOR

…….

Jaime Ramiro Freire Freire

C.I. # 1803272119

APROBACIÓN DEL TUTOR

Yo, JOSELITO RICARDO NARANJO SANTAMARÍA, con C.I. # **1802621241**en mi calidad de Tutor del trabajo de Graduación sobre el tema **"LA AUDITORÍA INFORMÁTICA Y SU INCIDENCIA EN LA DISPONIBILIDAD DE LOS SISTEMAS DE INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO EL SAGRARIO LTDA. EN EL 2010"**, desarrollado por Jaime Ramiro Freire Freire, estudiante del VIII Seminario de Graduación de la carrera de Contabilidad y Auditoría, considero que dicho Trabajo de Graduación reúne requisitos tanto técnicos como científicos y corresponde a las normas establecidas en el Reglamento de Graduación de Pregrado, modalidad Seminarios de la Universidad Técnica de Ambato y en el normativo para la presentación de Trabajos de Graduación de la Facultad de Contabilidad y Auditoría

Por lo tanto, autorizo la presentación del mismo ante el organismo pertinente, para que sea sometido a evaluación por la Comisión de Calificador designada por el H. Consejo Directivo.

Ambato, 13 de octubre del 2011

EL TUTOR

……..

C.P.A. DR. JOSELITO RICARDO NARANJO SANTAMARÍA

C.I. # 1802621241

APROBACION DEL TRIBUNAL DE GRADO

El Tribunal de Grado, aprueba el Trabajo de Graduación, sobre el tema: "LA AUDITORÍA INFORMÁTICA Y SU INCIDENCIA EN LA DISPONIBILIDAD DE LOS SISTEMAS DE INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO EL SAGRARIO LTDA. EN EL 2010" elaborado por Jaime Ramiro Freire Freire, estudiante del VIII Seminario de Graduación, el mismo que guarda conformidad con las disposiciones reglamentarias emitidas por la Facultad de Contabilidad y Auditoría de la Universidad Técnica de Ambato.

Ambato, 13 de octubre del 2011

Para constancia firma

…….	…….
DR. GERMAN SALAZAR	DRA. PATRICIA JIMENEZ

…….

PRESIDENTE DEL TRIBUNAL

DEDICATORIA

El presente trabajo de investigación va dirigido como aporte al área de auditoría interna de la Cooperativa de Ahorro y Crédito El Sagrario Ltda. con la finalidad de que pueda ayudarse para el control interno de las tecnologías de información y comunicaciones.

INDICE

Contenido **Página**

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

CAPÍTULO VI

PROPUESTA

ÍNDICE DE TABLAS

Contenido **Página**

INDICE DE GRÁFICOS Y FIGURAS

Contenido **Página**

RESUMEN EJECUTIVO

Las tecnologías de información y comunicaciones se han convertido en estrategias de diferenciación de todas las empresas, aquellas que mayormente tienen sus procesos automatizados generan una gran ventaja competitiva sobre otras empresas. En las instituciones financieras cada vez está de manifiesto nuevos servicios y productos basados en la tecnología que ponen al servicio de todos sus clientes.

Sin embargo, la falta de controles y revisiones periódicas de las tecnologías de información mediante auditorias informáticas, no garantizan la disponibilidad, confidencialidad, integridad y seguridad de la información, generando grandes pérdidas económicas para las empresas.

Uno de los motivos por los cuales no se realizan auditorias informáticas, es la falta de personal capacitado en esta área y de una guía básica de aplicación de auditorías informáticas; el presente proyecto de investigación ha sido desarrollado con la finalidad de proporcionar al departamento de auditoría interna de la Cooperativa de Ahorro y Crédito “El Sagrario” Ltda. una guía de auditorías informáticas que permita realizar periódicamente la revisión de las tecnologías de información y comunicaciones.

INTRODUCCIÓN

El presente trabajo de investigación está enfocado en analizar las Auditorias Informáticas y su incidencia en la disponibilidad de los sistemas de información de la Cooperativa de Ahorro y Crédito el Sagrario en el 2010.

En el primer capítulo se encuentra planteado el problema a investigar y los objetivos a cumplir dentro de la investigación.

En el segundo capítulo se hace referencia al marco teórico de la investigación, se citan los antecedentes, fundamentaciones que enfocan al tema en un área legal y conceptual, y la formulación de la hipótesis que va ser comprobada en la investigación.

El tercer capítulo explica los métodos y técnicas de investigación a utilizarse para la recolección de información necesaria para la elaboración del trabajo de investigación.

En el cuarto capítulo se determina la población y selección de la muestra, mediante fórmulas y procedimientos estadísticos, se presentan los resultados de las encuestas y principalmente se realiza la comprobación de la hipótesis planteada.

En el quinto capítulo se emiten las conclusiones y recomendaciones derivadas del resultado de la encuesta y comprobación de la hipótesis.

En el sexto capítulo se presenta la propuesta de solución al problema planteado, se proporciona un marco teórico para la aplicación de las auditorias informáticas y principalmente una guía de auditoría informática con su plan de acción.

CAPÍTULO I
EL PROBLEMA DE INVESTIGACIÓN

1.1. TEMA DE INVESTIGACIÓN

"La auditoría informática y su incidencia en la disponibilidad de los sistemas de información en la Cooperativa de Ahorro y Crédito El Sagrario Ltda. en el 2010"

1.2. PLANTEAMIENTO DEL PROBLEMA

1.2.1. Contextualización

1.2.1.1. Contexto macro

El creciente uso de las tecnologías de información y comunicaciones en el sistema financiero en el Ecuador, ha permitido mejorar enormemente la calidad de servicio a todos los clientes, hoy en día es muy común escuchar servicios de banca en línea, banca móvil, pero así mismo es común escuchar la presencia de fraudes informáticos y robos electrónicos a usuarios del sistema financiero debido a la debilidad en los controles de seguridad.

Las Cooperativas de Ahorro y Crédito, igual que las entidades bancarias se encuentran innovando hacia nuevos servicios en línea, lo cual implica mantener un sistema de control robusto que evite poner en riesgo la seguridad, confidencialidad, integridad y disponibilidad de la información.

El inadecuado control interno de las tecnologías de información, puede afectar gravemente la disponibilidad de los sistemas de información, y la atención al público. A menudo, en muchas instituciones escuchamos la frase "No tenemos sistema", y esto se debe a un sinnúmero de

circunstancias como: daño de un servidor, daño de la base de datos, pérdida de energía del centro de cómputo, mala práctica profesional; todos estos riesgos se pueden mitigar siempre y cuando exista un buen control interno.

Debido al inadecuado control interno de las tecnologías de información en las Cooperativas y con el incremento de delincuentes electrónicos, hackers informáticos, pueden ser sus sistemas de información fácilmente vulnerables.

1.2.1.2. Contexto meso

En la provincia de Tungurahua poseen su oficina matriz 5 Cooperativas que están bajo el control de la Superintendencia de Bancos y Seguros, de las cuales todas están en tendencia de ofrecer nuevos servicios basados en la tecnología, sin embargo sólo una de las Cooperativas realizan el control a través de auditorías informáticas internas, dos contratan una auditoría externa y dos no han realizado ninguna auditoría informática. Esto denota una clara debilidad en el control interno de las tecnologías de información y comunicaciones, por lo cual la presente investigación puede ser una guía para las diferentes instituciones financieras para fortalecer la disponibilidad de los sistemas de información.

La falta de políticas de control interno para la tecnología de información así como la inaplicabilidad de estándares internacionales de gobernabilidad y seguridad en las Cooperativas, pueden conllevar a que no toda la tecnología de información sea auditada y por ende se tenga accesos a información confidencial no autorizada.

El riesgo de incidentes tecnológicos puede presentarse en mayor o menor escala según sea el grado de control interno que mantiene una Cooperativa, cuando se presenta un incidente de tecnología que pueda

afectar la disponibilidad de los sistemas de información, los grandes afectados son los socios y clientes, quienes pueden asociar la falta de servicio, a la incompetencia del personal, a la falta de liquidez de la institución, o a la falta de prevención; lo cual puede afectar la imagen de la Cooperativa generando desconfianza entre sus socios y clientes.

Las Tecnologías de Información y Comunicaciones, se pueden ver afectadas por eventos externos. En la zona centro del país, tenemos latente el riesgo de erupción del volcán Tungurahua, los auditores internos deben ser capaces de recomendar si los controles implementados son suficientes para mitigar la presencia de riesgos externos como desastres naturales, incendios, terremotos, entre otros.

1.2.1.3. Contexto micro

La Cooperativa de Ahorro y Crédito “El Sagrario Ltda.”, fue fundada el 10 de junio de 1964, con el objeto de mejorar las condiciones de vida y satisfacer las necesidad comunes de ahorro y crédito de la población del centro del país, actualmente posee 9 oficinas ubicadas en 7 provincias a nivel nacional, cuenta con más de 70.000 socios y supera los 100 empleados directos. En noviembre del 2007 obtiene el certificado de calidad ISO 9001:2000 a los productos de créditos, inversiones, cuentas de ahorro, atención en ventanillas, tarjetas de débitos, recaudación tributaria, acreditaciones de roles, trasferencias de remesas entre los más importantes. Actualmente ofrece una diversidad de productos apoyados en la tecnología; productos tradicionales como Ahorro, Crédito e Inversiones y productos innovadores como Recaudación de Impuestos, Transacciones en Línea vía WEB, Pagos de servicios básicos, Transferencias Internacionales, mensajería y recargas de minutos celular. Adicionalmente está en proyecto la creación de recaudación de obligaciones patronales y créditos en línea.

La Cooperativa El Sagrario cuenta con un departamento de auditoría interna integrado por 3 personas quienes están encargados del control interno, sin embargo ninguna de estas personas realizan auditorías informáticas debido a que no cuenta con el conocimiento suficiente para efectuarlas. En cambio, el departamento de tecnología está integrado por 6 personas, encargadas del desarrollo de sistemas informáticos y de la administración de toda la infraestructura de red, comunicaciones y seguridades.

Es muy importante que los auditores internos cuenten con una guía para realizar auditorías informáticas que les permita mejorar el control interno y asegurar la disponibilidad de los sistemas de información. Más aún, en la actualidad que la falta de políticas y controles en tecnología, pueden ocasionar vulnerabilidades en los sistemas de información y generar pérdidas económicas.

1.2.2. Análisis crítico

1.2.2.1. Árbol de problemas

Gráfico 1. Árbol de Problemas

Fraudes Informáticos	Sistemas de Información vulnerables	Tecnologías de la información no auditados	Acceso a información confidencial	Baja disponibilidad de los sistemas de información	Servicios y productos inseguros
INADECAUDO CONTROL INTERNO DE LAS TECNOLOGIAS DE INFORMACION					
Debilidad en los controles de seguridad	Incremento de hackers informáticos	Insuficientes políticas de control para auditorias informáticas	Inaplicación de Normas de control basados en COBIT - ISO 27001	Auditorias Informáticas Limitadas	Revisión superficial de nuevos productos y servicios basados en la tecnología

Fuente: Investigación de campo (2011)

Elaborado Por: Jaime Freire

1.2.2.2. Relación causa-efecto

Basándose en la información obtenida en la Matriz de Análisis de Situaciones – MÁS (ver Anexo 1). Se desprende que la causa principal para el inadecuado control interno de las tecnologías de información es ocasionada por las auditorias informáticas limitadas, lo cual puede ocasionar una baja disponibilidad de los sistemas de información en la Cooperativa de Ahorro y Crédito El Sagrario Ltda.

1.2.3. Prognosis

De continuar con un inadecuado control interno de las tecnologías de información de la Cooperativa El Sagrario, está expuesta a vulnerabilidades en sus sistemas informáticos poniendo en riesgo la disponibilidad, confidencialidad e integridad de la información.

En las revisiones anuales que realiza la Superintendencia de Bancos, pueden quedar al descubierto la auditoria informática limitada que práctica el departamento de auditoría, así como detectar deficiencias tecnológicas lo cual puede ser motivo de sanciones y multas.

De mantenerse el problema, la Cooperativa queda muy expuesta a delitos informáticos, lo cual puede afectar gravemente la imagen y provocar una corrida de fondos, inclusive hasta llegar al cierre de la institución.

1.2.4. Formulación del problema

- ¿Son las auditorias informáticas limitadas, la principal causa para la baja disponibilidad de los sistemas de información en la Cooperativa “El Sagrario Ltda.” en el 2010?

1.2.5. Preguntas directrices

- ¿Son convenientes las políticas de auditorías informáticas vigentes en la Cooperativa de Ahorro y Crédito El Sagrario Ltda.?
- ¿Existen procesos críticos de tecnología que pueden afectar mayormente la disponibilidad de los sistemas de información?
- ¿Se mantiene una guía de aplicación de auditorías informáticas para el control interno de las Tecnologías de información y comunicaciones?

1.2.6. Delimitación

- **Campo:** Auditoria
- **Área:** Auditoria Integral
- **Aspecto:** Auditoria Informática
- **Temporal:** El tiempo del problema es del año del 2010
  El tiempo de investigación del 08 enero del 2011 hasta el 30 de septiembre del 2011.
- **Espacial:** La investigación se realizará en la Cooperativa de Ahorro y Crédito El Sagrario Ltda. Ver (Anexo 2)

1.3. JUSTIFICACIÓN

El presente proyecto es necesario realizarlo debido a la necesidad que tiene la Cooperativa de Ahorro y Crédito “El Sagrario Ltda.” de mantener un adecuado control interno sobre las tecnologías de información para asegurar la disponibilidad de los sistemas de información y mantener una atención de calidad a sus miles de socios y clientes.

Todos los productos y servicios que brinda la Cooperativa El Sagrario están soportados por las tecnologías de información y comunicaciones, por lo cual un estudio de aplicación de auditorías informáticas va generar

un gran impacto en la prevención de incidentes de tecnología. En la actualidad el utilizar la tecnología implica estar expuestos a un sinnúmero de riesgos que pueden ocasionar desde pérdidas de información hasta millonarias pérdidas económicas, por lo cual la implementación de controles a tiempo, permiten mitigar la ocurrencia de un evento de riesgo.

Debido a la experiencia en el área de tecnología y al conocimiento adquirido sobre las mejores prácticas de auditorías, es factible y viable proponer una guía de auditoría informática que pueda ser utilizada por los auditores internos de la institución. Los auditores internos serán los principales beneficiarios del presente proyecto quienes en base a la guía planteada podrán realizar auditorías informáticas básicas.

1.4. OBJETIVOS

1.4.1. Objetivo general

- Contribuir con la aplicación de auditorías informáticas internas para asegurar la disponibilidad de los sistemas de información y mejorar el control de las Tecnologías de Información en la Cooperativa de Ahorro y Crédito “El Sagrario Ltda.”

1.4.2. Objetivos específicos

- Analizar las políticas de auditorías informáticas vigentes en la Cooperativa El Sagrario para establecer su pertinencia.
- Definir los procesos críticos de tecnología que pueden afectar la disponibilidad de los sistemas de información para establecer acciones de prevención y control.
- Proponer una guía de auditoría informática para mejorar el control interno de las tecnologías de información.

CAPÍTULO II
MARCO TEÒRICO

2.1. ANTECEDENTES INVESTIGATIVOS

Localmente no se han realizado investigaciones relacionadas a la auditoria informática, sin embargo fuera del país existen algunas obras bibliográficas que sirven para tomar de referencia para la siguiente investigación.

Basándose en el estudio de **Alonso Tamayo Alzate (2005, Internet),** podemos manifestar que la gran mayoría de personas tienen hoy en día que ver con el manejo de la información, ya sea porque trabajan directamente proporcionando datos de entrada, procesando o utilizando los resultados que produce una computadora, o indirectamente a través de la comercialización, fabricación o suministro de insumos informáticos, la tecnología de los sistemas de información está cambiando el modo de vida de la gente y pocos son los ámbitos del diario vivir que han quedado por fuera del vertiginoso desarrollo de la era de la informática y comunicaciones. A través de la tecnología se maneja millones de dólares, por lo tanto es necesario que las empresas den la importancia necesaria al control interno informático.

La dificultad en el manejo de grandes volúmenes de información la necesidad de disponer de información integra, oportuna, segura y confiable, dio origen a la revolución informática, la cual ha generado una creciente dependencia para las empresas y usuarios en general, que se beneficia diariamente de ella con el registro y procesamiento de operaciones; por consiguiente surge la imperiosa necesidad de ejercer control en este campo y es a través de la Auditoria de Sistemas la encargada de estudiar, analizar y asesorar todo lo referente al control del área de sistemas y los recursos involucrados en su desarrollo.

La auditoría de sistemas es la parte de la auditoría interna que se encarga de llevar a cabo la evaluación de normas, controles, técnicas y procedimientos que se tiene establecidos en una empresa para lograr la confiabilidad, oportunidad, seguridad y confidencialidad de la información que procesa a través de computadores; es decir, en estas evaluaciones se está involucrando tanto los elementos técnicos como humanos que intervienen en el proceso de la información.

La auditoría en informática es la revisión y evaluación de los controles, sistemas procedimientos de informática; de los equipos de cómputo, su utilización eficiencia y seguridad, de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

Según **Maria Rocio Calero de la Paz (2005, p. 51-54),** la tecnología juega un papel de creciente relevancia en los mercados actuales. Diversas innovaciones tecnológicas están introduciendo cambios significativos en los procesos de prestación de servicios diferentes industrias. En este sentido, nuevos servicios digitales basados en Internet están alterando de forma sustancia cómo interactúan las compañías, empelados y consumidores durante la prestación de servicios. Estos cambios también se están reflejando de forma significativa en el sector bancario, en un contexto comercial caracterizado por una creciente importancia de las tecnologías de Internet y el interés de las entidades financieras en orientar a sus clientes hacia la utilización de los nuevos canales de distribución.

Las actuales tasas y el crecimiento de la utilización de servicios de banca electrónica, evidencian de forma clara la elevada relevancia de las tecnologías digitales para el futuro del sector bancario a nivel internacional. La capacidad de las entidades para ayudar a que sus

clientes encuentren de forma natura el camino hacia las formas de distribución más económicas será un aspecto crítico para lograr la transición hacia banca de la próxima generación. Los clientes realizarán sus operaciones más habituales sin acercarse a las oficinas, ya que solo irán en busca de asesoramiento para las operaciones de mayor importancia.

Dadas estas ventajas, las entidades financieras están intentando desviar a sus clientes hacia sus servicios por Internet. Impulsando las iniciativas adecuadas, se puede conseguir el reto variar el comportamiento de los clientes. Sin embargo, es importante evitar iniciativas que conlleven cambios obligatorios perjudiciales para los clientes: el objetivo debe ser conciliar las preferencias de los clientes con la rentabilidad ofrecida por los distintos canales de distribución de servicios financieros.

2.2. FUNDAMENTACION FILOSOFICA

La presente investigación se fundamenta en el paradigma positivista, el cual parte de supuestos que luego deben ser comprobados mediante una medición cuantitativa.

Los supuestos que se determinen dentro del control interno de las tecnologías de información en la Cooperativa El Sagrario, serán analizados y comprobados, para luego establecer reglas generales de solución

2.3. FUNDAMENTACION LEGAL

La presente investigación se enmarca dentro de normas y políticas internacionales, nacionales e institucionales, las cuales citamos a continuación.

En el **Libro I. Normas generales para la aplicación de la ley general de instituciones del sistema financiero, Titulo X - De la gestión y administración de riesgos, Capitulo V.- De la gestión del riesgo operativo**, **del 20 de octubre del 2005,** establece los principales controles que hay que implementar sobre la tecnología:

4.3. Tecnología de información.- Las instituciones controladas deben contar con la tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas, procesos y procedimientos que aseguren una adecuada planificación y administración de la tecnología de información.

Según **IT Governance Institute (2005,8-10),** Para muchas empresas, la información y la tecnología que las soportan representan sus más valiosos activos, aunque con frecuencia son poco entendidos. Las empresas exitosas reconocen los beneficios de la tecnología de información y la utilizan para impulsar el valor de sus interesados (stakeholders). Estas empresas también entienden y administran los riesgos asociados, tales como el aumento en requerimientos regulatorios, así como la dependencia crítica de muchos procesos de negocio en tecnología. La necesidad del aseguramiento del valor de tecnología, la administración de los riesgos asociados a tecnología, así como el incremento de requerimientos para controlar la información, se entienden ahora como elementos clave del gobierno de la empresa. El valor, el riesgo y el control constituyen la esencia del gobierno de tecnología. El

gobierno de tecnología es responsabilidad de los ejecutivos, del consejo de directores y consta de liderazgo, estructuras y procesos organizacionales que garantizan que la tecnología de la empresa sostiene y extiende las estrategias y objetivos organizacionales. Más aún, el gobierno de tecnología integra e institucionaliza las buenas prácticas para garantizar que la tecnología de la empresa sirva como base a los objetivos del negocio. De esta manera, el gobierno de tecnología facilita que la empresa aproveche al máximo su información, maximizando así los beneficios, capitalizando las oportunidades y ganando ventajas competitivas. Estos resultados requieren un marco de referencia para controlar la TI, que se ajuste y sirva como soporte al Committee Of Sponsoring Organisations Of The Treadway Commission Control interno—Marco de Referencia integrado, el marco de referencia de control ampliamente aceptado para gobierno de la empresa y para la administración de riesgos, así como a marcos compatibles similares. Las organizaciones deben satisfacer la calidad, los requerimientos fiduciarios y de seguridad de su información, así como de todos sus activos. La dirección también debe optimizar el uso de los recursos disponibles de TI, incluyendo aplicaciones, información, infraestructura y personas. Para descargar estas responsabilidades, así como para lograr sus objetivos, la dirección debe entender el estatus de su arquitectura empresarial para la TI y decidir qué tipo de gobierno y de control debe aplicar.

Los objetivos de control para la Información y la Tecnología relacionada, brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica.

Los conceptos de arquitectura empresarial ayudan a identificar aquellos recursos esenciales para el éxito de los procesos, es decir, aplicaciones, información, infraestructura y personas. En resumen, para proporcionar la información que la empresa necesita para lograr sus objetivos, los recursos de TI deben ser administrados por un conjunto de procesos

agrupados de forma natural. Pero, ¿cómo puede la empresa poner bajo control la TI de tal manera que genere la información que la empresa necesita? ¿Cómo puede administrar los riesgos y asegurar los recursos de TI de los cuales depende tanto? ¿Cómo puede la empresa asegurar que TI logre sus objetivos y soporte los del negocio? Primero, la dirección requiere objetivos de control que definan la última meta de implantar políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar un nivel razonable para garantizar que: Se alcancen los objetivos del negocio. Se prevengan o se detecten y corrijan los eventos no deseados.

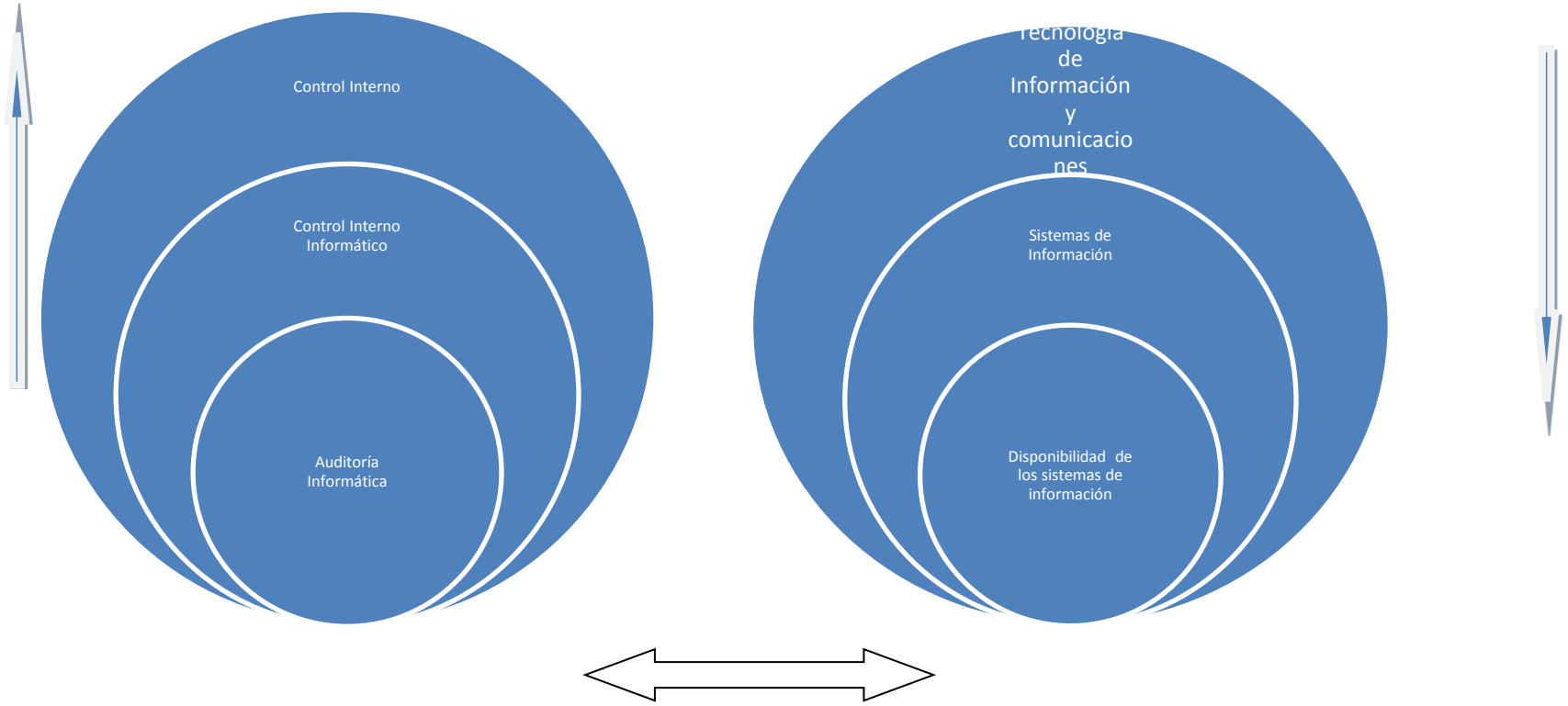
Según **el Manual de políticas y procedimientos de Tecnología (2009,2-3),** La Cooperativa debe contar con Tecnología de Información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitando interrupciones del negocio y logrando que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones. En este Manual se definen políticas y procedimientos que aseguren una adecuada planificación y Administración de la Tecnología de Información.

La Ley de Comercio electrónico (2010), busca que las transacciones efectuadas electrónicamente tengan el respaldo de un contrato legalmente celebrado, que la firma electrónica tenga todas las características de validez y legitimidad, que los documentos electrónicos que soportan una transacción tengan perfecta validez, tanto para efectos comerciales como tributarios. Además la Ley pretende salvaguardar la privacidad de la información que se encuentra en la red, sancionando penalmente a quienes utilicen indebidamente esta información.
Sin duda el comercio electrónico será un sistema que revolucionará la forma de comprar y vender bienes y servicios y su utilización es creciente en el mundo.

2.4. RED CATEGORÍAS FUNDAMENTALES

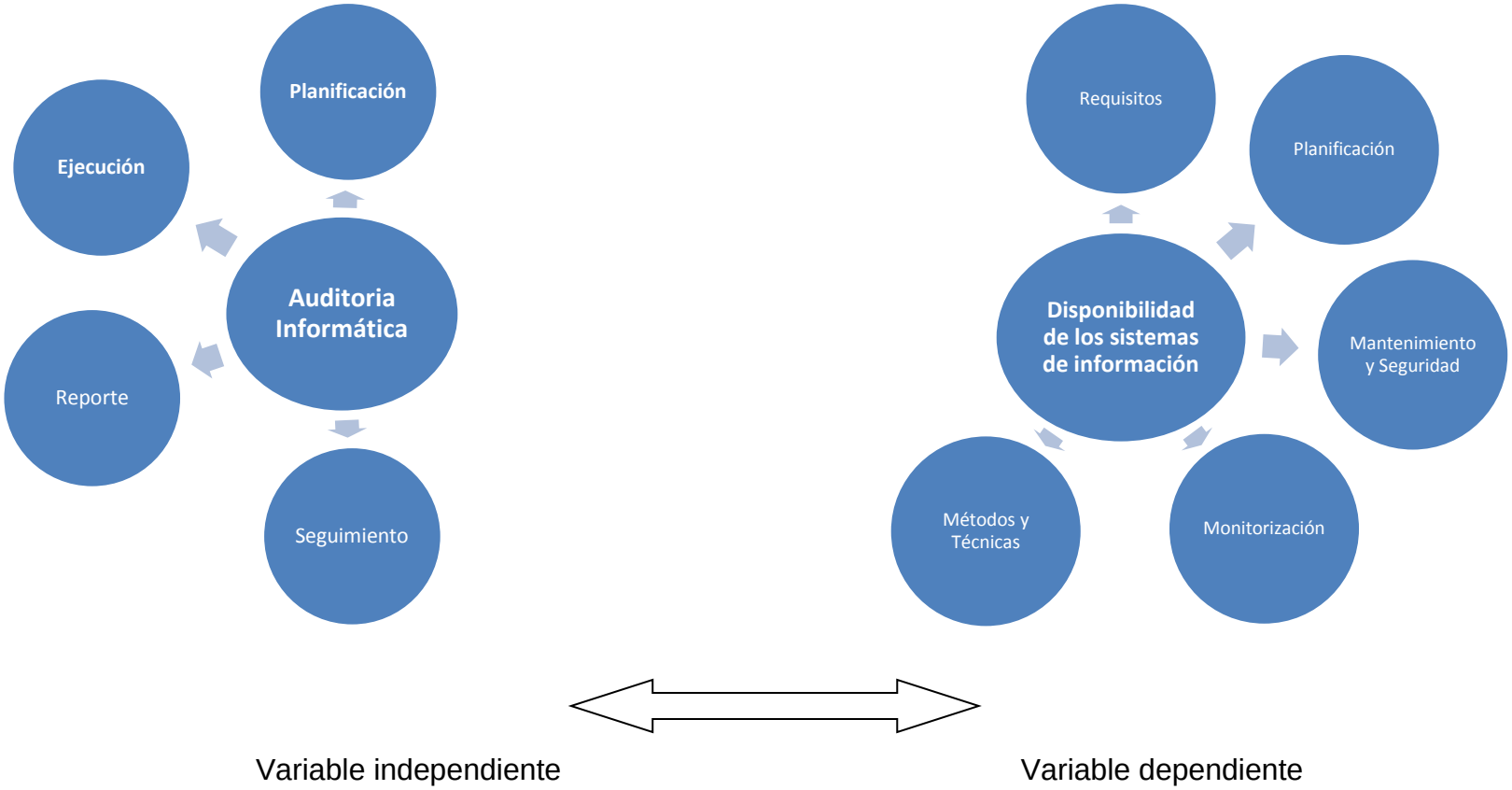
2.4.1. Gráficos de inclusión interrelacionados

- **Superordinación conceptual**



Variable independiente Variable dependiente

- **Subordinación conceptual**



2.4.2. Visión dialéctica de conceptualizaciones que sustentan las variables del problema

2.4.2.1. Marco conceptual variable independiente

Según **José Dagoberto Pinilla**, **(2005:1-4)**, **el control Interno** comprende el plan de organización y la totalidad de los métodos, sistemas y procedimientos, que en forma ordenada, se adoptan en una organización, para asegurar la protección de todos sus recursos, la obtención de información correcta, segura y oportuna, la promoción de economía, eficiencia y efectividad operacional y la adhesión del personal a los objetivos y políticas debidamente predefinidos por la dirección.

El área de control interno debe ser creada con la visión de auditar a todos los procesos de la Cooperativa y no únicamente con un alcance de los estados financieros. Las tecnologías de información y comunicaciones son consideradas procesos críticos dentro de las instituciones financieras por lo cual se debe tener una estructura adecuada para su revisión.

Según **José Dagoberto Pinilla**, **(2005:1-4)**, **el control interno informático** puede definirse como el sistema integrado al proceso administrativo, en la planeación, organización, dirección y control de las operaciones con el objeto de asegurar la protección de todos los recursos informáticos y mejorar los índices de economía, eficiencia y efectividad de los procesos operativos computarizados

El control interno informático debe orientarse al cumplimiento de los siguientes objetivos:

- Establecer como prioridad la seguridad y protección de la información del sistema computacional y de los recursos informáticos de la empresa.

- Promover la confiabilidad, oportunidad y veracidad de la captación de datos, su procesamiento en el sistema y la emisión de informes en la empresa.
- Implementar los métodos, técnicas y procedimientos necesarios para coadyuvar al eficiente desarrollo de las funciones, actividades y tareas de los servicios computacionales, para satisfacer los requerimientos de sistemas en la empresa.
- Instaurar y hacer cumplir las normas, políticas y procedimientos que regulen las actividades de sistematización de la empresa.
- Establecer las acciones necesarias para el adecuado diseño e implementación de sistemas computarizados, a fin de que permitan proporcionar eficientemente los servicios de procesamiento de información en la empresa

Según **Jose Antonio Echenique (2006, p. 16-18),** la **auditoria informática** es la revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

De acuerdo con **JUNTA DE ESTÁNDARES DE LA ASOCIACIÓN DE AUDITORÍA Y CONTROL DE SISTEMAS DE INFORMACIÓN (2005**), la auditoría informática deberá comprender no sólo la evaluación de los equipos de cómputo o de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información. Para la realización de una auditoria informática se deben tomar en cuenta las siguientes actividades:

a. Planificación.

En la planificación de una auditoria informática se deben cumplir con los siguientes aspectos:

- El auditor debe planear el alcance de la auditoría informática para cubrir los objetivos planteados y cumplir con las leyes aplicables y las normas profesionales de auditoría.
- El auditor debe desarrollar y documentar un enfoque de auditoría basado en riesgos.
- El auditor debe desarrollar y documentar un plan de auditoría que detalle la naturaleza y los objetivos de la auditoría, los plazos y alcance, así como los recursos requeridos.
- El auditor debe desarrollar un programa y/o plan de auditoría detallando la naturaleza, los plazos y el alcance de los procedimientos requeridos para completar la auditoría.
- Para una función de auditoría interna, debe desarrollarse/actualizarse un plan, al menos una vez al año, para las actividades permanentes. El plan debe servir como marco de referencia para las actividades de auditoría y servir para abordar las responsabilidades establecidas por el estatuto de auditoría. El nuevo/actualizado plan debe ser aprobado por un consejo de administración.
- Para el caso de una auditoría externa, normalmente debe prepararse un plan para cada una de las tareas, sean o no de auditoría. El plan debe documentar los objetivos de la auditoría.
- El auditor debe obtener un entendimiento de la actividad que está siendo auditada. El grado del conocimiento requerido debe ser determinado por la naturaleza de la organización, su entorno y riesgos, y por los objetivos de la auditoría.
- El auditor debe realizar una evaluación de riesgos para brindar una garantía razonable de que todos los elementos materiales serán

cubiertos adecuadamente durante la auditoría. En este momento, es posible establecer las estrategias de auditoría, los niveles de materialidad y los recursos necesarios.

- El programa y/o plan de auditoría puede requerir ajustes durante el desarrollo de la auditoría para abordar las situaciones que surjan (nuevos riesgos, suposiciones incorrectas o hallazgos en los procedimientos ya realizados) durante la auditoría.

b. Ejecución de la Auditoria.

A continuación se enuncian normas que proporcionar asesoría con respecto a la realización de las auditorias:

- Supervisión. El personal de auditoría debe ser supervisado para brindar una garantía razonable de que se lograrán los objetivos de la auditoría y que se cumplirán las normas profesionales de auditoría aplicables.
- Evidencia. Durante el transcurso de la auditoría, el auditor debe obtener evidencia suficiente, confiable y pertinente para alcanzar los objetivos de auditoría. Los hallazgos y conclusiones de la auditoría deberán ser soportados mediante un apropiado análisis e interpretación de dicha evidencia.
- Documentación. El proceso de auditoría deberá documentarse, describiendo las labores de auditoría realizadas y la evidencia de auditoría que respalda los hallazgos y conclusiones del auditor.
- Se deben establecer los roles y responsabilidades del equipo de auditoría al iniciarse la auditoría, y como mínimo deben definirse los roles de decisión, ejecución y revisión.
- Las labores realizadas durante la ejecución del trabajo deben organizarse y documentarse siguiendo procedimientos documentados predefinidos. La documentación debe incluir aspectos tales como los objetivos y alcance del trabajo, el

programa de auditoría, los pasos de auditoría realizados, la evidencia recogida, los hallazgos, conclusiones y recomendaciones.

- La documentación de auditoría debe ser suficiente para permitir que una tercera entidad independiente vuelva a realizar todas las tareas realizadas durante la auditoría para llegar a las mismas conclusiones.
- La documentación de auditoría debe incluir detalles de quién realizó cada tarea de auditoría y sus funciones. Como regla general, cada tarea, decisión, paso o resultado de la auditoría realizado por un miembro o grupo de miembros del equipo deberá ser revisado por otra persona del equipo, nombrada de acuerdo con la importancia del elemento considerado.
- El auditor debe planificar el uso de la evidencia de auditoría obtenida de manera coherente con la importancia del objetivo de la auditoría y el tiempo y esfuerzo involucrados en obtener la evidencia de auditoría.
- La evidencia de auditoría debe ser suficiente, confiable y pertinente para formar una opinión o respaldar los hallazgos y conclusiones del auditor. Si, en opinión del auditor, la evidencia de auditoría obtenida no cumple con estos criterios, el auditor deberá obtener evidencia de auditoría adicional.

c. Reporte de Auditoria

Las siguientes normas establecen y proporcionar asesoría sobre la generación del informe, a fin de que el auditor pueda cumplir con esta responsabilidad para que se presente un documento que sea muy claro para el personal:

- El auditor debe suministrar un informe, en un formato apropiado, al finalizar la auditoría. El informe debe identificar la organización, los

destinatarios previstos y respetar cualquier restricción con respecto a su circulación.

- El informe de auditoría debe indicar el alcance, los objetivos, el período de cobertura y la naturaleza, plazo y extensión de las labores de auditoría realizadas.
- El informe debe indicar los hallazgos, conclusiones y recomendaciones, así como cualquier reserva, calificación o limitación que el auditor tuviese en cuanto al alcance de la auditoría.
- El auditor debe tener evidencia de auditoría suficiente y apropiada para respaldar los resultados reportados.
- Al emitirse, el informe del auditor debe ser firmado, fechado y distribuido de acuerdo con los términos del estatuto de auditoría o carta de compromiso.
- El formato y contenido del informe generalmente varían según el tipo auditoría realizada. Un auditor puede realizar cualquiera de las siguientes acciones:

    - Auditoría (de manera directa o como testigo)
    - Revisión (de manera directa o como testigo)
    - Procedimientos acordados

- Cuando se requiera que el auditor proporcione una opinión sobre el entorno de control y exista evidencia de auditoría sobre una debilidad material o significativa, el auditor no deberá concluir que los controles internos son eficaces. El informe del auditor debe describir la debilidad material o significativa y el efecto en el logro de los objetivos de los criterios de control.
- El auditor debe comentar el contenido del informe en borrador con la gerencia del área bajo revisión antes de la finalización y divulgación, e incluir los comentarios de la gerencia en el informe final cuando corresponda.

- Cuando el auditor encuentre deficiencias significativas en el entorno de control, el auditor debe informar sobre estas deficiencias al comité de auditoría o a la autoridad responsable y comentar en el informe que se han comunicado dichas deficiencias significativas.
- Cuando el auditor emita informes separados, el informe final deberá hacer referencia a todos los informes separados.
- El auditor debe considerar y evaluar si comunicará a la gerencia acerca de las deficiencias en los controles internos de menor magnitud que las deficiencias significativas. En tales casos, el auditor debe informar al comité de auditoría o a la autoridad responsable que se han comunicado a la gerencia dichas deficiencias del control interno.
- El auditor debe solicitar y evaluar la información sobre los hallazgos, las conclusiones y las recomendaciones de informes anteriores a fin de determinar si se han implementado las acciones apropiadas de manera oportuna.

d. Monitoreo y Control

Las siguientes normas proporcionan asesoría con respecto a las actividades de seguimiento realizadas durante un proceso de auditoría, que deben ser tomadas en cuenta:

- Después de informar/reportar sobre los hallazgos y las recomendaciones, el auditor debe solicitar y evaluar la información relevante para concluir si la gerencia tomó las acciones apropiadas de manera oportuna.
- Si las acciones propuestas por la gerencia para implementar las recomendaciones notificadas se proporcionaron al auditor, se comentaron con éste, dichas acciones deberán registrarse en el informe final como la respuesta de la gerencia.

- La naturaleza, los plazos y la extensión de las actividades de seguimiento deben tener en cuenta la importancia de los hallazgos reportados y el impacto, en caso de no haberse tomado las acciones correctivas. Los plazos de las actividades de seguimiento de una auditoría en relación con el informe original deben basarse en el juicio profesional y depender de una serie de consideraciones tales como la naturaleza o magnitud de los riesgos y costos asociados a la entidad.
- La función de auditoría interna debe establecer un proceso de seguimiento para monitorear y asegurar que las acciones de la gerencia efectivamente han sido implementadas o que la gerencia superior ha aceptado el riesgo de no haber tomado la acción pertinente. La responsabilidad por estas actividades de seguimiento puede definirse en el estatuto de auditoría.
- Cuando la gerencia proporcione información sobre las acciones tomadas para implementar las recomendaciones y el auditor tenga dudas con respecto a la información suministrada, se deberán llevar a cabo las pruebas apropiadas u otros procedimientos para determinar la posición o estado reales antes de concluir las actividades de seguimiento.
- Puede presentarse un informe, sobre el estado de las actividades de seguimiento, que incluya las recomendaciones aceptadas no implementadas, ante el comité de auditoría en caso de que éste se haya establecido, o, como alternativa, al nivel apropiado de la gerencia de la entidad.
- Como parte de las actividades de seguimiento, el auditor deberá evaluar si los hallazgos no implementados siguen siendo importantes.

2.4.2.2. Marco conceptual variable dependiente

Basados en la investigación de **Ramón Carlos Suarez (2007, 2-30),** podemos manifestar que la **Tecnología de la información** es la ciencia que estudia los medios técnicos y los procesos empleados en las diferentes ramas de la industria y de los negocios que actúan sobre los datos y la información, los mismos que son enviados o transmitidos a través de sistemas de comunicación. Una buena gestión de tecnología debe enfocarse en los siguientes procesos:

Planeación y organización: Abarca las decisiones estratégicas y tácticas que definen la manera en que la tecnología de información contribuirá de mejor manera para el logro de los objetivos de la Entidad. También se refiere a la manera en que esta visión estratégica genere planes, organización, infraestructura tecnológica y procedimientos administrativos.

Adquisición e Implementación: para poner en práctica las estrategias definidas se deben identificar las soluciones de tecnología, adquirirlas o desarrollarlas y por su puesto hacerlas operativas (implementación) integrándolas como procedimientos del día a día. Forman parte de esta área todas las modificaciones que hacen posible la continuidad operativa de lo implantado, tanto para adecuaciones que devienen de cambios en el entorno como aquellas que se refieren a mejoras operativas.

Producción y Servicios: Esta área abarca las actividades que relacionadas con los sistemas en producción de los servicios de tecnología, engloban las actividades tradicionales de producción, las de entrenamiento, los procedimientos para garantizar la continuidad de los servicios, operaciones de seguridad. También abarcan las actividades de Soporte a los sistemas de producción. Esta área incluye el procesamiento de los datos por sistemas de aplicación.

Monitoreo: Todos los procesos de tecnología deben ser evaluados regularmente, tanto en cuanto a su calidad, como al cumplimiento de los requerimientos de control. Esta área atiende la participación de la gerencia y demás órganos de línea en los procesos de retroalimentación de los mecanismos de verificación y la evaluación proveniente de auditorías internas y externas.

De acuerdo a Ecolink (2009), podemos manifestar que los Sistemas de Información son un conjunto de elementos interrelacionados con el propósito de prestar atención a las demandas de información de una organización, para elevar el nivel de conocimientos que permitan un mejor apoyo a la toma de decisiones y desarrollo de acciones.

Un sistema de información realiza cuatro actividades básicas: **entrada, almacenamiento, procesamiento y salida de información**.

Entrada de Información: Es el proceso mediante el cual el Sistema de Información toma los datos que requiere para procesar la información. Las entradas pueden ser manuales o automáticas. Las manuales son aquellas que se proporcionan en forma directa por el usuario, mientras que las automáticas son datos o información que provienen o son tomados de otros sistemas o módulos. Esto último se denomina interfaces automáticas.

Almacenamiento de información: Los datos son almacenados en base de datos, los cuales deben cumplir con políticas de replicación y respaldo de datos para garantizar la disponibilidad, confidencialidad, integridad y seguridad de la información.

Procesamiento de Información: Es la capacidad del Sistema de Información para efectuar cálculos de acuerdo con una secuencia de operaciones preestablecida. Estos cálculos pueden efectuarse con datos

introducidos recientemente en el sistema o bien con datos que están almacenados. Esta característica de los sistemas permite la transformación de datos fuente en información que puede ser utilizada para la toma de decisiones.

Según **ITIL V3 (2011),** el objetivo primordial de la Gestión de la Disponibilidad es asegurar que los servicios tecnología, estén disponibles y funcionen correctamente siempre que los clientes y usuarios deseen hacer uso de ellos en el marco de los acuerdos de los niveles de servicio. Las responsabilidades de la Gestión de la Disponibilidad incluyen:

- Determinar los requisitos de disponibilidad en estrecha colaboración con los clientes.
- Garantizar el nivel de disponibilidad establecido para los servicios de tecnología.
- Monitorizar la disponibilidad de los sistemas de información.
- Proponer mejoras en la infraestructura y servicios TI con el objetivo de aumentar los niveles de disponibilidad.

Los indicadores clave sobre los que se sustenta el proceso de Gestión de la Disponibilidad se resumen en:

- Disponibilidad: porcentaje de tiempo sobre el total acordado en que los servicios Tecnología han sido accesibles al usuario y han funcionado correctamente.
- Fiabilidad: medida del tiempo durante el cual los servicios han funcionado correctamente de forma ininterrumpida.

La disponibilidad depende del correcto diseño de los servicios de tecnología, su correcto mantenimiento y la calidad de los servicios internos y externos acordados. Los principales beneficios de una correcta Gestión de la Disponibilidad son:

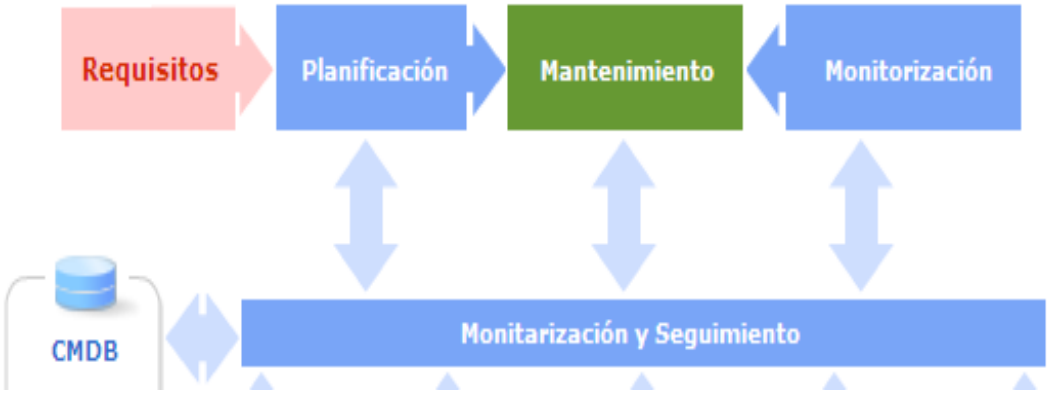
- Cumplimiento de los niveles de disponibilidad acordados.
- Se reducen los costes asociados a un alto nivel de disponibilidad.
- El cliente percibe una mayor calidad de servicio.
- Se aumentan progresivamente los niveles de disponibilidad.
- Se reduce el número de incidentes.

Las principales dificultades con las que topa la Gestión de la Disponibilidad son:

- No se monitoriza correctamente la disponibilidad real del servicio.
- No existe compromiso con el proceso dentro de la organización TI.
- No se dispone de las herramientas de software y personal adecuado.
- Los objetivos de disponibilidad no están alineados con las necesidades del cliente.
- Falta de coordinación con los otros procesos.
- Los proveedores internos y externos no reconocen la autoridad del Gestor de la Disponibilidad por falta de apoyo de la dirección.

Los procesos de gestión de la disponibilidad se muestran en el siguiente gráfico:

Gráfico 2. Procesos de Gestión de la disponibilidad



Fuente: Investigación de campo (2011)

Elaborado Por: Jaime Freire

a. Requisitos de Disponibilidad

Es indispensable cuantificar los requisitos de disponibilidad para la correcta elaboración de los acuerdos de niveles de servicio. La disponibilidad propuesta debe encontrase en línea tanto con los necesidades reales del negocio como con las posibilidades de la organización de tecnología.

Aunque en principio todos los clientes estarán de acuerdo con unas elevadas cotas de disponibilidad es importante hacerles ver que una alta disponibilidad puede generar unos costes injustificados, dadas sus necesidades reales. Quizá unas pocas horas sin un determinado servicio pueden representar poco más allá de una pequeña inconveniencia mientras que la certeza de un servicio prácticamente continuo y sin interrupciones puede requerir la replicación de sistemas u otras medidas igualmente costosas que no van a tener una repercusión real en la rentabilidad del negocio. Para llevar a cabo eficientemente está tarea es necesario que la Gestión de la Disponibilidad:

- Identifique las actividades clave del negocio.
- Cuantifique los intervalos razonables de interrupción de los diferentes servicios dependiendo de sus respectivos impactos.
- Establezca los protocolos de mantenimiento y revisión de los servicios TI.
- Determine las franjas horarias de disponibilidad de los servicios de tecnología.

b. Planificación

La correcta planificación de la disponibilidad permite establecer unos niveles adecuados tanto en lo que respecta a las necesidades reales del negocio como a las posibilidades de la organización de tecnología.

El documento que debe recoger los objetivos de disponibilidad presentes y futuros y que medidas son necesarias para su cumplimiento es el Plan de Disponibilidad. Este plan debe recoger:

- La situación actual de disponibilidad de los servicios de tecnología. Obviamente esta información debe ser actualizada periódicamente.
- Herramientas para la monitorización de la disponibilidad.
- Métodos y técnicas de análisis a utilizar.
- Definiciones relevantes y precisas de las métricas a utilizar.
- Planes de mejora de la disponibilidad.
- Expectativas futuras de disponibilidad.

c. Diseño para la Disponibilidad

Es crucial para una correcta Gestión de la Disponibilidad participar desde el inicio en el desarrollo de los nuevos servicios de tecnología de forma que estos cumplan los estándares plasmados en el Plan de Disponibilidad.

Un diferente nivel de disponibilidad puede requerir cambios drásticos en los recursos utilizados o en las actividades necesarias para suministrar un determinado servicio de tecnología. Si éste se diseña sin tener en cuenta futuras necesidades de disponibilidad puede ser necesario un completo rediseño al cabo de poco tiempo, incurriendo en costes adicionales innecesarios.

d. Mantenimiento y Seguridad

Aunque hayamos realizado un correcto diseño de los servicios según el Plan de Disponibilidad y se hayan tomado todas las medidas preventivas necesarias, tarde o temprano, nos habremos de enfrentar a interrupciones

del servicio. En esos casos es necesario recuperar el servicio lo antes posible para que no tenga un efecto indeseado sobre los niveles de disponibilidad acordados.

e. Monitorización de la Disponibilidad

La monitorización de la disponibilidad del servicio y la elaboración de los informes correspondientes son dos de las principales actividades de la Gestión de la Disponibilidad. Desde el momento de la interrupción del servicio hasta su restitución o "tiempo de parada" el incidente pasa por distintas fases que deben ser individualizadamente analizadas:

- Tiempo de detección: es el tiempo que transcurre desde que ocurre el fallo hasta que la organización TI tiene constancia del mismo.
- Tiempo de respuesta: es el tiempo que transcurre desde la detección del problema hasta que se realiza un registro y diagnóstico del incidente.
- Tiempo de reparación/recuperación: periodo de tiempo utilizado para reparar el fallo o encontrar un "workaround" o solución temporal al mismo y devolver el sistema a la situación anterior a la interrupción del servicio.

Gráfico 3. Interrupción y recuperación del servicio

Fuente: Investigación de campo (2011)

Elaborado Por: Jaime Freire

Es importante determinar métricas que permitan medir con precisión las diferentes fases del ciclo de vida de la interrupción del servicio. El cliente debe conocer estas métricas y dar su conformidad a las mismas para evitar malentendidos. En algunos casos es difícil determinar si el sistema está "caído o en funcionamiento" y la interpretación puede diferir entre proveedores y clientes, por lo tanto, estás métricas deben de poder expresarse en términos que el cliente pueda entender.

Algunos de los parámetros que suele utilizar la Gestión de la Disponibilidad y que debe poner a disposición del cliente en los informes de disponibilidad correspondientes incluyen:

- Tiempo Medio de Parada (Downtime): que es el tiempo promedio de duración de una interrupción de servicio, e incluye el tiempo de detección, respuesta y resolución.
- Tiempo Medio entre Fallos (Uptime): es el tiempo medio durante el cual el servicio está disponible sin interrupciones.
- Tiempo Medio entre Incidentes: es el tiempo medio transcurrido entre incidentes que es igual a la suma del Tiempo Medio de Parada y el Tiempo Medio entre Fallos. El Tiempo Medio entre Incidentes es una medida de la fiabilidad del sistema.

f. Técnicas

Es habitual definir la disponibilidad en tanto por ciento de la siguiente manera:

$$\% \text{ Disponibilidad} = \frac{(AST - DT)}{AST} \cdot 100$$

Dónde:
AST se corresponde con el tiempo acordado de servicio, DT es el tiempo de interrupción del servicio durante las franjas horarias de disponibilidad acordadas.
Por ejemplo, si el servicio es 24/7 y en el último mes el sistema ha estado caído durante 4 horas por tareas de mantenimiento la disponibilidad real del servicio fue:

$$\% \text{ Disponibilidad} = \frac{(720 - 4)}{720} \cdot 100 = 99{,}4\ \%$$

La Gestión de la Disponibilidad tiene a su disposición un buen número de métodos y técnicas que le permiten determinar qué factores intervienen en la disponibilidad del servicio y que le permiten consecuentemente prever qué tipo de recursos se deben asignar para las labores de prevención, mantenimiento y recuperación, así como elaborar planes de mejora a partir de dichos análisis.

2.5. HIPOTESIS

Con la presente investigación se va demostrar que la aplicación de los controles recomendados en las auditorias informáticas aumenta la disponibilidad de los sistemas de información en la Cooperativa “El Sagrario Ltda. en el periodo 2010”.

2.6. SEÑALAMIENTO DE LAS VARIABLES DE LA HIPÓTESIS

- **Variable independiente:** Auditorias informáticas
- **Variable dependiente:** disponibilidad de los sistemas de información
- **Unidad de observación:** Cooperativa “El Sagrario Ltda.”.
- **Términos de relación:** aumenta

CAPÍTULO III
METODOLOGÍA DE LA INVESTIGACIÓN

3.1. MODALIDAD BÁSICA DE LA INVESTIGACIÓN

La modalidad básica de investigación a utilizar en este proyecto es la investigación de campo la cual se realiza en el lugar de los hechos *"in situ",* utilizando fuentes primarias de información como entrevistas, encuestas, observación

Polonsky & Waller (2011), resalta la importancia de la investigación de campo que es el estudio sistemático de los hechos en el lugar en que se producen los acontecimientos. En esta modalidad el investigador toma contacto en forma directa con la realidad, para obtener información de acuerdo con los objetivos del proyecto

Adicionalmente este proyecto utilizará la investigación documental-bibliográfica, que tiene por propósito detectar, ampliar y profundizar diferentes enfoques, teorías, conceptualizaciones y criterios de diversos autores sobre una cuestión determinada, basándose en documentos (fuentes primarias), o en libros, revistas, periódicos, y otras publicaciones (fuentes secundarias).- su aplicación se recomienda especialmente en estudios sociales comparados de diferente modelos, tendencia o de realidades socioculturales; en estudios geográficos, históricos, geopolíticos, literarios, entre otros. (Polonsky & Waller, 2011).

3.2. NIVEL O TIPO DE INVESTIGACIÓN

Existen varios niveles de investigación que se puede utilizar en los proyectos de investigación entre los más importantes citamos los siguientes:

3.2.1. Investigación exploratoria

Esta investigación tiene por objeto ayudar a que el investigador se familiarice con la situación problema, identifique las variables más importantes, reconozca otros cursos de acción, proponga pistas idóneas para trabajos posteriores y puntualice cuál de esas posibilidades tiene la máxima prioridad en la asignación de los escasos recursos presupuestarios de la empresa. En pocas palabras, la finalidad de los estudios exploratorios es ayudar a obtener, con relativa rapidez, ideas y conocimientos en una situación. Es un tipo de investigación extremadamente útil como paso inicial en los procesos de investigación. La utilización de este método tipo de investigación se aplicara a través de entrevistas al personal de los procesos gerencial, cadena de valor y apoyo

3.2.2. Investigación descriptiva

Los estudios descriptivos exigen que el investigador identifique de antemano las preguntas específicas que desea contestar, cómo las responderá y las implicaciones que posiblemente tengan para el gerente de mercadotecnia. Es preciso que se fije una finalidad bien definida. Es probable que la investigación descriptiva proporcione resultados que dan origen a otros trabajos de la misma índole. Aplicando este nivel de investigación se conseguirá: describir características de los grupos operativos, describir fortalezas y debilidades de la empresa, medir la eficacia de los controles de tecnología aplicada.

3.2.3. Investigación asociación de variables

La utilidad de este nivel de investigación en el presente trabajo estará relacionada con la definición del problema, revisión de las literaturas

citadas, tomando en consideración la medición de las variables, su grado de relación o asociación.

3.3. POBLACIÓN Y MUESTRA

3.3.1. Población

Una población está determinada por sus características definitorias, por tanto el conjunto de elementos que posea esta característica se denomina población o universo. Según **Polonsky & Waller (2011),** p*oblación* es la totalidad del fenómeno a estudiar en donde las unidades de población poseen una característica común a la cual se estudia, y da origen a los datos de investigación.

Para el desarrollo del presente trabajo de investigación, se aplicará la fórmula de la población finita por proporción, por conocer el número de personal que labora en la Cooperativa de Ahorro y Crédito EL Sagrario Ltda, quienes están ubicados en cada una de las agencias de acuerdo a lo siguiente:

Tabla 1. Detalle de la Población

Oficina	Total Empleados
MATRIZ	35
RIOBAMBA	15
LATACUNGA	14
QUITO	8
GUARANDA	10
BABAHOYO	9
SIMON BOLIVAR	6
MILAGRO	8
TOTAL	105

Fuente: Nomina de Empleados Cooperativa El Sagrario Ltda.

Elaborado por: Jaime Freire

3.3.2. Muestra

Cuando seleccionamos algunos de los elementos con la intención de averiguar algo sobre la población de la cual están tomados, nos referimos a ese grupo de elementos como *muestra*. Esperamos, desde luego, que lo que averiguamos en la muestra sea cierto para la población como conjunto. Este puede o no ser el caso, cuan exacta sea la información que recibimos correspondiente con lo que hallaríamos por un censo comparable de la población, depende en gran manera de la forma en que sea seleccionada la muestra.

Tabla 2. Valores Z para determinación del tamaño de la Muestra

Nivel de Confianza (%)	AREA	Z
95 %	0.45	1.65
99 %	0.49	2.33

Fuente: Profesor Rubio López

Elaborado por: Jaime Freire

3.3.2.1 Calculo de la Muestra

Para el cálculo de la muestra se considera un nivel de confianza del 95%, con un margen de error que no excede del 5% y una probabilidad de éxito de un 50%. La simbología a utilizar es la siguiente:

z= Unidades estándar correspondiente al nivel de confianza empleado (95% según tabla equivale a 1,65) (ver tabla)

E= Es el máximo error permisible

p= es la probabilidad de éxito de que ocurra un suceso

q= Es la probabilidad de que no ocurra un suceso (q=1-p)

N= Es el tamaño de la población

n= Tamaño de la Muestra

NC=Nivel de Confianza

Para el cálculo de la muestra de la presente investigación vamos utilizar la fórmula de cálculo de una población finita.

$$n = \frac{z^2 Npq}{(N-1)E^2 + z^2 pq}$$

Datos:

NC= 95% ⟶ Z= 1.65

E = 5% = 0,05

N= 105

p= 50% = 0,5 q= (1-p)

q= (1-0,5)

q= 0,5

$$n = \frac{(1,65)^2(105)(0,5)(0,5)}{(105-1)\ (0,05)^2 + (1,65)^2\ (0,5)\ (0,5)}$$

n = 75.97 ⟶ n = 76

3.3.2.2 Determinación de la muestra por oficina.

El tamaño de la muestra es 76 personas, se determina la cuota de muestreo utilizando el muestreo probabilístico por conglomerado, por cuanto la población se subdivide en unidades que para nuestro caso serían las distintas agencias de la Cooperativa El Sagrario, quedando distribuido de la siguiente manera:

Tabla 3. Determinación del tamaño de la muestra por oficina

Oficina	Total Empleados	% de participación	Muestra
MATRIZ	35	33	25
RIOBAMBA	15	14	11
LATACUNGA	14	13	10
QUITO	8	8	6
GUARANDA	10	10	7
BABAHOYO	9	9	7
SIMON BOLIVAR	6	6	4
MILAGRO	8	8	6
TOTAL	105	100%	76

Fuente: Nomina de Empleados Cooperativa El Sagrario Ltda.

Elaborado por: Jaime Freire

3.4. OPERACIONALIZACIÓN DE LAS VARIABLES

3.4.1. Operacionalización de la variable independiente

VARIABLE INDEPENDIENTE: Auditoria Informática				
Conceptualización	**Categorías**	**Indicadores**	**Ítems Básicos**	**Técnicas de recolección**
Las auditorias informáticas se conceptúa como: Es la revisión y evaluación de los controles, sistemas y procedimientos de la Tecnología de Información, sus recursos, utilización eficiencia y seguridad para lograr los objetivos del negocio	Evaluación administrativa del área de TI.	Cumplimiento de planes operativos > 95%	¿ Porque el plan operativo no se cumple al 100%	Cuestionario (Anexo 3)
	Evaluaciones de hardware	Equipos inventariados sobre el total de equipos >=90%	¿Por qué el 10 % de equipos no se encuentran inventariados?	Cuestionario (Anexo 3)
		Equipos que cumplen el estándar / sobre total de equipos>80%	¿Por qué el 20% de los equipos se encuentran desactualizados y no cumplen estándares?	
	Evaluaciones de software	Déficit de licencias menor a 10 % del total de licencias adquiridas	¿Por qué se instala software no licenciado en la institución?	Cuestionario (Anexo 3)
		Numero de errores en aplicativo financiero < al 5 por ciento de funcionalidades puestas en producción	Por qué se producen un 5% de errores al momento de publicar en producción nuevos cambios	

3.4.2. Operacionalización de la variable dependiente

VARIABLE DEPENDIENTE: Disponibilidad de los sistemas de información				
Conceptualización	**Categorías**	**Indicadores**	**Ítems Básicos**	**Técnicas de recolección**
La disponibilidad de los sistemas de información se conceptúa como: Se refiere al tiempo en que los sistemas de información se encuentran disponibles para las actividades requeridas por los procesos del negocio.	Disponibilidad de Base de Datos	La disponibilidad de la base de datos debe ser un 99.6% mensual	¿Cuántas horas sin base de datos puede soportar la institución?	Cuestionario (Anexo 3)
		Ingresos directos a base de datos menor o igual 1% de numero de objetos creados	¿Han existido fraudes internos por acceso a la base de datos de producción?	
	Disponibilidad de Comunicaciones	La disponibilidad de comunicaciones debe ser superior al 99.6%	¿Es necesario contar con enlaces de backup para tener una disponibilidad mayor al 99.6%?	Cuestionario (Anexo 3)
		Cumplimiento mínimo de dos mantenimientos preventivos al año	¿Es necesaria la realización de dos mantenimientos como mínimo en los enlaces de comunicación?	

3.5. PLAN DE RECOLECCIÓN DE INFORMACIÓN

Metodológicamente para **Luis Herrera E. y otros (2002: 174-178 y 183-185)**, la construcción de la información se opera en dos fases: plan para la recolección de información y plan para el procesamiento de información.

Este plan contempla estrategias metodológicas requeridas por los objetivos e hipótesis de investigación, de acuerdo con el enfoque escogido, considerando los siguientes elementos:

- **Definición de los sujetos:**

Los sujetos que van a ser investigados son los empleados que laboran en las distintas oficinas de la Cooperativa de Ahorro y Crédito el Sagrario Ltda. principalmente el Subgerente de tecnología y el Auditor Interno.

- **Selección de las técnicas a emplear en el proceso de recolección de información**.

  Las técnicas a utilizar son la entrevista y la encuesta mediante las cuales se pretende obtener la mayor cantidad de información para nuestro proyecto de investigación.

- **Instrumentos seleccionados o diseñados de acuerdo con la técnica escogida para la investigación**.

El instrumento para la recolección de información, es el cuestionario que es un conjunto de preguntas, preparado cuidadosamente, sobre los hechos y aspectos que interesan en una investigación, para que sea contestado por la población o su muestra.

- **Explicitación de procedimientos para la recolección de información.**

El método de investigación a utilizarse en el presente proyecto es el Deductivo.

El método deductivo es aquel que parte de verdades previamente establecidas como principio general para luego aplicarlo a casos individuales y comprobar así su validez. La deducción o conclusión va de los principios generales ya conocidos a lo particular; recurriendo para ello a la aplicación, comprobación y demostración.

Tabla 4. Procedimiento de recolección de información

TÉCNICAS	**PROCEDIMIENTO**
Encuesta	¿Cómo? método deductivo
	¿Dónde? Cooperativa El Sagrario
	¿Cuándo? 10/06/2011

Fuente: Investigación de Campo (2011)

Elaborado por: Jaime Freire

3.6. PLAN DE PROCESAMIENTO DE INFORMACIÓN

3.6.1 Revisión crítica de la información recogida. Es decir limpieza de información defectuosa: contradictoria, incompleta, no pertinente, etc.

3.6.2 Repetición de la recolección. En ciertos casos individuales, para corregir fallas de contestación.

3.6.3 Tabulación o cuadros según variables de cada hipótesis: manejo de información, estudio estadístico de datos para presentación de resultados.

Tabla 5. Cuantificación de resultados

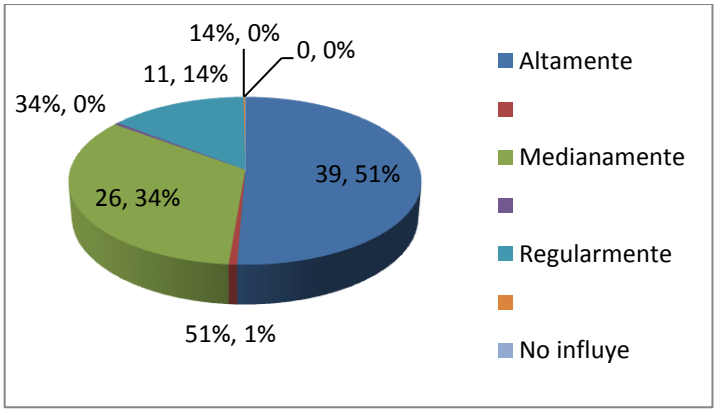
PREGUNTAS	X	y	z	TOTALES
1				
2				
N				

Fuente: Investigación de Campo (2011)

Elaborador por: Jaime Freire

- **Representaciones gráficas**. Ejemplo de figura a ser utilizada para la presentación visual porcentual de los resultados cuantificados en la tabla anterior.

Gráfico 4. Representación gráfica de resultados



Fuente: Investigación de Campo (2011)

Elaborador por: Jaime Freire

CAPITULO IV

ANALISIS E INTERPRETACION DE RESULTADOS

4.1 / 4.2 ANÁLISIS E INTERPRETACION DE RESULTADOS

Cada uno de los resultados del cuestionario aplicado a los empleados de la Cooperativa EL Sagrario Ltda se analiza e interpreta a continuación:

Pregunta 1. ¿En qué grado considera usted, que la aplicación del plan de continuidad y contingencias vigente en la institución, ayuda a mantener la disponibilidad de los sistemas de información?

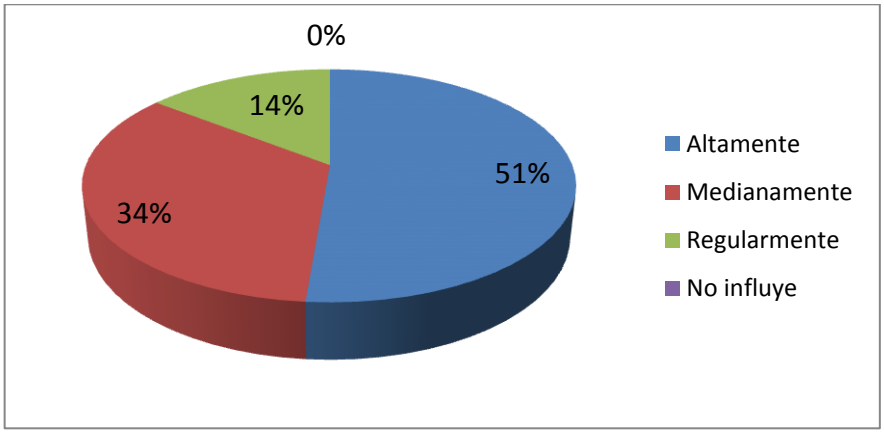
Tabla 6. Resultados de la pregunta 1 de la encuesta

Agencia	Altamente		Medianamente		Regularmente		No influye		Total
	Frecuencia	Porcentaje	Frecuencia	Porcentaje	Frecuencia	Porcentaje	Frecuencia	Porcentaje	Frecuencia
Matriz	12	48%	8	32%	5	20%	0	0	25
Riobamba	6	55%	3	27%	2	18%	0	0	11
Latacunga	5	50%	4	40%	1	10%	0	0	10
Quito	4	67%	2	33%	0	0%	0	0	6
Guaranda	3	43%	3	43%	1	14%	0	0	7
Babahoyo	4	57%	2	29%	1	14%	0	0	7
Simon Bolìvar	2	50%	2	50%	0	0%	0	0	4
Milagro	3	50%	2	33%	1	17%	0	0	6
Consolidado	**39**	**51%**	**26**	**34%**	**11**	**14%**	**0**	**0%**	**76**

Fuente: Encuesta realizada al personal de la Cooperativa El Sagrario.

Elaborado por: Jaime Freire

Gráfico 5. Resultados de la pregunta 1 de la encuesta



Fuente: Encuesta realizada al personal de la Cooperativa El Sagrario.

Elaborado por: Jaime Freire

Análisis. Del 100% de los encuestados, el 51% sostiene que el plan de continuidad y contingencias ayuda **altamente** a mantener la disponibilidad de los sistemas de información; el 34% considera que ayuda **medianamente**; el 14% que ayuda **regularmente** y el 0% que **no influye**. Según los resultados por unidad se obtiene que la agencia de Quito tiene el mayor porcentaje de personas que responden **Altamente** con un 67%, mientras que la agencia Guaranda tiene el porcentaje más bajo que responden **Altamente** con un 43%.

Interpretación. De acuerdo a los resultados obtenidos se observa que todos los empleados manifiestan que el plan de continuidad y contingencias ayuda a mantener la disponibilidad de los sistemas de información, por tal motivo es muy importante que este documento sea revisado periódicamente y abarque la mayoría de eventos de riesgos que se puedan presentar.

Pregunta 2. ¿Considera usted que la implementación de los controles que se recomiendan en las auditorías informáticas influyen en el aumento de la disponibilidad de los sistemas de información?

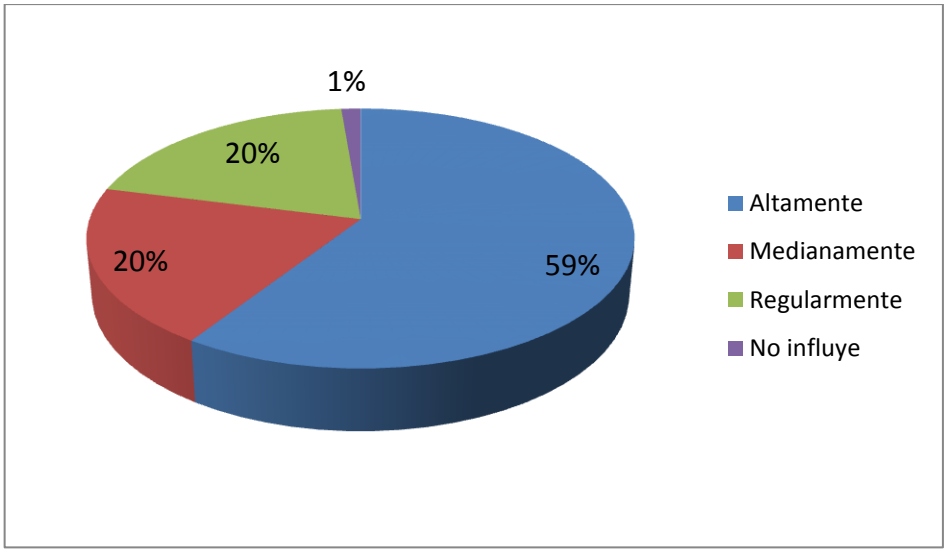
Tabla 7. Resultados de la pregunta 2 de la encuesta

Agencia	Altamente		Medianamente		Regularmente		No influye		Total
	Frecuencia	Porcentaje	Frecuencia	Porcentaje	Frecuencia	Porcentaje	Frecuencia	Porcentaje	Frecuencia
Matriz	14	56%	5	20%	5	20%	1	4%	25
Riobamba	7	64%	2	18%	2	18%	0	0%	11
Latacunga	6	60%	2	20%	2	20%	0	0%	10
Quito	4	67%	1	17%	1	17%	0	0%	6
Guaranda	4	57%	2	29%	1	14%	0	0%	7
Babahoyo	5	71%	1	14%	1	14%	0	0%	7
Simon Bolìvar	2	50%	1	25%	1	25%	0	0%	4
Milagro	3	50%	1	17%	2	33%	0	0%	6
Consolidado	**45**	**59%**	**15**	**20%**	**15**	**20%**	**1**	**1%**	**76**

Fuente: Encuesta realizada al personal de la Cooperativa El Sagrario.

Elaborado por: Jaime Freire

Gráfico 6. Resultados de la pregunta 2 de la encuesta



Fuente: Encuesta realizada al personal de la Cooperativa El Sagrario.

Elaborado por: Jaime Freire

Análisis. Del 100% de los encuestados, el 59% sostiene que la aplicación de los controles que se recomiendan en las auditorias informáticas influye **Altamente** en el aumento de la disponibilidad de los sistemas de información; el 20% considera que influye **Medianamente**; el 20% que influye **Regularmente** y el 1% que **No influye**. Según los resultados por unidad se obtiene que en la agencia Matriz existe únicamente una persona que manifiesta que las auditorias no influyen en la disponibilidad de los sistemas.

Interpretación. De acuerdo a los resultados obtenidos se concluye que es muy importante que se realicen auditorias informáticas en la organización con la finalidad de mantener una alta disponibilidad de los sistemas de información.

Pregunta 3. ¿La misión, objetivos y planes operativos del área de tecnología fueron difundidos en el último año?

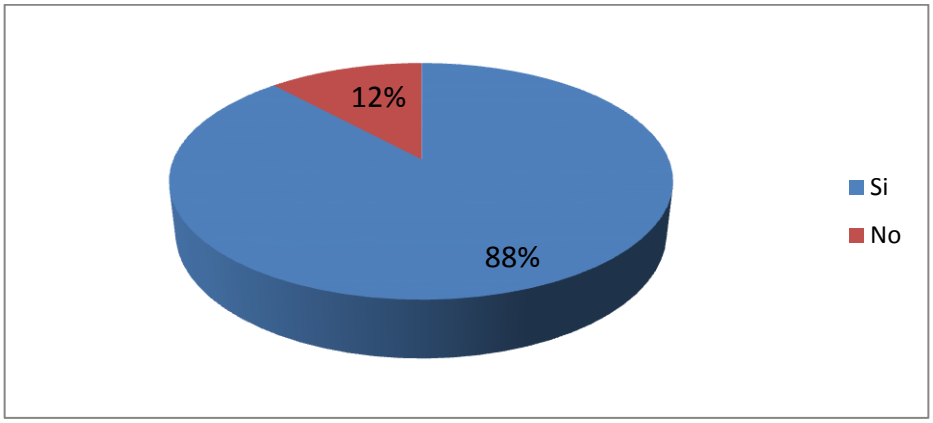
Tabla 8. Resultados de la pregunta 3 de la encuesta

Agencia	Si		No		Total Frecuencia
	Frecuencia	Porcentaje	Frecuencia	Porcentaje	
Matriz	23	92%	2	8%	25
Riobamba	10	91%	1	9%	11
Latacunga	8	80%	2	20%	10
Quito	5	83%	1	17%	6
Guaranda	5	71%	2	29%	7
Babahoyo	6	86%	1	14%	7
Simon Bolìvar	4	100%	0	0%	4
Milagro	6	100%	0	0%	6
Consolidado	**67**	**88%**	**9**	**12%**	**76**

Fuente: Encuesta realizada al personal de la Cooperativa El Sagrario.

Elaborado por: Jaime Freire

Gráfico 7. Resultados de la pregunta 3 de la encuesta



Fuente: Encuesta realizada al personal de la Cooperativa El Sagrario.

Elaborado por: Jaime Freire

Análisis. Del 100% de los encuestados, el 88% responde que **si** se ha difundido la misión, objetivos y planes operativos del área de tecnología, un 12% considera que **no** se ha difundido. Se observa también que las agencias de Simón Bolívar y Milagro su personal considera en un 100% que si fueron difundidas, esto se debe a que las oficinas fueron reciamente aperturadas.

Interpretación. De acuerdo a los resultados obtenidos se concluye que si se están difundiendo la misión, objetivos y planes operativos del área de tecnología desde el ingreso del personal a la Cooperativa.

Pregunta 4. ¿Considera que los mantenimientos realizados a los equipos de cómputo son suficientes para su correcta operatividad?

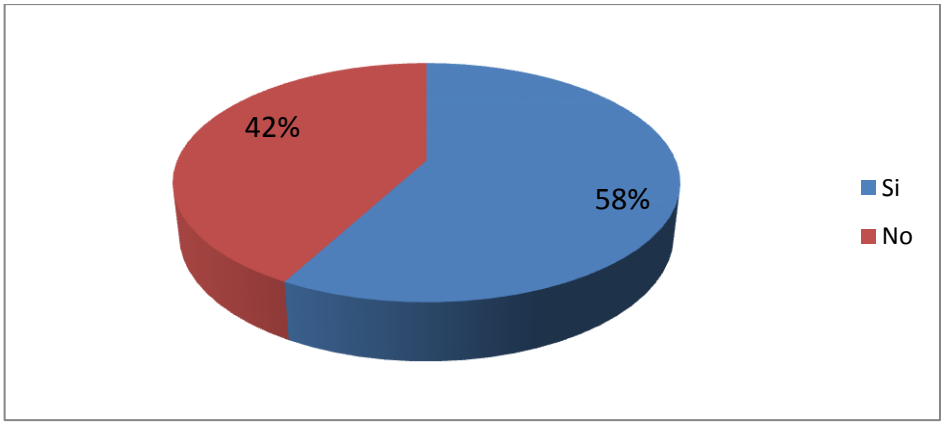
Tabla 9. Resultados de la pregunta 4 de la encuesta

Agencia	Si		No		Total Frecuencia
	Frecuencia	Porcentaje	Frecuencia	Porcentaje	
Matriz	13	52%	12	48%	25
Riobamba	5	45%	6	55%	11
Latacunga	5	50%	5	50%	10
Quito	4	67%	2	33%	6
Guaranda	3	43%	4	57%	7
Babahoyo	4	57%	3	43%	7
Simon Bolìvar	4	100%	0	0%	4
Milagro	6	100%	0	0%	6
Consolidado	**44**	**58%**	**32**	**42%**	**76**

Fuente: Encuesta realizada al personal de la Cooperativa El Sagrario.

Elaborado por: Jaime Freire

Gráfico 8. Resultados de la pregunta 4 de la encuesta



Fuente: Encuesta realizada al personal de la Cooperativa El Sagrario.

Elaborado por: Jaime Freire

Análisis. Del 100% de los encuestados, el 58% responde que los mantenimientos realizados a los equipos de cómputo **si** son suficientes para su correcta operatividad, sin embargo un 42% considera que el mantenimiento **no** es suficiente.

Interpretación. De acuerdo a los resultados obtenidos se concluye que es necesario revisar la política de mantenimiento de equipos para mejorar la percepción de los empleados.

Pregunta 5. ¿Se encuentra satisfecho con el aplicativo informático Financial Business System?

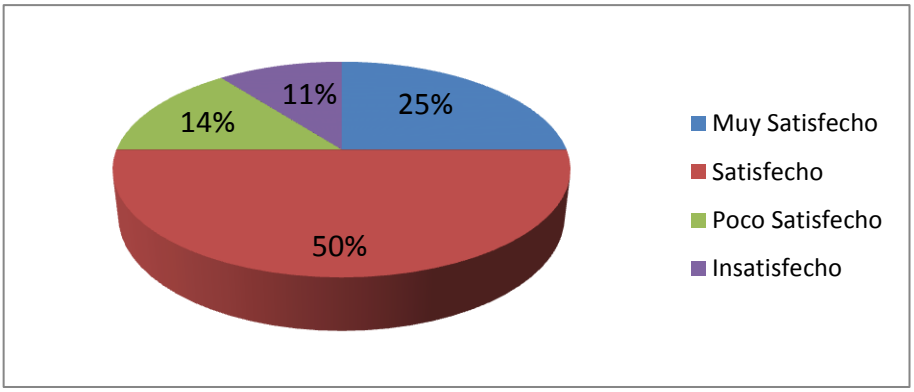
Tabla 10. Resultados de la pregunta 5 de la encuesta

Agencia	Muy Satisfecho		Satisfecho		Poco Satisfecho		Insatisfecho		Total
	Frecuencia	Porcentaje	Frecuencia	Porcentaje	Frecuencia	Porcentaje	Frecuencia	Porcentaje	Frecuencia
Matriz	4	16%	14	56%	5	20%	2	8%	25
Riobamba	2	18%	5	45%	2	18%	2	18%	11
Latacunga	2	20%	6	60%	1	10%	1	10%	10
Quito	1	17%	3	50%	1	17%	1	17%	6
Guaranda	2	29%	3	43%	1	14%	1	14%	7
Babahoyo	2	29%	3	43%	1	14%	1	14%	7
Simon Bolìvar	2	50%	2	50%	0	0%	0	0%	4
Milagro	4	67%	2	33%	0	0%	0	0%	6
Consolidado	**19**	**25%**	**38**	**50%**	**11**	**14%**	**8**	**11%**	**76**

Fuente: Encuesta realizada al personal de la Cooperativa El Sagrario.

Elaborado por: Jaime Freire

Gráfico 9. Resultados de la pregunta 5 de la encuesta



Fuente: Encuesta realizada al personal de la Cooperativa El Sagrario.

Elaborado por: Jaime Freire

Análisis. Del 100% de los encuestados, el 75% de empleados se encuentran **Muy Satisfechos y Satisfechos** con el aplicativo informático Financial Business System, el 14% se encuentra **Poco Satisfecho** y un 11% de **Insatisfechos**.

Interpretación. Sin embargo que el aplicativo informático financial tiene una buena satisfacción, es necesario que se busquen mejoras para seguir incrementando el grado de satisfacción del mismo.

Pregunta 6. ¿Los problemas que usted ha reportado al área de tecnología han sido atendidos oportunamente?

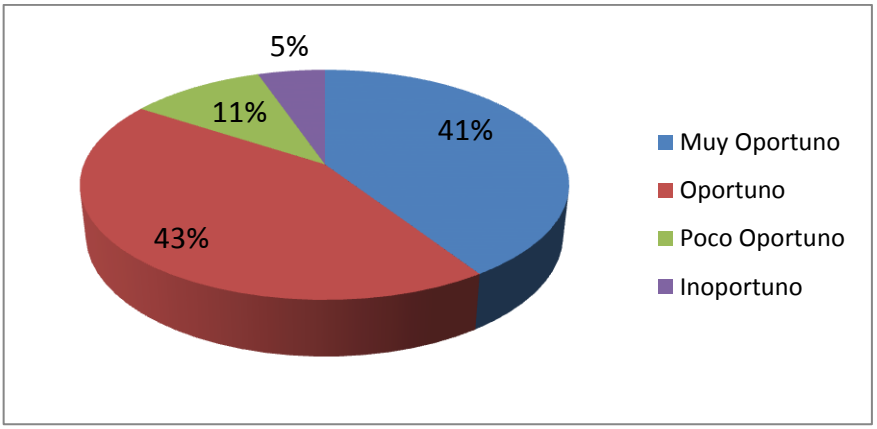
Tabla 11. Resultados de la pregunta 6 de la encuesta

Agencia	Muy Oportuno		Oportuno		Poco Oportuno		Inoportuno		Total
	Frecuencia	Porcentaje	Frecuencia	Porcentaje	Frecuencia	Porcentaje	Frecuencia	Porcentaje	Frecuencia
Matriz	8	32%	14	56%	2	8%	1	4%	25
Riobamba	4	36%	4	36%	2	18%	1	9%	11
Latacunga	4	40%	4	40%	1	10%	1	10%	10
Quito	3	50%	2	33%	1	17%	0	0%	6
Guaranda	3	43%	3	43%	1	14%	0	0%	7
Babahoyo	3	43%	2	29%	1	14%	1	14%	7
Simon Bolìvar	2	50%	2	50%	0	0%	0	0%	4
Milagro	4	67%	2	33%	0	0%	0	0%	6
Consolidado	**31**	**41%**	**33**	**43%**	**8**	**11%**	**4**	**5%**	**76**

Fuente: Encuesta realizada al personal de la Cooperativa El Sagrario.

Elaborado por: Jaime Freire

Gráfico 10. Resultados de la pregunta 6 de la encuesta



Fuente: Encuesta realizada al personal de la Cooperativa El Sagrario.

Elaborado por: Jaime Freire

Análisis. Del 100% de los encuestados, el 84% de empleados considera que sus problemas reportados al área de tecnología son atendidos **Muy Oportunamente y Oportunamente;** el 11% manifiesta que es **Poco Oportuno** la atención de problemas y un 5% **Inoportuno**.

Interpretación. De acuerdo a los resultados obtenidos se puede concluir que los empleados tienen una percepción buena del servicio que ofrece el área de tecnología, sería muy importante seguir atendiendo de forma oportuna todos los requerimientos solicitados.

Pregunta 7. ¿La falta de disponibilidad en los sistemas de información se produce por qué no se prevé de controles para ciertos incidentes de tecnología?

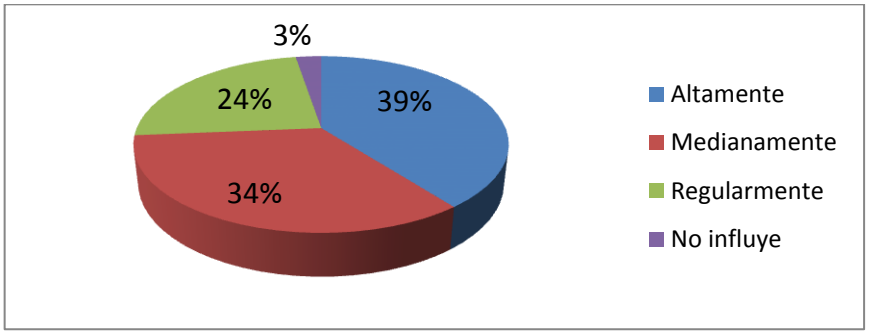
Tabla 12. Resultados de la pregunta 7 de la encuesta

Agencia	Altamente		Medianamente		Regularmente		No influye		Total
	Frecuencia	Porcentaje	Frecuencia	Porcentaje	Frecuencia	Porcentaje	Frecuencia	Porcentaje	Frecuencia
Matriz	8	32%	10	40%	5	20%	2	8%	25
Riobamba	3	27%	5	45%	3	27%	0	0%	11
Latacunga	3	30%	4	40%	3	30%	0	0%	10
Quito	2	33%	2	33%	2	33%	0	0%	6
Guaranda	3	43%	2	29%	2	29%	0	0%	7
Babahoyo	5	71%	1	14%	1	14%	0	0%	7
Simon Bolìvar	2	50%	1	25%	1	25%	0	0%	4
Milagro	4	67%	1	17%	1	17%	0	0%	6
Consolidado	**30**	**39%**	**26**	**34%**	**18**	**24%**	**2**	**3%**	**76**

Fuente: Encuesta realizada al personal de la Cooperativa El Sagrario.

Elaborado por: Jaime Freire

Gráfico 11. Resultados de la pregunta 7 de la encuesta



Fuente: Encuesta realizada al personal de la Cooperativa El Sagrario.

Elaborado por: Jaime Freire

Análisis. Del 100% de los encuestados, el 39% de empleados considera que la falta de disponibilidad en los sistemas de información se produce **Altamente** por qué no se prevé de controles para ciertos incidentes de tecnología; un 34% considera que el impacto es **Medianamente,** el 24% **Regularmente** y un 3% piensa que **no influye**.

Interpretación. De acuerdo a los resultados obtenidos se puede concluir que es necesario prevenir controles para la mayoría de incidente de tecnología que puedan ocurrir con la finalidad de mejorar la disponibilidad de los sistemas de información.

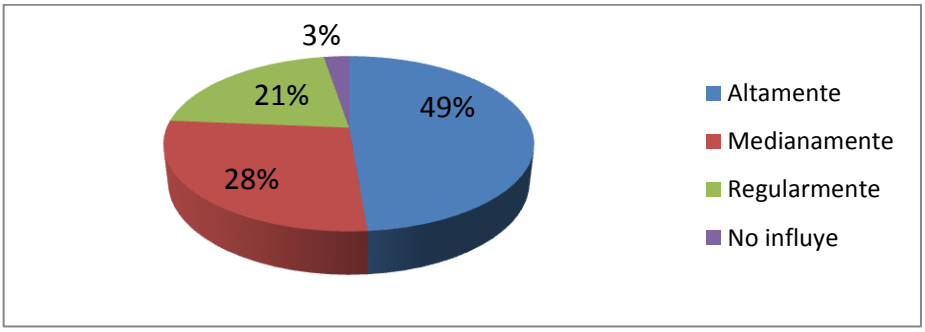
Pregunta 8. ¿Considera que las auditorias informáticas son limitadas debido a que no existe personal interno especializado para estas actividades?

Tabla 13. Resultados de la pregunta 8 de la encuesta

Agencia	Altamente		Medianamente		Regularmente		No influye		Total Frecuencia
	Frecuencia	Porcentaje	Frecuencia	Porcentaje	Frecuencia	Porcentaje	Frecuencia	Porcentaje	
Matriz	11	44%	7	28%	5	20%	2	8%	25
Riobamba	4	36%	4	36%	3	27%	0	0%	11
Latacunga	4	40%	3	30%	3	30%	0	0%	10
Quito	3	50%	2	33%	1	17%	0	0%	6
Guaranda	4	57%	2	29%	1	14%	0	0%	7
Babahoyo	5	71%	1	14%	1	14%	0	0%	7
Simon Bolìvar	2	50%	1	25%	1	25%	0	0%	4
Milagro	4	67%	1	17%	1	17%	0	0%	6
Consolidado	**37**	**49%**	**21**	**28%**	**16**	**21%**	**2**	**3%**	**76**

Fuente: Encuesta realizada al personal de la Cooperativa El Sagrario.
Elaborado por: Jaime Freire

Gráfico 12. Resultados de la pregunta 8 de la encuesta



Fuente: Encuesta realizada al personal de la Cooperativa El Sagrario.
Elaborado por: Jaime Freire

Análisis. Del 100% de los encuestados, el 49% de los empleados considera que las auditorias informáticas son limitadas, debido **Altamente** a que no existe personal interno especializado para estas actividades, un 28% considera que el impacto es **medio**, el 21% **regular** y un 3% que **no influye.**

Interpretación. De acuerdo a los resultados obtenidos la mayoría de empleados considera que es necesaria la realización de auditorías informáticas con personal interno.

Pregunta 9. ¿Los equipos de cómputo con que cuenta en su puesto de trabajo son adecuados para el cumplimiento de sus labores diarias?

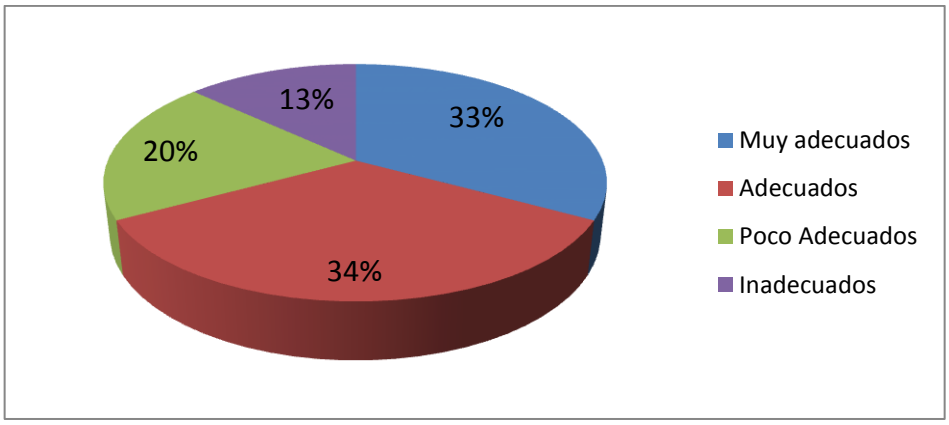
Tabla 14. Resultados de la pregunta 9 de la encuesta

Agencia	Muy adecuados		Adecuados		Poco Adecuados		Inadecuados		Total Frecuencia
	Frecuencia	Porcentaje	Frecuencia	Porcentaje	Frecuencia	Porcentaje	Frecuencia	Porcentaje	
Matriz	6	24%	9	36%	7	28%	3	12%	25
Riobamba	2	18%	5	45%	3	27%	1	9%	11
Latacunga	2	20%	4	40%	2	20%	2	20%	10
Quito	2	33%	2	33%	1	17%	1	17%	6
Guaranda	2	29%	2	29%	1	14%	2	29%	7
Babahoyo	3	43%	2	29%	1	14%	1	14%	7
Simon Bolìvar	3	75%	1	25%	0	0%	0	0%	4
Milagro	5	83%	1	17%	0	0%	0	0%	6
Consolidado	**25**	**33%**	**26**	**34%**	**15**	**20%**	**10**	**13%**	**76**

Fuente: Encuesta realizada al personal de la Cooperativa El Sagrario.

Elaborado por: Jaime Freire

Gráfico 13. Resultados de la pregunta 9 de la encuesta



Fuente: Encuesta realizada al personal de la Cooperativa El Sagrario.

Elaborado por: Jaime Freire

Análisis. Del 100% de los encuestados, el 77% considera que sus equipos son **Muy adecuados** y **adecuados** para el cumplimiento de sus funciones, el 20% considera que sus equipos son **Poco adecuados** y un 13% **inadecuados**. El personal de la agencia de Guaranda considera mayormente que posee equipos poco adecuados para su trabajo.

Interpretación. De acuerdo a los resultados obtenidos, es importante que el personal cuente con equipos funcionales para el trabajo; existen muchos empelados que no tienen los equipos adecuados para cumplir con sus funciones.

Pregunta 10. ¿Usted ha sido capacitado en el último año sobre normas, políticas y buenas prácticas de seguridad que debe tomar en cuenta en sus funciones?

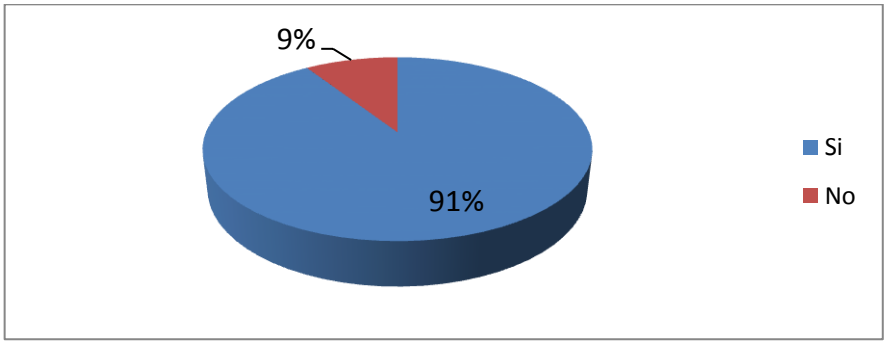
Tabla 15. Resultados de la pregunta 10 de la encuesta

Agencia	Si		No		Total Frecuencia
	Frecuencia	Porcentaje	Frecuencia	Porcentaje	
Matriz	23	92%	2	8%	25
Riobamba	10	91%	1	9%	11
Latacunga	9	90%	1	10%	10
Quito	5	83%	1	17%	6
Guaranda	6	86%	1	14%	7
Babahoyo	6	86%	1	14%	7
Simon Bolìvar	4	100%	0	0%	4
Milagro	6	100%	0	0%	6
Consolidado	**69**	**91%**	**7**	**9%**	**76**

Fuente: Encuesta realizada al personal de la Cooperativa El Sagrario.

Elaborado por: Jaime Freire

Gráfico 14. Resultados de la pregunta 10 de la encuesta



Fuente: Encuesta realizada al personal de la Cooperativa El Sagrario.

Elaborado por: Jaime Freire

Análisis. Del 100% de los encuestados, el 91% responde que **si** ha sido capacitado en el último año sobre normas, políticas y buenas prácticas de seguridad y 9% que no ha sido capacitado.

Interpretación. De acuerdo a los resultados obtenidos se concluye que la mayoría del personal está siendo capacitado en normas y políticas de seguridad lo cual es muy preventivo especialmente en instituciones financieras.

4.3. VERIFICACIÓN DE LA HIPÓTESIS

Para la verificación de la hipótesis planteada en el presente proyecto de investigación se aplicará la prueba del Chi cuadrado (X^2), a partir de las frecuencias observadas y esperadas para cada una de las categorías. Los paso para la demostración de la hipótesis por Chi cuadrado (X^2) son:

1. Determinación de fe y completar la tabla de contingencia.
2. Planteamiento de las hipótesis (Ho, Ha)
3. Determinamos Nivel de significación (α).
4. Encontramos grados de libertad (v)
5. Determinamos x^2 crítico (tabla)
6. Calculamos x^2
7. Decisión.- CONCLUSION

Durante la ejecución de los pasos para la demostración de la hipótesis se va utilizar la siguiente simbología:

X^2 = Chi cuadrado

Ho = Hipótesis Nula.

Ha = Hipótesis Alternativa

k = número de filas o (categorías)

j = número de columnas (variables)

v = Grados de libertad

fe = Frecuencia esperada

fo = frecuencia observada

α=Nivel de significación

4.3.1. Determinación de la frecuencia esperada y tabla de contingencia

Para la determinación de la frecuencia esperada y completar la tabla de contingencia, se consideran como **categorías o filas** a las siguientes preguntas realizadas en la encuesta:

Pregunta 2¿Considera usted que la implementación de los controles que se recomiendan en las auditorías informáticas influyen en el aumento de la disponibilidad de los sistemas de información?

Pregunta 7. ¿La falta de disponibilidad en los sistemas de información se produce por qué no se prevé de controles para ciertos incidentes de tecnología?

Pregunta 8. ¿Considera que las auditorias informáticas son limitadas debido a que no existe personal interno especializado para estas actividades?

Como **columnas o variables** de la tabla, se consideran las posibles respuestas que se pueden otorgar a cada una de las preguntas y que son: Altamente, Medianamente, Regularmente, No influye.

Tabla 16. Tabla de frecuencias observadas

	Respuestas					
Preguntas	**Altamente**	**Medianamente**	**Regularmente**	**No influye**	**Total**	**%**
Pregunta 2	45	15	15	1	**76**	33%
Pregunta 7	30	26	18	2	**76**	33%
Pregunta 8	37	21	16	2	**76**	33%
Total	**112**	**62**	**49**	**5**	**228**	100%

Fuente: Encuesta realizada al personal de la Cooperativa El Sagrario.

Elaborado por: Jaime Freire

Tabla17. Tabla de frecuencias esperadas

fo	fe	(fo-fe)	$(fo - fe)^2$	$\frac{(fo-fe)^2}{fe}$
45	37,33	7,67	58,78	1,57
30	37,33	-7,33	53,78	1,44
37	37,33	-0,33	0,11	0,00
15	20,67	-5,67	32,11	1,55
26	20,67	5,33	28,44	1,38
21	20,67	0,33	0,11	0,01
15	16,33	-1,33	1,78	0,11
18	16,33	1,67	2,78	0,17
16	16,33	-0,33	0,11	0,01
1	1,67	-0,67	0,44	0,27
2	1,67	0,33	0,11	0,07
2	1,67	0,33	0,11	0,07
			(X^2)	**6,64**

Fuente: Cálculos realizados en base a tabla de frecuencias observadas.

Elaborado por: Jaime Freire

4.3.2. Planteamiento de la hipótesis

Ho: fo=fe.- La aplicación de los controles que se recomiendan en las auditorias informáticas **si aumenta** la disponibilidad de los sistemas de información en la Cooperativa “El Sagrario Ltda.” en el 2010.

Ha: fo≠fe. La aplicación de los controles que se recomiendan en las auditorias informáticas **no aumenta** la disponibilidad de los sistemas de información en la Cooperativa “El Sagrario Ltda.” en el 2010.

4.3.3. Determinación del Nivel de Significancia

Para la demostración de la hipótesis se utiliza el ensayo unilateral hacia la derecha, con un nivel de confianza de 95% es decir a 1.64 dentro de la curva por lo tanto el nivel de significación es 5% equivalente a α = 0,05

Nivel de significancia

α = 5% → 0,05

4.3.4. Encontramos los grados de libertad "v"

Para determinar los grados de libertad se utiliza la siguiente fórmula:

v = (k-1) (j-1) **(**más de una variable)

Dónde:

k= número de filas (del cuadro de frecuencias observadas)
j= número de columnas (del cuadro de frecuencias observadas)

Entonces

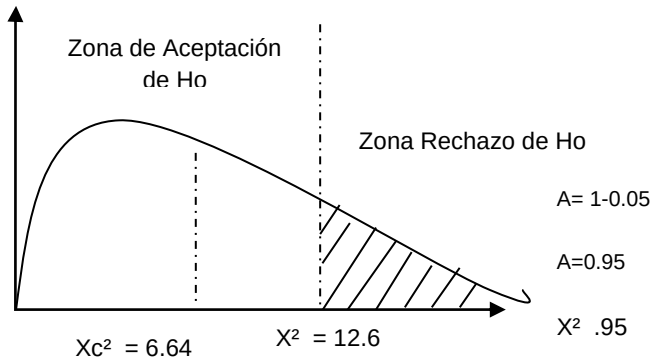
Para nuestro caso k=3 y j=4
v = (k-1) (j-1)
v= (3-1) (4-1)
v = (2) (3)
v = 6

4.3.5. Determinamos (X^2) crítico (tabla)

Considerando la tabla de valores percentiles para la distribución del chi cuadrado con grados de libertad, el Chi cuadrado **es igual a 12.6** con un valor de los grados de libertad de 6 y un nivel de significancia de 0.95.

X^2 =.95 y **v =** 6

Gráfico 15. Gráfico de Chi cuadrado



Fuente: Investigación de campo(2011)

Elaborado por: Jaime Freire

4.3.6. Calculamos (X²)

Fórmula

$$X^2 = \sum \left| \frac{(fo - fe)^2}{fe} \right|$$

X² calculado= 6.64 (Según Tabla del paso numero 1)

4.3.7. Decisión-Conclusión

Como (X²) calculado de 6.64 está en zona de aceptación de Ho, se acepta la Hipótesis Ho

Conclusión. Una vez realizado el cálculo de Chi Cuadrado se concluye que la aplicación de los controles que se recomiendan en las auditorias informáticas **si aumenta** la disponibilidad de los sistemas de información en la Cooperativa “El Sagrario Ltda.” en el 2010.

CAPITULO V
CONCLUSIONES Y RECOMENDACIONES

Una vez que se ha realizado la investigación de campo, enfocada al control de auditorías informáticas y su incidencia en la disponibilidad de los sistemas de información, se establecen las siguientes conclusiones y recomendaciones:

5.1. CONCLUSIONES

- La falta de auditorías informáticas internas puede poner en riesgo la disponibilidad de los sistemas de información y del adecuado control de las Tecnologías de Información en la Cooperativa de Ahorro y Crédito “El Sagrario Ltda.”

- En los manuales vigentes en la institución no se establecen políticas claras para la realización de auditorías informáticas, sin embargo de que la mayor cantidad de operaciones que realiza la Cooperativa están soportadas por las Tecnologías de Información.

- Una vez realizada la investigación de campo se establece que los procesos críticos de tecnología son: Desarrollo de Software, Administración de contingencias y Administración de seguridades, los cuales tienen mayor incidencia en la disponibilidad de los sistemas.

- Una guía de auditoría informática bien estructurada puede ser útil para el personal de control interno que labora en la Cooperativa que no tiene conocimientos de las tecnologías de información vigente.

5.2. RECOMENDACIONES

- Se deben realizar auditorías informáticas internas periódicamente con la finalidad de determinar a tiempo los controles necesarios que se deben implementar para asegurar la disponibilidad de los sistemas de información.

- Es necesario que se actualicen los manuales de control de la Cooperativa, estableciendo políticas claras para la realización de auditorías informáticas, incluyendo entre otras cosas: periodos de ejecución, áreas críticas a ser revisadas, determinación de límites de riesgos que se puede aceptar.

- Se recomienda que se hagan pruebas y revisiones de cumplimiento de la metodología de desarrollo de software, del plan de contingencias y de las seguridades implementadas en la institución, con cada auditoría informática que se realice.

- La guía de auditoría informática que se va proponer debe considerar todas las áreas de acción de las tecnologías de información de la Cooperativa El Sagrario, con la finalidad de determinar el riesgo de cada proceso.

- Es importante que la guía de auditoría que se va proponer se base en estándares internacionales de auditoría informática con la finalidad de tomar las mejores prácticas ya existentes y que son realizadas en la mayoría de empresas a nivel mundial.

CAPÍTULO VI
PROPUESTA

6.1. DATOS INFORMATIVOS

6.1.1. Título

Desarrollar una guía de auditoría informática para el control interno de las tecnologías de información.

6.1.2. Institución Ejecutora

Cooperativa de Ahorro y Crédito “El Sagrario” Ltda.

6.1.3. Beneficiarios

- Proceso de Tecnología de la Información.
- Proceso de Control Interno.
- Proceso de Administración de Riesgos Integrales.

6.1.4. Ubicación:

La Cooperativa de Ahorro y Crédito “El Sagrario” Ltda., tiene su oficina Matriz en la Ciudad de Ambato en las calles Sucre y Quito Esquina. Cuenta con 10 agencias a nivel nacional ubicado en la ciudad de Ambato, Riobamba, Latacunga, Quito, Guaranda, Babahoyo y Milagro.

6.1.5. Tiempo Estimado para la ejecución

El tiempo estimado para la ejecución de esta propuesta es de 240 días es decir del periodo comprendido entre Enero y Julio del 2011.

6.1.6. Equipo técnico responsable:

El equipo que va realizar y supervisar la siguiente investigación es:

- Investigador: Jaime Ramiro Freire Freire
- Auditor Interno Dr. Marcelo Tasigchana
- Instructor de Investigación: Dra. Mercedes Acosta
- Tutor de la investigación Dr. CPA Joselito Naranjo

6.1.7. Costo

Tabla18. Tabla de costos del proyecto.

Detalle	Descripción	Valor Estimado
Capacitación de la guía de auditoría informática para el equipo de auditores internos	Se estima un curso de 40 horas para tres personas. El costo hora es de 9.5 tomando como referencia el costo hora del Subgerente de Tecnología de la Cooperativa.	380.00 USD
Supervisión en la ejecución de una primera auditoria informática.	Se estima un total de 45 horas para la supervisión de la primera auditoria a realizar. El costo hora es de 9.5 tomando como referencia el costo hora del Subgerente de Tecnología de la Cooperativa.	430.00 USD
Transporte para revisión en Oficinas.	El viaje por oficina se estima 50 USD por 8 oficinas.	400.00 USD
Suministros de oficina	Hojas, cartuchos adicionales.	200.00 USD
TOTAL		1410.00 USD

Fuente: Investigación de Campo (2011)

Elaborado por: Jaime Freire

6.2. ANTECEDENTES

La falta de auditorías informáticas internas puede poner en riesgo la disponibilidad de los sistemas de información y del adecuado control de las Tecnologías de Información en la Cooperativa de Ahorro y Crédito “El Sagrario Ltda.”

En los manuales vigentes en la institución no se establecen políticas claras para la realización de auditorías informáticas, sin embargo que la mayor cantidad de operaciones que realiza la Cooperativa están soportadas por las Tecnologías de Información. Es necesario que se actualicen los manuales de control de la Cooperativa, estableciendo políticas claras para la realización de auditorías informáticas, incluyendo entre otras cosas: periodos de ejecución, áreas críticas a ser revisadas, determinación de límites de riesgos que se puede aceptar.

Una vez realizada la investigación de campo se establece que los procesos críticos de tecnología son: Desarrollo de Software, Administración de contingencias y Administración de seguridades, los cuales tienen mayor incidencia en la disponibilidad de los sistemas, por lo tanto es necesario realizar revisiones de cumplimiento de la metodología de desarrollo de software, del plan de contingencias y de las seguridades implementadas en la institución, con cada auditoría informática que se realice

Una guía de auditoría informática bien estructurada puede ser útil para el personal de control interno que labora en la Cooperativa que no tiene conocimientos de las tecnologías de información vigente. Por lo tanto se debe considerar todas las áreas de acción de las tecnologías de información de la Cooperativa El Sagrario, especificando el porcentaje de riesgo que se puede asumir con cada evento.

6.3. JUSTIFICACIÓN

Con la finalidad de confirmar si las auditorias informáticas inciden en la disponibilidad de los sistemas de información, se plantearon a cada uno de los empleados de la Cooperativa las siguientes interrogantes:

- ¿Considera usted que la implementación de los controles que se recomiendan en las auditorías informáticas influyen en el aumento de la disponibilidad de los sistemas de información?
- ¿La baja disponibilidad en los sistemas de información se produce por qué no se prevé de controles para ciertos incidentes de tecnología?
- ¿Considera usted que las auditorias informáticas son limitadas debido a que no existe personal interno especializado para estas actividades?

Interpretando los resultados obtenidos se puede manifestar que un mejor control interno sobre las tecnologías de información puede coadyudar de gran manera a mantener una alta disponibilidad de los sistemas de información y todos los servicios de tecnología.

Por tal motivo la guía de auditoría informática propuesta, así como la definición de procesos críticos y políticas de control para las tecnologías de información, contribuirán en mejorar la disponibilidad de los sistemas de información de la Cooperativa.

6.4. OBJETIVOS

6.4.1. Objetivo General

Adoptar una guía de auditoría informática para el control interno de las tecnologías de información.

6.4.2. Objetivos Específicos

- Definir las actividades a seguir para la planificación de una auditoría informática.
- Definir los mecanismos para la ejecución de una auditoria informática con la finalidad evaluar la administración y operatividad de los recursos de tecnología de información
- Establecer los lineamientos para la elaboración del reporte de auditoría informática y el seguimiento al cumplimiento de las actividades.

6.5. ANÁLISIS DE FACTIBILIDAD

La aplicación de la presente propuesta es viable ya que se cuenta con la autorización de la Gerencia General para llevar a cabo la ejecución de la misma, se analizan los siguientes factores.

6.5.1. Análisis Técnico-Tecnológico

Para la realización de este proyecto se utilizará la infraestructura tecnológica actual, por lo cual no es necesario adquirir equipos adicionales para aplicar este proyecto. Por otro lado se requiere que el equipo auditor tenga un amplio conocimiento técnico por lo cual la capacitación es un aspecto muy importante a tomar en cuenta pero que no es un impedimento para poder aplicar la propuesta, por estos motivos se considera que la aplicación de la propuesta es muy factible realizarle en el aspecto técnico tecnológico.

6.5.2. Análisis Económico.

Uno de los principales costos que se incurre para la aplicación de la propuesta es en la capacitación al equipo de auditores internos sobre la

guía de auditoría informática desarrollada, así como en la supervisión de la primera auditoria.

Los costos estimados para aplicar la propuesta son los siguientes:

Tabla19. Tabla de costos del proyecto.

Detalle	Descripción	Valor Estimado
Capacitación de la guía de auditoría informática para el equipo de auditores internos.	Se estima un curso de 40 horas para tres personas. El costo hora es de 9.5 tomando como referencia el costo hora del Subgerente de Tecnología de la Cooperativa.	380.00 USD
Supervisión en la ejecución de una primera auditoria informática.	Se estima un total de 45 horas para la supervisión de la primera auditoria a realizar. El costo hora es de 9.5 tomando como referencia el costo hora del Subgerente de Tecnología de la Cooperativa.	430.00 USD
Transporte para revisión en Oficinas.	El viaje por oficina se estima 50 USD por 8 oficinas.	400.00 USD
Suministros de oficina	Hojas, cartuchos adicionales.	200.00 USD.
TOTAL		1410.00 USD

Fuente: Investigación de Campo (2011)

Elaborado por: Jaime Freire

6.5.3. Análisis ambiental y social

La aplicación de la presenta propuesta no va generar ninguna alteración del medio ambiente, sin embargo creemos que en el aspecto social puede contribuir a la prevención de fraudes informáticos al establecer a tiempo controles de seguridad. Esta guía de auditoría informática se podría aplicar en varias instituciones financieras, por lo cual se considera que es factible la aplicación de esta propuesta.

6.5.4. Análisis Legal

La presente propuesta no tiene ningún impedimento legal, al contrario existen normas de cumplimiento obligatorio establecidos por la Superintendencia de Bancos, que exige la realización de auditorías informáticas a las tecnologías de información de las instituciones financieras controladas por lo cual se considera que es muy factible su aplicación.

6.6. FUNDAMENTACIÓN CIENTÍFICA TÉCNICA

De acuerdo **a la Junta de Estándares de la Asociación de Auditoría y Control de Sistemas de Información (2005),** quienes establecieron estándares, directrices y procedimientos para la realización de auditoría de sistemas de información se presentas las siguientes definiciones y estándares.

6.6.1. Definiciones de Auditoria Informática.

La auditoría informática es la revisión y evaluación de los controles, sistemas y procedimientos de la Tecnología de Información, sus recursos, utilización eficiencia y seguridad para lograr los objetivos del negocio.

Se basa en la ejecución de procedimientos de auditoría utilizando el computador a través del uso de paquetes informáticos de análisis de datos, hojas electrónicas, bases de datos y otros tipos de utilitarios o paquetes informáticos.

.

6.6.2. Alcance de la Auditoria.

La Auditoría Informática puede tener el siguiente alcance dependiendo de las necesidades del negocio o la alta dirección:

- La evaluación administrativa del área de Tecnología.
- La evaluación del cumplimiento de las políticas y procedimientos de Tecnología.
- La evaluación de la eficiencia y eficacia de los sistemas de información en producción.
- Evaluación del ciclo de vida del desarrollo de los sistemas de información.
- Evaluación de las operaciones o áreas específicas a nivel de redes, bases de datos y el soporte o servicio brindado.
- Evaluación de los riesgos y la seguridad de la información.
- Auditoría forense o legal de los sistemas de información.

Se podría considerar los siguientes procesos de tecnología para la evaluación.

Planeación Estratégica:

- Plan Estratégico de Tecnología alineada con el negocio
- Evaluación de Riesgos de Tecnología.
- Políticas y procedimientos inherentes al proceso de planeación estratégica.
- Plan Operativo Anual de Tecnología.
- Presupuesto de Tecnología.

- Estructura Orgánico Funcional de Tecnología.
- Comité Tecnológico.
- Políticas y procedimientos actualizados
- Actas de Confidencialidad del personal de Tecnología.
- Inventario y control de los Activos de Tecnología: Hardware, Software, Medios y Documentación.
- Políticas y procedimientos de adquisición de recursos de tecnología de información de acuerdo a la planificación estratégica.
- Disponer de documentación técnica detallada de la infraestructura tecnológica.
- Indicadores de medición de los recursos tecnológicos.

Operaciones y Soporte:

- Elaboración de los manuales operativos de cada uno de los servicios y procesos críticos de Tecnología en base a las políticas y procedimientos establecidos. Por ejemplo, deberán elaborarse los manuales operativos de administración de bases de datos, administración del ciclo de vida de los sistemas, seguridad de Tecnología planeación estratégica, administración de los recursos de red, etc.
- Establecer Acuerdos de Nivel de Servicio entre la Unidad de Tecnología y los clientes internos, considerando los tiempos mínimos de respuesta frente a la llamada de los usuarios.
- Disponer de una Mesa de Ayuda o Help Desk para atender los requerimientos de los Usuarios en forma oportuna bajo procedimientos claros y específicos.
- La elaboración de un manual operativo para el soporte a usuarios, en donde se establezcan las acciones a seguirse en los diferentes escenarios que pudieran presentarse como producto de las llamadas de los Usuarios de Tecnología.

- Disponer de políticas y procedimientos para la administración de eventos e incidentes que abarque su registro, análisis y correcciones, mediante una base de datos que sea actualizada en forma continua tanto por la Unidad de Tecnología como por parte de los usuarios a medida que vayan ocurriendo los incidentes, con la finalidad de disminuir su frecuencia.
- Disponer de manuales de configuraciones de los recursos de Tecnología.
- Establecer responsabilidades de los usuarios frente al uso de los recursos de tecnología de información.
- Se deben establecer políticas y procedimientos para una correcta administración de los activos de Tecnología, que incluya por lo menos: manejo de inventarios, categorización, mantenimiento, responsables, dadas de baja, renovación de recursos, entre otras cosas. Dicha administración debe abarcar el hardware, el software, manuales operativos, formularios internos, manuales de diseño de sistemas de información y manuales de Usuario.
- La Administración de los servicios de Tecnología es compleja, requiere de actualización técnica constante.
- Diseño integral de los servicios de redes y comunicaciones, bases de datos, desarrollo de aplicaciones, soporte a usuarios, etc.
- Planificación de medidas preventivas y correctivas contra amenazas y para la optimización y calidad de la infraestructura corporativa
- Definir políticas y procedimientos para la administración integral de los servicios de Tecnología, lo que incluye su monitoreo y mejoramiento continuo.
- Disponer de recursos y servicios de TI de alta disponibilidad para garantizar la continuidad y calidad de las redes y comunicaciones de la Entidad.
- Disponer de proveedores principales y secundarios de los servicios de red.

- Implementar herramientas de administración y monitoreo proactivos bajo protocolos que garanticen seguridad, control y calidad.
- Políticas, procedimientos y mecanismos de protección frente a ataques internos y externos a la red corporativa
- Definir políticas de control de acceso y segregación de redes (VLAN's).
- Restricción de accesos remotos y protección de los mismos (VPN's).
- Estandarización y seguimiento de normas de seguridad para el cableado estructurado y diseño del core de la red
- Controles lógicos, protección perimetral y en profundidad y ethical hacking.

Servicios Provistos por Terceros:

- Diseñar y poner en vigencia un manual Institucional para la contratación de servicios provistos por terceros que incluya los servicios de Tecnología.
- Definir las especificaciones técnicas y legales para los diferentes tipos de contratos de servicios tercerizados: desarrollo y mantenimiento de sistemas, enlaces dedicados de internet, mantenimiento de equipos, etc.
- Definir en todos los contratos de servicios tercerizados la contraparte técnica por parte de la Institución, que realizará la supervisión del cumplimiento de los contratos y que vigilará el cumplimiento de las especificaciones técnicas establecidas.
- Definir formalmente el procedimiento para la celebración de contratos entre la Institución y proveedores externos, estableciendo responsables para la elaboración, revisión, aprobación, suscripción y supervisión de los contratos.

- Establecer un manual Operativo para el monitoreo de los servicios provistos por terceros, a nivel, cualitativo y cuantitativo, de tal forma que se pueda conocer el grado de cumplimiento de los proveedores, eventos de caídas de servicios, el establecimiento y control de los acuerdos de nivel de servicio, entre otras cosas. Deben existir acuerdos de Nivel de Servicio con cada uno de los proveedores de TI que considere entre otras cosas: niveles mínimos de calidad, tiempo de respuesta ante incidentes, penalizaciones por mal servicio o incumplimiento, acuerdos de confidencialidad, etc.
- Establecer Acuerdos de Nivel de Servicio entre la unidad de Sistemas y los proveedores externos, considerando lo siguiente:
- Definir los servicios ofrecidos por la Unidad de Sistemas.
- Cuantificar el mínimo nivel de servicio a recibirse.
- Personal técnico asignado para brindar los servicios de soporte.
- Disponibilidad y confiabilidad del servicio recibido.
- Categorización de las llamadas de soporte y tiempos de atención.
- Planes de contingencia provistos por el proveedor en caso de falla en los servicios.
- Acuerdos de Confidencialidad de la información.
- Acuerdos de control de calidad y monitoreo del servicio recibido.
- Penalizaciones en caso de incumplimiento.

Sistemas de Información:

- Metodología para la administración de proyectos de sistemas de información.
- Establecer una metodología formal para la administración del ciclo de vida de los sistemas de información, así como de nuevas adquisiciones y proyectos
- Adecuada segregación de funciones en el desarrollo de aplicaciones y control de versiones

- Separación de las áreas de desarrollo, preproducción y producción
- Adecuadas pruebas y autorización de cambios. Monitoreo de los cambios efectuados
- Adecuada capacitación y entrenamiento de los Usuarios en los cambios efectuados
- Disponer de manuales técnicos y de Usuario debidamente formalizados y actualizados
- Incorporar al manual para la administración del ciclo de vida de los sistemas de información, los procedimientos para aquellos cambios que por su urgencia o criticidad deban ser realizados de emergencia.
- En cada una de las fases del ciclo de vida de los sistemas de información, deben existir entregables (informes) que permitan un control de cada una de ellas y que permitan auditoras posteriores. Así mismo, donde sea concerniente, debe existir la participación y firma de aprobación del usuario responsable del cambio.
- Deben formularse procedimientos de control de calidad para todo el ciclo de vida del desarrollo de los sistemas de información, considerando el uso de estándares de programación, validaciones, controles, manuales técnicos y de usuarios, entre otros aspectos importantes.
- El cambio de versiones de los sistemas de información debe realizarse en base a un procedimiento formal, de registro, aprobación y monitoreo. Debe preverse mantener respaldo de las versiones de los sistemas de información en forma histórica y documentada.
- Previo a la puesta en producción deben existir análisis de impacto de los cambios realizados previo a su puesta en producción. Durante y posterior a la puesta en producción, debe realizarse un monitoreo del éxito de los cambios implementados.
- Formalizar la capacitación al personal en los cambios efectuados a las aplicaciones. Realizar por lo menos dos veces al año,

capacitaciones integrales con el personal, en donde se abarquen los cambios realizados a las aplicaciones.

- Establecer procedimientos formales para la elaboración de los Manuales Técnicos y de Usuario y adicionalmente, procedimientos para controlar su actualización continua y adecuada.
- Definir políticas de monitoreo para evaluar el cumplimiento de la metodología de desarrollo de software.

Seguridad de la Información:

- Disponer de Políticas de Seguridad de la Información
- Procedimientos de seguridad de la Información
- Plan de Seguridad de Información aprobado y revisado anualmente
- Cumplimiento de las normativas legales:
    - Identificación de la legislación aplicable
    - Licenciamiento de software
    - Propiedad Intelectual
    - Protección de la privacidad e información personal
    - Prevención del uso no autorizado de la tecnología.

- Procedimientos de evaluación de las debilidades y amenazas relacionados con tecnología.
- Pruebas de seguridad en los sistemas operativos, bases de datos, redes de datos y aplicaciones.
- Planes de acción para implementación de controles de seguridad.
- Requerimientos de control de acceso definidos y documentados.
- Requerimientos de seguridad para las aplicaciones
- Alta, baja y bloqueo de usuarios y actualizaciones de roles y perfiles.

6.6.3. Enfoque de la Auditoria

El enfoque de auditoría informática se fundamenta en lo siguiente:

- Desarrollar e implementar un enfoque de auditoría basado en los riesgos de la organización en cumplimiento de los estándares, directrices y mejores prácticas de auditoría informática.
- Planear auditorías específicas para validar que las tecnologías de información y los sistemas de negocio estén protegidos y controlados.
- Llevar a cabo auditorías en conformidad con los estándares, directriz y mejores prácticas de auditoría informática para lograr los objetivos planeados de auditoría.
- Comunicar los hallazgos emergentes, los riesgos potenciales y los resultados de la auditoría a la alta dirección.
- Asesorar sobre la implementación de la administración de riesgos y las prácticas de control dentro de la organización al tiempo que se mantiene la independencia

6.6.4. Estándares o Normas a evaluar

Para la realización de las auditorias informáticas se deben establecer los Estándares y normas sobre las cuales se van evaluar la gestión de tecnología. Para la aplicación de la auditoria consideramos se base en 3 normas que son las más aplicadas:

a. Normas establecidas por la Superintendencia de Bancos y Seguros
b. Gestión de servicio de tecnología establecida por ITIL
c. Normas de seguridad PCI para tarjetas.

a. Normas establecidas por la Superintendencia de Bancos y Seguros.

La Superintendencia de Bancos y Seguros la normativa para la gestión de tecnología la cual se cita a continuación:

Con el objeto de garantizar que la administración de la tecnología de Información soporte adecuadamente los requerimientos de operación Actuales y futuros de la entidad, las instituciones controladas deben contar al menos con lo siguiente:

- El apoyo y compromiso formal del directorio u organismo que haga sus veces y la alta gerencia;
- Un plan funcional de tecnología de información alineado con el plan estratégico institucional; y, un plan operativo que establezca las actividades a ejecutar en el corto plazo (un año), de manera que se asegure el logro de los objetivos institucionales propuestos;
- Tecnología de información acorde a las operaciones del negocio y al volumen de transacciones, monitoreada y proyectada según las necesidades y crecimiento de la institución;
- Un responsable de la información que se encargue principalmente de definir y autorizar de manera formal los accesos y cambios funcionales a las aplicaciones y monitorear el cumplimiento de los controles establecidos;
- Políticas, procesos y procedimientos de tecnología de información definidos bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento, debidamente aprobados por el directorio u organismo que haga sus veces, alineados a los objetivos y actividades de la institución;

- Difusión y comunicación a todo el personal involucrado de las mencionadas políticas, procesos y procedimientos, de tal forma que se asegure su implementación; y,
- Capacitación y entrenamiento técnico al personal del área de tecnología de información y de los usuarios de la misma.

Con el objeto de garantizar que las operaciones de tecnología de información satisfagan los requerimientos de la entidad, las instituciones controladas deben contar al menos con lo siguiente:

- Manuales o reglamentos internos, debidamente aprobados por el directorio u organismo que haga sus veces, que establezcan como mínimo las responsabilidades y procedimientos para la operación el uso de las instalaciones de procesamiento de información y respuestas a incidentes de tecnología de información;
- Un procedimiento de clasificación y control de activos de tecnología de información, que considere por lo menos, su registro e identificación, así como los responsables de su uso y mantenimiento, especialmente de los más importantes;

Con el objeto de garantizar que los recursos y servicios provistos por terceros, se administren con base en responsabilidades claramente definidas y estén sometidas a un monitoreo de su eficiencia y efectividad, las instituciones controladas deben contar al menos con lo siguiente:

- Requerimientos contractuales convenidos que definan la propiedad de la información y de las aplicaciones; y, la responsabilidad de la empresa proveedora de la tecnología en caso de ser vulnerables sus sistemas, a fin de mantener la integridad, disponibilidad y confidencialidad de la información; y,
- Requerimientos contractuales convenidos que establezcan que las aplicaciones sean parametrizables, que exista una transferencia

del conocimiento y que se entregue documentación técnica y de usuario, a fin de reducir la dependencia de las instituciones controladas con proveedores externos y los eventos de riesgo operativo que esto origina.

Con el objeto de garantizar que el sistema de administración de seguridad satisfaga las necesidades de la entidad para salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas, las instituciones deben contar al menos con lo siguiente:

- Políticas y procedimientos de seguridad de la información que establezcan sus objetivos, importancia, normas, principios, requisitos de cumplimiento, responsabilidades y comunicación de los incidentes relativos a la seguridad; considerando los aspectos legales, así como las consecuencias de violación de estas políticas;
- La identificación de los requerimientos de seguridad relacionados con la tecnología de información, considerando principalmente: la evaluación de los riesgos que enfrenta la institución; los requisitos legales, normativos, reglamentarios y contractuales; y, el conjunto específico de principios, objetivos y condiciones para el procesamiento de la información que respalda sus operaciones;
- Los controles necesarios para asegurar la integridad, disponibilidad y confidencialidad de la información administrada;
- Un sistema de administración de las seguridades de acceso a la información, que defina las facultades y atributos de los usuarios, desde el registro, eliminación y modificación, pistas de auditoría; además de los controles necesarios que permitan verificar su cumplimiento en todos los ambientes de procesamiento;
- Niveles de autorización de accesos y ejecución de las funciones de procesamiento de las aplicaciones, formalmente establecidos, que

garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude;

- Adecuados sistemas de control y autenticación para evitar accesos no autorizados, inclusive de terceros; y, ataques externos especialmente a la información crítica y a las instalaciones de procesamiento;

Con el objeto de garantizar la continuidad de las operaciones, las instituciones controladas deben contar al menos con lo siguiente:

- Controles para minimizar riesgos potenciales de sus equipos de computación ante eventos imprevistos, tales como: fallas, daños o insuficiencia de los recursos de tecnología de información; robo; incendio; humo; inundaciones; polvo; interrupciones en el fluido eléctrico, desastres naturales; entre otros;
- Políticas y procedimientos de respaldo de información periódicos, que aseguren al menos que la información crítica pueda ser recuperada en caso de falla de la tecnología de información o con posterioridad a un evento inesperado;
- Mantener los sistemas de comunicación y redundancia de los mismos que permitan garantizar la continuidad de sus servicios; y,
- Información de respaldo y procedimientos de restauración en una ubicación remota, a una distancia adecuada que garantice su disponibilidad ante eventos de desastre en el centro principal de procesamiento.

Con el objeto de garantizar que el proceso de adquisición, desarrollo, implementación y mantenimiento de las aplicaciones satisfagan los objetivos del negocio, las instituciones deben contar con lo siguiente:

- Una metodología que permita la adecuada administración y control del proceso de compra de software y del ciclo de vida de desarrollo

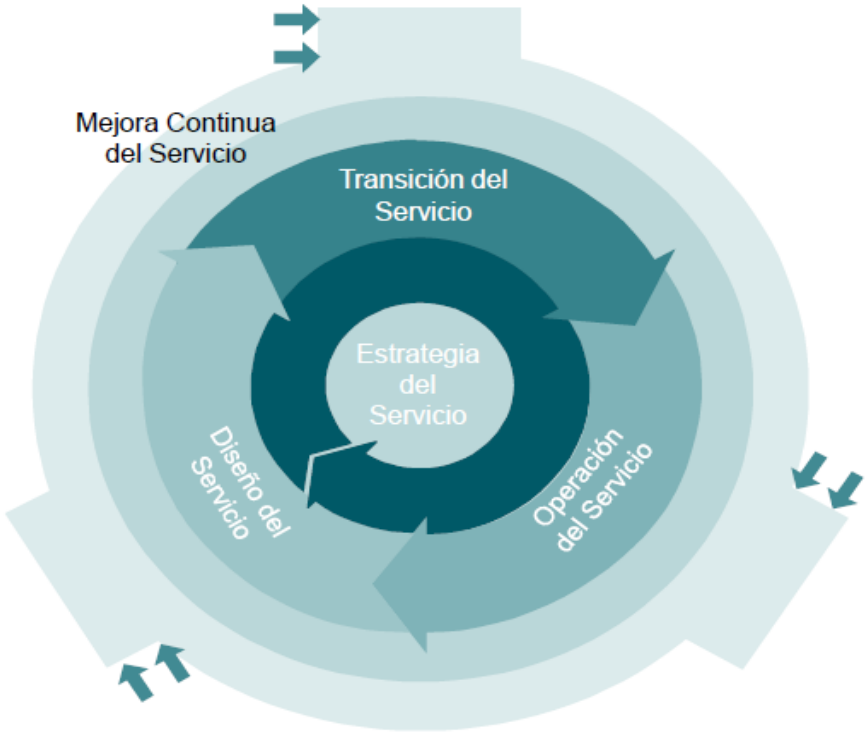
y mantenimiento de aplicaciones, con la aceptación de los usuarios involucrados;

- Con el objeto de garantizar que la infraestructura tecnológica que soporta las operaciones, sea administrada, monitoreada y documentada de forma adecuada, las instituciones controladas deberán contar con políticas y procedimientos que permitan la adecuada administración, monitoreo y documentación de las bases de datos, redes de datos, software de base y hardware.

b. Gestión de servicio de tecnología establecida por ITIL

Information Technology Infrastructure Library (ITIL). Es un conjunto de publicaciones de mejores prácticas para la gestión de servicios de Tecnología. ITIL marca las mejores prácticas de acuerdo al ciclo de vida del servicio que se resumen en el siguiente gráfico:

Gráfico 16. Ciclo de vida del Servicio



Fuente: Investigación de Campo (2011)

Elaborado por: Jaime Freire

Estrategia del Servicio (SS)

Su propósito es definir la perspectiva, posición, planes y patrones que un proveedor de servicio debe poder ejecutar para satisfacer los resultados de negocios de una organización.

Sus objetivos principales son proporcionar:

- Una comprensión de lo que es la estrategia y una identificación clara de la definición de los servicios y los clientes que los usan.
- La capacidad de definir como se crea y entrega el valor y un medio para identificar las oportunidades, proveer servicios y como explotarlos.
- Un modelo claro de prestación de servicios que articula como se entregarán y financiarán los servicios, a quienes se les entregarán y con qué propósito.
- El medio para comprender la capacidad organizacional requerida para entregar la estrategia.
- Documentación y coordinación de cómo se usan los activos de servicio para entregar servicios, y como optimizar su desempeño.

Los procesos de la Estrategia del Servicio (SS) son:

- Gestión estratégica de los servicios de TI. Responsable de definir y mantener la perspectiva, posición, planes, y patrones de una organización con respecto a sus servicios y la gestión de los mismos. Una vez que la estrategia ha sido definida, la gestión estratégica de servicios de TI también es responsable de garantizar que se logren los resultados previstos del negocio.
- Gestión del portafolio de servicios. Responsable de la gestión del portafolio de servicios. Este proceso asegura que el proveedor de

servicios tenga una combinación adecuada de servicios para satisfacer los requerimientos de resultados del negocio a un nivel adecuado de inversión. La gestión del portafolio de servicios considera a los servicios en términos de valor que ofrecen al negocio.

- Gestión financiera de servicios de Tecnología. Es la función y los procesos responsables de la gestión de la elaboración del presupuesto, la contabilidad y los requerimientos de cobro del proveedor de servicios de tecnología. La gestión financiera de servicios de tecnología asegura un nivel adecuado de financiamiento para diseñar, desarrollar y entregar servicios que respondan a la estrategia de la organización de una manera rentable.
- Gestión de la demanda. Es el proceso responsable de entender, anticipar e influir en la demanda servicios por parte de los clientes. El proceso de gestión de demanda trabaja con la gestión de capacidad para asegurar que el proveedor de servicios tenga suficiente capacidad para satisfacer la demanda requerida.
- Gestión de relaciones del negocio. Es el proceso responsable de mantener una relación positiva con los clientes. La gestión de relaciones del negocio identifica las necesidades del cliente y asegura que el proveedor de servicios sea capaz de satisfacer estas necesidades con un adecuado cat6logo de servicios.

Diseño del Servicio (DS)

El propósito es diseñar servicios de tecnología, junto con las prácticas, procesos y políticas de tecnología que los rijan, para llevar a cabo la estrategia del proveedor de servicios y facilitar la introducción de estos servicios en ambientes soportados, asegurando la entrega de servicios de calidad, la satisfacci6n de los clientes y la prestaci6n rentable de servicios.

Su objetivo es, diseñar servicios de tecnología de manera tan efectiva que se requiera un mínimo de mejoras durante el ciclo de vida.

En diseño del servicio consta de los siguientes procesos:

- Coordinación del diseño. Responsable de coordinar todas las actividades de diseño de servicios, procesos y recursos. La coordinación del diseño asegura la consistencia y efectividad del diseño de servicios de TI, sistemas de información de gestión de servicios, arquitecturas, tecnologías, procesos, información y métricas, sean estos nuevos o modificados.
- Gestión del catálogo de servicios. Responsable de proporcionar y mantener el catálogo de servicios y de asegurar que esté disponible para aquellos que están autorizados a acceder.
- Gestión de niveles de servicios. Responsable de negociar acuerdos de nivel de servicios alcanzables y de asegurar que estos se cumplan. Es responsable de asegurar que todos los procesos de gestión de servicios de Tecnología, acuerdos de nivel operativo y de los contratos de soporte sean adecuados para los objetivos de nivel de servicio acordados.
- Gestión de disponibilidad. Responsable de asegurar que los servicios de tecnología cumplan con las necesidades actuales y futuras de disponibilidad del negocio de una manera rentable y oportuna. La gesti6n de disponibilidad define, analiza, planifica, mide y mejora todos los aspectos de la disponibilidad de los servicios de tecnología, y asegura que todas las infraestructuras de tecnología, procesos, herramientas, roles, etc., sean apropiados pare los objetivos de nivel de servicio acordado para la disponibilidad.
- Gestión de capacidad. Responsable de asegurar que la capacidad de los servicios de tecnología y la infraestructura puedan cumplir

con los requerimientos acordados, relacionados con la capacidad y el desempeño de una manera rentable y oportuna. La gestión de capacidad considera todos los recursos necesarios para proporcionar un servicio de tecnología, y se preocupa de satisfacer las necesidades tanto de la capacidad actual y futura, así como del desempeño del negocio.

- Gestión de continuidad de servicios de tecnología. Responsable de gestionar los riesgos que podrán afectar seriamente los servicios de tecnología. Garantiza que el proveedor de servicios de tecnología siempre pueda entregar niveles mínimos de servicio que hayan sido acordados, al reducir los riesgos a un nivel aceptable.
- Gestión de seguridad de la información. Responsable de asegurar que la confidencialidad, integridad y disponibilidad de los activos, información, datos y servicios de tecnología de una organización satisfagan las necesidades acordadas del negocio.
- Gestión de proveedores. Responsable de la obtención de valor por el dinero pagado a los proveedores, asegurándose que todos los contratos y acuerdos con proveedores apoyen las necesidades del negocio, y que todos los proveedores cumplan sus compromisos contractuales.

Transición del Servicio (ST)

Su propósito es asegurar que los servicios nuevos, modificados o retirados cumplan con las expectativas del negocio tal y como fueron documentados en las fases de Estrategia del servicio y Diseño del servicio.

Sus objetivos son:

- Planear y administrar eficiente y efectivamente los cambios en los servicios.

- Administrar los riesgos relacionados con servicios nuevos, modificados o retirados.
- Implementar con éxito versiones dentro de los ambientes soportados.
- Establecer las expectativas correctas sobre el funcionamiento y uso de los servicios nuevos o modificados.
- Asegurar que los cambios en los servicios crean el valor esperado para el negocio.
- Proporcionar una buena calidad del conocimiento e información acerca de los servicios y activos del servicio.

Sus procesos son:

- Planificación de la transición y soporte. Responsable de la planificación de todos los procesos de transición de servicios y de la coordinación de los recursos que requieren.
- Gestión del cambio. Responsable de controlar el ciclo de vida de todos los cambios, permitiendo que se realicen cambios que son beneficiosos, minimizando la interrupción de servicios de tecnología.
- Gestión de activos de servicio y configuración. Responsable de asegurar que los activos, requeridos para entregar servicios, están debidamente controlados, y que hay información precisa y confiable sobre esos activos y que esté disponible cuando y donde se necesite. Esta información incluye detalles de cómo se han configurado los activos y las relaciones entre ellos.
- Gestión de liberación e implementación. Responsable de la planificación, programación y control de la construcción, prueba e implementación de liberaciones y de proporcionar nuevas funcionalidades que son requeridas por el negocio al tiempo que proteja la integridad de los servicios existentes.

- Validación y pruebas de servicio. Responsable de la validar y probar un servicio de tecnología nuevo o modificado. Este proceso garantiza que el servicio de tecnología coincida con la especificación de diseño y satisfaga las necesidades del negocio.
- Evaluación de cambios. Responsable de la evaluación formal de un servicio de tecnología, nuevo o modificado, para asegurar que los riesgos han sido gestionados y para ayudar a determinar si se autoriza el cambio.
- Gestión del conocimiento. Responsable de compartir perspectivas, ideas, experiencias e información, y de asegurar que estas están disponibles en el lugar correcto y en el momento adecuado. El proceso de gestión del conocimiento permite tomar decisiones informadas, y mejora la eficiencia al reducir la necesidad de redescubrir el conocimiento.

Operación del Servicio (SO)

Su propósito es coordinar y llevar a cabo las actividades y procesos requeridos para la entrega y gestión de servicios de tecnología a los usuarios y clientes del negocio, bajo los niveles acordados. Es además responsable por la administración del día a día de la tecnología utilizada para la entrega y soporte a los servicios.

Sus objetivos son:

- Mantener la confianza y satisfacción del negocio a través de una entrega y soporte efectivos y eficientes de los servicios de tecnología acordados.
- Minimizar los impactos de las interrupciones en las actividades del día a día del negocio.

- Asegurar que el acceso a los servicios de tecnología acordados es proporcionado solamente a aquellos que cuentan con la autorización para recibirlo.

Sus procesos son:

- Gestión de eventos. Responsable de gestionar los eventos durante todo su ciclo de vida. La gestión de eventos es una de las principales actividades de las operaciones de tecnología.
- Gestión de incidente. Responsable de la gestión del ciclo de vida de todos los incidentes. La gestión de incidentes asegura que se restablezca la operación normal de servicio lo antes posible y se minimice el impacto al negocio
- Cumplimiento de solicitudes. Responsable de la gestión del ciclo de vida de todas las solicitudes de servicio.
- Gestión de problemas. Responsable de la gestión del ciclo de vida de todos los problemas. La gestión de problemas previene proactivamente la ocurrencia de incidentes y minimiza el impacto de los incidentes que no se pueden prevenir.
- Gestión de acceso. Responsable de permitir que los usuarios hagan uso de los servicios de tecnología, datos u otros activos. Ayuda a proteger la confidencialidad, integridad y disponibilidad de los activos, garantizando que solo los usuarios autorizados pueden accederlos o modificarlos.

Mejora Continua del Servicio (SCI)

Su propósito es alinear los servicios de tecnología con las necesidades cambiantes del negocio al identificar e implementar mejoras a estos servicios para que soporten los procesos de negocio.

Sus objetivos son:

- Revisar, analizar y hacer recomendaciones de las oportunidades de mejora en cada fase del ciclo de vida del servicio.
- Revisar y analizar los resultados de ejecución de los niveles de servicio.
- Identificar e implementar actividades individuales para mejorar la calidad en el servicio de tecnología.
- Mejorar la efectividad en costos en la entrega de servicios de tecnología.
- Asegurar que sean usados métodos de gestión de calidad para soportar las actividades de mejora continua.
- Asegurar que los procesos tengan objetivos y medidas claramente definidos, que permitan la mejora.
- Entender que medir, porqué se está midiendo y cuál es el resultado exitoso que debe existir.

c. Normas de seguridad PCI para tarjetas

Las Normas de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (PCI) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y para facilitar la adopción de medidas de seguridad consistentes a nivel mundial. Las PCI DSS proporcionan una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los titulares de tarjetas. Las PCI DSS se aplican a todas las entidades que participan en los procesos de las tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios, así como también todas las demás entidades que almacenan, procesan o transmiten datos de titulares de tarjetas. Las PCI DSS constituyen un conjunto mínimo de requisitos para proteger datos de titulares de tarjetas y se pueden mejorar con el uso de controles y prácticas adicionales para mitigar otros riesgos.

A continuación, encontrará una descripción general de los 12 requisitos de las PCI DSS.

Gráfico 17. Normas de seguridad PCI

Normas de seguridad de datos de la PCI: descripción general de alto nivel

Desarrollar y mantener una red segura	1. Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta 2. No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores
Proteger los datos del titular de la tarjeta	3. Proteja los datos del titular de la tarjeta que fueron almacenados 4. Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas
Mantener un programa de administración de vulnerabilidad	5. Utilice y actualice con regularidad los programas o software antivirus 6. Desarrolle y mantenga sistemas y aplicaciones seguras
Implementar medidas sólidas de control de acceso	7. Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa 8. Asignar una ID exclusiva a cada persona que tenga acceso por computador 9. Restringir el acceso físico a los datos del titular de la tarjeta
Supervisar y evaluar las redes con regularidad	10. Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas 11. Pruebe con regularidad los sistemas y procesos de seguridad
Mantener una política de seguridad de información	12. Mantenga una política que aborde la seguridad de la información para todo el personal

Fuente: Investigación de Campo (2011)

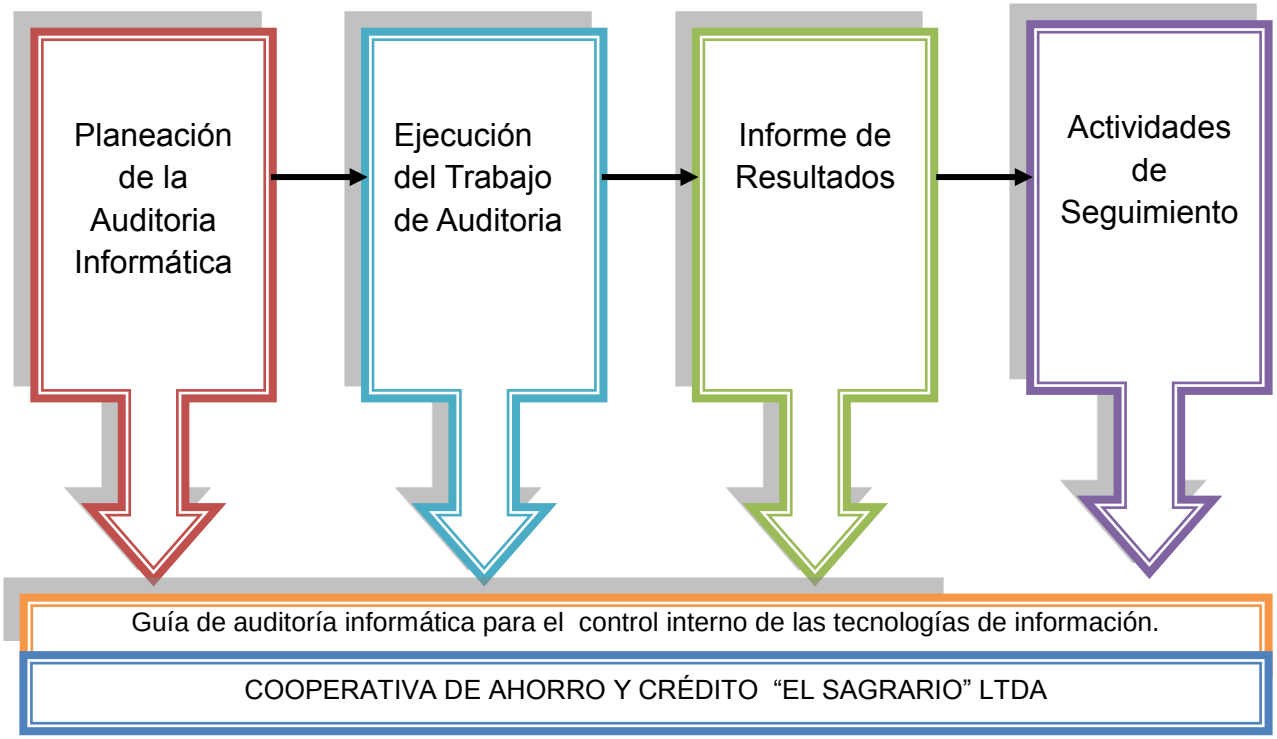
Elaborado por: Jaime Freire

6.7 METODOLOGÍA

6.7.1 Modelo Operativo

Para la realización de la auditoria informática en la Cooperativa el Sagrario se puede seguir el siguiente modelo operativo el cual está basado en los estándares, directrices y procedimientos dictados por ISACA, la misma que es una organización internacional encargada de dictar normas y procedimiento para los gobiernos de tecnología como para áreas de control. El modelo operativo está basado en 4 fases principales.

Gráfico 18. Modelo Operativo



Fuente: Investigación de Campo (2011)

Elaborado por: Jaime Freire

6.7.2. Plan de Acción

Tabla 20. Plan de Acción

Fases	Actividades	Recursos	Responsables	Tiempo
Planeación de la Auditoria Informática	Definir los objetivos y alcance de la auditoria	Suministros de oficina	Auditor Interno	1 día
	Realizar una reunión previa con la alta gerencia, dueños de procesos	Proyector, computadora	Auditor Interno	2 días
	Recopilar información preliminar.	Manuales y procedimientos	Auditor Interno	5 días
	Realizar un análisis de Riesgos	Manual de riesgos	Auditor Interno	5 días

	Elaborar el programa de auditoría.	Guía de Auditoria Informática	Auditor Interno	5 días
Ejecución del Trabajo de Auditoria	Diagnóstico de los procesos de tecnología	Equipo de Cómputo	Auditor Interno	30 días
	Revisión técnica de los procesos de tecnología	Transporte, Viáticos, Suministros de Oficina	Asistentes de Auditoria	30 días
	Documentar, las labores de auditoría.			
Informe de Resultados	Elaborar el Informe Preliminar	Suministros de Oficina	Asistente de Auditoria	5 días
	Presentar el informe preliminar a la Alta Gerencia	Sala de reuniones, Proyector.	Asistente de Auditoria	1 día
	Entregar informe definitivo.	Suministros de oficina	Auditor Interno	5 días
Actividades de Seguimiento	Elaborar un cronograma de seguimientos	Informe de Auditoria	Auditor Interno	Trimestral
	Realizar los seguimientos y elaborar el informe sobre el cumplimiento.			

Fuente: Investigación de Campo (2011)

Elaborado por: Jaime Freire

6.7.3. Fases de la auditoria.

De acuerdo al plan de acción se han definido las siguientes fases para la auditoria informática.

- Planeación de la Auditoria Informática.
- Ejecución del Trabajo de Auditoria
- Informe de Resultados
- Actividades de Seguimiento

6.7.3.1. Planeación de la Auditoria Informática

En la panificación de la auditoria se recomienda que se realicen los siguientes procesos:

Gráfico 19. Procesos de Planeación

Fuente: Investigación de Campo (2011)

Elaborado por: Jaime Freire

a. Definir los objetivos y alcance.

Se debe definir claramente los objetivos que se persigue al realizar la auditoria y la áreas o puntos que se van a revisar. Los objetivos deben estar orientados a detallar cuáles componentes de la materia se auditarán, y en base a que norma se va evaluar.

En la definición del alcance se debe detallar cuáles son los procesos o componentes de tecnología que va a ser auditados, se puede realizar una auditoría integral a todos los procesos de tecnología o a su vez realizar un

examen especial a un solo proceso como por ejemplo: Examen especial al proceso de Administración de Tecnología para verificar el cumplimiento de las normas establecidas por la superintendencia de bancos y seguros.

b. Realizar una reunión previa con la alta gerencia, dueños de procesos

Con el fin de tener una visión preliminar de los procesos de tecnología, es conveniente que se mantenga una reunión con la Gerencia General, dueños de los procesos para conocer el desempeño de los procesos de tecnología, lo cual va servir al auditor para determinar empíricamente el grado de conformidad que tienen los usuarios en relación a cada uno de los procesos de tecnología.

Como resultado de esta reunión se debe obtener información relevante (cuantitativa y cualitativa) que permita al equipo de trabajo conocer las principales características de la materia a auditar así como identificar los asuntos significativos del trabajo, enfocándose en identificar principalmente los riesgos relevantes de la materia y sus mecanismos de control y monitoreo, evaluar si se justifica o no la actualización de los objetivos del trabajo, y finalmente determinar las estrategias frente al trabajo

c. Recopilar información preliminar.

El auditor debe recopilar la mayor información posible para comprender o actualizar el conocimiento de la materia a auditar; estructura organizacional, procesos de negocio, operaciones y procesos de tecnología con el propósito de identificar preliminarmente los riesgos en los que se deberá focalizar el trabajo.

Es necesario conocer la normativa externa e interna, información técnica, sistemas operativos, bases de datos, comunicaciones, etc. Que pudiera tener un impacto significativo en la materia a auditar. Entre los documentos que se deben solicitar se encuentran:

- Manuales de Políticas y Procedimientos de Tecnología.
- Manuales Operativos de los procesos de Tecnología.
- Bitácoras o registros de eventos de Tecnología.
- Manuales Técnicos y de Diseño de los Sistemas de Información.
- Inventarios de Hardware y Software.
- Contratos con proveedores de servicios de Tecnología.
- Planes estratégicos y operativos de Tecnología.
- Inventario de roles y perfiles de acceso a los sistemas de información.
- Manual de Seguridades.
- Manual de contingencias y continuidad del negocio.
- Demás documentación que considere necesario el auditor.

d. Realizar un análisis de Riesgos

El análisis de riesgos realizada en la planeación de Auditoría Informática, ayuda a identificar los riesgos y vulnerabilidades a las que están expuestos los recursos de tecnología y los controles para su mitigación.

Se debe evaluar el proceso de administración integral de riesgos de la organización y su alcance dentro de la gestión de riesgos de Tecnología.

El enfoque del auditor debe ser hacia los aspectos de mayor riesgo que pudieran afectar la integridad, confidencialidad y disponibilidad de la información. Como por ejemplo, administración de base de datos, metodología de desarrollo de software, planes de contingencia y continuidad, manual de seguridad.

En base al análisis de riesgos realizado por el auditor se deberá establecer los controles y los procesos a ser evaluados.
Adicionalmente existe el riesgo de auditoría: El riesgo de que el informe de auditoría pueda contener errores materiales que pudieran no ser detectados durante el examen de auditoría.

El Riesgo de Auditoría se pueden clasificar en:

- Riesgo Inherente: Error material o significativo cuando se combina con otros errores encontrados durante la auditoría, suponiendo que no existen controles compensatorios.
- Riesgo de Control: Error material que no es detectado por los controles implementados.
- Riesgo de Detección: Riesgo de usar un procedimiento inadecuado y se concluya que no existen errores materiales cuando realmente existen.
- Riesgo General: Combinación de los riesgos individuales de auditoría para cada objetivo de control.

e. Elaborar el programa de auditoría.

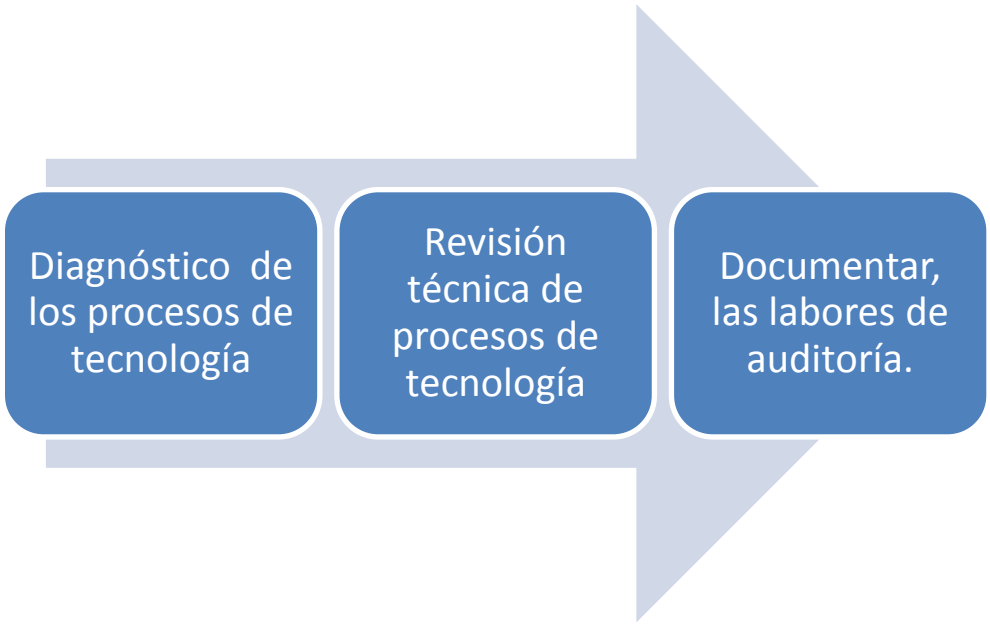
Los programas de auditoría establecen el alcance y el objetivo que se busca con el examen a realizarse.
Establece los procedimientos de auditoría para lograr evidencia suficiente y competente para obtener y sustentar las conclusiones y recomendaciones de auditoría.

6.7.3.2. Ejecución de la auditoria informática.

Las actividades a realizar durante la ejecución de la auditoría están principalmente enfocadas a identificar y evaluar los riesgos asociados a

las materias a auditar, para reducir, compartir o aceptar dichos riesgos y para probar las actividades de control y/o monitoreo. Durante este proceso es necesario que se tomen en cuenta los siguientes procesos

Gráfico 20. Procesos para la fase de ejecución



Fuente: Investigación de Campo (2011)

Elaborado por: Jaime Freire

a. Diagnóstico de los procesos de tecnología.

Para realizar el diagnóstico de los procesos de tecnología se deben elaborar cuestionarios de acuerdo a los estándares o normas contra los cuales se desea evaluar y definir el nivel de cumplimiento.

a.1. Se propone los siguientes cuestionarios de evaluación:

1. Cuestionario para la evaluación de cumplimiento de las normas establecidas por la superintendencia de bancos.

Tabla 21. Cuestionario para evaluación de normas de la superintendencia de bancos

¿La entidad cuenta con una planificación estratégica de Tecnología de Información (TI) que considere planes a largo y corto plazo acordes con la misión y las estrategias de negocio de la organización?	Nivel de Cumplimiento
Planificación estratégica de la tecnología de información, aprobada y respaldada por un procedimiento formal.	
Plan operativo anual y presupuesto aprobados formalmente.	
Cuenta con una estructura orgánico - funcional de TI acorde con los servicios que brinda, así como con un comité directivo que supervise sus servicios.	
Existe un manual de políticas y procedimientos de tecnología de información aprobado formalmente, difundidos y comunicados.	
Cuenta con un plan de entrenamiento y capacitación anual para el personal de TI acorde con las necesidades para la ejecución de sus funciones, y considera un plan de entrenamiento anual para usuarios de los servicios de información.	

¿La entidad ha definido procedimientos para garantizar que las operaciones de TI satisfagan los requerimientos de la entidad?	Nivel de Cumplimiento
Los usuarios y la función de tecnología de información cuentan con acuerdos escritos que describan los niveles de servicio en términos cualitativos y cuantitativos y responsabilidades de ambas partes.	
El área de TI ha definido procedimientos para la administración de incidentes y problemas incluyendo su registro, análisis y solución oportuna.	
El área de TI ha establecido y documentado procedimientos para las operaciones de tecnología de información.	
El área de TI ha establecido procedimientos para soporte a usuarios, dentro de una función de Help Desk o Mesa de Control y Ayuda.	
Existen procedimientos para la administración de activos de tecnología que incluyan su registro, clasificación, control y responsables de su uso y mantenimiento.	

¿La administración de servicios tecnológicos provistos por terceros considera los criterios de contratación institucionales, responsabilidades y monitoreo de la prestación del servicio para garantizar que satisface los requerimientos de la entidad?	Nivel de Cumplimiento
Los servicios de TI provistos por terceros se administran de acuerdo con las políticas institucionales de contratación de servicios.	
Los contratos de servicios de TI provistos por terceros definen la propiedad de la información así como las responsabilidades de cada parte.	
La entidad ha designado una contraparte técnica que sea responsable de administrar las relaciones con terceros.	
Los contratos consideran la transferencia de conocimiento y entrega de documentación técnica y de usuario, así como la aceptación del usuario (si aplica).	

Se ha definido un procedimiento formal y continuo de monitoreo sobre la prestación de servicio de terceros, con el fin de asegurar el cumplimiento de los acuerdos del contrato.	

¿La entidad cuenta con un sistema de administración de seguridad de la información que garantice su integridad, disponibilidad y confidencialidad?	Nivel de Cumplimiento
La entidad cuenta con políticas y procedimientos de seguridad de la información aprobadas formalmente, difundidas e implementadas; incluyendo aquellas relacionadas con servicios de transferencia y transacciones electrónicas, si aplica.	
La entidad ha identificado los requerimientos de seguridad relacionados con la tecnología de información y ha implementado los controles necesarios para minimizar el impacto de las vulnerabilidades e incidentes de seguridad.	
La entidad cuenta con un sistema de administración de las seguridades de acceso a la información y niveles de autorización de accesos para ejecución de las funciones de procesamiento.	
La entidad dispone de un plan de evaluación del desempeño del sistema de administración de la seguridad de la información que permita tomar acciones para mejorarlo.	
La entidad cuenta con condiciones físicas y ambientales necesarias para garantizar la seguridad de la información y el correcto funcionamiento del entorno de la infraestructura de tecnología de información.	

¿La entidad cuenta con políticas y procedimientos para la adquisición, desarrollo, implementación y mantenimiento de las aplicaciones que garanticen que éstas satisfacen los requerimientos del negocio?	Nivel de Cumplimiento
La entidad dispone de una metodología para la administración del ciclo de vida de desarrollo, mantenimiento y/o adquisición de aplicaciones incluyendo procedimientos para migración de información si aplica.	
La entidad cuenta con un procedimiento de monitoreo para evaluar el cumplimiento de la metodología del ciclo de vida de desarrollo de sistemas.	
La entidad tiene procedimientos formales para administración de versiones que garanticen el registro, evaluación y autorización de los cambios previo a su implantación y la revisión posterior contra los resultados planeados.	
La entidad considera la ejecución de un plan de entrenamiento de las nuevas implementaciones efectuadas, a los usuarios involucrados y al grupo de operaciones de la función de TI.	
La entidad cuenta con procedimientos formales que garanticen que la documentación técnica y de usuario se mantiene actualizada y disponible para los usuarios.	

¿La entidad cuenta con políticas y procedimientos que garanticen una adecuada administración, monitoreo y documentación de la infraestructura tecnológica?	Nivel de Cumplimiento
Cuenta con procesos para adquirir, implementar y actualizar la infraestructura tecnológica de acuerdo con las estrategias tecnológicas establecidas.	

Dispone de políticas y procedimientos formales para la administración del desempeño y la capacidad de los recursos de TI que incluya su revisión periódica, el desempeño actual y el pronóstico de las necesidades futuras.	
Existen políticas y procedimientos de administración de configuraciones de la infraestructura tecnológica que permita garantizar una mayor disponibilidad, minimice los problemas de producción y los resuelva más rápido.	
Ha efectuado un levantamiento de la documentación correspondiente a la infraestructura tecnología incluyendo bases de datos, redes de datos, software de base y hardware.	
Ha establecido políticas formales y controles para detectar y evitar la instalación de software no autorizado o no licenciado, así como instalar y actualizar periódicamente aplicaciones de detección y eliminación de virus informático y demás software malicioso.	

Fuente: Investigación de Campo (2011)

Elaborado por: Jaime Freire

2. Cuestionario para establecer la madurez de los procesos de Servicios de Diseño de ITL.

Tabla 22. Cuestionario para establecer la madurez de los proceso

Coordinación del diseño	Nivel de Cumplimiento
Coordinar todas las actividades de diseño en los proyectos	
Planear y coordinar los recursos y sus habilidades a lo largo del diseño de servicios nuevos y/o modificados	
Asegurar que el diseño de los servicios y los SDPs generados son manejados de acuerdo a lo acordado durante la transición	
Monitorear y mejorar el desempeño de la etapa de diseño de servicio del ciclo de vida	
Asistir y soportar cada proyecto	
Definir y mantener políticas y métodos	
Planificar los recursos y capacidades de diseño	
Coordinar actividades de diseño	
Gestionar riesgos de diseño y situaciones	
Mejorar el diseño del servicio	
Planear diseños individuales	
Coordinar diseños individuales	
Monitorear diseños individuales	
Revisar diseños y asegurar la entrega del servicio	
Están definidos y asignados los roles del proceso	
Se realiza la definición, medición y comparación contra metas de las métricas del proceso	

Gestión del catálogo de servicios	Nivel de Cumplimiento
Se documenta la definición del servicio	
Se mantiene comunicación con la gestión del portafolio de servicio para acordar el contenido del portafolio y del catálogo	
Se produce y mantiene el catálogo de servicios	
Asegurar que la información del catálogo de servicios esté alineada al negocio y a los procesos del negocio.	
Se mantiene comunicación con el negocio y gestión de continuidad de servicios de TI	
Se mantiene comunicación con los equipos de soporte, proveedores y gestión de configuración para el catálogo de servicios técnico	
Se mantiene comunicación con la gestión de relaciones del negocio y con gestión de niveles de servicio para asegurar que la información está alineada al negocio y a sus procesos	
Están definidos y asignados los roles del proceso	
Se realiza la definición, medición y comparación contra metas de las métricas del proceso	

Gestión de niveles de servicio	Nivel de Cumplimiento
Se determinan los requerimientos para nuevos servicios	
Se determinan los requerimientos para cambios en los servicios existentes	
Se negocian, documentan y acuerdan dichos requerimientos para nuevos servicios	
Se monitorea y mide el desempeño del servicio	
Se cuenta con un proceso para recolectar y medir la satisfacción del cliente	
Monitorear y mejorar la satisfacción del cliente con la calidad del servicio entregado	
Se cuenta con SLAs, OLAs, y contratos para establecer los requerimientos con clientes y entre las áreas	
Se revisan y ajustan dichos SLAs y OLAs	
Se cuenta con un procedimiento para desarrollar y documentar los contactos y relaciones ya sea con el negocio, clientes o stakeholders	
Se realiza dicho procedimiento para desarrollar y documentar los contactos y relaciones con el negocio, clientes o stakeholders	
Se miden, periódicamente, los servicios para validar su desempeño	
Se cuenta con plantillas y estándares actualizados de los SLAs y OLAs	
Se mantienen actualizados las plantillas y estándares de los SLAs y OLAs	
Se realizan revisiones del servicio para proponer mejoras por medio del plan de mejora del servicio (SIP)	
Están definidos y asignados los roles del proceso	
Se realiza la definición, medición y comparación contra metas de las métricas del proceso	

Gestión de la capacidad	Nivel de Cumplimiento
Se produce y mantiene un plan de la capacidad	
Generar tendencias del nivel actual de utilización de los componentes	
Gestión de capacidad apoya en acordar los requerimientos de nivel de servicios [SLRs]	
Apoya a la gestión de niveles de servicio para entender las capacidades y desempeño que el cliente requiere	

Se realiza el diseño de la configuración de los servicios, participa en el diseño de nuevos servicios o cambio en los mismos	
Se realizan recomendaciones para la adquisición de hardware y software	
Se verifica y apoya en la negociación de los SLAs para prever el rendimiento y requerimientos del servicio	
Se realizan modelaciones para asegurar que los recursos están disponibles	
Se analizan el desempeño de los servicios y componentes para predecir el uso de los recursos y monitorear el crecimiento actual del negocio vs el crecimiento pronosticado	
Se realiza el control y administración de eventos de umbrales de capacidad para asegurar que se mantienen los niveles apropiados de manera continua	
Se generan alarmas/alertas cuando ocurre una brecha	
Se realiza la dimensión de aplicaciones para estimar recursos requeridos	
Ayudar con el diagnóstico y resolución de incidentes y problemas relacionados con la capacidad y el desempeño	
Se evalúa el impacto de todos los cambios en el plan de la capacidad y el rendimiento y capacidad de todos los recursos y servicios	
Están definidos y asignados los roles del proceso	
Se realiza la definición, medición y comparación contra metas de las métricas del proceso	

Gestión de disponibilidad	Nivel de Cumplimiento
Producir y mantener un plan de disponibilidad adecuado	
Evaluar el impacto de todos los cambios en el plan de disponibilidad y en el rendimiento y capacidad de todos los servicios y recursos	
Asegurar medición proactiva para mejorar la disponibilidad de los servicios	
Se realizan monitoreo, mediciones y análisis de la disponibilidad del servicio	
Se analizan los eventos e incidentes causantes de la indisponibilidad del servicio	
Se realizan un análisis para identificar causa raíz de las interrupciones del servicio hacia el usuario	
Se identifican las VBFs [Vital Business Functions]	
Se cuenta con un diseño de la disponibilidad / alta disponibilidad de los servicios	
Se cuenta con el nivel de disponibilidad requerido por el negocio basado en el costo total del servicio proporcionado por TI	
Se tienen identificados los componentes y productos base	
Se busca mejorar la disponibilidad utilizando componentes duplicados para aplicar soluciones con redundancia completa	
Se gestionan y analizan los riesgos para evaluar vulnerabilidad de las fallas dentro de la configuración y capacidad de los servicios de TI	
Se realizan mantenimientos planeados y preventivos de los elementos	
Se tiene documentado el PSO [project service outage], con detalle de todos los servicios fuera de servicio dentro de los horarios acordados	
Están definidos y asignados los roles del proceso	
Se realiza la definición, medición y comparación contra metas de las métricas del proceso	

Gestión de disponibilidad	Nivel de Cumplimiento
Producir y mantener un plan de disponibilidad adecuado	
Evaluar el impacto de todos los cambios en el plan de disponibilidad y en el rendimiento y capacidad de todos los servicios y recursos	
Asegurar medición proactiva para mejorar la disponibilidad de los servicios	
Se realizan monitoreo, mediciones y análisis de la disponibilidad del servicio	
Se analizan los eventos e incidentes causantes de la indisponibilidad del servicio	
Se realizan un análisis para identificar causa raíz de las interrupciones del servicio hacia el usuario	
Se identifican las VBFs [Vital Business Functions]	
Se cuenta con un diseño de la disponibilidad / alta disponibilidad de los servicios	
Se cuenta con el nivel de disponibilidad requerido por el negocio basado en el costo total del servicio proporcionado por TI	
Se tienen identificados los componentes y productos base	
Se busca mejorar la disponibilidad utilizando componentes duplicados para aplicar soluciones con redundancia completa	
Se gestionan y analizan los riesgos para evaluar vulnerabilidad de las fallas dentro de la configuración y capacidad de los servicios de TI	
Se realizan mantenimientos planeados y preventivos de los elementos	
Se tiene documentado el PSO [project service outage], con detalle de todos los servicios fuera de servicio dentro de los horarios acordados	
Están definidos y asignados los roles del proceso	
Se realiza la definición, medición y comparación contra metas de las métricas del proceso	

Gestión de la seguridad de la información	Nivel de Cumplimiento
Se cuenta con políticas de seguridad de la información	
Las políticas son revisadas y ajustadas de acuerdo a las necesidades de la organización	
Se comunican y aplican dichas políticas	
La información sólo puede ser observada o divulgada para aquellos que tienen el derecho de saberlo	
La información está completa, exacta y protegida contra modificaciones no autorizadas	
La información está disponible y puede ser usada al momento de ser requerida y que los sistemas que la almacenan pueden resistir ataques y recuperarse o prevenir fallas	
Se tienen implementados y se revisan controles de seguridad	
Se evalúa y clasifica la documentación e información de los activos de información	
Se realizan análisis y reportes sobre incidentes mayores relacionados con la seguridad	
Se realiza reducción en los incidentes y las brechas relacionados con seguridad	
Se llevan a cabo revisiones, auditorías y pruebas de acceso	
Se realizan acciones a partir de los resultados de dichas revisiones y auditorías	

Se cuenta con un sistema de gestión de seguridad de la información que incluye los controles de seguridad, riesgos, brechas y reportes necesarios para mantener la política	
Están definidos y asignados los roles del proceso	
Se realiza la definición, medición y comparación contra metas de las métricas del proceso	

Gestión de continuidad de servicios de TI	Nivel de Cumplimiento
Se tienen establecidas las políticas de continuidad del servicio	
Se tienen definidos los requerimientos de continuidad del servicio	
Se desarrolla un análisis del impacto al negocio y evaluación de riesgos	
Se realiza la documentación de dicho análisis	
Se tienen documentadas las opciones de recuperación	
Se desarrollan e implementan los planes de continuidad del servicio	
Se realizan pruebas a dichos planes de continuidad del servicio	
Se asegura que el plan de continuidad de TI soporte el plan de continuidad del negocio	
Se realiza una educación, concientización y entrenamiento sobre los planes de continuidad del servicio	
Se realizan revisiones regulares o un programa de pruebas para asegurar la continuidad del servicio	
Negociar y acordar, con los proveedores la entrega de las medidas de recuperación necesarias para soportar los planes de continuidad	
Existe una revisión regular de los entregables	
Están definidos y asignados los roles del proceso	
Se realiza la definición, medición y comparación contra metas de las métricas del proceso	

Gestión de proveedores	Nivel de Cumplimiento
Se tiene identificada, implementada y aplicada la política de proveedores	
Se tienen identificadas las necesidades del negocio, se realiza un declaración de los requerimientos/licitación	
Se cuenta con un procedimiento para la evaluación y selección de proveedores	
Se tiene identificado el método de compra y criterios de evaluación	
Se tienen definidos los criterios para negociar el contrato, objetivos, términos y condiciones	
Se establecen nuevos proveedores y contratos de acuerdo a las necesidades del negocio	
Se cuenta con una categorización de proveedores y contratos, se evalúan para asegurar el progreso a través de los cambios en la organización	
Se realiza la gestión del desempeño del proveedor y contrato para controlar la operación y entrega del servicio	
Se realizan revisiones del alcance del servicio contra las necesidades, objetivos y acuerdos	
Se realizan la gestión del fin del contrato para asegurar que se toman en cuenta todos los aspectos	
Mantenimiento de un sistema de proveedores y contratos (SCMIS)	
Están definidos y asignados los roles del proceso	
Se realiza la definición, medición y comparación contra metas de las métricas del proceso	

3. Cuestionario para establecer el grado de cumplimiento de las normas PCI.

Tabla 23. Cuestionario de evaluación de normas PCI

EXISTENCIA DE NORMATIVA	Nivel de Cumplimiento
Normas y / o estándares de configuración de firewall(s); esto también aplica para las reglas y/o listas de acceso aplicadas a routers, switches y acces points	
Políticas y procedimientos de retención y eliminación de información	
Norma del manejo adecuado y aceptable del PAN, incluyendo ocultamiento del número de tarjeta (PAN) en módulos del flujo(s) que no requieran el despliegue del número PAN completo, norma o política que prohíbe el envío del PAN por mensajería, chat, email, etc.	
Política y procedimientos de manejo, distribución, destrucción de medios de almacenamiento de información, incluyendo papel y medios electrónicos.	
Norma de sincronización de relojes en los componentes del sistema.	
Política de seguridad de la información, incluyendo la política general y la política de riesgos a la información. Así mismo se deben poner los responsables por su verificación, divulgación y cumplimiento.	
Políticas y procedimientos de retención y eliminación de información. Tabla de Retención Documental/Electrónica	
Políticas o Normas de no almacenamiento (prohibición explícita) de datos sensibles de tarjetahabiente tales como banda magnética, código de verificación (CVC2, CVV2, CID, CAV2), PIN y bloque de PIN.	
Norma del manejo adecuado y aceptable del PAN, incluyendo ocultamiento del número de tarjeta (PAN) en módulos del flujo(s) que no requieran el despliegue del número PAN completo. Política o Norma que prohíbe el envío del PAN por mensajería, chat, email, etc.	
Procedimientos de gestión de llaves de encripción utilizadas para cifrar los datos de los tarjetahabientes.	
Políticas, Normas y/o Procedimientos de uso, gestión y actualización de software y definiciones de Antivirus - AntiMalware.	
Políticas y Procedimientos de administración de parches y actualizaciones a componentes del sistema. (Procedimiento de gestión de vulnerabilidades)	
Políticas y procedimientos de desarrollo de software seguro. Basado en normas industriales. Ejemplo: CMMI, OWASP, TICKIT, entre otras	
Procedimiento de control de cambios a los sistemas de información.	
Política de Control de Acceso a Datos y Componentes de Sistema de la Organización. Métodos documentados de Autenticación de los usuarios.	
Mapa/Cuadro/Matriz de Roles y Privilegios de Acceso a los Sistemas de Información. (RBAC - Roled Based Access Control).	
Políticas, normas, procedimientos y estándares de administración de roles, usuarios y contraseñas.	
Procedimientos y normas de control de acceso físico a las instalaciones de la organización, identificación de visitantes y empleados, entre otros.	

Procedimiento de almacenamiento seguro (interno y/o externo) de Backup.	
Política y procedimientos de almacenamiento, manejo, distribución y destrucción de medios de almacenamiento de información, incluyendo papel y medios electrónicos.	
Norma de sincronización de relojes en los componentes del sistema.	
Políticas y procedimientos de administración, protección, retención y revisión de Logs.	
Procedimientos de gestión de vulnerabilidades y pruebas de penetración (Ethical Hacking).	
Organigrama de la organización y del área de Tecnología.	
Diagramas de flujo y/o procedimientos operativos relacionados con tarjetas.	
Política de seguridad de la información, incluyendo la política general y la política de riesgos a la información. Así mismo se deben indicar los responsables por su verificación, divulgación y cumplimiento.	
Estructura del equipo (comité) o rol responsable por la seguridad de la información en la organización, definiendo roles, funciones, etc.	
Procedimiento de revisión de políticas de seguridad de la información.	
Procedimientos de seguridad en las operaciones diarias. (Revisión de Logs, Gestión de usuarios, soporte técnico, etc)	
Políticas de uso aceptable. incluyendo la de acceso a internet, mensajería instantánea, manejo de correo electrónico, manejo de laptops, medios removibles, acceso remoto, autenticación y cualquier uso de tecnología en la organización, entre otros.	
Procedimientos y normas de acceso remoto al ambiente de datos de los tarjetahabientes. Sea por RAS o VPN.	
Plan o procedimiento de divulgación de políticas.	
Políticas, planes y programas de concientización en seguridad de la información y protección de datos de los tarjetahabientes.	
Procedimientos de selección, contratación y retiro de personal.	
Políticas y procedimientos para gestión de la contratación y supervisión de proveedores de servicio.	
Plan y Procedimientos de respuesta a incidentes de Seguridad	

Fuente: Investigación de Campo (2011)

Elaborado por: Jaime Freire

a.2. Proceso para la evaluación.

Para realizar la evaluación se toman en cuenta, entrevistas realizadas al personal del área, a los clientes del área, así como evidencia de procedimientos, reportes, evaluaciones, herramientas de apoyo. Una vez recopilada y analizada la información se procede a evaluar, utilizando la tabla de madurez de los procesos, donde:

- Se contemplan 5 niveles de madurez para determinar el estatus actual de la empresa en donde cada enunciado a evaluar es una

aseveración y debe contestarse de acuerdo a cómo se realizan actualmente las actividades de la empresa evaluada.

- La calificación se da en base a una escala con valores del 0 al 5 donde, 5 es totalmente de acuerdo con el enunciado y 0 es totalmente desacuerdo, este último valor se utiliza cuando no se obtuvo evidencia del punto evaluado por ningún medio posible, hay que tomar en cuenta que se pueden dar medios puntos. Siendo el total de posibles respuestas [0, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, 5].
- Una vez evaluado los cuestionarios, se genera un promedio y se obtiene el valor que determina el nivel de madurez. Para interpretar el valor obtenido se tienen a continuación los diferentes niveles de madurez y su interpretación:

Gráfico 21. Niveles de Madurez

Nivel 1: Inicial (0 – 1.4)
• El área mantiene un enfoque basado en funciones, existen silos de información y las áreas se miden por cumplimiento de objetivos funcionales.
• No se cumplen los objetivos y/o se llevan acabo las actividades críticas del proceso.
Nivel 2: Repetible (1.5 – 2.4)
• Se mantiene el enfoque funcional en TI, sin embargo se llevan acabo algunas actividades del proceso al compartirse información y objetivos entre 2 o más áreas.
• El desarrollo de las actividades es informal al no contarse con procedimientos definidos.
Nivel 3: Definido (2.5 – 3-4)
• El proceso está definido y documentado.
• El enfoque del área mantiene su organización funcional, sin embargo se definen roles y responsabilidades de proceso.
• Se generan evidencias del desarrollo de las actividades, sin embargo éstas no se llevan a cabo de manera sistemática.
Nivel 4: Administrado (3.5 – 4-4)
• El desarrollo de las actividades es estándar y sistemático.
• El proceso se ha probado al menos una vez y se ha llevado a cabo de manera consistente y es proactivo.
• Se generan y coordinan las relaciones entre procesos de TI.
Nivel 5: Optimizado (4.5 -5.0)
• El proceso se lleva a cabo de manera eficiente y efectiva, tiene metas y objetivos estratégicos alineados con la estrategia de negocio y de TI.
• Se integran acciones y planes de mejora a los procesos, a su coordinación y se evidencia el valor hacia el negocio.

Fuente: Investigación de Campo (2011)

Elaborado por: Jaime Freire

b. Revisión técnica de procesos de tecnología

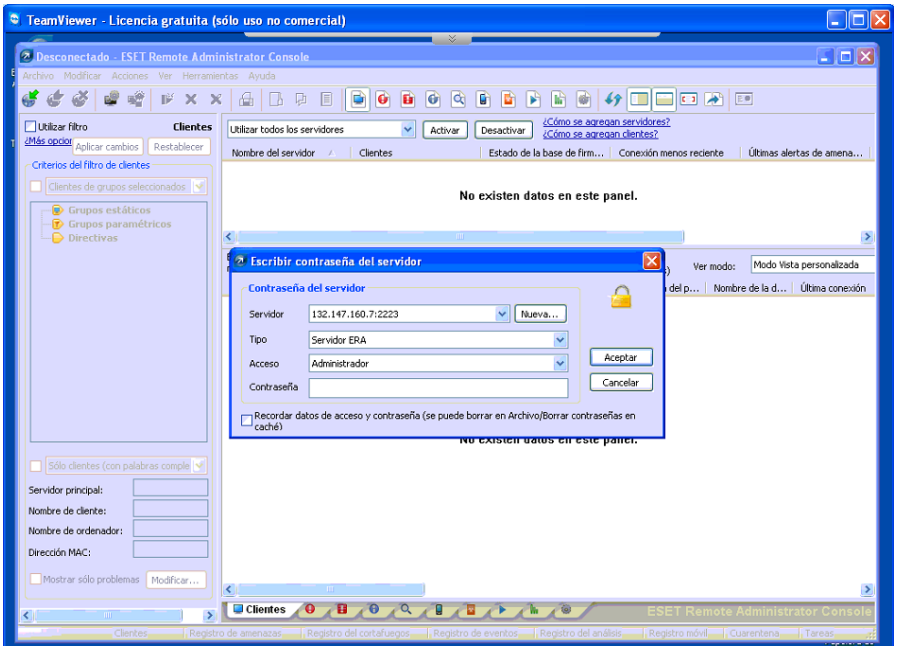
Uno de los procesos más críticos de la tecnología es las seguridades de las mismas, por tal motivo se indica el proceso para la verificación del adecuado funcionamiento de Antivirus, Dominio y Firewall.

b.1. Revisión de servidor de Antivirus.

Para verificar que en todos los equipos de la red se encuentre instalado un antivirus se recomienda realizar con el apoyo del encargado de la administración del antivirus los siguientes pasos:

1. Ingresar a la consola de administración. Para lo cual es necesario que se digite una clave, se mostrara la siguiente pantalla.

Gráfico 22. Pantalla de Ingreso a la consola del antivirus

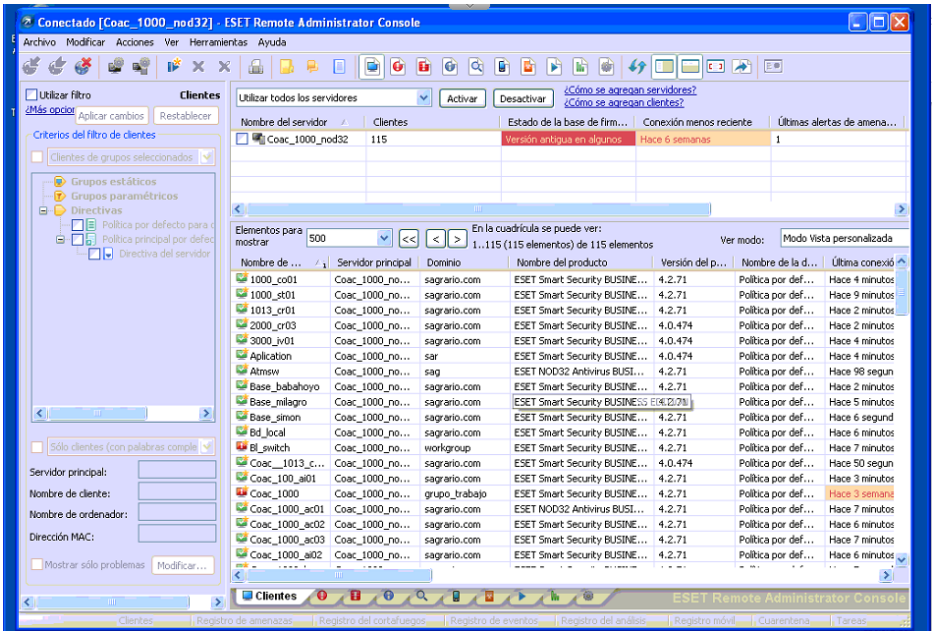


Fuente: Investigación de Campo (2011)

Elaborado por: Jaime Freire

2. Revisar cada uno de los equipos. En la consola de administración se debe revisar todos los equipos instalados y verificar si concuerda con los que se encuentran en el inventario de hardware. La pantalla que se muestra es la siguiente:

Gráfico 23. Pantalla principal de consola de antivirus

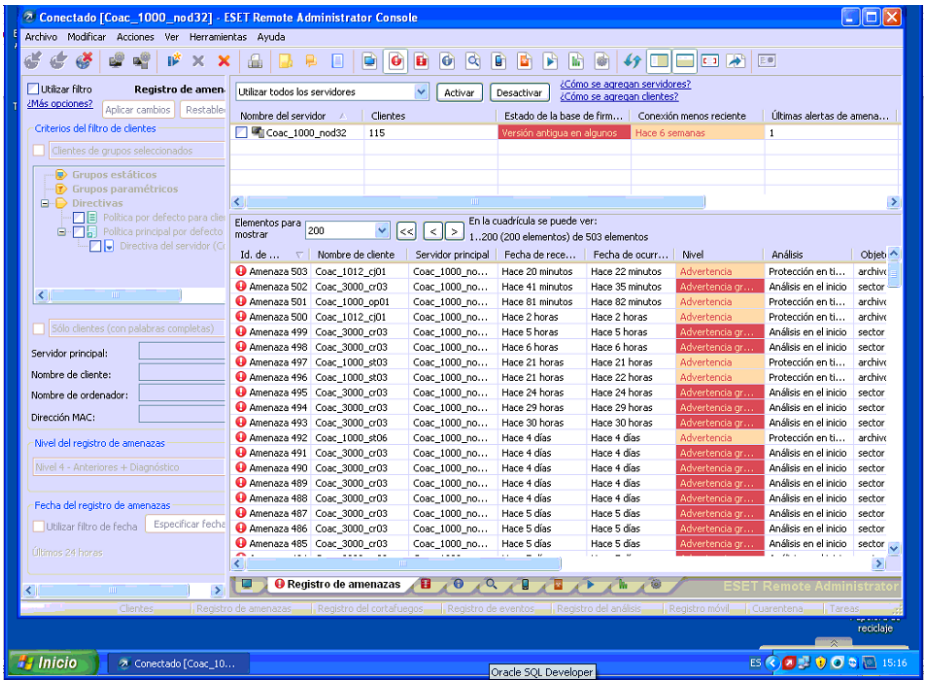


Fuente: Investigación de Campo (2011)

Elaborado por: Jaime Freire

3. Explorar opciones de consola. Dentro de las opciones de consola, se pueden ir explorando las amenazas presentadas a los equipos, los diferentes eventos de actualización. Para lo cual se deben ir seleccionando las pestanas en la parte inferior como se muestra en la siguiente pantalla.

Gráfico 24. Exploración de opciones en la consola.



Fuente: Investigación de Campo (2011)

Elaborado por: Jaime Freire

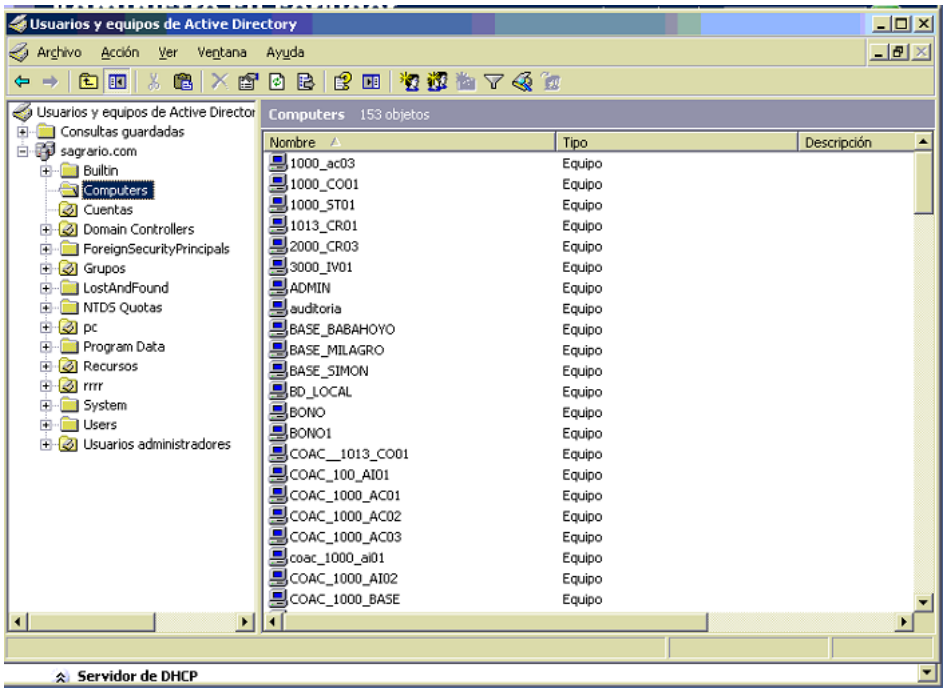
b.2. Revisión de servidor de dominio

El Servidor de dominio es utilizado para validar los accesos a los equipos de red. Sirve para administrar todos los equipos y usuarios que forman parte de una red de trabajo. En conjunto con el Administrador de dominio se debe ingresar al mismo, de acuerdo al siguiente procedimiento:

1. Ingresar a la opción de Administre sus servidor. Mediante esta opción se puede ingresar a la consola de administración del dominio.
2. Verificar los grupos de usuario, usuarios y equipos registrados. En la consola principal se puede verificar los grupos de usuarios, usuarios y equipos de trabajo registrados, revisar cada uno de ellos y pedir una

explicación. Por lo general debe existir creado mínimo 3 grupos de usuarios. Ejemplo. Administradores, Usuarios Avanzados, usuarios Restringidos. En la siguiente pantalla se muestra la consola.

Gráfico 25. Consola de administración de Dominio



Fuente: Investigación de Campo (2011)

Elaborado por: Jaime Freire

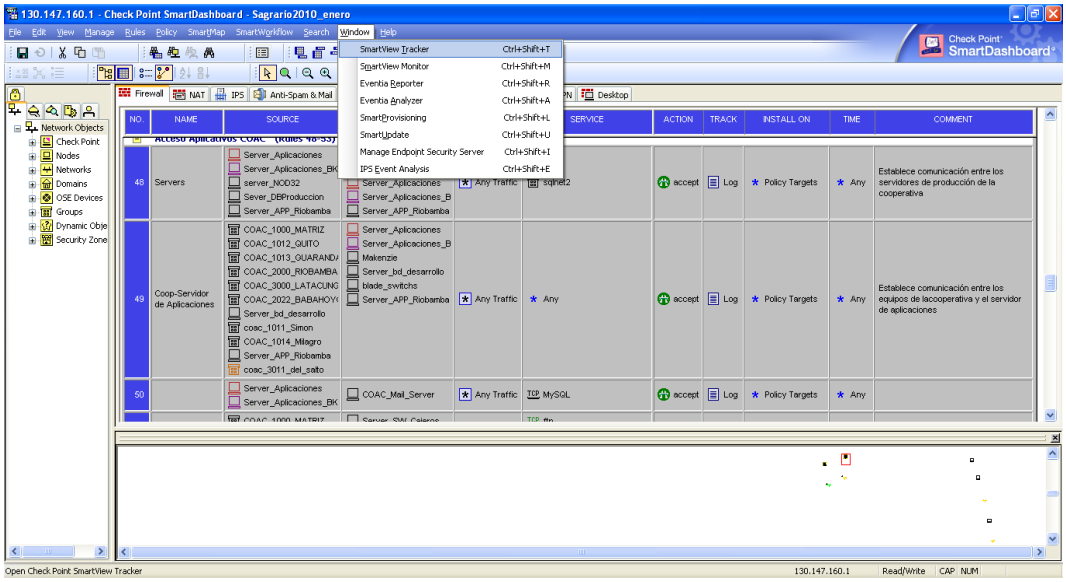
3. Revisión de Inventario de Hardware y Software. El servidor de dominio puede servir para verificar los inventarios de software y hardware, mediante la inspección de las características de los equipos que se encuentran en la consola de dominio

b.3. Revisión de servidor de firewall.

El firewall es utilizado para administrar los accesos a los recursos de tecnología. El auditor informático en conjunto con el administrador de

firewall debería revisar todas las reglas creadas, para que se utilizan y quien autorizó su creación. La pantalla de administración de Firewall es la siguiente:

Gráfico 26. Pantalla de administración del Firewall



Fuente: Investigación de Campo (2011)

Elaborado por: Jaime Freire

b.4. Tips generales para la ejecución de la auditoria

Durante el transcurso de la auditoría, se debe obtener la evidencia suficiente, confiable y pertinente para alcanzar los objetivos de auditoría. Los hallazgos y conclusiones de la auditoría deberán ser soportados mediante un apropiado análisis e interpretación de dicha evidencia. Se explican algunas recomendaciones a seguir durante la ejecución de la auditoria:

- Para evaluar el cumplimiento de normativa interna se deberá elaborar cuestionarios de acuerdo a los manuales de políticas y procedimientos establecidos.
- Para la revisión de cumplimiento de planes operativos, de capacitación y de mantenimiento se deberá solicitar los mismos y

las evidencias del cumplimiento de cada una de las actividades definidos en los planes. De no existir uno de estos planes o el incumplimiento no actividades se considera como hallazgo.

- Para la verificación de inventarios de software y hardware se recomienda realizar una comparación entre lo especificado en el inventario con los equipos físicamente. Para lo cual se puede seleccionar una muestra de equipos de diversas oficinas y diversos tipos, Se sugiere realizar esta revisión con el encargado de los activos de tecnología.
- Para la verificación del nivel de servicio entregado por el área de tecnología, se sugiere que se realice un requerimiento y se haga el seguimiento al mismo, con el objeto de determinar si es resuelto de acuerdo a los niveles de servicio especificado.
- Para la revisión del cumplimiento de los servicios provistos por terceros, se deberá solicitar los contratos del año en curso y verificar que se cumpla con los artículos definidos en el mismo.
- Para evaluar los accesos al sistema se debe comparar el inventario de perfiles de acceso de una muestra de usuarios con los que tiene realmente al momento de acceder al sistema. Mediante esta acción puede verificar que únicamente tiene asignado los permisos que se detallan en el inventario.
- Para evaluar los respaldos de información de base de datos, se procederá a solicitar el respaldo de alguna fecha que conste en la bitácora de respaldos y conjuntamente con el encargado de estas actividades se procederá a recuperar la información. El no poder recuperar la información se puede considerar de alto riesgo.
- En el desarrollo de sistemas de información, se debe verificar que cada versión que se publique en producción haya cumplido con todas las etapas de desarrollo, para lo cual se debe pedir los documentos que están descritos en la metodología.
- En el desarrollo de sistemas se debe mantener los manuales de usuario y técnicos actualizados, con el fin de revisar que se

encuentren actualizados, se debe solicitar los últimos cambios realizados al sistema y verificar que se encuentren las descripciones correspondientes tanto en el manual de usuario como en el manual técnico.

- Para los casos de aplicaciones web transaccionales, es necesarios que se verifique se cumpla por lo menos con lo siguiente:
    - Tener por lo menos 3 dominios contratados con la finalidad de evitar clonación de páginas. Se sugiere: www.elsagrario.fin.ec, www.elsagrario.com y www.elsagrario.ec .
    - La página transaccional debe tener un certificado de seguridad (SSL), se puede verificar este particular cuando al abrir la página empieza siempre con https.
    - La página transaccional debe abrirse únicamente desde la página principal de la Cooperativa.
    - Se debe tener por lo menos dos tipos de autentificación, por clave y por tarjeta de coordenadas, es recomendable la autentificación realizarlo por token.
    - El servidor donde se encuentra el equipo debe tener diferente direccionamiento IP que todos los servidores y debe estar aislado a través de un firewall de seguridad.

- Para verificar los planes de contingencia se recomienda, tomar algunos eventos de riesgo y ejecutar el plan establecido para cada evento en base a los tiempos y responsables que se especifiquen en el instructivo.

c. Documentar, las labores de auditoría realizadas

El proceso de auditoría deberá documentarse, con la finalidad de tener todas las evidencias de auditoría que respalda los hallazgos y conclusiones del auditor.

Se recomienda realizar principalmente capturas de pantallas, tomar fotografías, y escanear documentos legalizados.

6.7.3.3. Informe de Resultados

El equipo auditor una vez terminada el proceso de auditoría deberá presentar un informe para lo cual debe considerar los siguientes puntos:

a. Elaborar el Informe Preliminar

El informe debe incluir solo observaciones importantes, si se incluye hechos pocos relevantes se desviara la atención del usuario de la auditoria.

El informe deberá contener entre otras cosas lo siguiente:

- Alcance de la auditoria
- Objetivos de la auditoria
- Periodo de cobertura
- Plazos y extensiones de las labores de auditoría realizadas
- Hallazgos
- Conclusiones y Recomendaciones

b. Presentar el informe preliminar a la Alta Gerencia.

Se recomienda previo a la entrega del informe definitivo, se de lectura de los hallazgos y recomendaciones relevantes a quienes conforman la alta gerencia y dueños de procesos.

c. Entregar informe definitivo.

Una vez actualizado el documento en base al informe preliminar se deberá entregar el informe definitivo.

6.7.3.4. Actividades de Seguimiento

a. Elaborar un cronograma de seguimientos

Se recomienda elaborar un cronograma de seguimientos dependiendo de los hallazgos encontrados y del plazo para las actividades que ha establecido los responsables de los procesos.

b. Realizar los seguimientos y elaborar el informe sobre el cumplimiento.

Se debe realizar un seguimiento a las actividades planificadas por los responsables de los procesos, con el fin de verificar su cumplimiento. Como evidencia del seguimiento de deberá dejar un informe.

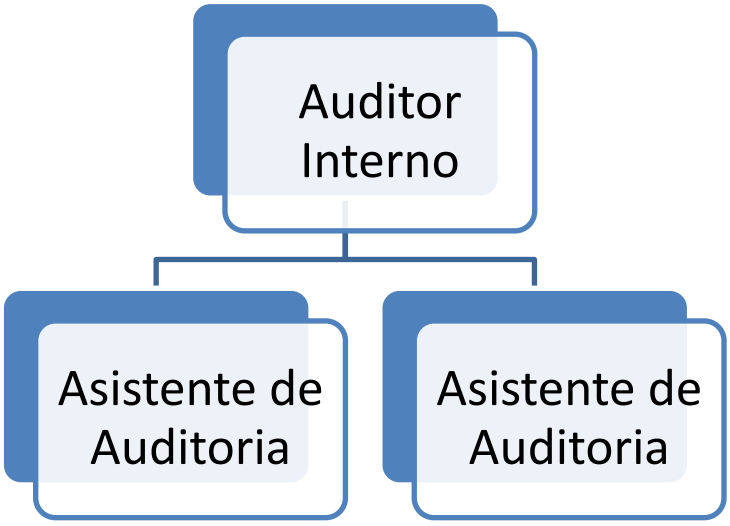
6.8. ADMINISTRACIÓN

6.8.1. Unidad que administra la propuesta

La unidad que administra esta propuesta es el departamento de Auditoría interna, el mismo que está formado por el Auditor Interno y dos asistentes de Auditoria. Adicionalmente esta propuesta puede ser utilizada por el área de riesgos de la Cooperativa con la finalidad de analizar las buenas prácticas de tecnología

6.8.2. Organigrama Estructural del departamento de auditoría.

Gráfico 27. Organigrama Estructural de Auditoria Interna



Fuente: Recursos Humanos Cooperativa El Sagrario.

Elaborado por: Jaime Freire

6.8.3 Funciones

Según el **Manual de Perfiles y Competencias de la Cooperativa El Sagrario (2010),** se detalla la misión y actividades esenciales de cada uno de los funcionarios del departamento de auditoría.

a. Auditor Interno

Misión del Puesto.

Vigilar el control interno de la institución, enfocado a normas y procedimientos internos y externos, asegurando el cumplimiento de los requisitos de los Organismos de Control.

Actividades esenciales

- Comprobar la existencia y el funcionamiento de los sistemas de control interno
- Velar porque las operaciones y procedimientos de la institución se ajusten a las disposiciones de la Ley, decretos, estatutos, reglamentos internos, técnica bancaria y las disposiciones de la Superintendencia de Bancos y Seguros.

b. Asistente de Auditoria

Misión del puesto.

Colaborar en la ejecución de las actividades del Auditor Interno en la revisión y evaluación de las actividades de la Cooperativa.

Actividades esenciales

- Ejecutar auditorias, exámenes especiales y supervisar el cumplimiento de observaciones y recomendaciones emitidos por la Unidad y Organismos Superiores
- Elaborar informes de resultados de auditorías efectuadas
- Verificar las transacciones, libros, balances y estados financieros de la Cooperativa.
- Verificar y evaluar el cumplimiento de políticas, leyes y reglamentos vigentes en la institución

6.9. PREVISIÓN DE LA EVALUACIÓN

Con el fin de determinar si la propuesta planteada cumple con los objetivos para los cuales fue desarrollada, se propone la realización de

un plan de evaluación, el mismo que se recomienda se realice posterior a la ejecución de las auditorias informáticas.

Tabla 24. Plan de Evaluación de la Propuesta

Nº	ITEMS	ACTIVIDAD
1	Qué evaluar?	Las auditorias informáticas y su incidencia en la disponibilidad de los sistemas de información de la Cooperativa de Ahorro y Crédito El Sagrario.
2	Por qué evaluar?	Porque es necesario determinar el grado de afectación que tiene la realización de auditorías informáticas para mejorar la disponibilidad de los sistemas de información.
3	Para qué evaluar?	Para determinar si la guía de auditoría informática contribuyó en el mejoramiento del control interno de las tecnologías de información.
4	Con qué criterios?	Disponibilidad de los sistemas de información
5	Indicadores	Disponibilidad de Base de Datos Disponibilidad de Comunicaciones Disponibilidad del Aplicativo Informático
6	Quién evalúa?	Subgerente de Tecnología Ingeniero de Producción Ingeniero de Infraestructura
7	Cuando evalúa?	Indicadores Mensuales
8	Con qué evaluar?	Control y Monitoreo realizado por los operadores del sistema.

Fuente: Investigación de Campo (2011)

Elaborado por: Jaime Freire

BIBLIOGRAFÌA

ECHENIQUE, Jose Antonio. (2006),"Auditoría en Informática", Primera Edición, McGraw-Hill, Ciudad de Mexico-Mexico, 233 pp.

HERRERA E. Luis, MEDINA F. Arnaldo, NARANJO L. Galo, PROAÑO B. Jaime, "Tutoría de la Investigación", Maestría en Gerencia de Proyectos Educativos y Sociales, Primera Edición, Asociación de Facultades Ecuatorianas de Filosofía y Ciencias de la Educación, AFEFCE, Quito - Ecuador, 2002, 319 pp.

IT GOVERNANCE INSTITUTE (2005), "COBIT 4.0", SIB, Quito– Ecuador, 21 pp.

COOPERATIVA EL SAGRARIO (2010). Manual de Perfiles y Competencias de la Cooperativa El Sagrario. Ambato-Ecuador. 50 pp.

COOPERATIVA EL SAGRARIO (2009). Manual de Políticas y Procedimientos de Tecnología. Ambato-Ecuador.2-3 pp.

PINILLA, Jose Dagoberto.(2005),"Auditoria Informática", Segunda Edición, Ecoe Ediciones, Bogotá-Colombia, 239 pp.

SUAREZ, RAMÓN CARLOS (2007). "Las auditoria Informáticas". Primera Edición, Ecoe Ediciones. Bogotá-Colombia.

SUPERINTENDENCIA DE BANCOS Y SEGUROS (2005), "Normas generales para la aplicación de la ley general de instituciones del sistema financiero Capitulo X - de la gestión y administración de riesgos Titulo V.- De la gestión del riesgo operativo", SIB, Quito– Ecuador, 19 pp.

CALERO P., Maria R. (2005), “Impacto de las nuevas tecnologías en los canales de distribución financiero”, (En línea) Disponible en: http://books.google.com/books?id=pkiQHNSt54EC&pg=PA54&dq=La+tecnologia+y+la+Banca&hl=es&ei=jt5ATaTnJoKB8gbv0PnnBA&sa=X&oi=book_result&ct=result&resnum=9&ved=0CE8Q6AEwCA#v=onepage&q&f=false (Fecha de Consulta 26-ene-2011).

DIALNET (2011), “Fundamentación epistemológica de los diseños de investigación naturalista” (en línea) Disponible en http://dialnet.unirioja.es/servlet/articulo?codigo=2860663 (Fecha de consulta:25-01-2011)

ITILV3(2011). ITIL-Gestión de Servicios TI (en línea). Recuperado de: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_disponibilidad/introduccion_objetivos_gestion_de_la_disponibilidad/introduccion_objetivos_gestion_de_la_disponibilidad.php**.** (Fecha de consulta: 30-05-2011).

JUNTA DE ESTÁNDARES DE LA ASOCIACIÓN DE AUDITORÍA Y CONTROL DE SISTEMAS DE INFORMACIÓN (2005) .NORMAS GENERALES PARA LOS SISTEMAS DE AUDITORÍA DE LA INFORMACIÓN.ISACA. Recuperado de:http://www.isaca.org/Knowledge-Center/Standards/Pages/Standards-for-IS-Auditing-Spanish-.aspx. (Fecha de consulta: 01-07-2011)

POLONSKY & WALLER (2011), “Investigación cualitativa” (en línea) Disponible en http://es.wikipedia.org/wiki/Investigaci%C3%B3n_cualitativa (fecha de consulta: 27-01-2011)

TAMAYO A., Alonso.(2001), “Auditoria de Sistemas una Visión Practica”, (En Línea) Disponible en:

http://books.google.com/books?id=HdtpS3UBCuMC&pg=PA14&dq=Controles+y+Seguridad+en+los+sistemas+de+informacion&hl=es&ei=VI5CTeiOHYuugQe9ovWaAg&sa=X&oi=book_result&ct=result&resnum=5&ved=0CEcQ6AEwBA#v=onepage&q&f=false (Fecha de Consulta 27-ene-2011).

TAMAYO A., Alonso.(2001), "Sistemas de Información", (En Línea) Disponible en: http://books.google.com/books?id=lsezichVfa8C&pg=PA116&dq=Controles+y+Seguridad+en+los+sistemas+de+informacion&hl=es&ei=VI5CTeiOHYuugQe9ovWaAg&sa=X&oi=book_result&ct=result&resnum=6&ved=0CEsQ6AEwBQ#v=onepage&q=Controles%20y%20Seguridad%20en%20los%20sistemas%20de%20informacion&f=false (Fecha de Consulta 27-ene-2011).

WIKIPEDIA, Enciclopedia Libre. (2009) "Investigación Cuantitativa", (En línea) Disponible en: http://es.wikipedia.org/wiki/Investigaci%C3%B3n_cuantitativa (Fecha de Consulta: 27-01-2011).

ANEXOS

ANEXO 1

MATRIZ DE ANALISIS DE SITUACIONES

Situación actual real negativa	Identificación del problema a ser investigado	Situación futura deseada positiva	Propuestas de solución al problema planteado
El departamento de auditoría interna de acuerdo a las políticas establecidas por la Superintendencia de Bancos y Seguros tiene que realizar auditorías informáticas con la finalidad de validar todos los aspectos tecnológicos que maneja la Cooperativa. Sin embargo no cuentan con una metodología donde se especifique las actividades a realizar y los aspectos técnicos que tiene que revisar. Por lo tanto la Cooperativa tiene que contratar personal externo para que cumplan con estas funciones lo cual no permite que los funcionarios del área de auditoría vayan adquiriendo conocimientos para que puedan realizar las auditorias informáticas y lo puedan realizar periódicamente	Inadecuado control interno de las Tics.	El personal de auditoría interna podrá aplicar auditorias informáticas basadas en una metodología donde se especifiquen todos los aspectos técnicos de revisión.	Investigar todas las áreas de tecnología que deben ser sometidas a revisión. Definir las normas de buenas prácticas tecnológicas que debe regular el área de tecnología. Consultar la normativa de riesgos operativos que deben aplicar las instituciones financieras y evaluar con lo que presenta actualmente la Cooperativa. Verificar todas las normas de seguridades que se deben aplicar en las instituciones financieras.

FUENTE: Investigación de campo (2011)

ELABORADO POR: EL AUTOR

ANEXO 2

REGISTRO ÚNICO DE CONTIBUYENTE – RUC

REGISTRO UNICO DE CONTRIBUYENTES
SOCIEDADES

SRi
Le hace bien al país!

NUMERO RUC: 1890037646001

RAZON SOCIAL: COOPERATIVA DE AHORRO Y CREDITO EL SAGRARIO LTDA

NOMBRE COMERCIAL: COOPERATIVA DE AHORRO Y

CLASE CONTRIBUYENTE: ESPECIAL

REP. LEGAL / AGENTE DE RETENCION: VELASTEGUI MORENO FREDY PATRICIO

CONTADOR: MORA PINOS MARIA KATHERINE

FEC. INICIO ACTIVIDADES:	17/04/1964	**FEC. CONSTITUCION:**	17/04/1964
FEC. INSCRIPCION:	31/10/1961	**FECHA DE ACTUALIZACIÓN:**	01/06/2010

ACTIVIDAD ECONOMICA PRINCIPAL:

ACTIVIDADES DE INTERMEDIACION MONETARIA REALIZADA POR COOPERATIVAS

DIRECCIÓN PRINCIPAL:

Provincia: TUNGURAHUA Cantón: AMBATO Parroquia: LA MATRIZ Barrio: EL ESPAÑOL Calle: SUCRE Número: S/N Intersección: QUITO Referencia ubicación: A UNA CUADRA DE LA GOBERNACION Telefono Trabajo: 032820417 Apartado Postal: 0000067 Telefono Trabajo: 032424456 Telefono Trabajo: 032417373 Fax: 032422213 Email: kmora@elsagrario.com Telefono Trabajo: 032420782

OBLIGACIONES TRIBUTARIAS:

* ANEXO RELACION DEPENDENCIA
* ANEXO TRANSACCIONAL SIMPLIFICADO
* DECLARACIÓN DE IMPUESTO A LA RENTA_SOCIEDADES
* DECLARACIÓN DE RETENCIONES EN LA FUENTE
* DECLARACIÓN MENSUAL DE IVA
* IMPUESTO A LA PROPIEDAD DE VEHÍCULOS MOTORIZADOS

SRi
SERVICIOS TRIBUTARIOS
REGIONAL CENTRO 1

# DE ESTABLECIMIENTOS REGISTRADOS:		**ABIERTOS:**	11
JURISDICCION:	REGIONAL CENTRO 1 TUNGURAHUA	**CERRADOS:**	1

FIRMA DEL CONTRIBUYENTE

SERVICIO DE RENTAS INTERNAS

Usuario: DESR020507 **Lugar de emisión:** AMBATO/BOLIVAR 1560 **Fecha y hora:** 01/06/2010

Página 1 de 5

SRi.gov.ec

Fuente: Investigación de Campo (2011)

Elaborado por: El Autor

ANEXO 3

CUESTIONARIO DE EVALUACION DE CONTROL

COOPERATIVA DE AHORRO Y CREDITO "EL SAGRARIO LTDA."
UNIVERSIDAD TECNICA DE AMBATO
FACULTAD DE CONTABILIDAD Y AUDITORIA

CUESTIONARIO DE EVALUACION DE CONTROL

DATOS

OFICINA……

FECHA……

OBJETIVO

Conocer el grado de satisfacción de los procesos y servicios de tecnología, así como la eficacia que pueden tener las auditorias informáticas en la institución.

INSTRUCCIONES

Lea detenidamente cada una de las preguntas y seleccione la respuesta que más se ajuste a la realidad de acuerdo a su criterio.

DESARROLLO

1.- ¿En qué grado considera usted, que la aplicación del plan de continuidad y contingencias vigente en la institución, ayuda a mantener la disponibilidad de los sistemas de información?

- ○ Altamente
- ○ Medianamente
- ○ Regularmente
- ○ No influye

2. ¿Considera usted que la implementación de los controles recomendados en las auditorías informáticas influyen en el aumento de la disponibilidad de los sistemas de información?

- ○ Altamente
- ○ Medianamente

- ○ Regularmente
- ○ No influye

3. ¿La misión, objetivos y planes operativos son difundidos periódicamente a todo el personal de la Cooperativa?

- ○ Si
- ○ No

4. ¿Considera que los mantenimientos realizados a los equipos de cómputo son suficientes para su correcta operatividad?

- ○ Si
- ○ No

5. ¿Se encuentra satisfecho con el aplicativo informático Financial Business System?

- ○ Muy Satisfecho
- ○ Satisfecho
- ○ Poco Satisfecho
- ○ Insatisfecho

6. ¿Los problemas que usted ha reportado al área de tecnología han sido atendidos oportunamente?

- ○ Muy Oportuno
- ○ Oportuno
- ○ Poco Oportuno
- ○ Inoportuno

7. ¿La falta de disponibilidad en los sistemas de información se produce por qué no se prevé de controles para ciertos incidentes de tecnología?

- ○ Altamente
- ○ Medianamente
- ○ Regularmente
- ○ No influye

8. ¿Considera que las auditorias informáticas son limitadas debido a que no existe personal interno especializado para estas actividades?

- ○ Altamente
- ○ Medianamente
- ○ Regularmente
- ○ No influye

9. ¿Los equipos de cómputo con que cuenta en su puesto de trabajo son adecuados para el cumplimiento de sus labores diarias?

- ○ Muy Adecuados
- ○ Adecuados
- ○ Poco Adecuados
- ○ Inadecuados

10. ¿Usted ha sido capacitado en el último año sobre normas, políticas y buenas prácticas de seguridad que debe tomar en cuenta en sus funciones?

- ○ Si
- ○ NO