

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE CONTADURÍA PÚBLICA



**“EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN
COMPUTARIZADOS EN LAS INSTITUCIONES AUTÓNOMAS DESDE LA
PERSPECTIVA DE LA AUDITORÍA INTERNA GUBERNAMENTAL”**

Trabajo de Investigación presentado por:

Pérez Méndez, Marina Raquel

Rivera, Alexis Guillermo

Serrano Gaitán, Ana Claudia

Para optar al grado de:

LICENCIADO EN CONTADURÍA PÚBLICA

Abril del 2010

San Salvador, El Salvador, Centroamérica

UNIVERSIDAD DE EL SALVADOR
AUTORIDADES UNIVERSITARIAS

Rector : Máster Rufino Antonio Quezada Sánchez

Secretario : Licenciado Douglas Vladimir Alfaro Chávez

Decano de la Facultad de
Ciencias Económicas : Máster Roger Armando Arias Alvarado

Secretario de la Facultad de
Ciencias Económicas : Máster José Ciriaco Gutierrez Contreras

Director de la Escuela de
Contaduría Pública : Licenciado Juan Vicente Alvarado Rodríguez

Coordinador de Seminario : Licenciado Roberto Carlos Jovel Jovel

Docente Director : Licenciado Mario Hernán Cornejo Pérez

Jurado Examinador : Licenciado Mario Hernán Cornejo Pérez
Licenciado Mauricio Ernesto Magaña Menéndez

Abril del 2010

San Salvador, El Salvador, Centro América

AGRADECIMIENTOS

Agradezco a Dios todopoderoso, por darme la vida, fuerzas, voluntad y la oportunidad de alcanzar este triunfo. A Mis padres José Orlando Pérez Evangelista, María Isabel Méndez, a mis abuelos Nicolás Pérez y Marina Evangelista, por haberme modelado con amor, sabiduría y acompañarme incondicionalmente. A Mi hermano Jaime Orlando, A José Marcos, por impulsarme a seguir adelante. Agradecimiento especial a mi asesor Lic. Mario Hernán Cornejo Pérez, por su amistad, paciencia y valioso apoyo. A mi grupo de tesis por compartir buenos y difíciles momentos para culminar nuestro trabajo. A mi familia, amigos y todas aquellas personas que son parte de mi vida, mi más sincera gratitud a su comprensión, estímulo y ayuda.

Marina Raquel Pérez Méndez

Agradezco a Jehová Dios por darme la vida, la salud y la perseverancia necesaria para culminar este gran paso en mi vida; por rodearme con mis abuelos, madre, hermana, hermanos, prima, tías, tíos y demás que me criaron, protegieron y trataron de inculcar valores mediante el ejemplo; por mi bella esposa que me brinda amor y fortaleza; por bendecirme de la forma más bella con mi hija tan esperada y amada; por colocar en mi camino amigos y compañeros sinceros; por permitirme tener a un asesor capaz y esmerado; por mis maravillosas compañeras de trabajo de graduación; por permitirme superar todos los obstáculos; por todo eso y más, muchas gracias.

Alexis Guillermo Rivera.

Agradezco a Dios por permitirme llegar hasta este momento tan importante de mi vida; a mis padres por su amor incondicional y encomendarme siempre a Dios; a mis hermanos por su compañía; a mi docente director por su constante estímulo, permanente disposición y desinteresada ayuda; a mi familia y amigos por acompañarme en momentos importantes; a mis compañeros de trabajo de graduación por hacer que mi participación fuera agradable.

Ana Claudia Serrano Gaitán

ÍNDICE

RESUMEN EJECUTIVO
INTRODUCCIÓN

	Pag.
<u>CAPÍTULO I</u>	
1. MARCO TEÓRICO	01
1.1. INSTITUCIONES AUTÓNOMAS	01
1.1.1. CONCEPTO, ANTECEDENTES, NORMATIVA LEGAL Y TÉCNICA QUE LAS REGULAN	01
1.2. SISTEMAS DE INFORMACIÓN COMPUTARIZADOS	03
1.2.1. ANTECEDENTES	03
1.2.2. GENERALIDADES DE LOS SISTEMAS DE INFORMACION COMPUTARIZADOS	04
1.3. CONTROL INTERNO	05
1.3.1. GENERALIDADES DEL CONTROL INTERNO	05
1.3.2. EVALUACIÓN DEL CONTROL INTERNO	07
1.4. AUDITORÍA INTERNA GUBERNAMENTAL	09
1.4.1. ANTECEDENTES	09
1.4.2. GENERALIDADES DE LA AUDITORÍA INTERNA GUBERNAMENTAL	10
1.5. MARCO LEGAL Y NORMATIVA TÉCNICA APLICABLES A LA AUDITORÍA INTERNA GUBERNAMENTAL	11
1.5.1. MARCO LEGAL	11
1.5.2. NORMATIVA TÉCNICA	15
1.5.3. OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS (COBIT)	20

CAPÍTULO II

2.	METODOLOGÍA Y DIAGNÓSTICO DE LA INVESTIGACIÓN	22
2.1.	TIPO DE INVESTIGACIÓN	22
2.2.	TIPO DE ESTUDIO	22
2.3.	DETERMINACIÓN DE LA POBLACIÓN	22
2.4.	DETERMINACIÓN DE LA MUESTRA	22
2.5.	UNIDADES DE ANÁLISIS	24
2.6.	INSTRUMENTOS Y TÉCNICAS DE INVESTIGACIÓN	24
2.7.	TABULACIÓN Y LECTURA DE DATOS	25
2.8.	DIAGNÓSTICO DE LA INVESTIGACIÓN	41

CAPÍTULO III

3.	EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS EN LAS INSTITUCIONES AUTÓNOMAS DESDE LA PERSPECTIVA DE LA AUDITORÍA INTERNA GUBERNAMENTAL	46
3.1.	PLANEACIÓN	46
3.1.1.	PLAN GENERAL DE AUDITORÍA	46
3.1.1.1.	OBJETIVO GENERAL	46
3.1.1.2.	OBJETIVOS ESPECÍFICOS	46
3.1.1.3.	ALCANCE DEL TRABAJO	47
3.1.1.3.1.	CONTROLES GENERALES	47
3.1.1.3.2.	CONTROLES DE DATOS	48
3.1.1.3.3.	CONTROLES DE APLICACIÓN	48
3.1.1.4.	ENFOQUE GENERAL	49
3.1.1.4.1.	CARACTERÍSTICAS DEL ENTORNO DE LA INSTITUCIÓN	49
3.1.1.4.2.	NORMAS QUE LA REGULAN	50
3.1.1.4.3.	MEDIO AMBIENTE DEL SECTOR DE LOS DIFERENTES	

	SERVICIOS	50
3.1.1.4.4.	AMBIENTE EXTERNO	50
3.1.1.4.5.	CLIMA ORGANIZACIONAL	51
3.1.1.4.6.	ANÁLISIS DE LAS CARACTERÍSTICAS DE LA ORGANIZACIÓN	52
3.1.1.4.7.	DESARROLLO DEL TALENTO HUMANO	53
3.1.1.4.8.	SISTEMAS DE INFORMACIÓN	53
3.1.1.5.	RESULTADO DE LA AUDITORÍA	54
3.1.1.6.	FUNDAMENTO DE LA AUDITORÍA	54
3.1.1.7.	RESPONSABLES DE LA AUDITORÍA	55
3.1.1.8.	CRONOGRAMA	55
3.1.1.9.	PRESUPUESTO DE RECURSOS	56
3.1.2.	ANÁLISIS GENERAL	56
3.1.2.1.	OBJETIVOS	56
3.1.2.2.	METAS	57
3.1.2.3.	PROCESOS Y ORGANIZACIÓN	57
3.1.2.4.	FUNCIONAMIENTO	60
3.1.2.5.	ENTORNO	60
3.1.2.5.1.	INDUSTRIALES	60
3.1.2.5.2.	ECONÓMICOS	62
3.1.2.5.3.	SOCIALES	62
3.1.2.5.4.	POLÍTICOS	62
3.1.2.5.5.	ECOLÓGICOS	62
3.1.2.6.	MARCO JURÍDICO	63
3.1.2.7.	NORMATIVA INTERNA	63
3.1.2.8.	INDICADORES DE GESTIÓN	64
3.1.2.9.	PROVEEDORES	64
3.1.3.	EXAMEN PRELIMINAR	65

3.1.3.1. ACTIVIDADES Y CONTROLES CLAVES	65
3.1.3.1.1. ACTIVIDADES CLAVES	65
3.1.3.1.2. CONTROLES CLAVES	65
3.1.3.2. ASUNTOS DE POTENCIAL IMPORTANCIA	65
3.1.3.3. RIESGOS	66
3.1.4. COMPRESIÓN DEL CONTROL INTERNO	66
3.1.4.1. AMBIENTE DE CONTROL	66
3.1.4.1.1. INTEGRIDAD Y VALORES ÉTICOS	66
3.1.4.1.2. COMPETENCIA DEL PERSONAL	67
3.1.4.1.3. FILOSOFÍA Y ESTILO DE LA ADMINISTRACIÓN	68
3.1.4.1.4. ESTRUCTURA ORGANIZACIONAL	68
3.1.4.1.5. ASIGNACIÓN DE AUTORIDAD Y RESPONSABILIDAD	68
3.1.4.1.6. POLÍTICAS Y PRÁCTICAS DE GESTIÓN DE RECURSOS HUMANOS	68
3.1.4.1.7. UNIDAD DE AUDITORÍA INTERNA	68
3.1.4.2. VALORACIÓN DE RIESGOS	69
3.1.4.2.1. CAMBIOS EN EL ENTORNO	69
3.1.4.2.2. REDEFINICIÓN DE LA POLÍTICA INSTITUCIONAL	70
3.1.4.2.3. REORGANIZACIONES O REESTRUCTURACIONES	70
3.1.4.2.4. INGRESO DE NUEVOS EMPLEADOS O ROTACIÓN	70
3.1.4.2.5. NUEVOS SISTEMAS Y PROCEDIMIENTOS	71
3.1.4.2.6. ACELERACIÓN DEL CRECIMIENTO	71
3.1.4.2.7. NUEVOS PRODUCTOS,	

	SERVICIOS, ACTIVIDADES O FUNCIONES	72
	3.1.4.2.8. CAMBIOS EN LA APLICACIÓN DE LOS PRINCIPIOS CONTABLES	72
	3.1.4.3. ACTIVIDADES DE CONTROL	72
	3.1.4.3.1. REALIZACIÓN DE REVISIONES	73
	3.1.4.3.2. PROCESOS DE INFORMACIÓN	73
	3.1.4.3.3. SEGREGACIÓN DE FUNCIONES	74
	3.1.4.4. INFORMACIÓN Y COMUNICACIÓN	74
	3.1.4.5. MONITOREO	75
	3.1.5. DETERMINACIÓN DE RIESGOS	75
	3.1.5.1. PARÁMETROS DE EVALUACIÓN DEL RIESGO	75
	3.1.5.2. MATRIZ DE RIESGOS	76
	3.1.5.3. PROGRAMAS DE AUDITORÍA	78
3.2.	EJECUCIÓN	78
	3.2.1. REALIZACIÓN DE PRUEBAS Y OBTENCIÓN DE EVIDENCIA	79
	3.2.2. PREPARACIÓN Y REFERENCIACIÓN DE PAPELES DE TRABAJO	80
	3.2.3. DESARROLLO DE HALLAZGOS Y SUS ATRIBUTOS	80
	3.2.4. COMUNICACIÓN PRELIMINAR DE RESULTADOS	81
	3.2.5. PREPARACIÓN DEL BORRADOR DE INFORME	81
3.3.	INFORME	82
	3.3.1. INTRODUCCIÓN	82
	3.3.2. OBJETIVOS DE LA AUDITORÍA	83
	3.3.3. ALCANCE DE LA AUDITORÍA	83
	3.3.4. LIMITACIONES EN EL ALCANCE DE LA AUDITORÍA	83
	3.3.5. LOGROS Y/O REALIZACIONES IMPORTANTES DE LA ADMINISTRACIÓN	84

3.3.6.	RESULTADOS	84
3.3.6.1.	HALLAZGOS DE AUDITORÍA	85
3.3.6.1.1.	TÍTULO	86
3.3.6.1.2.	CONDICIÓN	87
3.3.6.1.3.	CRITERIO	87
3.3.6.1.4.	CAUSA	87
3.3.6.1.5.	EFECTO	87
3.3.6.1.6.	RECOMENDACIÓN	88
3.3.6.1.7.	COMENTARIOS DE LA ADMINISTRACIÓN	88
3.3.6.1.8.	COMENTARIOS DE AUDITORÍA	88
3.3.6.1.9.	GRADO DE CUMPLIMIENTO	88
3.3.6.1.10.	CONCLUSIÓN	89
3.3.7.	CONCLUSIONES	89
3.3.8.	RECOMENDACIONES	90
<u>CAPÍTULO IV</u>		
4.	CONCLUSIONES Y RECOMENDACIONES	91
4.1.	CONCLUSIONES	91
4.2.	RECOMENDACIONES	92
	BIBLIOGRAFÍA	94
	ANEXOS	96

RESUMEN EJECUTIVO

El marco legal y normativa técnica aplicable a la auditoría gubernamental, así como el surgimiento de nuevas y mejores herramientas de evaluación del control interno, vuelven necesario que las instituciones autónomas de El Salvador cuenten con unidades de auditoría interna capaces de realizar de forma metódica la evaluación referente al control interno de los sistemas de información computarizados, dada su relevancia en la facilitación del logro de los objetivos institucionales.

En este trabajo de investigación se plantea la problemática relacionada a la no existencia de una metodología que permita evaluar, en concordancia a los aspectos legales y normativa técnica anteriormente citados, que retome las mejores prácticas internacionales de tecnologías de información contra las cuales se puedan juzgar las desviaciones en el control interno de los sistemas de información computarizados.

Para superar la problemática anterior, se propone utilizar como marco de comparación los dominios Adquirir e Implantar (AI) y Entregar y Dar Soporte (DS) desarrollados por los Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT). El utilizar dichos dominios permitiría responder preguntas claves como: ¿los controles internos son eficientes y efectivos?, ¿se miden y reportan los riesgos y el control?, ¿se detectan los problemas antes de que sea demasiado tarde? Sin dejar de lado los requerimientos legales de obligatoriedad para el desarrollo de las actividades de auditoría interna gubernamental.

Al dar respuestas a las interrogantes planteadas con anterioridad, las instituciones autónomas podrían controlar los efectos no deseados del uso de sistemas de información computarizados, en la medida que sus auditores internos desarrollen el trabajo bajo esta metodología técnicamente apropiada, que potencie su rol de evaluador y asesor dentro de las mismas, brindando a través de sus recomendaciones mejoras que conlleven a estas el alcanzar la eficiencia, eficacia y economía en sus actividades.

INTRODUCCIÓN

Las instituciones autónomas en El Salvador fueron concebidas de tal manera que por medio de ellas se cubran aquellas necesidades de la sociedad que el Gobierno con su aparato normal no lograría cubrir y ya que en la actualidad el uso de tecnología en estas, es esencial si se pretende lograr dentro de ellas un mayor grado de eficiencia, eficacia y economía en las operaciones, se vuelve primordial que dicho recurso sea diseñado, implantado, mantenido y evaluado con el fin de que cumpla el objetivo por el cual se utiliza.

Los sistemas de información computarizados forman parte del uso de estas tecnologías, pero no son en sí un objetivo, si no una herramienta de la cual la dirección de las instituciones echan mano para la consecución de las metas por la cual estas existen, por tanto estas deben ser evaluadas de una manera técnica y profesional para que del resultado de dicha evaluación se logren identificar los riesgos existentes o probables y la manera de prevenirlos, atenuarlos o eliminarlos.

Este trabajo de investigación pretende brindar la metodología que abarque lo anterior, enfocada primordialmente a la evaluación del control interno de los sistemas de información computarizados desde la perspectiva de la auditoría interna gubernamental, para ello se realizó un diagnóstico que abarcó una muestra de las instituciones que forman parte del sector autónomo de El Salvador.

Este trabajo se encuentra dividido en cuatro capítulos, los cuales se detallan a continuación:

Capítulo I: contiene el marco teórico que identifica y desarrolla los aspectos relevantes que forman parte del estudio como aspectos legales, normativos y técnicos, lo cual provee la información necesaria para facilitar su comprensión.

Capítulo II: se especifica la metodología que se aplicó para el desarrollo de esta investigación, entre la cual se encuentra la unidad de estudio, los criterios que fueron utilizados para determinar la muestra y las técnicas y herramientas que permitieron llevarla a cabo. Es presentado el resultado del estudio, analizando e interpretando los datos obtenidos, lo que permitió brindar la propuesta, conclusiones y recomendaciones.

Capítulo III: es presentada la propuesta que permite darle solución a la problemática detectada, la cual contiene ejemplificada la metodología de evaluación del control interno de los sistemas de información computarizados, para lo cual se utiliza una institución hipotética que posee las características del sector autónomo de El Salvador.

Capítulo IV: enmarca las conclusiones y recomendaciones elaboradas por el equipo que desarrolló la investigación.

CAPÍTULO I

1. MARCO TEÓRICO

1.1 INSTITUCIONES AUTÓNOMAS

1.1.1 CONCEPTO, ANTECEDENTES, NORMATIVA LEGAL Y TÉCNICA QUE LAS REGULAN

Según la Corte Suprema de Justicia “Los entes autónomos se caracterizan porque su patrimonio y el manejo presupuestario de éste, guardan estrecha relación con el Fondo General del Estado. Las instituciones autónomas han tenido su origen en la administración central, de la cual son independientes en lo administrativo y financiero, pero dicha independencia persigue la única finalidad de lograr una mayor eficiencia y especialización en el servicio público o actividades específicas cuya prestación es necesaria para el cumplimiento de los fines del estado, y por tales razones que el estado ejerce un control permanente sobre ellas”.

Desde la década de los años 50 se han creado diversas instituciones autónomas que han pretendido proveer de modernidad al funcionamiento del Estado, estando a tono con el desarrollo de la economía de los años o en todo caso lograr ser eficientes ante problemas que no eran abordados de dicha manera, volviéndose a la vez imperioso que estas instituciones cuenten con las bases legales adecuadas para el logro de sus objetivos así como estar provistas de medios tecnológicos que les permitan ser más rápidas y dinámicas en la respuesta ante los problemas que abordan. Esto hace necesario evaluar de manera fiable que si los objetivos que pretende alcanzar la institución autónoma a través de dichos medios se están logrando de la mejor manera.

La normativa legal que regula a estas Instituciones, la cual se ha desarrollado con el paso del tiempo, es la siguiente:

CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA DE EL SALVADOR

En ella se sustenta la creación de las instituciones autónomas, es así como en el artículo 225 se establece que “Cuando la ley lo autoriza, el Estado, para consecución de sus fines, podrá separar bienes de la masa de la Hacienda Pública o asignar recursos del Fondo General, para constitución o incremento de patrimonios especiales destinados a instituciones públicas”.

LEY DE LA CORTE DE CUENTAS DE LA REPÚBLICA

El 31 de agosto de 1995 la Asamblea Legislativa decreta una actualizada ley que pretende instituir el Sistema Nacional de Control y Auditoría de la Gestión Pública y en su artículo 1 establece que “La Corte de Cuentas de la República, que en esta Ley podrá denominarse La Corte, es el organismo encargado de fiscalizar, en su doble aspecto administrativo y jurisdiccional, la Hacienda Pública en general y la ejecución del presupuesto en particular, así como de la gestión económica de las entidades a que se refiere la atribución cuarta del artículo 195 y los incisos 4 y 5 del Artículo 207 de la Constitución de la República”; esta ha sido reformada en 5 ocasiones siendo la última el Decreto Legislativo N° 151 del 02 de octubre de 2003, publicado en el Diario Oficial N° 193, tomo N° 361, del 17 de octubre de 2003.

LEY ORGÁNICA DE ADMINISTRACIÓN FINANCIERA DEL ESTADO

El 23 de noviembre de 1995 la Asamblea Legislativa de la República de El Salvador decreta esta Ley, con el objeto de:

- Normar y armonizar la gestión financiera del sector público;
- Establecer el Sistema de Administración Financiera Integrado que comprende los Subsistemas de Presupuesto, Tesorería, Inversión y Crédito Público y Contabilidad Gubernamental.

La Ley establece la sujeción de las instituciones autónomas a las disposiciones de dicha ley, la cual con el objeto de armonizarse a los tiempos, ha tenido 6 reformas siendo la última el Decreto Legislativo N° 586 del 10 de abril de 2008, publicado en el Diario Oficial N° 71, tomo N° 379, del 18 de abril de 2008.

NORMAS DE AUDITORÍA GUBERNAMENTAL (NAG)

El 14 septiembre de 2004 el Presidente de la Corte de Cuentas decreta las Normas de Auditoría Gubernamental (NAG) que tienen por objetivo la efectiva planificación, ejecución y comunicación de los resultados de la auditoría gubernamental, siendo estas de obligatoria aplicación por parte de los auditores internos; dichas normas han tenido una reforma, D.C.C. N° 291 de fecha 19 de diciembre de 2006, publicado en el Diario Oficial N° 9, tomo N° 374, del 15 de enero de 2007.

NORMAS TÉCNICAS DE CONTROL INTERNO (NTCI)

El Presidente de la Corte de Cuentas de la República las decreta el 14 septiembre de 2004 y vienen a derogar la anterior normativa del año 2000, estas más recientes han sido adecuadas al Informe presentado por la Comisión Treadway, conocido como informe COSO, proporcionando una nueva conceptualización referente al Control Interno.

1.2 SISTEMAS DE INFORMACIÓN COMPUTARIZADOS

1.2.1 ANTECEDENTES

A medida que el tiempo ha transcurrido las entidades han tenido que trabajar con una enorme cantidad de documentos y deben poder utilizarlos con gran rapidez y exactitud, por lo que se creó y modificó la manera para procesar estos registros, es así como nace un instrumento para el procesamiento automático de estas grandes cantidades de datos, las computadoras; las que son utilizadas en la actualidad en casi todas las entidades.

Hoy en día es casi imposible visualizar una entidad sin que en ella exista por lo menos una computadora y en consecuencia un programa informático, es decir instrucciones previamente determinadas.

Desde que comenzaron a funcionar las computadoras, en los años cincuentas, se han introducido grandes perfeccionamientos en su organización, velocidad y economía. Sin embargo

aunque la computadora por medio de sus programas informáticos pueda automatizar labores en forma más precisa y rápida que un ser humano, siempre lo necesita porque él dirige el funcionamiento de la máquina. De igual forma las personas, dentro de la sociedad o dentro de una institución está sujeto a normas que debe acatar para alcanzar objetivos y metas.

1.2.2 GENERALIDADES DE LOS SISTEMAS DE INFORMACION COMPUTARIZADOS

Los Sistemas de Información Computarizados se han convertido en una herramienta que permite obtener información en menor tiempo y de mayor calidad. Un sistema según el libro de Sistemas y Procedimientos Contable de Fernando Catacora Carpio, “es un conjunto de elementos, entidades o componentes que se caracterizan por ciertos atributos identificables que tienen relación entre sí, y que funcionan para lograr un objetivo común”.

Un sistema de información computarizado está compuesto por los siguientes elementos: hardware, software, recursos humanos, y normas, todos estos tienen relación entre sí, y funcionan para lograr que los datos se conviertan en información útil para la toma de decisiones.

No existen sistemas de información computarizados absolutamente confiables, para que un sistema sea razonablemente seguro debe cumplir con las siguientes condiciones:

- Integridad
- Confidencialidad
- Disponibilidad
- Irrefutabilidad

Para eso se crea un sistema de control interno que minimice los riesgos lo mejor posible y brinde una seguridad razonable de que la información procesada por el sistema se esta efectuando de acuerdo con las normas y procedimientos establecidos, para que la información tenga las siguientes características: calidad, oportunidad, cantidad y relevancia

El problema de minimizar esos riesgos es una situación tan general que se han creado diversas metodologías que buscan unificar internacionalmente la manera que reducirlos y resguardar la información de las diversas instituciones. Una de ellas es la siguiente:

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍA RELACIONADA (COBIT).

El *IT Governance Institute* (ITGI) se establece en 1998 con el fin de que los pensamientos y estándares utilizados internacionalmente tuvieran una evolución en lo que corresponde a la dirección y control de la Tecnología de Información (TI) en una entidad. Es así como el ITGI establece los objetivos de control para la Información y la Tecnología relacionada (COBIT). Dichos objetivos “brindan buenas prácticas a través de un marco de trabajo de dominios y procesos”, estas buenas prácticas son en realidad el resultado de los consensos de expertos y con un enfoque fuerte en el control y menos en la ejecución. Al utilizar estas buenas prácticas propuestas por el COBIT se brinda una medida contra la cual se logra juzgar cuando las cosas no vayan bien.

1.3 CONTROL INTERNO

1.3.1 GENERALIDADES DEL CONTROL INTERNO

Controles internos son los procedimientos efectuados internamente con el fin de lograr el cumplimiento de objetivos dentro de una entidad, institución o compañía. El sistema de control interno según las Normas Técnicas de Control Interno en su artículo 2 “se entiende por sistema de control interno el conjunto de procesos continuos e interrelacionados realizados por la máxima autoridad, funcionarios y empleados, diseñados para proporcionar seguridad razonable en la consecución de sus objetivos”.

Los controles pueden ser de tres tipos: preventivos, de detección y correctivos como se señalan en el artículo 27 de la Ley de la Corte de Cuentas “El control interno previo y concurrente se

efectuará por los servidores responsables del trámite ordinario de las operaciones y no por unidades especializadas, cuya creación para este objeto está prohibida.

El Control Interno posterior, que evalúa la efectividad de los otros controles, se hará profesionalmente por la unidad de auditoría interna, de acuerdo con lo que establezcan las Normas Técnicas de Auditoría Gubernamental”

Los Objetivos del control interno son variados pero lo que se busca primordialmente es:

- Evitar o reducir errores, irregularidades y desperdicios
- Salvaguardar los activos
- Comprobar la calidad, cantidad, relevancia y oportunidad de la información
- Impulsar la eficiencia, eficacia y economía en adhesión a normas y políticas fijadas por la administración.

Para las instituciones autónomas los objetivos del control interno están enfocados en COSO, en el considerando segundo de las NTCl se puede leer lo siguiente: “Que el informe presentado por la Comisión Treadway, conocido como informe COSO, proporciona una nueva conceptualización del Control Interno, por lo tanto las actuales Normas de Técnicas de Control Interno emitidas por la Corte de Cuentas de la República, requieren de una adecuación, de conformidad al informe COSO”. Las Normas Técnicas del Control Interno en su artículo número 3 reza lo siguiente: “El sistema de control interno tiene como finalidad coadyuvar con la Institución en el cumplimiento de los siguientes objetivos:

- Lograr eficiencia, efectividad y eficacia de las operaciones
- Obtener confiabilidad y oportunidad de la información, y
- Cumplir con leyes, reglamentos, disposiciones administrativas y otras regulaciones aplicables”

Los componentes del marco integrado, que establece el informe COSO, está formado por cinco componentes, que también son retomados por las Normas Técnicas de Control Interno en su

artículo 4 que establece lo siguiente: “Los componentes orgánicos del sistema de control interno son: ambiente de control; valoración de riesgos; actividades de control, información y comunicación; y monitoreo”.

Como plantea el artículo 6 de las Normas Técnicas de Control Interno “el sistema de control interno proporciona una seguridad razonable para el cumplimiento de los objetivos institucionales”. Para que esto suceda se debe verificar de manera constante que los controles internos establecidos por la institución autónoma se estén efectuando de acuerdo con los parámetros fijados.

1.3.2 EVALUACIÓN DEL CONTROL INTERNO

De acuerdo con las Normas de Auditoría Gubernamental en su apartado 2.4.1 “El entendimiento y evaluación del funcionamiento del sistema de control interno se realizará con el propósito de identificar las operaciones, componentes o actividades que requieren un examen detallado e identificar las recomendaciones a ser implementadas para su fortalecimiento”.

Esta evaluación tiene la finalidad de otorgar una seguridad razonable de que el sistema de control interno establecido por la administración de una institución podrá prevenir, detectar y corregir oportunamente deficiencias dentro de la realización de las diversas operaciones que se dan dentro de la misma, evitando que la información se vea afectada.

El artículo 35 de las Normas Técnicas de Control Interno establece que se pueden realizar autoevaluaciones del control interno: “Los niveles gerenciales y de jefatura responsables de una unidad o proceso, deben determinar la efectividad del sistema de control interno propio, al menos una vez al año”.

El artículo 36 de las Normas Técnicas de Control Interno establece que se pueden realizar evaluaciones separada de la siguiente manera: “La unidad de auditoría interna, la Corte de

Cuentas, las Firmas Privadas de Auditoría y demás instituciones de control y fiscalización, evaluarán periódicamente la efectividad del sistema de control interno institucional”.

Existen métodos para documentar y evaluar el control interno de una institución, entre ellos se encuentran:

- Cuestionarios
- Narrativas
- Flujogramas (Secuenciales, columnares y analíticos)

Los métodos que son aceptados para las instituciones autónomas, según el Manual de Auditoría Gubernamental de Agosto de 2006 en su capítulo VIII evaluación del control interno:

- “Método descriptivo o narrativa: por este método se relacionan en los papeles de trabajo las diversas características del control interno, clasificadas por actividades unidades organizativas, funcionarios y empleados, o registros contables o administrativos que intervienen en el sistema
- Método gráfico o flujograma: consiste en presentar objetivamente a la organización y los procedimientos que tienen efecto en las unidades organizativas o actividades; o bien, en la preparación de graficas combinadas de la organización y sus procesos
- Método de cuestionario: se plantean las cuestiones que usualmente constituyen los aspectos básicos del sistema de control interno. Estos temas se desarrollan de antemano en forma de lista de preguntas que posteriormente se contestan en las oficinas de la entidad, obteniendo la respuesta de los servidores responsables de los procesos, verificando siempre de las medidas de control realmente en vigor”

La eliminación de los riesgos mediante el control interno es casi imposible debido a que la información, aun siendo automatizada, depende en gran medida de los seres humanos; las tecnologías en las que se apoyan las instituciones para almacenar, procesar y presentar la información se encuentra en constante cambio; la relación costo-beneficio que deben tener los controles internos no permiten que varios de estos se implanten dentro de las mismas.

1.4 AUDITORÍA INTERNA GUBERNAMENTAL

1.4.1 ANTECEDENTES

Según la Reseña Histórica de la Corte de Cuentas de la República, en el año de 1939 entró en vigencia la “Ley Orgánica de la Corte de Cuentas de La Republica de El Salvador”, donde el control gubernamental es confiado ha dicho organismo.

Posteriormente por medio del Decreto Legislativo N° 438 publicado el 25 de septiembre de 1995 en el Diario Oficial N° 176, tomo 328 se encuentra una actualizada Ley de la Corte de Cuentas de la República donde se establecía la creación de unidades de auditoría interna dentro de las instituciones del gobierno.

En el artículo 34 de dicha ley, así: “En las entidades y organismos a que se refiere el inciso primero del artículo 3 de esta Ley, se establecerá una sola unidad de auditoría interna, bajo la dependencia directa de la máxima autoridad.

La Unidad de Auditoría Interna efectuará auditoría de las operaciones, actividades y programas de la respectiva entidad u organismo y de sus dependencias.

Se exceptúan de lo establecido en el inciso primero de esta disposición a las entidades u organismos del sector público cuyo presupuesto de funcionamiento es inferior a cinco millones de colones, debiendo en todo caso cumplir con las normas técnicas de control interno, en lo que les fueren aplicables”.

El inciso primero del artículo 3 de la Ley en referencia, reza lo siguiente: “Están sujetas a la fiscalización y control de la Corte todas las entidades y organismos del sector público y sus servidores, sin excepción alguna”

1.4.2 GENERALIDADES DE LA AUDITORÍA INTERNA GUBERNAMENTAL

En la actualidad y de acuerdo al Código de Ética del Instituto de Auditores Internos, la Auditoría Interna es “una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno”.

En las Normas Técnicas de Control Interno, en su artículo 13 se establece que “En todas las instituciones del sector público a que se refiere el artículo 1 de las presentes Normas, la máxima autoridad deberá asegurar el establecimiento y fortalecimiento de una Unidad de Auditoría Interna”.

A pesar de ser una unidad administrativa que se encuentra dentro de la institución está debe tener presente la Independencia Funcional, como lo señala el artículo 35 de la Ley de la Corte de Cuentas: “La unidad de auditoría interna tendrá plena independencia funcional. No ejercerá funciones en los procesos de administración, control previo, aprobación, contabilización o adopción de decisiones dentro de la entidad.

En caso de destitución, traslado o supresión de partida presupuestaria del cargo de un servidor de la unidad de auditoría interna, deberá razonarse con expresión de las causas legales y notificando a la Corte, para efectos de posteriores auditorías”.

De igual forma lo estipula el Instituto de Auditores Internos en las Normas Internacionales para el ejercicio Profesional de la Auditoría Interna en sus normas sobre atributos 1100 Independencia y Objetividad, establece “La actividad de auditoría interna debe ser independiente, y los auditores internos deben ser objetivos en el cumplimiento de su trabajo”.

1.5 MARCO LEGAL Y NORMATIVA TÉCNICA APLICABLES A LA AUDITORÍA INTERNA GUBERNAMENTAL

1.5.1 MARCO LEGAL

Existe variada legislación que le es aplicable, la cual debe tomarse como la base de las actividades que las unidades de auditoría interna realizan dentro de las instituciones autónomas, esta es la siguiente:

CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA DE EL SALVADOR

La Constitución Política de la República de El Salvador de 1983 es el marco base de toda la legislación de la República y aquello que se pretenda regular legalmente debe de tener el sustento constitucional correspondiente. Dicho eso, se dibuja la relevancia de la norma constitucional en el nacimiento de cualquier actividad del Estado y en concordancia a todo ello es necesario establecer las bases constitucionales que les dan vida a las instituciones autónomas como se menciona en un principio.

Por otro lado, existe la institución denominada Corte de Cuentas de la República que es la encargada del control y fiscalización de la Hacienda Pública, ello en base al Artículo 195 que establece “La fiscalización de la Hacienda Pública en general y de la ejecución del Presupuesto en particular, estará a cargo de un organismo independiente del Órgano Ejecutivo, que se denominará Corte de Cuentas de la República”, en ese mismo orden se le brindan las siguientes atribuciones:

- Vigilar la recaudación, la custodia, el compromiso y la erogación de los fondos públicos; así como la liquidación de impuestos, tasas, derechos y demás contribuciones, cuando la ley lo determine;
- Aprobar toda salida de fondos del Tesoro Público, de acuerdo con el presupuesto; intervenir en todo acto que de manera directa o indirecta afecte al Tesoro Público o al Patrimonio del Estado y refrendar los actos y contratos relativos a la deuda pública;

- Vigilar, inspeccionar y glosar las cuentas de los funcionarios y empleados que administren o manejen bienes públicos y conocer de los juicios a que den lugar dichas cuentas;
- Fiscalizar la gestión económica de las Instituciones y empresas estatales de carácter autónomo y de las entidades que se costeen con fondos del Erario o que reciban subvención o subsidio del mismo;
- Examinar la cuenta que sobre la gestión de la Hacienda Pública rinda el Órgano Ejecutivo a la Asamblea, e informar a ésta del resultado de su examen;
- Dictar los reglamentos necesarios para el cumplimiento de sus atribuciones;
- Informar por escrito al Presidente de la República, a la Asamblea Legislativa y a los respectivos superiores jerárquicos de las irregularidades relevantes comprobadas a cualquier funcionario o empleado público en el manejo de bienes y fondos sujetos a fiscalización;
- Velar porque se hagan efectivas las deudas a favor del Estado y Municipios;
- Ejercer las demás funciones que las leyes le señalen.

LEY ORGÁNICA DE ADMINISTRACIÓN FINANCIERA DEL ESTADO

Así como existe la base del nacimiento de las instituciones autónomas, también se encuentra la que regula las actividades financieras de ellas; esta se encuentra en la Ley Orgánica de Administración Financiera del Estado, la cual en cumplimiento a su objeto crea el Sistema de Administración Financiera Integrado (SAFI) que a la vez tiene los siguientes objetivos:

- Establecer los mecanismos de coordinación de la administración financiera entre las entidades e instituciones del sector público, para implantar los criterios de economía, eficiencia y eficacia en la obtención y aplicación de los recursos públicos;
- Fijar la organización estructural y funcional de las actividades financieras en las entidades administrativas;
- Establecer procedimientos para generar, registrar y proporcionar información financiera útil, adecuada, oportuna y confiable, para la toma de decisiones y para la evaluación de la gestión de los responsables de cada una de las áreas administrativas;

- Establecer como responsabilidad propia de la dirección superior de cada entidad del sector público la implantación, mantenimiento, actualización y supervisión de los elementos componentes del sistema de administración financiera integrado; y,
- Establecer los requerimientos de participación activa y coordinada de las autoridades y las unidades ejecutoras del sector público en los diversos procesos administrativos derivados de la ejecución del SAFI.

Además, se crean los siguientes Subsistemas que se describen como sigue:

- Subsistema de Presupuesto: comprende los principios, técnicas, métodos y procedimientos empleados en las diferentes etapas o fases que integran el proceso presupuestario.
- Subsistema de Tesorería: comprende todos los procesos de percepción, depósito, erogación, transferencia y registro de los recursos financieros del tesoro público; recursos que, puestos a disposición de las entidades y organismos del sector público, se utilizan para la cancelación de obligaciones contraídas con aplicación al Presupuesto General del Estado.
- Subsistema de Inversión y Crédito Público: En lo relativo a la Inversión Pública, ésta deberá compatibilizarse con los objetivos de Desarrollo Nacional y Sectorial, y con los recursos disponibles, coordinando la acción estatal en materia de inversiones con el Programa Monetario y Financiero, y el Presupuesto Público. El Subsistema de Crédito Público tiene como finalidad obtener, dar seguimiento y controlar recursos internos y externos, originados por la vía del endeudamiento público. Tales recursos solamente podrán ser destinados al financiamiento de proyectos de inversión de beneficio económico y social, situaciones imprevistas o de necesidad nacional y convenidos para refinanciar los pasivos del sector público, incluyendo los intereses respectivos.
- Subsistema de Contabilidad Gubernamental: es el elemento integrador del Sistema de Administración Financiera y está constituido por un conjunto de principios, normas y procedimientos técnicos para recopilar, registrar, procesar y controlar en forma sistemática toda la información referente a las transacciones del sector público,

expresable en términos monetarios, con el objeto de proveer información sobre la gestión financiera y presupuestaria.

LEY DE LA CORTE DE CUENTAS DE LA REPÚBLICA

Es La ley de la Institución encargada del sistema nacional de control y auditoría de la gestión pública, y en esta se establece la obligatoriedad de la existencia de las Unidades de Auditoría Interna en todas las entidades del sector público; además, como se establece más adelante, es la Corte de Cuentas de la República la encargada de dictar disposiciones reglamentarias, políticas, normas técnicas y procedimientos para el ejercicio de la auditoría en el sector público.

Así también, en esta legislación se especifica que el control interno posterior de las entidades del sector público se efectúa mediante la auditoría gubernamental, la cual se denominará interna cuando la practiquen las unidades administrativas pertinentes de las entidades y organismos del sector público, mediante dicho tipo de auditoría se puede examinar:

- Las transacciones, registros, informes y estados financieros;
- La legalidad de las transacciones y el cumplimiento de otras disposiciones;
- El control interno financiero;
- La planificación, organización, ejecución y control interno administrativo;
- La eficiencia, efectividad y economía en el uso de los recursos humanos, ambientales, materiales, financieros y tecnológicos;
- Los resultados de las operaciones y el cumplimiento de objetivos y metas.

En lo que compete a las unidades de auditoría interna esta ley establece, además de la existencia de tales unidades, lo siguiente:

- Efectuarán auditoría de las operaciones, actividades y programas de la respectiva entidad u organismo y de sus dependencias;
- Tendrán plena independencia funcional. No ejercerá funciones en los procesos de administración, control previo, aprobación, contabilización o adopción de decisiones dentro de la entidad;

Las unidades de auditoría interna y su personal tendrán el acceso irrestricto a registros, archivos y documentos que sustentan la información e inclusive a las operaciones en sí, en cuanto la naturaleza de la auditoría lo requiera

1.5.2 NORMATIVA TÉCNICA

La siguiente normativa técnica debe tomarse como la base de las actividades que las unidades de auditoría interna realizan dentro de las instituciones autónomas:

NORMAS DE AUDITORÍA GUBERNAMENTAL (NAG)

Debido a que corresponde a un sector especial para la realización de auditorías y dicho sector posee un ente rector que emite la normativa técnica que se aplica a esta actividad, las normas de aplicación se denominan Normas de Auditoría Gubernamental (NAG), dichas normas son de aplicación obligatoria para los auditores internos y su objeto es la efectiva planificación, ejecución y comunicación de los resultados de la auditoría gubernamental.

Las NAG poseen premisas básicas, las cuales son:

- El término "Auditoría" incluye tanto la auditoría financiera, la operacional o de gestión, y los exámenes especiales;
- Los funcionarios públicos y otros a los que se les ha confiado el manejo, custodia, recaudación, administración, autorizaciones, refrendos, aval, distribución, seguimiento y control, de fondos, bienes u otros recursos públicos, son responsables de emplearlos con eficiencia, efectividad y economía;
- Los servidores públicos a quienes se les ha confiado recursos públicos, son responsables de cumplir las leyes, reglamentos y demás disposiciones aplicables; así como de establecer y de mantener controles efectivos a fin de que se garantice alcanzar las metas y objetivos, salvaguardando los recursos correspondientes;
- Los informes de auditoría gubernamental son importantes elementos de control y responsabilidad pública. La auditoría le otorga credibilidad a la información presentada por la Administración u obtenida de ella, al obtener y evaluar objetivamente la evidencia.

Las NAG se dividen en Normas Generales, dichas normas son:

NORMAS GENERALES RELACIONADAS CON EL AUDITOR

- Capacidad profesional
- Independencia
- Debido cuidado profesional
- Confidencialidad

NORMAS GENERALES RELACIONADAS CON LA FASE DE EXAMEN

- Planificación
- Seguimiento a recomendaciones de informes anteriores
- Supervisión del proceso de auditoría
- Control interno
- Cumplimiento de leyes y regulaciones aplicables
- Evidencia de auditoría
- Control de calidad

NORMAS GENERALES RELACIONADAS CON LA FASE DE INFORMES

- Informe y comunicación de resultados
- Trámite de los informes

También se definen las Normas Específicas y se dividen en:

NORMAS ESPECÍFICAS RELATIVAS A LA AUDITORÍA OPERACIONAL O DE GESTIÓN-FINANCIERA-ESPECIAL

- Planificación
- Ejecución
- Informe y comunicación de resultados

NORMAS TÉCNICAS DE CONTROL INTERNO (NTCI)

También existe normativa técnica aplicable al control interno de las instituciones autónomas, al igual que las anteriores normas (NAG) son emitidas por la Corte de Cuentas de la República, y su aplicación de igual forma es de carácter obligatorio.

Como se mencionó anteriormente estas Normas Técnicas de Control Interno (NTCI) definen el Sistema de Control Interno como “el conjunto de procesos continuos e interrelacionados realizados por las máxima autoridad, funcionarios y empleados, diseñados para proporcionar seguridad razonable en la consecución de sus objetivos”.

De acuerdo al informe COSO, el cual es retomado por estas NTCI, existen cinco componentes del control interno, estos componentes son:

AMBIENTE DE CONTROL:

Establece el fundamento de la institución, para influir la práctica del control en sus servidores. Es la base de los otros componentes del control interno, proporcionando los elementos necesarios para permitir el desarrollo de una actitud positiva y de apoyo para el control interno y para una gestión escrupulosa.

Los factores del ambiente de control incluyen: la integridad y los valores éticos, la competencia del personal, la filosofía y el estilo de administración, la estructura organizacional, la asignación de autoridad y responsabilidad, las políticas y prácticas de gestión de recursos humanos y la unidad de auditoría interna. Las normas contenidas en este componente son:

Normas relativas al ambiente de control

- Integridad y valores éticos
- Compromiso con la competencia
- Estilo de gestión
- Estructura organizacional

- Definición de áreas de autoridad, responsabilidad y relaciones de jerarquía
- Políticas y prácticas para la administración del capital humano
- Unidad de auditoría interna

VALORACIÓN DE RIESGOS:

Cada institución enfrenta una variedad de factores de riesgo derivados de fuentes externas e internas, que deben ser considerados para alcanzar los objetivos institucionales. Por eso, una condición previa para la valoración de riesgos es el establecimiento de objetivos, enlazados en niveles diferentes y consistentes internamente. La valoración de riesgos es la identificación y análisis de los riesgos relevantes para el logro de los objetivos, formando una base para la determinación de cómo deben administrarse los riesgos. Las normas del componente son:

Normas relativas a la valoración de riesgos

- Definición de objetivos institucionales
- Planificación participativa
- Identificación de riesgos
- Análisis de riesgos identificados
- Gestión de riesgos

ACTIVIDADES DE CONTROL:

Son las políticas y procedimientos que permiten obtener una seguridad razonable del cumplimiento de las directrices administrativas. Tales actividades ayudan a asegurar que se están tomando las acciones necesarias para enfrentar los factores de riesgo implicados en el logro de los objetivos de la institución. Estas se dan en todos los niveles de la organización; incluyen un rango de actividades tan diversas como aprobaciones y autorizaciones, conciliaciones, seguridad de activos, rotación del personal, rendición de fianzas y segregación de funciones. Este componente posee las siguientes normas:

Normas relativas a las actividades de control

- Documentación, actualización y divulgación de políticas y procedimientos
- Actividades de control
- Definición de políticas y procedimientos de autorización y aprobación
- Definición de políticas y procedimientos sobre activos
- Registros
- Definición de políticas y procedimientos sobre rotación de personal
- Definición de políticas y procedimientos sobre garantías o cauciones
- Definición de políticas y procedimientos de los controles generales de los sistemas de información
- Definición de políticas y procedimientos de los controles de aplicación.

INFORMACIÓN Y COMUNICACIÓN:

Deben establecerse los procesos para que la administración activa pueda identificar, registrar y comunicar información, relacionada con actividades y eventos internos y externos relevantes para la organización. Las normas correspondientes a este componente son:

Normas relativas a la información y comunicación

- Adecuación de los sistemas de información y comunicación
- Proceso de identificación, registro y recuperación de la información
- Características de la información
- Efectiva comunicación de la información
- Archivo institucional

MONITOREO:

El sistema de control interno tiene que someterse a un proceso continuo de monitoreo, bajo la responsabilidad de la máxima autoridad y niveles gerenciales de cada entidad. Son actividades que se realizan para valorar la calidad del funcionamiento del sistema de control interno en el tiempo y asegurar razonablemente que los resultados de las auditorías y de otras revisiones, se

atiendan con prontitud. Este último componente posee estas normas:

Normas relativas al monitoreo

- Monitoreo sobre la marcha
- Monitoreo mediante autoevaluación del Sistema de Control Interno
- Evaluaciones separadas
- Comunicación de los resultados del monitoreo

1.5.3 OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS (COBIT)

Los Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT por sus siglas en inglés) poseen un marco de trabajo que la dirección de las entidades debe implantar, esto con la intención de contribuir a cumplir las necesidades del negocio de la siguiente manera:

- Estableciendo un vínculo con los requerimientos del negocio
- Organizando las actividades de tecnología de la información en un modelo de procesos generalmente aceptado
- Identificando los principales recursos de tecnología de la información a ser utilizados
- Definiendo los objetivos de control gerenciales a ser considerados

Es de mencionar que así como COSO es generalmente aceptado como el marco de trabajo de control interno para las instituciones, COBIT es el marco de trabajo de control interno generalmente aceptado para tecnología de la información. Este al implantarse trae beneficios y entre estos se incluyen:

- Mejor alineación, con base en su enfoque de negocios
- Una visión, entendible para la gerencia, de lo que hace TI
- Propiedad y responsabilidades claras, con base en su orientación a procesos
- Aceptación general de terceros y reguladores
- Entendimiento compartido entre todos los participantes, con base en un lenguaje común

- Cumplimiento de los requerimientos COSO para el ambiente de control de tecnología de la información.

En el curso de gobernar efectivamente la Tecnología Informática, COBIT determina cuatro dominios que deben ser administrados, esto son:

PLANEAR Y ORGANIZAR (PO):

Cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que la TI pueda contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada, y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada.

ADQUIRIR E IMPLANTAR (AI):

Para llevar a cabo la estrategia de tecnología de la información, las soluciones de tecnología de la información necesitan ser identificadas, desarrolladas o adquiridas así como la implementación e integración en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio.

ENTREGA Y DAR SOPORTE (DS):

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales.

MONITOREAR Y EVALUAR (ME):

Todos los procesos de tecnología de la información deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

CAPÍTULO II

2. METODOLOGÍA Y DIAGNÓSTICO DE LA INVESTIGACIÓN

2.1 TIPO DE INVESTIGACIÓN

El tipo de investigación, para el problema de la no existencia de una metodología para la evaluación del control interno de los sistemas de información computarizados en las instituciones autónomas desde la perspectiva de la auditoría interna gubernamental, se hizo a través del método hipotético deductivo, ya que se partió de una hipótesis y se pasó de afirmaciones de carácter general a hechos particulares para poder dar al final una solución al problema planteado.

2.2 TIPO DE ESTUDIO

La investigación se basó en un estudio tipo analítico descriptivo, ya que además de dirigirse a determinar cómo está la situación de las variables que se estudian y evaluar diversos aspectos del fenómeno a investigar, se analizó por qué ocurre este fenómeno y en qué condiciones se da.

2.3 DETERMINACIÓN DE LA POBLACIÓN

Las instituciones autónomas dentro del área metropolitana de San Salvador y que al 30 de junio de 2008 tenían constituida la unidad de auditoría interna son 44.

2.4 DETERMINACIÓN DE LA MUESTRA

La fórmula estadística utilizada para determinar el tamaño de muestra es la siguiente:

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

Donde:

n = Tamaño necesario de la muestra

N = Población

e = El máximo error permisible en la muestra

p = El grado de aceptación que tendrá la hipótesis

q = El grado de rechazo de la hipótesis

z = Nivel de confianza

Sustituyendo datos se tiene:

N = 44

e = 0.08

p = 0.75

q = 0.25

z = 0.92 → 1.75

El valor que resultó de la tabla de áreas bajo la curva normal es de 1.75

De acuerdo a la información anterior y mediante la aplicación de la fórmula estadística antes mencionada, se obtuvo una muestra de 30 instituciones autónomas. Como se muestra a continuación:

$$n = \frac{(1.75)^2 (0.75) (0.25) (44)}{(0.08)^2 (44 - 1) + (1.75)^2 (0.75) (0.25)}$$

$$n = 29.74 \approx 30$$

n = 30 Instituciones

2.5 UNIDADES DE ANÁLISIS

El trabajo de investigación se llevó a cabo tomando como universo de estudio las instituciones autónomas que al 30 de junio de 2008 tenían constituida la unidad de auditoría interna y dichas oficinas se encuentren dentro del área metropolitana de San Salvador, lo cual permitió contar con resultados actualizados con respecto a las actividades desarrolladas por estas unidades en lo referente a la evaluación de los Sistemas de Información Computarizados de las instituciones correspondientes.

2.6 INSTRUMENTOS Y TÉCNICAS DE INVESTIGACIÓN

INSTRUMENTO

CUESTIONARIO: Se utilizó el cuestionario por la capacidad que brindan de proporcionar información sobre un mayor número de instituciones en un periodo breve, por la facilidad para obtener, cuantificar, analizar e interpretar datos y la eliminación de sesgos que introduce el encuestador. A través de su utilización se recolectó la información de campo necesaria para demostrar que la problemática planteada existe y que requiere una solución.

TÉCNICA

BIBLIOGRÁFICA: Se efectuó una recopilación de la información bibliográfica disponible en la parte legal y técnica, mediante la utilización de las distintas fuentes, tanto primarias como secundarias.

EL MUESTREO: Se aplicó la fórmula estadística para poblaciones finitas, ya que la cantidad de instituciones autónomas es una cifra conocida.

2.7 TABULACIÓN Y LECTURA DE DATOS

PREGUNTA N° 1

¿Posee la institución sistemas de información computarizados?

OBJETIVO:

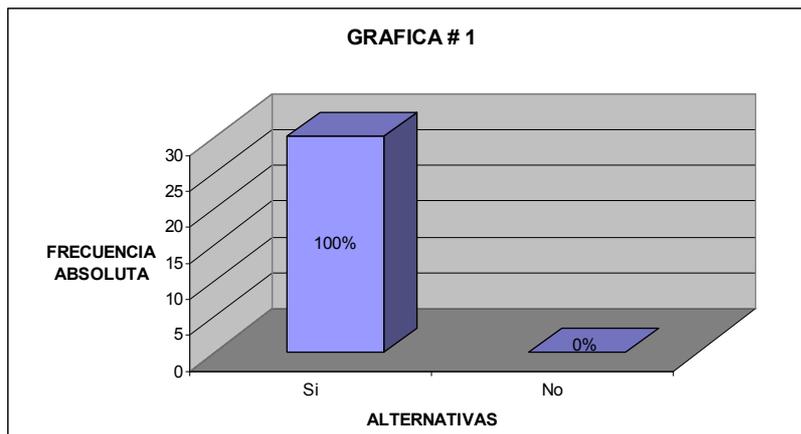
Investigar cuantas instituciones autónomas poseen sistemas de información computarizados

RESULTADOS:

TABLA N° 1 Instituciones que poseen sistemas de información computarizados

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	30	100%
No	0	0%
Total	30	100%

GRÁFICA N° 1 Instituciones que poseen sistemas de información computarizados



ANÁLISIS:

Como se muestra el gráfico N° 1 el 100% de las instituciones autónomas si poseen sistemas de información computarizados

PREGUNTA N° 2

¿Las Normas Técnicas de Control Interno de la institución contemplan el área de los sistemas de información computarizados?

OBJETIVO:

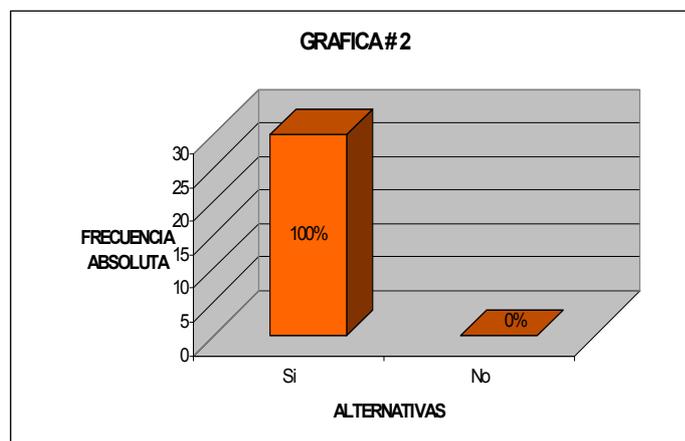
Conocer si las Normas Técnicas de Control Interno de la institución autónoma contemplan el área de los sistemas de información computarizados

RESULTADOS:

TABLA N° 2 Instituciones donde las NTCl contemplan el área de los sistemas de información computarizados

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	30	100%
No	0	0%
Total	30	100%

GRÁFICA N° 2 Instituciones donde las NTCl contemplan el área de los sistemas de información computarizados



ANÁLISIS:

En el gráfico N° 2 podemos observar que todas las instituciones autónomas de la muestra afirman que las normas técnicas de control interno contemplan el área de los sistemas de información computarizados.

PREGUNTA N° 3

¿Se tomó en cuenta algún marco de referencia, para normar el control interno de los sistemas de información computarizados?

OBJETIVO:

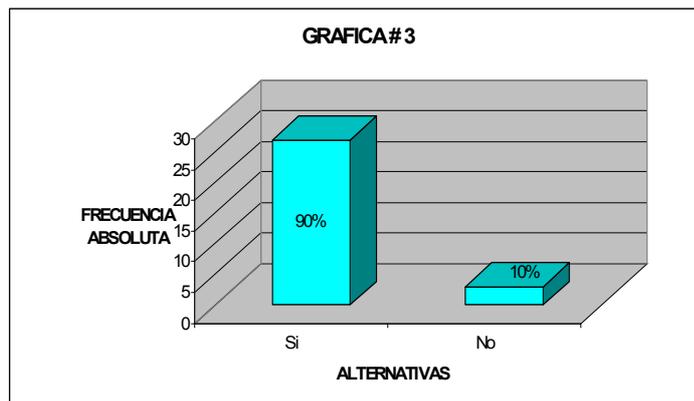
Establecer si en el proceso de adaptación de las normas utilizadas por la institución para el control interno de los sistemas de información computarizados, se tomo en cuenta algún marco de referencia.

RESULTADOS:

TABLA N° 3 Instituciones que tomaron en cuenta marco de referencia para normar el control interno

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	27	90%
No	3	10%
Total	30	100%

GRÁFICA N° 3 Instituciones que tomaron en cuenta marco de referencia para normar el control interno



ANÁLISIS:

Según se muestra en el gráfico N° 3 el 90% de las instituciones autónomas normaron el control interno de los sistemas de información computarizados, basándose en un marco de referencia y un 10% no se basaron en un marco de referencia para normar el control interno de los sistemas de información.

PREGUNTA N° 4

¿Posee la institución, manual para el desarrollo de las actividades de la unidad de auditoría interna?

OBJETIVO:

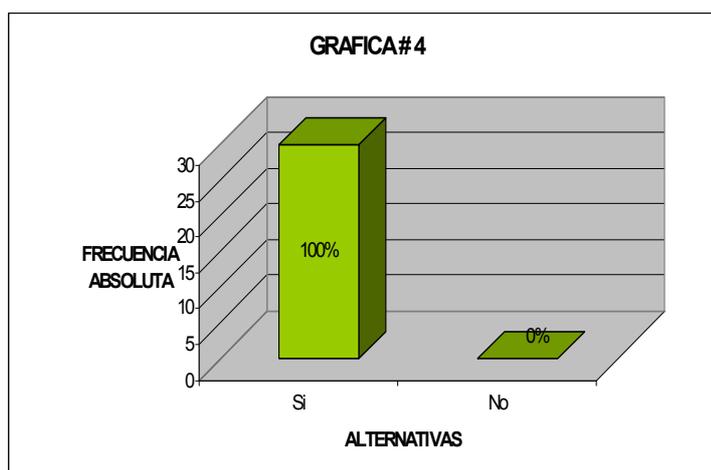
Determinar si la institución autónoma posee manual para el desarrollo de las actividades de la unidad de auditoría interna

RESULTADOS:

TABLA N° 4 Instituciones que poseen manual para el desarrollo de las actividades de la unidad de auditoría interna

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	30	100%
No	0	0%
Total	30	100%

GRÁFICA N° 4 Instituciones que poseen manual para el desarrollo de las actividades de la unidad de auditoría interna



ANÁLISIS:

El 100% de las instituciones autónomas confirmaron que si poseen manual para el desarrollo de las actividades de la unidad de auditoría interna.

PREGUNTA N° 5

¿Los planes de trabajo anuales de la unidad de auditoría interna, contemplan la evaluación de los sistemas de información computarizados de la institución?

OBJETIVO:

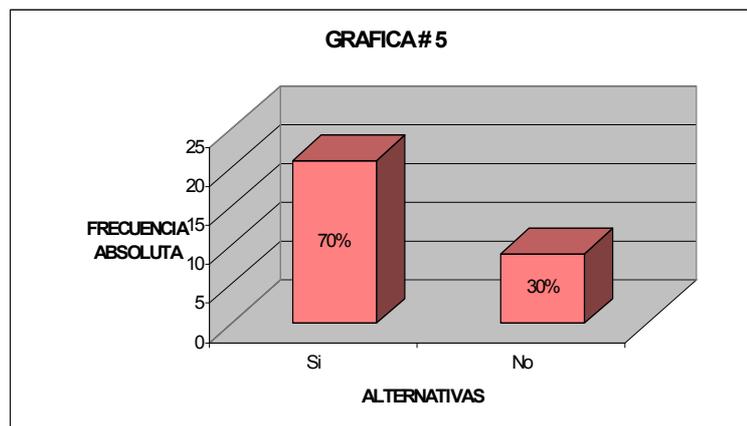
Verificar si los planes de trabajo anuales de la unidad de auditoría interna, contemplan la evaluación de los sistemas de información computarizados de la institución

RESULTADOS:

TABLA N° 5 Instituciones que contemplan la evaluación de los sistemas de información computarizados en los planes de trabajo anuales

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	21	70%
No	9	30%
Total	30	100%

GRÁFICA N° 5 Instituciones que contemplan la evaluación de los sistemas de información computarizados en los planes de trabajo anuales



ANÁLISIS:

De las unidades de auditoría interna en las instituciones un 70%, afirma que en sus planes de trabajo anual contemplan la evaluación de los sistemas de información computarizados y un 30% no toman en cuenta la evaluación de esa área.

PREGUNTA N° 6

¿Se cuenta con alguna referencia técnica para evaluar los sistemas de información computarizados?

OBJETIVO:

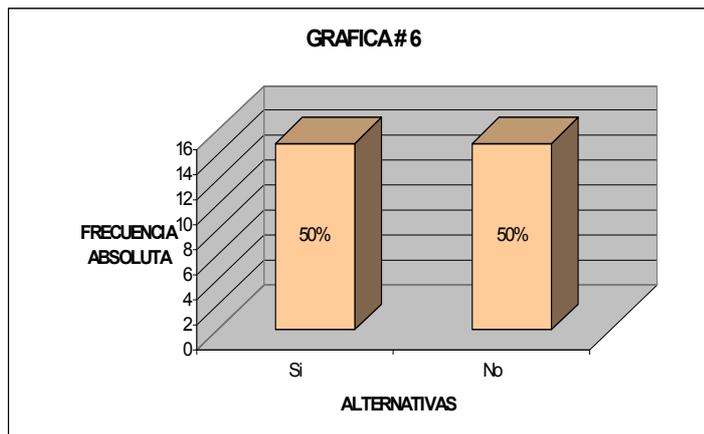
Saber si la unidades de auditoria interna cuentan con alguna referencia técnica para evaluar los sistemas de información computarizados

RESULTADOS:

TABLA N° 6 Unidades de auditoria interna que cuentan con referencia técnica para evaluar los sistemas de información computarizados

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	15	50%
No	15	50%
Total	30	100%

GRAFICA N° 6 Unidades de auditoria interna que cuentan con referencia técnica para evaluar los sistemas de información computarizados



ANÁLISIS:

El 50% de las unidades de auditoria interna cuentan con alguna referencia técnica para evaluar los sistemas de información computarizados y el resto no cuenta con referencia técnica.

PREGUNTA N° 7

¿Cuenta la unidad de auditoría interna con personal idóneo para evaluar los sistemas de información computarizados?

OBJETIVO:

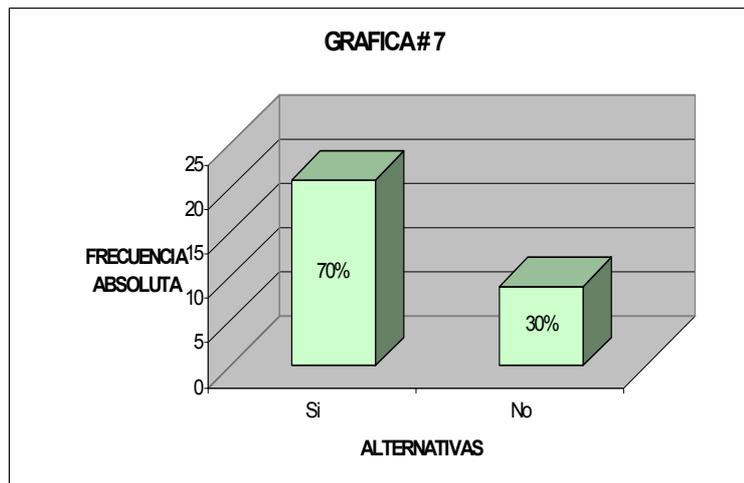
Determinar si la unidad de auditoría interna cuenta con personal idóneo para evaluar los sistemas de información computarizados

RESULTADOS:

TABLA N° 7 Unidades de auditoría interna que cuentan con personal idóneo para evaluar los sistemas de información computarizados

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	21	70%
No	9	30%
Total	30	100%

GRAFICA N° 7 Unidades de auditoría interna que cuentan con personal idóneo para evaluar los sistemas de información computarizados



ANÁLISIS:

Un 70% de las unidades de auditoría interna cuentan con personal idóneo para evaluar los sistemas de información computarizados y un 30% consideran que no cuentan con personal idóneo para evaluar los sistemas de información computarizados.

PREGUNTA N° 8

¿Cuáles de los siguientes profesionales componen la unidad de auditoría interna?

OBJETIVO:

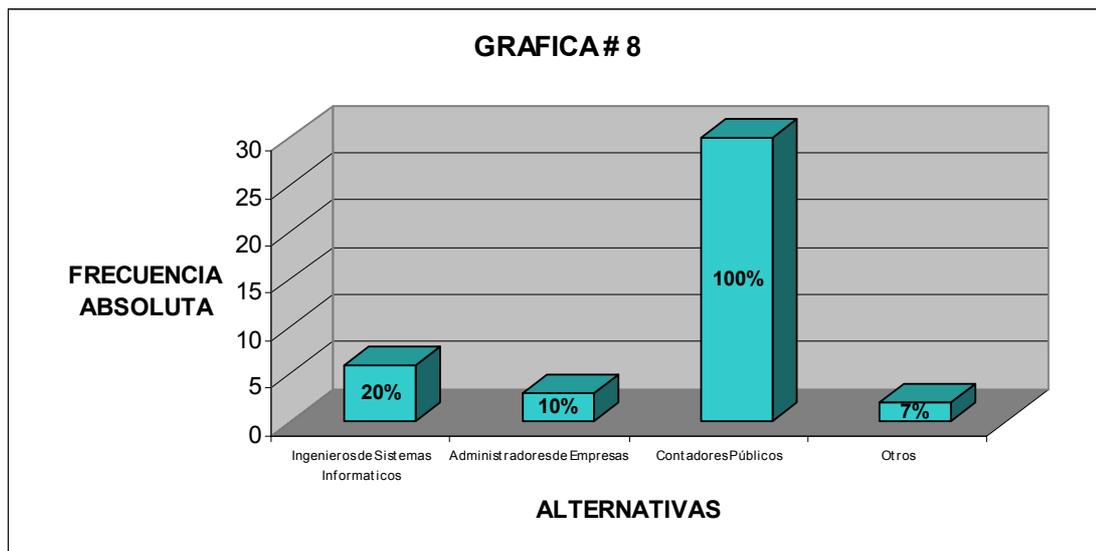
Conocer que profesionales integran la unidad de auditoría interna

RESULTADOS:

TABLA N° 8 Profesionales que componen la unidad de auditoría interna

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Ingenieros de Sistemas Informáticos	6	20%
Administradores de Empresas	3	10%
Contadores Públicos	30	100%
Otros	2	7%

GRAFICA N° 8 Profesionales que componen la unidad de auditoría interna



El total es superior a 100% porque era posible dar varias respuestas

ANÁLISIS:

El 20% de las instituciones esta compuesto, en la unidad de auditoría interna, por Ingenieros de Sistemas Informáticos; un 10% por Administradores de Empresas; el 100% por Contadores Públicos; y 7% por otros profesionales.

PREGUNTA N° 9

¿Se capacita al personal de la unidad de auditoría interna para el desarrollo de las evaluaciones de los sistemas de información computarizados?

OBJETIVO:

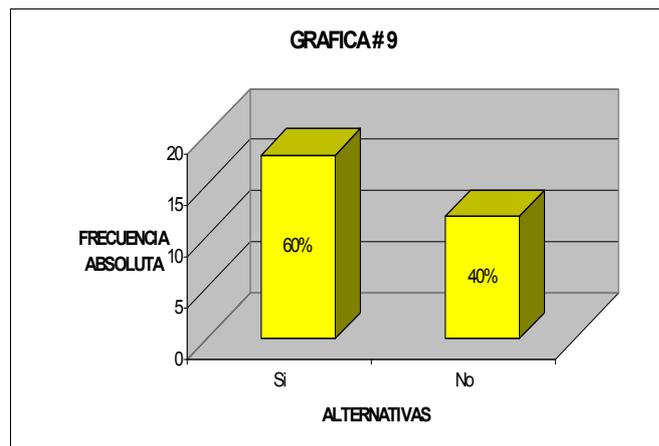
Investigar si el personal de la unidad de auditoría interna recibe capacitaciones para el desarrollo de las evaluaciones de los sistemas de información computarizados

RESULTADOS:

TABLA N° 9 Instituciones que capacitan al personal de la unidad de auditoría interna para el desarrollo de las evaluaciones de los sistemas de información computarizados

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	18	60%
No	12	40%
Total	30	100%

GRAFICA N° 9 Instituciones que capacitan al personal de la unidad de auditoría interna para el desarrollo de las evaluaciones de los sistemas de información computarizados



ANÁLISIS:

En el 60% de las instituciones el personal de auditoría interna recibe capacitaciones para evaluar los sistemas de información computarizados y un 40% no reciben capacitaciones.

PREGUNTA N° 10

¿Durante el año 2008, cuántas horas de capacitación se han recibido en la unidad de auditoría interna?

OBJETIVO:

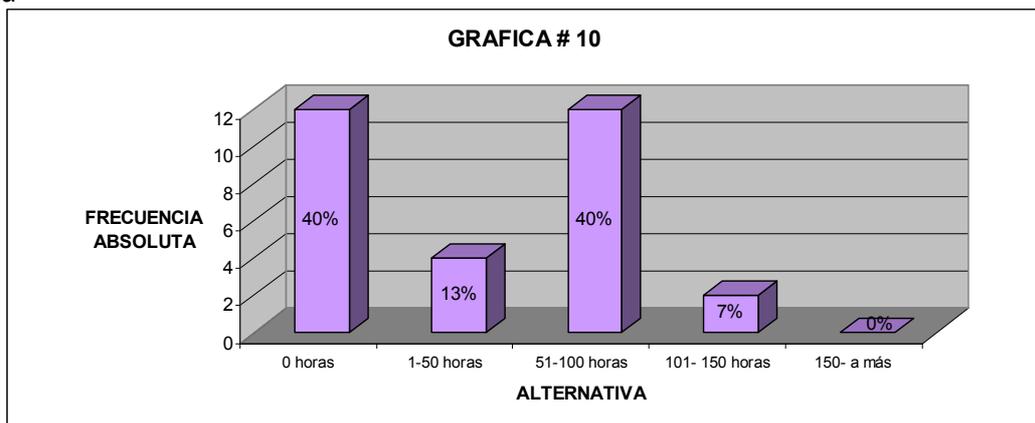
Determinar la cantidad de horas de capacitación recibidas por el personal de auditoría interna, durante el año 2008

RESULTADOS:

TABLA N° 10 Horas de capacitación recibidas, durante el 2008, en la unidad de auditoría interna

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
0 horas	12	40%
1-50 horas	4	13%
51-100 horas	12	40%
101- 150 horas	2	7%
150- a más	0	0%
Total	30	100%

GRAFICA N° 10 Horas de capacitación recibidas, durante el 2008, en la unidad de auditoría interna



ANÁLISIS:

El 40% de las instituciones no ha recibido ninguna hora de capacitación; un 13% ha recibido capacitaciones de 1 a 50 horas; un 40% recibió de 51 a 100 horas; el 7% recibió de 101 a 150 horas y en ninguna institución se recibieron más de 150 horas al año.

PREGUNTA N° 11

¿Utilizan técnicas asistidas por computadora para las evaluaciones de los sistemas de información computarizados?

OBJETIVO:

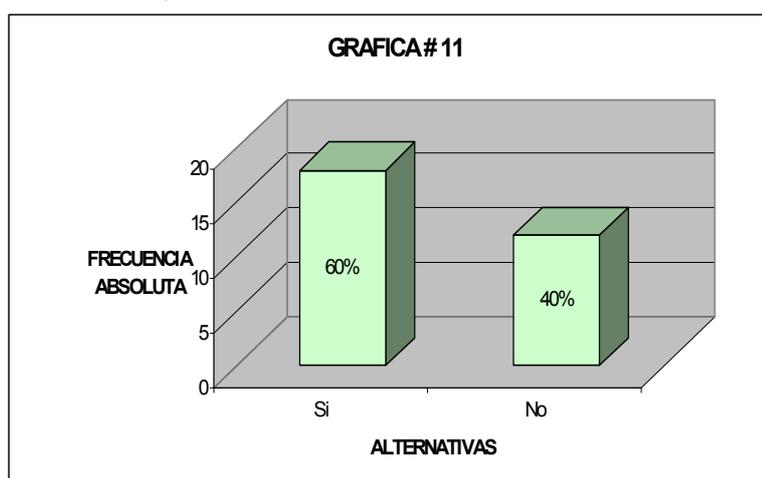
Conocer si para las evaluaciones de los sistemas de información computarizados, utilizan técnicas asistidas por computadora

RESULTADOS:

TABLA N° 11 Utilización de técnicas asistidas por computadora para las evaluaciones de los sistemas de información computarizados

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	18	60%
No	12	40%
Total	30	100%

GRAFICA N° 11 Utilización de técnicas asistidas por computadora para las evaluaciones de los sistemas de información computarizados



ANÁLISIS:

En el 60% de las instituciones se utilizan técnicas asistidas por computadora para las evaluaciones de los sistemas de información computarizados y en un 40% no son utilizadas.

PREGUNTA N° 12

¿El trabajo desempeñado por la unidad de auditoría interna se desarrolla en base a las Normas de Auditoría Gubernamental-NAG adoptadas por la Corte de Cuentas de la República?

OBJETIVO:

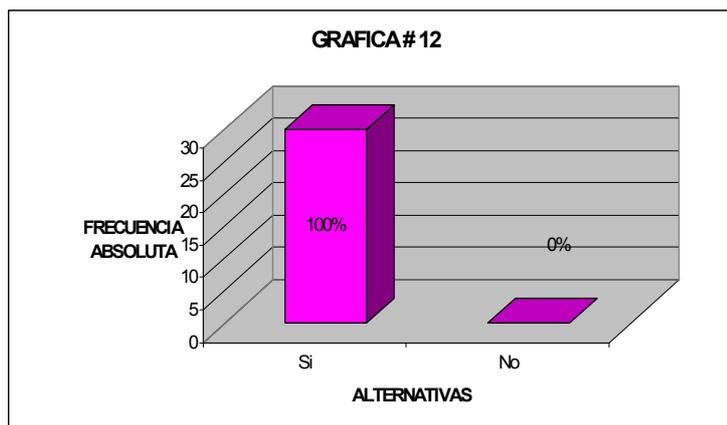
Determinar si el trabajo desempeñado por la unidad de auditoría interna se desarrolla en base a las Normas de Auditoría Gubernamental-NAG adoptadas por la Corte de Cuentas de la República

RESULTADOS:

TABLA N° 12 Unidades de auditoria interna que desempeñan su trabajo en base a las Normas de Auditoria Gubernamental adoptadas por la Corte de Cuentas de la Republica

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	30	100%
No	0	0%
Total	30	100%

GRAFICA N° 12 Unidades de auditoria interna que desempeñan su trabajo en base a las Normas de Auditoria Gubernamental adoptadas por la Corte de Cuentas de la Republica



ANÁLISIS:

El gráfico N° 12 muestra que el 100% de las unidades de auditoria interna desarrollan su trabajo en base a Normas de Auditoría Gubernamental-NAG adoptadas por la Corte de Cuentas de la República.

PREGUNTA N° 13

¿Considera que las Normas de Auditoría Gubernamental-NAG poseen la metodología para la correcta evaluación del control interno de los sistemas de información computarizados?

OBJETIVO:

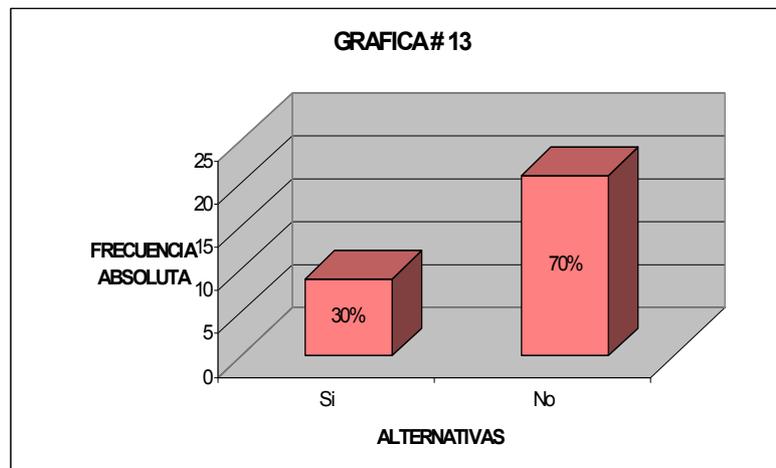
Investigar si las unidades de auditoria interna consideran que las Normas de Auditoria Gubernamental-NAG poseen la metodología para la correcta evaluación del control interno de los sistemas de información computarizados

RESULTADOS:

TABLA N° 13 Unidades de auditoria interna que consideran que las Normas de Auditoria Gubernamental poseen la metodología para la correcta evaluación del control interno de los sistemas de información computarizados

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	9	30%
No	21	70%
Total	30	100%

GRAFICA N° 13 Unidades de auditoria interna que consideran que las Normas de Auditoria Gubernamental poseen la metodología para la correcta evaluación del control interno de los sistemas de información computarizados



ANÁLISIS:

Un 30% de las unidades de auditoría interna consideran que las Normas de Auditoría Gubernamental – NAG poseen la metodología para la correcta evaluación del control interno de los sistemas de información computarizados y un 70% consideran que las Normas de Auditoría Gubernamental – NAG no poseen la metodología para la correcta evaluación pues la tiene en forma generalizada.

PREGUNTA N° 14

¿Estaría de acuerdo con la elaboración de una metodología para la evaluación del control interno de los sistemas de información computarizados-SIC en las instituciones autónomas desde la perspectiva de la auditoría interna gubernamental?

OBJETIVO:

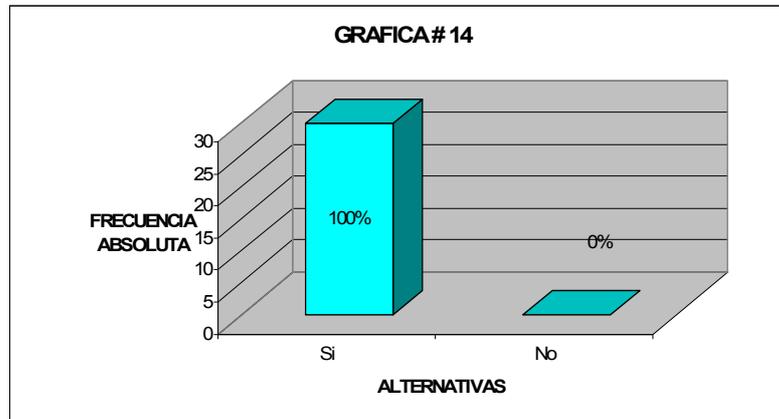
Establecer la aceptación de la elaboración de una metodología para la evaluación del control interno de los sistemas de información computarizados-SIC en las instituciones autónomas desde la perspectiva de la auditoría interna gubernamental

RESULTADOS:

TABLA N° 14 Instituciones que estarían de acuerdo con la elaboración de una metodología para la evaluación del control interno de los sistemas de información computarizados desde la perspectiva de la auditoría interna gubernamental

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	30	100%
No	0	0%
Total	30	100%

GRAFICA N° 14 Instituciones que estarían de acuerdo con la elaboración de una metodología para la evaluación del control interno de los sistemas de información computarizados desde la perspectiva de la auditoría interna gubernamental



ANÁLISIS:

El 100% estaría de acuerdo con la elaboración de una metodología para la evaluación del control interno de los sistemas de información computarizados – SIC en las instituciones autónomas desde la perspectiva de la auditoría interna gubernamental.

PREGUNTA N° 15

Si la respuesta anterior fue positiva, ¿Utilizaría usted esta metodología para la evaluación del control interno de los sistemas de información computarizados-SIC en la institución autónoma donde labora?

OBJETIVO:

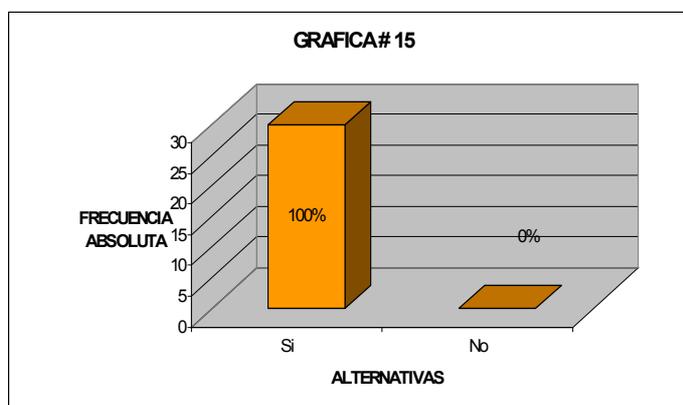
Establecer la aceptación en la utilización de una metodología para la evaluación del control interno de los sistemas de información computarizados-SIC en las instituciones autónomas desde la perspectiva de la auditoría interna gubernamental

RESULTADOS:

TABLA N° 15 Instituciones que estarían de acuerdo con la utilización de una metodología para la evaluación del control interno de los sistemas de información computarizados desde la perspectiva de la auditoría interna gubernamental

Alternativa	Frecuencia Absoluta	Frecuencia Relativa
Si	30	100%
No	0	0%
Total	30	100%

GRAFICA N° 15 Instituciones que estarían de acuerdo con la utilización de una metodología para la evaluación del control interno de los sistemas de información computarizados desde la perspectiva de la auditoría interna gubernamental



ANÁLISIS:

El 100% de las instituciones autónomas utilizaría esta metodología para la evaluación del control interno de los sistemas de información computarizados – SIC en la institución donde la labora.

2.8 DIAGNÓSTICO DE LA INVESTIGACIÓN

EVALUACIÓN DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS

De acuerdo a la investigación se pueden establecer que las instituciones autónomas en un 100% poseen sistemas de información computarizados, que todas las unidades de auditoría interna de estas instituciones poseen un manual propio para el desarrollo de sus actividades, pero a pesar de lo anterior existe un 30% de estas unidades que no contemplan en sus planes de trabajo anuales la evaluación de dichos sistemas de información y el 40% no utiliza técnicas asistidas por computador. De lo anterior se puede destacar la importancia que los sistemas de información computarizados han cobrado en el desarrollo de las actividades y en el logro de objetivos y metas de las instituciones, pero a pesar de ello una buena parte de las unidades de auditoría interna no le dan la relevancia debida al momento de incluirlas en sus evaluaciones o desarrollarlas con el uso de tecnologías adecuadas.

Evaluación de los sistemas de información computarizados

Cuadro Número 1

Nº de pregunta	Respuesta obtenida	Valor absoluto	Valor porcentual
1	Poseen sistemas de información computarizados	30	100%
4	Poseen manual para el desarrollo de las actividades de la unidad de auditoría interna	30	100%
5	Contemplan la evaluación de los sistemas de información computarizados en los planes de trabajo anuales	21	70%
11	Utilizan técnicas asistidas por computadora para las evaluaciones de los sistemas de información computarizados	18	60%

MARCO LEGAL Y NORMATIVA TECNICA

Dentro de las Normas Técnicas de Control Interno de las instituciones autónomas, en un 100% se norman estos sistemas, responden además, que en un 90% de casos se utilizó un marco de referencia que permitiera normar dicha área; pero al momento de evaluar dichos sistemas, todas las unidades de auditoría interna basan su trabajo en NAG, pero un 70% de estas unidades consideran que las NAG no poseen una metodología correcta que permita la evaluación del control interno de los sistemas de información computarizados y solamente un 50% poseen una referencia técnica que les guíe en dicha evaluación. Aquí se puede resaltar el hecho de que las autoridades encargadas de establecer el sistema de control interno de las instituciones reconocen la importancia de los sistemas de información al incluirlos en la normativa técnica y que en su mayoría se auxiliaron de un marco de referencia para ello.

Marco legal y normativa técnica

Cuadro Número 2

Nº de pregunta	Respuesta obtenida	Valor absoluto	Valor porcentual
2	Instituciones donde las NTCI contemplan el área de los sistemas de información computarizados	30	100%
3	Tomaron en cuenta un marco de referencia para normar el control interno de los sistemas de información computarizados	27	90%
6	Cuentan con referencia técnica para evaluar los sistemas de información computarizados	15	50%
12	Desempeñan su trabajo en base a Normas de Auditoría Gubernamental adoptadas por la Corte de Cuentas de la República	30	100%
13	Consideran que las NAG poseen la metodología para la correcta evaluación del control interno de los sistemas de información computarizados	9	30%

RECURSOS HUMANOS

Las Unidades de Auditoría Interna consideran en un 70% que su personal es idóneo para la evaluación de los sistemas de información computarizados; el 100% cuenta con Licenciados en Contaduría Pública dentro de su equipo, un 20% con Ingenieros en Sistemas de información, 10% con Licenciados en Administración de Empresas, el 7% con otro tipo de profesionales; además existe un 40% de Unidades en las que no se recibe capacitación para el desarrollo de la evaluación de los SIC y del 60% que ha recibido capacitaciones, el 40% recibió en el último año entre 51 y 100 horas de capacitación, seguidos por un 13% que recibió entre 1 y 50 horas y un 7% que recibió entre 101 y 150 horas. De las anteriores respuestas se destaca que en su mayoría las unidades de auditoría interna están consientes de la necesidad y búsqueda de capacitación para el desarrollo de su trabajo, pero aún existe una cantidad considerable que no desarrolla la educación continuada, esto último se vuelve una debilidad importante para las unidades de auditoría interna.

Recursos humanos

Cuadro Número 3

Nº de pregunta	Respuesta obtenida	Valor absoluto	Valor porcentual
7	Cuentas con personal idóneo para evaluar los sistemas de información computarizados	21	70%
8	Profesionales que componen la unidad de auditoria interna:		
	Ingenieros de Sistemas de Información	6	20%
	Administradores de Empresas	3	10%
	Contadores Públicos	30	100%
	Otros	2	7%

9	Capacitan al personal de la unidad de auditoría interna para el desarrollo de las evaluaciones de los sistemas de información computarizados	18	60%
10	Horas de capacitación recibidas, durante el 2008, en la unidad de auditoría interna:		
	0 horas	12	40%
	1-50 horas	4	13%
	51-100 horas	12	40%
	101-150 horas	2	7%
	150-a más	0	0%

METODOLOGIA PARA LA EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACION COMPUTARIZADOS

Las unidades de auditoría interna fueron rotundas en considerar en un 100% que estaban de acuerdo en la elaboración de una metodología para la evaluación del control interno de los sistemas de información computarizados en las instituciones autónomas desde la perspectiva de la auditoría interna gubernamental y a utilizar dicha metodología. En estas dos respuestas se pone de manifiesto que las unidades de auditoría interna reconocen la necesidad de contar con una evaluación técnica estructurada dirigida a los sistemas de información computarizados y que ellas como evaluadoras del control interno están dispuestas a retomar esta metodología y llenar esos vacíos existentes al momento de ejercer las evaluaciones.

Metodología para la evaluación del control interno de los sistemas de información computarizados

Cuadro Número 4

N° de pregunta	Respuesta obtenida	Valor absoluto	Valor porcentual
14	Instituciones que están de acuerdo con la elaboración de una metodología para la evaluación del control interno de los sistemas de información computarizados desde la perspectiva de la auditoría interna gubernamental	30	100%
15	Instituciones que están de acuerdo con la utilización de una metodología para la evaluación del control interno de los sistemas de información computarizados desde la perspectiva de la auditoría interna gubernamental	30	100%

CAPÍTULO III

3. EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS EN LAS INSTITUCIONES AUTÓNOMAS DESDE LA PERSPECTIVA DE LA AUDITORÍA INTERNA GUBERNAMENTAL

3.1 PLANEACIÓN

3.1.1 PLAN GENERAL DE AUDITORÍA

La auditoría se ha planeado de forma técnica y profesional, obteniendo el conocimiento y comprensión relativa a los sistemas de información computarizados del Instituto del Café, para proceder a evaluar el Sistema de Cuentas por Cobrar. La auditoría será desarrollada según las técnicas y procedimientos establecidos en las Normas de Auditoría Gubernamental emitidas por la Corte de Cuentas de la República.

3.1.1.1 OBJETIVO GENERAL

Emitir un informe sobre la evaluación del control interno lógico del sistema de información computarizado que controla las cuentas por cobrar del Instituto de Café, para ayudar a la dirección de dicha institución en el cumplimiento de sus funciones y responsabilidades, proporcionándole análisis objetivos, evaluaciones y recomendaciones.

3.1.1.2 OBJETIVOS ESPECIFICOS

- Examinar las actividades de control generales de seguridad lógica para el sistema de cuentas por cobrar, identificando claramente los riesgos de virus, acceso no autorizado y la destrucción potencial de rastros de auditoría.

- Evaluar las actividades de control de datos de seguridad lógica para el sistema de cuentas por cobrar, asegurando la integridad de la información en la captura, proceso y diseminación de la misma.
- Verificar los controles de aplicación de seguridad lógica para el sistema de cuentas por cobrar, determinando que el sistema operativo, los programas y los datos no puedan ser alterados sin autorización.

3.1.1.3 ALCANCE DEL TRABAJO

Se evaluarán los controles lógicos del sistema de información computarizado que controla las cuentas por cobrar de la institución, por el periodo comprendido entre el 01 de enero al 31 de marzo de 2009, a fin de determinar la eficiencia y eficacia de estos en la eliminación, prevención y/o mitigación de la posibilidad de que los riesgos de manipulación indebida de la información se materialicen.

3.1.1.3.1 CONTROLES GENERALES

- Integridad de la información
- Tecnología contra software malicioso
- Administración de privilegios
- Detección de intrusos
- Protección de información sensible
- Administración de acceso
- Identidades de usuario

3.1.1.3.2 CONTROLES DE DATOS

- Disponibilidad
- Integridad
- Flujo
- Almacenamiento y conservación

3.1.1.3.3 CONTROLES DE APLICACIÓN

- Diseño de pistas de auditoría
- Mecanismos de autorización
- Simulación paralela
- Informes de excepción
- Evaluaciones periódicas al software
- Registro de actividades de cada terminal
- Balanceo
- Control de archivos
- Control de archivos maestros
- Procedimientos de corte
- Integridad de la configuración
- Programación de tareas en secuencia eficiente
- Automatización del monitoreo de cambios a sistemas aplicativos
- Administración de incidentes
- Control de versiones
- Integridad de transacciones
- Pruebas de regresión

3.1.1.4 ENFOQUE GENERAL

La auditoría se realizará teniendo en cuenta el direccionamiento hacia los siguientes factores y características:

3.1.1.4.1 CARACTERÍSTICAS DEL ENTORNO DE LA INSTITUCIÓN

Las características del entorno del Instituto del Café se encuentran contenidas en los siguientes componentes:

a) INSTITUCIÓN:

Es una institución autónoma al servicio del sector cafetalero de El Salvador.

b) CANALES DE MERCADEO:

La institución ha establecido un plan de mercadeo que contempla la identificación de actores y escenarios sensibles para el desarrollo de canales de comunicación mercadológico, entre ellos: participación en ferias nacionales e internacionales, capacitación de los actores involucrados en la industria, identificación y utilización de medios especializados en la materia café internacionalmente, identificación de influenciadores, etc.

c) CLIENTES:

Los clientes de la institución son internos y externos.

- Clientes internos:
 - Empleados
 - Junta Directiva
- Clientes externos:
 - Productores
 - Comercializadores
 - Exportadores
 - Compradores

- Organismos internacionales
- Gobiernos

d) COMPETIDORES:

No existen competidores a nivel nacional, pero si internacional, como lo son las instituciones homólogas de países productores de café que tratan de posicionar el producto de sus respectivos países.

3.1.1.4.2 NORMAS QUE LA REGULAN

La institución se encuentra regulada en sus actividades principales por su Ley de creación y por el Reglamento de Aplicación de dicha Ley.

3.1.1.4.3 MEDIO AMBIENTE DEL SECTOR DE LOS DIFERENTES SERVICIOS

El Instituto del Café se enfoca en la prestación de servicios a los diversos actores de la industria del café, entre ellos, productores, intermediarios, beneficiadores, exportadores y tiendas especializadas de café. Entre los principales servicios prestados se encuentran:

- Certificación de las diferentes calidades de cafés exportables
- Levantamiento de estadísticas referentes a la producción, exportación y comercialización interna del café
- Mercadeo interno y externo del café salvadoreño
- Capacitación en tostado, barismo y catación
- Concesión de préstamos de apoyo para la caficultura

3.1.1.4.4 AMBIENTE EXTERNO

El ambiente externo se encuentra demarcado por la relaciones que la institución tiene con otras entidades del sector público y privado, sirviendo como enlace entre ambas a fin de mejorar el

clima de participación e identificación de objetivos comunes que redunden en mejoras económicas, sociales y medioambientales a los productores de café salvadoreño.

Además, la institución es la representante del país para el sector caficultor salvadoreño ante la comunidad internacional, entre dicha comunidad se encuentran gobiernos de países, empresas procesadoras de café, intermediarios de café, vendedores mayoristas y minoristas, vendedores de cafés especiales con valor agregado, etc.

3.1.1.4.5 CLIMA ORGANIZACIONAL

La institución ha efectuado un diagnóstico de su clima organizacional, y sus principales resultados son los siguientes:

- ESTRUCTURA ORGANIZATIVA:
La estructura organizacional de la institución, de acuerdo a los documentos consultados, es adecuada puesto que existe una segregación de funciones incompatibles y la definición de funciones y procedimientos específicos para todas sus dependencias.
- RESPONSABILIDAD:
La asignación de autoridad y responsabilidad está a cargo del Presidente de la Junta Directiva de la Institución.
- RECOMPENSA:
La administración premia a sus empleados de manera verbal y con reconocimientos públicos, enviando como acciones de personal las felicitaciones y reconocimientos por escrito a los expedientes de personal.
- RELACIONES:
La institución mantiene relaciones inter-institucionales con otras dependencias del gobierno que tienen incidencia en el establecimiento de políticas económicas o que

inciden en la industria cafetalera, como lo son el Ministerio de Economía, Ministerio de Agricultura y Ganadería y Ministerio de Hacienda; además, al interior de la institución las diferentes divisiones mantienen comunicación permanente para el desarrollo coordinada de sus actividades programadas.

- COOPERACIÓN:

La institución desarrolla sus actividades principales con cooperación económica o logística proveniente de diversos organismos, tanto nacionales como extranjeros, públicos y privados.

- ESTÁNDARES:

Al interior se han establecido estándares para: capacitación a los actores de la agroindustria del café, certificación de calidades de café, otorgamientos de créditos a productores.

- CONFLICTOS:

Para la normalización de las relaciones laborales que se ven afectadas por el surgimiento de conflictos de todo tipo, se involucran las jefaturas de las áreas y de no ser solucionadas a ese nivel son escaladas al nivel inmediato superior hasta que se resuelven de manera satisfactoria.

- IDENTIDAD:

La administración ha logrado establecer el sentido de pertenencia entre sus empleados, lo que potencia la identidad institucional.

3.1.1.4.6 ANÁLISIS DE LAS CARACTERÍSTICAS DE LA ORGANIZACIÓN

Debido al tamaño de su estructura y uso de tecnologías, la institución ha logrado eficiencia y economía en varios de sus aspectos organizacionales y de desarrollo de actividades; lo anterior

le permite adecuarse con mayor facilidad a los retos que la globalización y apertura de nuevos mercados le imponen, pero el aumento de la carga de actividades a su vez provoca una disminución en la efectividad del logro de todas las metas, debido a la sobrecarga de trabajo que pesa sobre sus empleados y directivos; además, el mayor uso de tecnologías abre espacios a los riesgos propios del uso de las mismas.

3.1.1.4.7 DESARROLLO DEL TALENTO HUMANO

Para la identificación de las áreas a mejorar y/o actualizar referente al recurso humano de la institución, la administración efectúa evaluaciones semestrales a todo el personal. Con la evaluación semestral realizada identifican y planifican las necesidades de capacitación por área y se asignan recursos para ello.

Dicho proceso ha sido afectado últimamente por la baja en los niveles de ingresos, por lo que la administración ha optado en la medida de lo posible de capacitar al personal internamente y haciendo mayor uso de mecanismos como boletines electrónicos vía email y suscripciones a revistas web.

3.1.1.4.8 SISTEMAS DE INFORMACIÓN

Se cuenta con sistemas de información destinados a gestionar la información referente a transacciones de la institución ó sistemas de procesamiento de transacciones, entre ellos se encuentran los implantados para gestionar:

- Contabilidad gubernamental
- Saldos bancarios
- Niveles de inventarios
- Cuentas por pagar
- Cuentas por cobrar
- Procesos de compras

- Papeles de trabajo de auditoría
- Recursos humanos
- Facturación

3.1.1.5 RESULTADO DE LA AUDITORÍA

Como resultado de la ejecución de los procedimientos incluidos en los programa de auditoría, elaborados en la planeación, se pretende proveer a la Corte de Cuentas de la República, y a la Junta Directiva del Instituto del Café, un informe de auditoría que permita:

- Retroalimentar al Instituto del Café en forma oportuna para que se corrijan las deficiencias identificadas y se tomen decisiones adecuadas, que garanticen el cumplimiento de las Leyes, Reglamentos, Normas y Procedimientos que regulan tal dependencia.
- Establecer las causas y efectos de las deficiencias identificadas y recomendar alternativas de solución.

3.1.1.6 FUNDAMENTO DE LA AUDITORÍA

La auditoría se realizará según lo establecido en las Normas de Auditoría Gubernamental emitidas por la Corte de Cuentas de la República.

Además de los objetivos de alto nivel que se encuentran en COBIT, relacionados a:

- Adquirir e implantar: Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como la implementación e integración en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio.
- Entregar y dar soporte: Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la

continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales.

3.1.1.7 RESPONSABLES DE LA AUDITORÍA

Supervisor:

- Licenciado Alexis Guillermo Rivera

Auditores:

- Licenciada Ana Claudia Serrano Gaitán
- Licenciada Marina Raquel Pérez Méndez

El personal clave del Instituto del Café, que será contactado durante el proceso de la auditoría para la obtención de información, es el siguiente:

Gerente de Informática:

- Ing. José Arturo Erazo

Encargado de soporte técnico:

- Lic. Jaime Adalberto Rivas

Encargada de mantenimiento de hardware:

- Licenciada Lisseth Isabel Ramos

Gerente Financiero

- Master Rodrigo Alberto Castro

3.1.1.8 CRONOGRAMA

El cronograma de actividades, contiene con detalle el proceso de auditoría. (Ver anexo 2)

3.1.1.9 PRESUPUESTO DE RECURSOS

Presupuesto de recursos asignados a la auditoría:

Presupuesto de recursos
Tabla número 1

Tiempo y Costo Proyectados 6 semanas (22 días hábiles: Del 1 de abril al 08 de mayo de 2009)				
Audidores	Participación	Tiempo (Hrs.)	Costo/Hora	Costo Total
Lic. Alexis Guillermo Rivera	30%	52	\$ 7.50	\$ 390.00
Lic. Ana Claudia Serrano Gaitán	35%	62	\$ 4.92	\$ 305.00
Lic. Marina Raquel Pérez Méndez	35%	62	\$ 4.92	\$ 305.00
Costo Total de la Auditoría				\$ 1,000.00

3.1.2 ANÁLISIS GENERAL

3.1.2.1 OBJETIVOS

Los objetivos planteados por la administración se encuentran definidos de la siguiente manera:

- Brindar servicios de certificación de café
- Levantar estadísticas de las diferentes actividades de comercialización de café
- Exponer en el interior y el exterior los valores agregados que posee el café salvadoreño
- Capacitar a los diferentes actores de la industria en las técnicas de tostado, barismo y catación
- Facilitar y proveer acceso al crédito a los productores de café

3.1.2.2 METAS

Las metas planteadas en base a los objetivos establecidos son las siguientes:

Metas
Tabla número 2

Productos	Unidad de medida	Trimestres				Anual
		1	2	3	4	
Certificaciones de café	Certificación	63	74	51	45	233
Estadísticas	Informe	3	-	1	-	4
Participaciones en ferias	Eventos	2	3	1	1	7
Capacitaciones	Capacitados	139	115	92	73	419
Créditos otorgados	Desembolsos	354	125	473	389	1,341

3.1.2.3 PROCESOS Y ORGANIZACIÓN

De acuerdo al Manual de procesos y procedimientos, los que se realizan en la institución son:

a) PROCESO DE CERTIFICACIÓN DE CAFÉ

Procedimientos incluidos:

- Recepción de solicitud de certificación
- Verificación de pago de certificación solicitada
- Asignación de técnico verificador a caso específico
- Programación de visita por parte de técnico asignado
- Realización de visita programada
- Elaboración de informe de resultados por visita realizada
- Emisión de certificado con resultado de verificación

b) PROCESO DE LEVANTAMIENTO DE ESTADÍSTICAS

Procedimientos incluidos:

- Recuperación de datos a utilizarse desde bases de la institución
- Establecimiento de estadísticas

- Publicación de estadísticas

c) PROCESO DE SELECCIÓN DE VÍAS DE MERCADEO

Procedimientos incluidos:

- Confirmación de ferias nacionales e internacionales a realizarse relacionadas con el sector
- Identificación de mercados de interés para el sector
- Selección de ferias en las cuales se participará
- Reservación de participación en ferias de interés seleccionadas
- Conformación de equipo de técnicos a participar en feria
- Desarrollo de mensaje país a transmitir en feria seleccionada
- Desarrollo de participación en feria
- Elaboración y presentación de informe de logros obtenidos

d) PROCESO DE CAPACITACIONES

Procedimientos incluidos:

- Establecimiento de programación anual de capacitaciones y su contenido
- Recepción de solicitud y pago de derechos de participación en capacitación programada
- Realización de capacitación
- Elaboración y presentación de informe de logros obtenidos

e) PROCESOS DE OTORGAMIENTO DE CRÉDITOS

Procedimientos incluidos:

- Recepción de solicitudes de créditos
- Asignación de técnico analista de solicitud
- Aceptación o denegación de solicitud de crédito
- Aseguramiento del crédito
- Desembolso de crédito

f) PROCESOS DE SELECCIÓN DE RECURSOS HUMANOS

Procedimientos incluidos:

- Identificación de necesidades de contratación
- Publicación de plazas vacantes
- Recepción de aplicaciones
- Discriminación de aplicaciones
- Evaluaciones a los aspirantes
- Selección de aspirante
- Notificación de selección realizada
- Inducción de personal

g) PROCESO DE TESORERÍA

Procedimientos incluidos:

- Recepción de pagos
- Transferencias entre cuentas
- Pago de bienes y servicios
- Cobranza
- Mantenimiento de aplicativo SAFI

h) PROCESO DE CONTABILIDAD

Procedimientos incluidos:

- Recepción de documentos probatorios
- Codificación de documentos
- Mantenimiento aplicativo SAFI
- Emisión de reportes financieros
- Presentación y envío de reportes financieros a partes involucradas

i) PROCESO DE COMPRAS

Procedimientos incluidos:

- Elaboración de plan anual de compras
- Recepción de solicitudes de gestión de compras
- Gestión de compras
- Recepción de bienes y servicios contratados
- Mantenimiento sistema COMPRAS

3.1.2.4 FUNCIONAMIENTO

El funcionamiento se define en las siguientes funciones:

a) FUNCIÓN PRINCIPAL:

- Prestar servicios diferenciados al sector caficultor salvadoreño

b) FUNCIONES ESPECÍFICAS:

- Representación del sector y del país ante gobiernos y organismos internacionales
- Mercadeo del café salvadoreño
- Financiamiento a los actores de la cadena productiva del café

3.1.2.5 ENTORNO

El entorno se compone de factores industriales, económicos, sociales, políticos, ecológicos, y otros relacionados con la institución.

3.1.2.5.1 INDUSTRIALES

En El Salvador existen aproximadamente 23,000 productores, de los cuales el 87% son pequeños productores, con propiedades menores de 25 manzanas y representan el 21% del total de la producción nacional.

Existen aproximadamente 80 exportadores autorizados y activos, los cuales se presentan estratificados por volumen de exportaciones de café por cosecha. Según registros, existen más de 215 beneficiadores pergamineros en El Salvador. En la torrefacción, unos 50 tostadores nacionales de café se encuentran registrados, entre pequeños, medianos y grandes.

En su proceso de transformación, el café recorre diferentes fases antes de llegar al consumidor. En primer lugar, la cadena comprende las actividades agrícolas que se realizan en las fincas, incluyendo la recolección de la cosecha; posteriormente sigue el beneficiado y secado del café. De esta última actividad, ya sea que se realice con máquina o al sol, resulta el denominado café pergamino, que es el producto final de esta fase productiva.

En seguida, el café pergamino seco se traslada a la trilla, donde se procede a eliminar la cubierta o pergamino que lo protege, convirtiéndolo así en café verde, para después clasificarlo según su tamaño y calidad de grano.

El café verde se destina principalmente para la exportación. Por otro lado, una pequeña parte de la producción nacional es orientada al consumo interno, la cual sigue las etapas finales del proceso productivo de la cadena: tostado, molido y empaçado. En el caso del café molido (ya sea cafeinado o descafeinado), después de un proceso de torrefacción, molienda, evaporación y aglomeración, se producen extractos y cafés solubles, bien sea para el consumo directo o para incorporarlo como esencia en otras bebidas, helados u otros productos alimenticios.

Además de su consumo final para el mercado interno e internacional, el café también puede utilizarse como insumo para la industria. En este caso el grano es sometido a otro proceso para extraerle la cafeína, la cual es utilizada por empresas de refrescos y farmacéuticas, aunque en una proporción mucho menor que para su consumo directo, y sin recurrirse a la torrefacción.

3.1.2.5.2 ECONÓMICOS

Para el país, el café continúa siendo una actividad de importancia estratégica para la sostenibilidad económica. A pesar de una pérdida relativa en el impacto dentro de la economía, favorecida por la evolución de El Salvador hacia una de las economías más libres del mundo que ha permitido la reconversión de los sectores productivos.

3.1.2.5.3 SOCIALES

La generación de empleo por parte del rubro cafetalero constituye, además, una de las principales contribuciones de este sector para mantener la estabilidad social y política del país, considerando que en condiciones normales el empleo del sector cafetalero representa cerca del 6% de la Población Económicamente Activa (PEA); a esto se le añade que la inversión que genera la propia actividad favorece el desarrollo de microempresas que contribuyen a reducir la migración de pobladores rurales hacia la ciudad y los problemas que ello implica.

3.1.2.5.4 POLÍTICOS

En la actualidad el entorno político estuvo liderado por las elecciones presidenciales del 15 de marzo de 2009, donde la oposición resultó ganadora, lo que provoca una incertidumbre acerca de los cambios que experimentará la estructura institucional del país después de la toma de posesión del nuevo gobierno el 1 de junio de 2009.

3.1.2.5.5 ECOLÓGICOS

El café es vital desde el punto de vista ecológico. Las externalidades positivas del café, aunque muy importantes, no están por el momento remuneradas ni interna ni externamente. Mientras varios países productores han cambiado sus tecnologías a cultivos de café bajo sol abierto, que utilizan fuertes cantidades de químicos, El Salvador ha mantenido su tradicional cultivo de café

bajo sombra. Bajo este abanico de árboles de sombra se encuentran cafés arábigos madurados lentamente, de los que se obtiene una bebida excepcional. Los últimos estudios en el campo revelan que El Salvador cuenta con un 2% de bosque primarios; las plantaciones de café representan aproximadamente un 9% de bosque adicional debido al uso intensivo de sombra que poseen los cafetales, el 95% de los cafetales son cultivados bajo sombra, más importante aún casi la totalidad de los bosques primarios o cerrados (alrededor del 80%) se encuentran rodeados por cafetales, funcionando como área de mitigación del impacto que pudiesen recibir dichos bosques del exterior. Si los cafetales desaparecen los bosques primarios estarían en peligro latente de desaparecer.

El bosque cafetalero tiene para el país una gran importancia hidrológica, además de proporcionar otros servicios ambientales como: servir como fuente de energía, capturar carbono y conservar la biodiversidad.

3.1.2.6 MARCO JURÍDICO

El marco jurídico de la institución es:

- Ley del Instituto del Café y su Reglamento
- Ley de la Corte de Cuentas de la República
- Código Tributario y su Reglamento de Aplicación
- Ley de Impuesto sobre la Renta y su Reglamento
- Ley de Ética Gubernamental y su Reglamento
- Normas de Auditoría Gubernamental
- Ley de la Administración Financiera del Estado
- Ley de Adquisiciones y Contrataciones de la Administración Pública

3.1.2.7 NORMATIVA INTERNA

La normativa interna de la institución es:

- Acuerdos de Junta Directiva
- Normas Técnicas de Control Interno Específicas

3.1.2.8 INDICADORES DE GESTIÓN

El seguimiento de la gestión institucional se realiza trimestralmente para evaluar el cumplimiento de las actividades programadas anualmente, en desarrollo de los objetivos de la institución.

Los indicadores de gestión utilizados para medir los resultados de las metas planteadas son los siguientes:

- Numero de certificaciones de café emitidas
- Cantidad de informes de estadísticas elaborados
- Total de participaciones en ferias
- Numero de personal capacitado
- Total de desembolsos de créditos otorgados

3.1.2.9 PROVEEDORES

Los principales proveedores de bienes y servicios del Instituto del Café son:

- Agua potable, S.A.
- Energía Eléctrica, S.A.
- Comunicaciones, S.A.
- Internet, S.A. de C.V.
- Librería y papelería, S.A. de C.V.
- Equipo Electrónico, S.A. de C.V.
- Mantenimientos, S.A. de C.V.

3.1.3 EXAMEN PRELIMINAR

3.1.3.1 ACTIVIDADES Y CONTROLES CLAVES

3.1.3.1.1 ACTIVIDADES CLAVES

La administración mantiene diversas actividades de supervisión y control, entre ellas se encuentran:

- Protección de la información
- Administración de tecnología contra malware
- Asignación de privilegios
- Administración de perfiles de usuarios y accesos
- Captura, procesamiento y salida de datos

3.1.3.1.2 CONTROLES CLAVES

Los controles claves identificados son:

- Control de intrusos
- Control de modificaciones al software
- Controles de adiciones, cambios y eliminaciones a la información
- Controles sobre derechos

3.1.3.2 ASUNTOS DE POTENCIAL IMPORTANCIA

Los asuntos de potencial importancia determinados son:

- Procesamiento de datos
- Seguridad lógica

3.1.3.3 RIESGOS

Para el área de gerencia de informática, objeto de evaluación se han identificado los siguientes riesgos:

- Accesos no autorizados al sistema
- Descargas de software malicioso desde la *world wide web*
- Pérdida de datos
- Inadecuado diseño de pistas de auditoría
- Falta de disponibilidad de la información
- Falta de evaluaciones al software
- Realización incompleta de respaldos
- Inadecuada asignación de accesos y privilegios
- Inadecuado borrado de información sensible

3.1.4 COMPRENSIÓN DEL CONTROL INTERNO

3.1.4.1 AMBIENTE DE CONTROL

El ambiente de control del Instituto del Café presenta las características que se listan:

3.1.4.1.1 INTEGRIDAD Y VALORES ÉTICOS

En cuanto a la integridad y valores éticos, la institución en general y sus empleados en particular, están obligados legalmente al cumplimiento de la Ley de Ética Gubernamental, cuyo objeto principal es normar la conducta de los servidores públicos respecto a los principios éticos que han de regir su desempeño en la administración pública, a fin de garantizar y promover el más alto grado de honestidad en el ejercicio de las funciones del Estado. En el Artículo 4 de la Ley se establecen 14 principios éticos, que los servidores públicos deben cumplir:

- Supremacía del interés público
- Probidad
- No discriminación
- Imparcialidad
- Justicia
- Transparencia
- Confidencialidad
- Responsabilidad
- Disciplina
- Legalidad
- Lealtad
- Decoro
- Eficiencia y eficacia
- Rendición de cuentas

3.1.4.1.2 COMPETENCIA DEL PERSONAL

Respecto a la competencia del personal, a continuación se detallan las jefaturas (nombres y profesiones) de la entidad:

Competencia del Personal
Tabla número 3

Nombre	Profesión	Jefatura
Alexis Guillermo Rivera	Lic. Contaduría Pública	Unidad de auditoría interna
Rodrigo Alberto Castro	Msc Finanzas	Gerencia financiera
José Arturo Erazo	Ing. Sistemas de Informáticos	Gerencia informática
Eduardo Girón Salazar	Lic. Economía	Gerencia de exportaciones
Humberto Ramírez	Ing. Industrial	Gerencia de capacitaciones
William Rodríguez	Ing. Agrónomo	Gerencia de catación

3.1.4.1.3 FILOSOFÍA Y ESTILO DE LA ADMINISTRACIÓN

Con relación a la filosofía y el estilo de administración, las autoridades superiores tienen una actitud de mejorar los controles existentes y de implementar las recomendaciones de auditoría Interna contenidas en los informes procedentes de las evaluaciones realizadas.

3.1.4.1.4 ESTRUCTURA ORGANIZACIONAL

La estructura organizacional de la entidad, documentalmente, es adecuada puesto que existe la segregación de funciones incompatibles y la definición de funciones y procedimientos específicos para sus dependencias.

3.1.4.1.5 ASIGNACIÓN DE AUTORIDAD Y RESPONSABILIDAD

La asignación de autoridad y responsabilidad está a cargo del Presidente de la Junta Directiva. Toma en cuenta las opiniones de los jefes de cada área de la institución, y en base a ello las decisiones correspondientes.

3.1.4.1.6 POLÍTICAS Y PRÁCTICAS DE GESTIÓN DE RECURSOS HUMANOS

Las políticas y prácticas de gestión de recursos humanos están centralizadas en el Departamento de Recursos Humanos las que deben ser acatadas por todos los empleados de la Institución.

3.1.4.1.7 UNIDAD DE AUDITORÍA INTERNA

La unidad de auditoría interna del Instituto del Café, adicional a lo mencionado en los numerales del 3.1.4.1.1 al 3.1.4.1.7, respecto a la Ley de Ética en general y a las normas de ética y conducta en particular, en el Capítulo I de las Normas Técnicas de Control Interno Específicas de

la entidad se han redactado las Normas Relativas al Ambiente de Control. Tales normas están contenidas en los artículos del 7 al 33 y se han clasificado en las siguientes secciones:

- Integridad y valores éticos
- Compromiso con la competencia
- Estilo de gestión
- Estructura organizacional
- Definición de áreas de autoridad, responsabilidad y relaciones de jerarquía
- Políticas y prácticas para la administración del capital humano
- Unidad de auditoría interna

3.1.4.2 VALORACIÓN DE RIESGOS

La valoración de riesgos se ha efectuado de manera general para el Instituto del Café, en el Capítulo II de las Normas. Los artículos que las contienen son del 34 al 47. La clasificación de éstas Normas se ha hecho en las siguientes secciones:

- Definición de objetivos
- Planificación participativa
- Identificación de riesgos
- Análisis de riesgos identificados
- Gestión de riesgos

3.1.4.2.1 CAMBIOS EN EL ENTORNO

Los cambios han formulado, en términos generales, un resultado deseable para la institución, ya que se proyectan con nuevas metas o redefinición de algunas de ellas, lo que le permite estar acorde a las necesidades de los tiempos actuales tan dinámicos.

Para ello se efectuó un examen exhaustivo de la situación actual, un análisis del entorno y de las características internas significativas, y una evaluación de las disposiciones legales, así como de

otros factores relevantes; todo este esfuerzo se tradujo en la definición clara de la misión, visión, objetivos generales y las acciones globales a ejecutar.

3.1.4.2.2 REDEFINICIÓN DE LA POLÍTICA INSTITUCIONAL

Son los procedimientos que permitieron obtener una seguridad razonable del cumplimiento de las directrices administrativas. Tales actividades ayudaron a asegurar que se están tomando las acciones necesarias para enfrentar los factores de riesgo implicados en el logro de los objetivos de la Institución.

3.1.4.2.3 REORGANIZACIONES O REESTRUCTURACIONES

Debe recordarse que los objetivos organizacionales y por ende los de las unidades cambiaron, lo cual implicó que la estructura orgánica debió variar para prestar, con eficiencia y eficacia, los servicios que le permiten cumplir con su cometido institucional. De igual manera, el repunte en el uso de las nuevas tecnologías ha logrado mejorar el desempeño y que al ser adquiridos implicaron un cambio en las estructuras.

3.1.4.2.4 INGRESO DE NUEVOS EMPLEADOS O ROTACIÓN

La administración tiene como política la rotación del personal, con el objeto que los empleados no tengan permanentemente control de partes específicas de una transacción ni de los recursos utilizados en ellas, lo que le brinda a la institución la seguridad relativa de que no se presentarán situaciones irregulares en relación con tales transacciones y recursos.

Asimismo, suministra parámetros de eficiencia mediante la comparación del desempeño de empleados distintos en la misma actividad, lo que permite descubrir más claramente las habilidades particulares de cada uno y asignarles las tareas que mejor desempeñan.

Lo anterior en conjunto al ingreso de nuevos empleados, constituye un mecanismo de capacitación pues al desarrollar actividades diferentes, tanto como un procedimiento normal o en el caso de sustituir empleados que se encuentran de vacaciones o incapacitados, los servidores entran en contacto con las diversas etapas de los procesos organizacionales, y así llegan a comprender mejor su participación en el logro de los objetivos.

Sin embargo, la administración debiera tener presente que la rotación de personal se puede llevar a cabo cuando la naturaleza de las funciones permita efectuarla, así como las disposiciones jurídicas y técnicas vigentes.

3.1.4.2.5 NUEVOS SISTEMAS Y PROCEDIMIENTOS

Los controles generales se aplican a todos los sistemas de información que posee la institución, ya sea en ambientes de mainframes, minicomputadores, redes y usuario final.

Incluyen para toda la Institución, normas y procedimientos que definen claramente la planeación, administración y control sobre:

- Las operaciones del centro de datos
- La adquisición, implementación y mantenimiento del software del sistema
- La seguridad de acceso
- El desarrollo y mantenimiento de aplicaciones, ya sean existentes o nuevos

3.1.4.2.6 ACELERACIÓN DEL CRECIMIENTO

De acuerdo al reporte de la Organización Internacional del Café para 2006, algunos países productores del grano han mejorado el consumo de café en su mercado interno.

Los salvadoreños han pasado de consumir 1.44 kg en 2002 a 1.85 kilogramos per cápita de café en 2006. A partir del análisis realizado en este diagnóstico y la utilización de los resultados del VI Censo de Población de 2007, nos permitió estimar un consumo per cápita de 1.98 kg de café

para El Salvador, favorecidos en este indicador por la nueva población reportada. Otros países productores como Brasil en ese periodo han pasado de consumir 4.59 kg a 5.1 kg; o los costarricenses, que pasaron de 3.62 kg a 4.77 kg.

3.1.4.2.7 NUEVOS PRODUCTOS, SERVICIOS, ACTIVIDADES O FUNCIONES

La oferta de café en el país se ha visto fortalecida en los últimos años por el surgimiento de cafeterías especializadas en la preparación de cafés de calidad al consumidor nacional. Estas cafeterías presentan locales muy atractivos al cliente, además de contar con equipo profesional para la preparación de cafés y con una amplia gama de bebidas a base de este grano y de personal muy bien entrenado para la preparación de la taza de café.

3.1.4.2.8 CAMBIOS EN LA APLICACIÓN DE LOS PRINCIPIOS CONTABLES

Hasta la fecha no existen cambios en la aplicación de los principios contables, dichos cambios son dictados por la Dirección General de Contabilidad Gubernamental, dependencia del Ministerio de Hacienda.

3.1.4.3 ACTIVIDADES DE CONTROL

Las Actividades de Control se han redactado de manera general para la institución en el Capítulo III de las NTCIE, Los artículos que las contienen son del 48 al 87.

En términos generales, las Normas agrupadas en este componente responsabilizan a las dependencias sobre el cumplimiento de los procedimientos contenidos cada uno en los Manuales de Organización y de Normas y Procedimientos existentes.

La clasificación de estas Normas se ha hecho en las siguientes secciones:

- Documentación, actualización y divulgación de políticas y procedimientos
- Políticas y procedimientos de autorización y aprobación

- Políticas y procedimientos sobre activos
- Uso de activos
- Adquisición de activos
- Disposición de activos
- Políticas de carácter financiero
- Políticas y procedimientos sobre diseño y uso de documentos y registros
- Políticas para el otorgamiento de prestaciones económicas
- Políticas relacionadas al recurso humano

3.1.4.3.1 REALIZACIÓN DE REVISIONES

La institución realiza la revisión periódica para valorar la calidad del funcionamiento de la institución en el tiempo y asegurar razonablemente que los hallazgos y los resultados de otras revisiones se atiendan con prontitud.

3.1.4.3.2 PROCESOS DE INFORMACIÓN

Los procesos de información se han establecido, para que la administración de la institución identifique, registre y comunique información relacionada con actividades, ya sean eventos internos o externos relevantes.

El proceso de información sirve, entre otros fines para:

- Tomar decisiones a todos los niveles
- Evaluar el desempeño de la institución, de sus programas
- Proyectos, procesos, actividades, operaciones
- Rendir cuenta de la gestión

El proceso de información se diseñó para apoyar la misión, políticas, estrategias y objetivos de la Institución, así mismo sustentará la formulación y supervisión de los planes anuales de trabajo,

con datos sobre los aspectos operacionales específicos y su comparación con las metas establecidas.

3.1.4.3.3 SEGREGACIÓN DE FUNCIONES

La segregación de funciones se da en todos los niveles de la institución; incluyen un rango de actividades tan diversas como aprobaciones y esta identificó el conocimiento y las habilidades que son necesarias para todas y cada una las funciones que se deben llevar a cabo para el mejor cumplimiento. Por ello, no solo se contrata el personal que posea el nivel de preparación y experiencia que se ajuste a los requisitos del puesto, sino también se proporciona la capacitación y adiestramiento necesarios.

Se incluyen aquellas autorizaciones y aprobaciones que se relacionan con todos los procesos institucionales, sean centrales o de soporte, separando y distribuyendo entre los diferentes cargos, aquellas funciones que, si se concentraran en una misma persona, pueden comprometer el equilibrio y eficacia del control interno.

Igualmente, las diversas fases que integran el proceso, transacción u operación, se distribuyen, entre los diversos funcionarios y unidades de la institución, de tal manera que el control total de su desarrollo está totalmente separado.

3.1.4.4 INFORMACIÓN Y COMUNICACIÓN

Las Normas relativas a la Información y Comunicación se han redactado de manera general para la entidad en el Capítulo IV de las NTCIE, Los artículos que las contienen son del 88 al 101.

En términos generales, las Normas agrupadas en este componente se refieren a la administración de la información institucional y de los sistemas de información que la procesan y almacenan.

La clasificación de estas Normas se ha hecho en las siguientes secciones:

- Adecuación de los sistemas de información y comunicación
- Características de la información
- Archivo institucional

3.1.4.5 MONITOREO

Las Normas relativas al Monitoreo se han redactado de manera general para la entidad en el Capítulo V de las NTCIE, Los artículos que las contienen son del 102 al 109.

En términos generales, las Normas agrupadas en este componente especifican las diferentes formas de vigilar el cumplimiento de los controles institucionales y quiénes son los responsables de tal actividad.

La clasificación de estas normas se ha hecho en las siguientes secciones:

- Monitoreo sobre la marcha
- Monitoreo mediante auto evaluaciones del sistema de control interno
- Evaluaciones separadas
- Control externo posterior
- Comunicación de los resultados del monitoreo

3.1.5 DETERMINACIÓN DE RIESGOS

3.1.5.1 PARÁMETROS DE EVALUACIÓN DEL RIESGO

La administración ha elaborado las Normas Técnicas de Control Interno Específicas de la Institución, y parte la elaboración de dichas normas es la determinación de riesgos, lo cual permitirá la más adecuada gestión de los mismos.

La guía utilizada para la elaboración de las normas mencionadas se encuentra en el Anexo No. 2 de la circular externa C. de C. No. 2/2005 emitida por la Corte de Cuentas de la República, titulada: Lineamientos específicos para la elaboración del Proyecto de Normas Específicas para el Sistema de Control Interno de cada entidad del Sector Público; en ellas se encuentra específicamente la Matriz de Riesgo, cuyo formato sugerido se desarrolla en el siguiente punto.

3.1.5.2 MATRIZ DE RIESGOS

El Instituto del Café para el logro de sus fines ha establecido una serie de objetivos básicos, los cuales han sido asignados a cada una de las unidades de conformidad a sus funciones. Dentro de estos objetivos, a la Gerencia de Informática Institucional se le ha asignado entre otros, el siguiente: Mantener una adecuada seguridad lógica de los sistemas información computarizados.

Para el logro del objetivo anterior, se han identificado los siguientes riesgos:

- Accesos no autorizados al sistema
- Descargas de software malicioso desde la *world wide web*
- Pérdida de datos
- Inadecuado diseño de pistas de auditoría
- Falta de disponibilidad de la información
- Falta de evaluaciones al software
- Realización incompleta de respaldos
- Inadecuada asignación de accesos y privilegios
- Inadecuada protección y borrado de información sensible

Se ha elaborado una matriz de riesgo a efecto de identificar sus áreas críticas, mediante la aplicación de variables como el impacto que pueda causar el riesgo (entendiéndose por éste las debilidades y amenazas) en cuanto a logro de los objetivos y la frecuencia de que ocurran dentro de la Gerencia de Informática.

Al respecto el Instituto de Café a través de su diagnóstico determinó la matriz siguiente:

El cálculo matemático del riesgo se realiza por medio de la ecuación siguiente: $ER = F \times I$

Donde:

ER= Exposición al riesgo.

F= Frecuencia de que el riesgo se concrete en el año.

I= Impacto reflejado en pérdida estimada, para cada caso en que el riesgo se concrete.

Matriz de Riesgos
Tabla número 4

Unidad Organizacional	Análisis de Riesgos			Exposición al Riesgo
	Riesgos	Frecuencia	Impacto	
Gerencia de Informática	Accesos no autorizados al sistema	1	3	3
	Descargas de software malicioso desde la <i>world wide web</i>	3	3	9
	Pérdida de datos	1	3	3
	Inadecuado diseño de pistas de auditoría	1	1	1
	Falta de disponibilidad de la información	2	2	4
	Falta de evaluaciones al software	3	2	6
	Realización incompleta de respaldos	3	3	9
	Inadecuada asignación de accesos y privilegios	3	3	9
	Inadecuada protección y borrado de información sensible	3	3	9

Frecuencia	Impacto
1 = Baja	1 = Bajo
2 = Moderada	2 = Moderado
3 = Alta	3 = Alto

INTERPRETACIÓN DE TABLA ANTERIOR:

El producto de la frecuencia por el impacto, nos determina la exposición al riesgo, lo cual implica que a mayor frecuencia e impacto es mayor la exposición al riesgo, dando como resultado, factores de riesgos más importantes que deben ser administrados o manejados a través del establecimiento de actividades de control que los elimine o minimice.

3.1.5.3 PROGRAMAS DE AUDITORÍA

Se han diseñado 3 programas de auditoría a la medida para auditar el Sistema Cuentas por Cobrar del Instituto del Café, lo cuales son:

- Controles generales
- Controles de datos
- Controles de aplicación

Cada uno de estos programas contiene procedimientos de auditoría, agrupados por elemento, según los objetivos perseguidos en cada uno de ellos, es así que en suma se tienen 28 elementos a evaluar, los cuales se describen de manera amplia en el numeral 3.1.1.3. Alcance del Trabajo. (Ver anexo 3)

3.2 EJECUCIÓN

La ejecución de auditoría comprende la realización de pruebas, la evaluación de controles y la recolección de evidencia suficiente, competente y confiable, para determinar si los asuntos de potencial importancia identificados, realmente son importantes para efectos de su inclusión en el informe final.

La fase de examen incluye lo siguiente:

- Realización de pruebas y obtención de evidencia
- Preparación y referenciación de PT

- Desarrollo de hallazgos y sus atributos
- Comunicación preliminar de resultados
- Preparación del borrador del informe

3.2.1 REALIZACIÓN DE PRUEBAS Y OBTENCIÓN DE EVIDENCIA

Los programas de auditoría establecen en sus procedimientos, las labores y las pruebas que deben realizarse. Estarán estructurados de manera que faciliten el desarrollo metódico del examen.

El auditor deberá preparar papeles de trabajo que sean suficientemente completos y detallados para proporcionar una comprensión global de la auditoría. La forma y contenido de los papeles de trabajo son afectadas por asuntos como:

- La naturaleza del trabajo
- La forma del dictamen del auditor
- La naturaleza y complejidad de la institución
- La naturaleza y condición de los sistemas de contabilidad y control interno de la institución
- Las necesidades en las circunstancias particulares de dirección, supervisión, y revisión del trabajo desempeñado por los auditores
- Metodología y tecnología de auditoría específicas usadas en el curso de la auditoría

La evidencia constituye la comprobación de los hechos, con documentación suficiente, competente y pertinente que sustenta las conclusiones del auditor. Es la información específica obtenida durante la labor de evaluación del control interno de los sistemas de información computarizado a través de técnicas de inspección, observación, investigación y confirmación, cómputo y procedimientos analíticos.

La actividad de evaluación del control interno de los sistemas de información computarizado se dedica a la obtención de la evidencia, dado que ésta provee una base racional para la formulación de juicios u opiniones. El término evidencia incluye documentos, fotografías, análisis de hechos efectuados por el auditor y en general, todo material usado para determinar si los criterios son alcanzados.

3.2.2 PREPARACIÓN Y REFERENCIACIÓN DE PAPELES DE TRABAJO

Como punto clave de control, el supervisor se encargará de revisar los papeles de trabajo para establecer si lo escrito en cada informe se encuentra debidamente sustentado y evidenciado, y además tenga una correcta referenciación. (Ver anexo 4)

3.2.3 DESARROLLO DE HALLAZGOS Y SUS ATRIBUTOS

El hallazgo se origina cuando al comparar la normativa incumplida (deber ser) con la observación (deficiencia señalada por los auditores) existe diferencia o incumplimiento.

Para el desarrollo del hallazgo se utilizará el formato "Hallazgo de Auditoría", una vez desarrollado, el auditor, lo entregará al supervisor, para su revisión e incorporación al borrador del informe de auditoría.

Establecido el hallazgo, se identifica la causa (el asunto o asuntos que originan el problema o situación) y el efecto (las consecuencias negativas que generan la situación o situaciones encontradas).

Es importante identificar los aspectos positivos o fortalezas institucionales, de las cuales se debe obtener la evidencia que las sustenten, ya que deberán reportarse con el propósito de balancear el efecto poco constructivo de un informe eminentemente negativo.

3.2.4 COMUNICACIÓN PRELIMINAR DE RESULTADOS

La comunicación de resultados a las personas relacionadas con las presuntas deficiencias, se realiza por escrito, en la medida en que se identifican dichas deficiencias, en el transcurso de la evaluación del control interno de los sistemas de información computarizado.

Con el propósito de garantizar su derecho de defensa, confirmar la presunta deficiencia y que todas las personas responsables de la actividad observada, estén enteradas de los resultados, para que tengan oportunidad de participar activamente en la presentación de evidencia para desvirtuar, modificar o confirmar las presuntas deficiencias y/o dar las explicaciones correspondientes, en beneficio de la objetividad de los resultados. Cuando se trate de ex funcionarios o ex empleados, la comunicación será en forma personal o por correo certificado, entregándola en su domicilio o lugar de trabajo.

Si en el transcurso de la auditoría se identifican posibles ilícitos penales, según opinión escrita de la Dirección Jurídica, el supervisor elaborará un informe, agregando al mismo las condiciones encontradas y la evidencia sustentatoria, remitiéndolo al Director de Auditoría correspondiente, quien lo suscribirá y lo comunicará de inmediato al Presidente de la Corte de la República, para los efectos legales consiguientes.

3.2.5 PREPARACIÓN DEL BORRADOR DE INFORME

En esta fase el supervisor deberá finalizar, con el apoyo de los auditores, la preparación del borrador de informe y resumen ejecutivo, los cuales serán revisados detalladamente por el Supervisor, en los siguientes aspectos: Resultados con su evidencia, ortografía, redacción, cuadros y gráficos.

3.3 INFORME

Las Normas de Auditoría Gubernamental emitidas por la Corte, en lo referente al informe y comunicación de resultados de la auditoría, establecen lo siguiente:

El equipo de auditoría gubernamental deberá preparar, editar y entregar un informe final de auditoría operacional, el cual debe ser oportuno, completo, exacto, objetivo y convincente. Asimismo el informe debe ser claro y conciso para que sea comprensible para los interesados, principalmente para aquellos que deben tomar decisiones respecto de las recomendaciones emitidas. La fase del informe incluye:

- Introducción
- Objetivos de la auditoría
- Alcance de la auditoría
- Limitaciones en el alcance de la auditoría
- Logros y/o realizaciones importantes de la administración
- Resultados
- Conclusiones
- Recomendaciones

3.3.1 INTRODUCCIÓN

Debe contener una descripción los fundamentos legales para la evaluación del control interno de los sistemas de información computarizados. El informe debe ser elaborado una vez que el Comité Técnico de Auditoría y los funcionarios de la entidad auditada hayan hecho las observaciones correspondientes.

Los informes de las auditorías, serán dirigidos a la máxima autoridad de la entidad auditada y deben incluir al menos:

- Resumen ejecutivo
- Informe de auditoría
- Fecha
- Incluir la leyenda Dios Unión Libertad
- Firma
- Identificación

3.3.2 OBJETIVOS DE LA AUDITORÍA

Los auditores deben exponer los objetivos por los que se llevó a cabo la evaluación del control interno de los sistemas de información computarizados. Expresar claramente los fines del informe implica normalmente indicar el asunto materia de la evaluación y el aspecto del desempeño examinado y, puesto que los resultados dependen de sus objetivos, los hallazgos y las conclusiones a que se han llegado.

3.3.3 ALCANCE DE LA AUDITORIA

El alcance deberá indicar la profundidad y cobertura del trabajo que se haya realizado para cumplir los objetivos de evaluación del control interno de los sistemas de información computarizados. Los auditores deben, en la medida que sea aplicable, establecer la relación que existe entre la muestra revisada y el universo, identificar la entidad, ubicación geográfica, especificar los tipos y fuentes de evidencias utilizados y explicar los problemas relacionados con la calidad u otros problemas relacionados con la evidencia.

3.3.4 LIMITACIONES EN EL ALCANCE DE LA AUDITORÍA

Dada las limitaciones de costo y de tiempo, no es factible examinar el 100%. Por lo tanto, es necesario examinar un porcentaje que sea representativo, y que permita al auditor llegar a una opinión.

Se debe incluir una referencia a las limitaciones impuestas al enfoque de la evaluación, debido a limitaciones inherentes a cualquier sistema de evaluación del control interno de los sistemas de información computarizados, pueden ocurrir errores o irregularidades y no ser detectados.

Además, la proyección de cualquier evaluación del control interno de los sistemas de información computarizados a períodos futuros, está sujeta al riesgo de que los procedimientos sean inadecuados, debido a cambios en las condiciones o a que la efectividad del diseño y operación de las políticas y procedimientos pueda deteriorarse.

3.3.5 LOGROS Y/O REALIZACIONES IMPORTANTES DE LA ADMINISTRACIÓN

Especialmente cuando las medidas adoptadas para mejorar un área pueden aplicarse en otras; los logros importantes de la administración que se han constatado durante la evaluación del control interno de los sistemas de información computarizados, comprendidos en el alcance de la evaluación y necesarios para cumplir sus objetivos, deben mencionarse en el informe, junto con las deficiencias detectadas.

Esa información será necesaria para presentar objetivamente la situación que han observado los auditores y para que el informe tenga el debido equilibrio. Además, el hecho que el informe mencione los logros puede conducir a propiciar que otros organismos gubernamentales que lean el informe adopten medidas para mejorar su desempeño.

3.3.6 RESULTADOS

En este apartado se debe de incluir los resultados del análisis del informe de evaluación del control interno de los sistemas de información computarizados, según sea el caso, incorporando las observaciones que los referidos informes contengan y estén sustentados con la respectiva evidencia.

Es posible que el auditor encuentre errores que por su materialidad pudiesen afectar, o que no tengan ningún impacto significativo. Si del análisis de dichos informes resulta que no existen observaciones que merezcan ser incorporadas, se hará mención de ello en este párrafo.

El informe debe describir sobre el sistema de control interno y el cumplimiento de leyes y reglamentos aplicables a la entidad sujeta a la evaluación del control interno de los sistemas de información computarizados, y presentar los resultados de esas pruebas, en los informes correspondientes.

El auditor debe informar sobre las irregularidades, actos ilegales y otros incumplimientos, condiciones reportables que deban informarse relacionadas con la evaluación del control interno de los sistemas de información computarizados, incluyendo debilidades materiales que tienen.

3.3.6.1 HALLAZGOS DE AUDITORÍA

El informe también incluirá los hallazgos significativos relacionados con la evaluación de las disposiciones legales y reglamentarias. El auditor desarrollará los hallazgos con todos sus atributos, los cuales deben constar en los papeles de trabajo y estar debidamente referenciados y documentados con la evidencia recopilada.

Los hallazgos en la auditoría, se definen como aquellos asuntos que llaman la atención del auditor, y que en su opinión, deben comunicarse, ya que representan deficiencias importantes que podrían afectar en forma negativa su capacidad para registrar, procesar, resumir y reportar información confiable y consistente.

Técnicamente surge un hallazgo, cuando al comparar la normativa incumplida (deber ser) con la observación (Deficiencia señalada por los auditores, lo que actualmente existe o se encuentra funcionando) existe diferencia.

Establecido el hallazgo, procedemos a su evaluación en términos de causa (Origen de la deficiencia) y efecto (Impacto cuantitativo o cualitativo ocasionado por la deficiencia señalada, o el impacto potencial que podría ocasionar la misma).

En este aspecto resulta de mucha utilidad precisar las causas y efectos, ya que al identificar las causas, el auditor tiene mayores elementos de juicio para proponer recomendaciones adecuadas. Cada hallazgo de evaluación del control interno de los sistemas de información computarizados, el auditor incluirá los comentarios, recopilados en las diversas fases, toda vez que estén relacionados con los hallazgos.

Los atributos de un hallazgo de auditoría son los siguientes:

- Título
- Condición
- Criterio
- Causa
- Efecto
- Recomendación
- Comentarios de la administración
- Comentarios de auditoría
- Grado de cumplimiento
- Conclusión

3.3.6.1.1 TÍTULO

Se agregará título para identificar los hallazgos, su redacción será breve y denotará la observación, los cuales serán enumerados correlativamente en el informe respectivo.

3.3.6.1.2 CONDICIÓN

Es la deficiencia comprobada y sustentada en los papeles de trabajo, evidencias suficientes y competentes. Cuyas características son:

- Denota “lo que es”
- Describe la deficiencia detectada por el auditor
- Debe ser objetiva
- Producto de verificación o comprobación
- Se sustenta con evidencias
- Opuesta al deber ser
- Debe explicarse por sí misma, por lo que su redacción no debe ser contradictoria o confusa

3.3.6.1.3 CRITERIO

Es el “deber ser” y que está contenida en alguna ley y/o reglamento y es el elemento que permite identificar que la condición se encuentra en oposición al criterio.

3.3.6.1.4 CAUSA

Es la razón o el motivo que genera el efecto obtenido de la comparación entre la condición y el criterio. La identificación de la causa contribuye a que los auditores gubernamentales, preparen recomendaciones constructivas en relación a las acciones correctivas que deban implantarse.

3.3.6.1.5 EFECTO

Impacto cuantitativo o cualitativo ocasionado por la deficiencia señalada, o el impacto potencial que podría ocasionar la misma.

Características:

- Ocasionado por la condición
- Categórico
- Evitar palabras o frases confusas en su redacción
- Se puede medir en términos cualitativos o cuantitativos

3.3.6.1.6 RECOMENDACIÓN

Son las acciones que la administración debe implementar para abordar la causa, y en algunas veces presenta soluciones a la condición.

3.3.6.1.7 COMENTARIOS DE LA ADMINISTRACIÓN

Son las respuestas y opiniones razonables que la administración de la institución emite en relación a los hallazgos y recomendaciones que el auditor presenta para la solución de los aspectos mencionados.

3.3.6.1.8 COMENTARIOS DE AUDITORÍA

Deberá agregarse comentarios de los auditores, cuando éstos difieran en parte o en su totalidad, de los comentarios de la administración. Los comentarios deberán ser claros y precisos.

3.3.6.1.9 GRADO DE CUMPLIMIENTO

El grado de cumplimiento de las recomendaciones que, podrá ser:

- Recomendación cumplida
- Recomendación en proceso, ó
- Recomendación no cumplida

3.3.6.1.10 CONCLUSIÓN

Finalizada la incorporación de los resultados de evaluación del control interno de los sistemas de información computarizados, el equipo de auditores desarrollará conclusiones desde la perspectiva de la institución auditada, observando los resultados y conclusiones.

3.3.7 CONCLUSIONES

Las conclusiones deben formularse explícitamente y no ser deducidas por los lectores. La fuerza de las conclusiones de los auditores depende de lo persuasivo de la evaluación del control interno de los sistemas de información computarizados que sustenta los hallazgos y lo convincente de la lógica usada para formular las conclusiones.

Se debe concluir sobre lo suficiente o adecuado de los tipos de controles evaluados, como lo son: Controles generales, Controles de datos, controles de aplicación, el procesamiento electrónico y la seguridad lógica.

El equipo de Auditoría Gubernamental deberá obtener evidencia suficiente, competente y oportuna, mediante la aplicación de los procedimientos de evaluación programados, que le permitan sustentar sus conclusiones y hallazgos sobre una base objetiva y real.

Los papeles de trabajos deben ser completos, de tal forma que muestren: La información y los hechos concretos, el alcance del trabajo efectuado, las fuentes de la información obtenida y las conclusiones respectivas.

Debe obtenerse evidencia suficiente, competente y relevante para fundamentar razonablemente los juicios y conclusiones que formulen los auditores. Permite al auditor valorar que la evidencia obtenida en el desarrollo de la evaluación del control interno de los sistemas de información computarizados cumpla con los requisitos de suficiencia, competencia y pertinencia, a efecto de

que las conclusiones estén adecuadamente respaldadas y permitan una opinión técnica, independiente y objetiva.

3.3.8 RECOMENDACIONES

Los auditores deben incluir en sus informes las recomendaciones con respecto a las medidas que se consideren apropiadas para corregir áreas problema y mejorar la operación. Cuando, basados en los hallazgos correspondientes, se demuestre que existe la posibilidad de mejorar significativamente la operación y el desempeño.

Deben formularse recomendaciones para que se cumpla con las leyes, reglamentos y demás disposiciones aplicables y se mejoren los controles de la administración cuando sean significativos los casos de incumplimiento y las deficiencias de control que se hayan observado.

Los informes que contienen recomendaciones constructivas pueden alentar la ejecución de mejoras en la conducción de los programas y actividades gubernamentales. Las recomendaciones son más constructivas cuando se encaminan a atacar las causas de los problemas observados, se refieren a acciones específicas y van dirigidas a quienes corresponde emprender esas acciones. Además, es necesario que las medidas que se recomiendan sean factibles y que su costo corresponda a los beneficios esperados.

CAPÍTULO IV

4. CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

Respecto al trabajo de investigación dirigido a la evaluación del control interno de los sistemas de información computarizados en las instituciones autónomas desde la perspectiva de la auditoría interna gubernamental, se puede concluir lo siguiente:

- Las unidades de auditoría interna de las instituciones autónomas en El Salvador, no se encuentran capacitadas para realizar de forma metódica la evaluación del control interno de los sistemas de información computarizados, debido a que están utilizando un marco legal y normativas técnicas, las cuales no incluyen una metodología para el área de los sistemas de información computarizados.
- La evaluación del control interno en los sistemas de información computarizados debe ser prioridad de los auditores internos gubernamentales, debido a la mayor incidencia que cada día tienen dichos sistemas en el logro de los objetivos institucionales, esta labor actualmente es cumplida a medias por el auditor interno al no echar mano de herramientas actualizadas desarrolladas por expertos en el tema de las tecnologías.
- La mayor parte de las capacitaciones que reciben los auditores internos de las instituciones autónomas no incluyen conocimientos actualizados que le permitan llevar a cabo evaluaciones del control interno de los sistemas de información computarizados de acuerdo al avance tecnológico de los mismos.

- Las unidades de auditoría interna no cuentan dentro de su recurso humano con personal experto en el área de tecnología informática provocando que la evaluación del control interno de los sistemas de información computarizado no se lleve a cabo de la mejor forma posible.
- Los sistemas de información computarizados, por su naturaleza tecnológica, son recursos con una gran flexibilidad al cambio, por lo cual deben ser evaluados en su control interno siguiendo esa misma lógica de flexibilidad ante los avances tecnológicos, y la falta de una adecuada metodología implica que exista deficiencia en medir la calidad de los sistemas de información computarizado que posee la institución.

4.2 RECOMENDACIONES

Respecto al trabajo de investigación dirigido a la evaluación del control interno de los sistemas de información computarizados en las instituciones autónomas desde la perspectiva de la auditoría interna gubernamental, se puede recomendar lo siguiente:

- A las instituciones autónomas, contemplar dentro del presupuesto designado a la unidad de auditoría interna una plaza para un experto en la operatividad de los sistemas de información computarizados, que ayude a los auditores con las tareas de evaluación del control interno de esta área.
- A las unidades de auditoría interna, capacitar a sus miembros para potenciar su rol asesor de la alta gerencia de las instituciones, mediante la ampliación y mejora constante de sus conocimientos a través de la educación continuada, incluyendo especialmente el área de sistemas de información computarizados.

- Al personal de las unidades de auditoría interna, aprovechar aquellas opiniones que surgen como el consenso de expertos relativo a las mejores prácticas en la gestión de los sistemas de información computarizados, utilizando estas prácticas recomendadas como el deber ser contra el cual evaluará las realidades tecnológicas de cada institución.
- A los miembros de las unidades de auditoría interna, utilizar el presente trabajo como herramienta que permita determinar el grado de cumplimiento de los controles internos de los sistemas de información computarizados, realizando las pertinentes acciones correctivas.
- A los alumnos que reciben la cátedra de auditoría de sistemas, emplear este trabajo de investigación como material de apoyo enfocado a la seguridad lógica de los sistemas de información computarizados.

BIBLIOGRAFÍA

Asamblea Legislativa de El Salvador. Año 1995. Ley Orgánica de Administración Financiera del Estado. Corte Suprema de Justicia.

Asamblea Legislativa de El Salvador. Año 1995. Ley de la Corte de Cuentas de la República. Corte Suprema de Justicia de El Salvador.

Asamblea Legislativa de El Salvador. Año 2002. Constitución de la Republica de El Salvador. Ediciones FESPAD. El Salvador

Asamblea Legislativa de El Salvador. Año 2006. Ley de Ética Gubernamental. Corte Suprema de Justicia de El Salvador.

Cocar Romano, Orlando. Año 2003. Primera Edición. “Metodología de la Investigación. Un Enfoque Práctico”. Talleres y Copiados Unidos. El Salvador

Comité Internacional de Prácticas de Auditoría. Año 2004. Declaraciones Internacionales de Prácticas de Auditoría.

Corte de Cuentas de la República. Año 2006. Manual de Auditoría Gubernamental. Corte Suprema de Justicia de El Salvador.

Corte de Cuentas de la República. Año 2004. Normas Técnicas de Control Interno. Corte Suprema de Justicia de El Salvador.

Corte de Cuentas de la República. Año 2004. Normas de Auditoría Gubernamental. Corte Suprema de Justicia de El Salvador.

García, Carlos Ernesto. Año 2008. Quinta Edición. "Gerencia Informática". Informatik, S.A. de C.V., San Salvador, El Salvador

Hernández Hernández, José Armando; Ramos Yanes, Pablo Antonio; Ventura Ventura, Luis Alonso. Año 1999. "La Auditoría de Sistemas una Necesidad en las Instituciones Autónomas, en el Proceso de Modernización del Estado". Trabajo de Graduación para optar al grado de Licenciado en Contaduría Pública. Universidad de El Salvador.

IT Governance Institute. Año 2005. COBIT versión 4.1. Glanser Services S.C. Objetivos de control para la información y tecnología relacionada

Jovel Jovel, Roberto Carlos. Año 2008. Primera Edición. "Guía Básica para Elaborar Trabajos de Investigación". Imprenta Universitaria. El Salvador

Madariaga Gorocica, Juan María. Año 2004. Primera Edición. "Manual Práctico de Auditoría". Ediciones Deusto.

Rojas Soriano, Raúl. Año 1991. Primera Edición. "Guía para Realizar Investigaciones Sociales". Offset y Diseño, S.A. de C.V.

The Institute of Internal Auditors. Año 2004. Normas internacionales para el ejercicio profesional de la auditoría interna.

ANEXOS

ÍNDICE DE ANEXOS

ANEXO 1	
Cuestionario	01
ANEXO 2	
Cronograma de actividades del proceso de auditoría	05
ANEXO 3	
Programas para evaluación del control interno de los sistemas de Información computarizados	06
ANEXO 4	
Ejecución de una sección de un programa para evaluación del control interno de los sistemas de información computarizados	30



UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONOMICAS
ESCUELA DE CONTADURÍA PÚBLICA



CUESTIONARIO DIRIGIDO A LAS INSTITUCIONES AUTÓNOMAS

Objetivo:

Obtener información sobre la existencia de una metodología para la evaluación del control interno de los sistemas de información computarizados-SIC en las instituciones autónomas desde la perspectiva de la auditoría interna gubernamental.

1. ¿Posee la institución sistemas de información computarizados?

a) Si b) No

2. ¿Las Normas Técnicas de Control Interno de la institución contemplan el Área de los sistemas de información computarizados?

a) Si b) No

3. ¿Se tomó en cuenta algún marco de referencia, para normar el control interno de los sistemas de información computarizados?

a) Si b) No

4. ¿Posee la institución, manual para el desarrollo de las actividades de la Unidad de Auditoría Interna?

a) Si b) No

5. ¿Los planes de trabajo anuales de la Unidad de Auditoría Interna, contemplan la evaluación de los sistemas de información computarizados de la institución?

a) Si b) No

6. ¿Se cuenta con alguna referencia técnica para evaluar los sistemas de información computarizados?

a) Si b) No

7. ¿Cuenta la Unidad de Auditoría Interna con personal idóneo para evaluar los sistemas de información computarizados?

a) Si b) No

8. ¿Cuáles de los siguientes profesionales componen la Unidad de Auditoría Interna?

a) Ingenieros de sistemas informáticos

b) Administradores de empresas

c) Contadores públicos

d) Otros: _____

9. ¿Se capacita al personal de la Unidad de Auditoría Interna para el desarrollo de las evaluaciones de los sistemas de información computarizados?

a) Si b) No

10. ¿Durante el año 2008, cuántas horas de capacitación se han recibido en la Unidad de Auditoría Interna?

a) 0 horas: _____

b) 1-50 horas: _____

c) 51-100 horas: _____

d) 101-150 horas: _____

e) 150 - a más horas: _____

11. ¿Utilizan técnicas asistidas por computadora para las evaluaciones de los sistemas de información computarizados?

a) Si b) No

12. ¿El trabajo desempeñado por la Unidad de Auditoría Interna se desarrolla en base a las Normas de Auditoría Gubernamental-NAG adoptadas por la Corte de Cuentas de la República?

a) Si b) No

13. ¿Considera que las Normas de Auditoría Gubernamental-NAG poseen la metodología para la correcta evaluación del control interno de los sistemas de información computarizados?

a) Si b) No

Porqué: _____

14. ¿Estaría de acuerdo con la elaboración de una metodología para la evaluación del control interno de los sistemas de información computarizados-SIC en las instituciones autónomas desde la perspectiva de la auditoría interna gubernamental?

a) Si b) No

15. Si la respuesta anterior fue positiva, ¿Utilizaría usted esta metodología para la evaluación del control interno de los sistemas de información computarizados-SIC en la institución autónoma donde labora?

a) Si b) No

Gracias por su tiempo y colaboración

ANEXO 3

Programas para evaluación del control interno de los
sistemas de información computarizados

PROGRAMA DE TRABAJO CONTROLES GENERALES		REF: CG		
INSTITUTO DEL CAFÉ				
UNIDAD DE AUDITORÍA INTERNA				
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS				
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)				
Periodo a examinar del 01 de enero al 31 de marzo de 2009				
Objetivos:				
a. Verificar la existencia y aplicación de controles lógicos generales referentes al sistema de información computarizado				
b. Evaluar la idoneidad y suficiencia de los controles generales establecidos				
c. Detectar desviaciones en la aplicación de las actividades de control general				
d. Recomendar mejoras que permitan detectar y/o corregir las desviaciones de control general detectadas				
No.	Procedimiento	Ref. PT's	Hecho por	Fecha
1	Elabore Hoja de Trabajo para revisión de controles			
2	Elabore Cédula Sumaria de Controles Generales			
	<u>Integridad de la información</u>			
3	Con respecto a los respaldos de información verifique: a) Que se realizan por lo menos diariamente b) Que se realizan comprobaciones de los realizados (integridad de la información) dedicando un equipo a modo de "sandbox" o caja de arena de pruebas específicas c) Que sean totales			

	<p>d) Que se resguarden en lugar seguro (disco removible/PC espejo del original, subidos a hostings especializados, en locales diferentes a donde reside la información primaria, etc.)</p> <p>e) Que se cuenten con borrados de información de los medios de almacenamiento antes de desecharlos</p> <p>f) Realización de simulacros</p>			
	<u>Tecnología contra software malicioso</u>			
4	<p>Enliste y verifique que se encuentre instalado el siguiente software (y evalúe en base a características mínimas), que se encuentren vigentes las licencias respectivas y activadas las actualizaciones automáticas:</p> <p>a) Firewall:</p> <ul style="list-style-type: none"> • Que proteja de accesos no autorizados • Capacidad de alertar sobre intentos de intrusión • Mantener registro para seguir pistas • Bloqueo de applets Java, controles ActiveX, cookies • Filtrado a nivel de aplicación para conexiones hacia el exterior (usadas para troyanos) • Cierta facilidad de instalación, configuración y uso <p>b) Antivirus:</p> <ul style="list-style-type: none"> • Que actualice los patrones o firmas por lo menos una vez por día • Que la empresa proveedora cuente con un equipo de soporte técnico con acceso a un 			

	<p>laboratorio especializado en códigos maliciosos y un tiempo de respuesta no mayor a 48 horas con orientación en español, en caso de infección</p> <ul style="list-style-type: none"> • Contar con distintos métodos de verificación y análisis de posibles códigos maliciosos, incluyendo el heurístico • Adaptable a las necesidades de diferentes usuarios • Poderse realizar la instalación remota tanto en red LAN como WAN • Que cuente con una consola central donde se reciba reporte de virus, mandar actualizaciones y personalizar a distintos usuarios • Que permitan la creación de discos de emergencia o rescate • Que no afecte el rendimiento o desempeño normal de los equipos (residente en memoria de lo más pequeño posible) • Número de falsos positivos que se den en rastreo normal como heurístico sean el mínimo posible • Mecanismo de auto protección que alerte de posibles infecciones por distintas vías: Internet, correo electrónico, red, etc. • Posibilidad de chequear el arranque así como los posibles cambios en el registro de aplicaciones 			
--	--	--	--	--

	<p>c) Anti-espías:</p> <ul style="list-style-type: none"> • Que permita seleccionar las unidades y carpetas a analizar • Que posea opciones de análisis (escanear registro, memoria, uso de heurística, etc.) • Detección y bloqueo de aplicaciones que intenten escribir en el registro del sistema operativo sin autorización • Capacidad de evitar el secuestro del navegador • Eliminación de spyware encontrado • Eliminación del contenido del caché, cookies, historial, etc. • Posibilidad de crear copia de seguridad • Escaneo en tiempo real y protección durante las descargas desde internet • Restauración de ficheros previamente eliminados • Bloqueo de instalación de barras de herramientas o ayudantes de navegador no deseados <p>d) Filtrado de IP:</p> <ul style="list-style-type: none"> • Bloqueo de programas y sitios 			
	<u>Administración de privilegios</u>			
5	<p>Compruebe con el administrador del sistema que se restringen los siguientes privilegios y verifique:</p> <p>a) Ejecución de instrucciones que afecten la</p>			

	<p>configuración del hardware</p> <p>b) Ejecución de instrucciones que afecten la configuración del sistema</p> <p>c) Actividades de montaje y examen de sistemas de archivos</p> <p>d) Creación, modificación y eliminación de usuarios</p> <p>e) Modificación de perfiles de usuario</p> <p>f) Adición y eliminación de periféricos</p> <p>g) Instalación-desinstalación de software</p> <p>h) Administración de contraseñas</p> <p>i) Administración de líneas terminales de usuario</p>			
	<u>Detección de intrusos</u>			
6	<p>Verifique que se posea un sistema de detección de intrusos (IDS) y que cumpla con las siguientes características:</p> <p>a) Alerta de la realización de un ataque exitoso</p> <p>b) Alerta de ataques en progreso</p> <p>c) Corto tiempo de respuesta</p> <p>d) Que no ofrezca falsos positivos, ni falsos negativos</p> <p>e) Que realice diagnóstico informando:</p> <ul style="list-style-type: none"> • en qué consiste el ataque • de donde procede • sugerencia de cómo paliarlo 			
	<u>Protección de información sensible</u>			
7	<p>Compruebe que la información sensible se cifre y se esconda</p>			
8	<p>Con respecto al cifrado verifique su solidez:</p> <p>a) Que se realice por volúmenes</p> <p>b) Que toda la información identificada como sensible</p>			

	<p>sea ubicada dentro del volumen cifrado</p> <p>c) Que posea la característica de llevar volúmenes cifrados en dispositivos portátiles de almacenamiento</p> <p>d) Que el volumen cifrado se encuentre cerrado, excepto cuando el administrador se encuentre leyendo o modificando la información contenida en este, para lo cual evalúe el cumplimiento del desmontaje del volumen en las siguientes situaciones:</p> <ul style="list-style-type: none"> • Que el administrador lo desconecte al no estar presente aunque sea por lapsos cortos • Desconectarlo antes de poner a “dormir” (hibernación y suspensión) el computador • Desconectarlo antes que de cualquier otra persona maneje el computador • Desconectarlo antes de insertar cualquier tipo de almacenamiento externo • Cuando el volumen se encuentre en memoria extraíble siempre: <ul style="list-style-type: none"> i. Desmontar el volumen apropiadamente ii. Desconectar la unidad externa o memoria extraíble, y iii. Retirar el dispositivo 			
9	<p>Relativo a esconder los archivos verifique el uso de la Esteganografía en sus facetas:</p> <p>a) Lingüística</p> <p>b) De datos</p>			

	<u>Administración de acceso</u>			
10	Compruebe con el administrador del sistema y de acuerdo a los roles de los usuarios que se habilite el uso de la información cuando se necesita y no se permite si no es imprescindible.			
11	Solicite al administrador del sistema el listado de los usuarios y verifique desde una terminal la solidez de las contraseñas: <ul style="list-style-type: none"> a) Que no existan contraseñas nulas b) Que no se utilizan las contraseñas que por defecto proporcionó el fabricante del sistema c) Que no se utilicen nunca nombres, números, o secuencia de caracteres relacionados con el usuario específico que se verifica d) Que las contraseñas de los usuarios se almacenan de forma cifrada y que no permita el algoritmo inverso e) Que las claves sean de tipo alfanumérico, combinando letras mayúsculas y minúsculas f) Que la extensión de la clave sea como mínimo de 8 caracteres g) Que sea cambiada con cierta regularidad 			
	<u>Identidades de usuario</u>			
12	Compruebe que se han establecido de manera integrada: <ul style="list-style-type: none"> a) Las identidades de los usuarios: <ul style="list-style-type: none"> • Que accedan a los diferentes recursos que por su trabajo tienen derecho con identidad única integrada 			

	<p>b) Estructura de autorización y autenticación:</p> <ul style="list-style-type: none"> • Que por medio de un directorio autentique al usuario y le conceda los permisos de acceso a los recursos específicos que tienen derechos como inicio de sesión único, siguiendo la secuencia: <ul style="list-style-type: none"> i. Solicitud de acceso a recursos ii. Evaluación de derechos asignados para determinar el permiso iii. Si el usuario cuenta con privilegios de acceso que se admita la solicitud de lo contrario que rechace la solicitud y deniegue el acceso 			
	<u>Comunicación y Conclusión</u>			
13	Elabore Cédula de Hallazgos			
14	Comunique cualquier situación observada que afecte los controles de aplicación			
15	Concluya sobre el área examinada			
Elaborador por:		Revisado por:		Supervisado por:
Fecha:		Fecha:		Fecha:

PROGRAMA DE TRABAJO CONTROLES DE DATOS		REF: CD		
INSTITUTO DEL CAFÉ				
UNIDAD DE AUDITORÍA INTERNA				
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS				
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)				
Periodo a examinar del 01 de enero al 31 de marzo de 2009				
Objetivos:				
a. Verificar la existencia y aplicación de controles lógicos de datos referentes al sistema de información computarizado				
b. Evaluar la idoneidad y suficiencia de los controles de datos establecidos				
c. Detectar desviaciones en la aplicación de las actividades de control de datos				
d. Recomendar mejoras que permitan detectar y/o corregir las desviaciones de control de datos detectadas				
No.	Procedimiento	Ref. PT's	Hecho por	Fecha
1	Elabore Cédula Sumaria de Controles de Datos			
	<u>Disponibilidad</u>			
2	<u>DISPONIBILIDAD</u> Verificar que exista un procedimiento para determinar que las bases de datos tienen integrado todos los registros comunes para que funcione en el momento que se necesitan y examinar lo siguiente: a) Que las bases de datos posean accesibilidad en cualquier momento y que se permita a diferentes			

	<p>usuarios la misma información simultáneamente</p> <p>b) Que la biblioteca de programas y datos mantenga un registro automático de las intervenciones al computador, cuando se utilizan estos programas y archivos y quien los utiliza.</p> <p>c) Que exista un registro de cada violación a los procedimientos con el fin de llevar estadísticas y frenar las tendencias mayores</p>			
3	<p><u>RESPALDO</u></p> <p>Verificar si se identifican los datos que deben ser respaldados y la periodicidad con que deben respaldarse, obteniendo un listado de los procedimientos de backup de la base de datos, cronogramas de backup y programas utilitarios de backup y asegúrese:</p> <p>a) Que como mínimo un backup incremental se esta realizando todas las noches</p> <p>b) Que los backup lógicos de la base de datos son programados en la noche, cuando los usuarios están fuera y los procesos han finalizado</p> <p>c) Que cuando se hacen backup lógicos la base de datos se encuentra en modo restringido</p> <p>d) Si se hace un backup lógico completo cada semana, para asegurarse que la base de datos completa esta respaldada</p> <p>e) Que un completo backup al sistema esta siendo realizado por lo menos cada mes</p>			

4	<p><u>RECUPERACIÓN</u></p> <p>Obtenga y revise la documentación de los procesos de pruebas de recuperación y verifique:</p> <p>a) Que se cumplan y funcionen los procedimientos para la recuperación de la bases de datos</p> <p>b) Que los procedimientos de recuperación sean capaces de restaurar la base de datos rápidamente</p> <p>c) La existencia de mecanismo de control para recuperar problemas menores y para transportar la información a otro computador de respaldo</p>			
	<u>Integridad</u>			
5	<p><u>RESTRICCIÓN EXTERNA DE LA INFORMACIÓN</u></p> <p>Confirmar que existan procedimientos para evitar la contaminación por virus, referirse a programas de control general sobre <i>Tecnología contra software malicioso</i></p>			
6	<p><u>RESTRICCIÓN INTERNA DE LA INFORMACIÓN</u></p> <p>Verificar la existencia de procedimientos para establecimiento de privilegios donde se de a cada usuario lo que necesita para cumplir con sus responsabilidades y asegúrese:</p> <p>a) Que el usuarios este adecuadamente restringido por el programa de aplicación de manera que no pueda escaparse del nivel de programa de aplicación y obtener acceso al sistema operativo a</p>			

	<p>la base de datos</p> <p>b) Que se asignen las limitaciones correspondientes a cada usuario del sistema informático. Esto significa, no darle más privilegios extras a un usuario, sino sólo los que necesita para realizar su trabajo</p> <p>c) Que cada usuario se autentica con la base de datos</p> <p>d) Que existe examen de cada perfil de usuario en las tablas de usuarios</p> <p>e) Que los roles y privilegios son usuario por usuario</p> <p>f) Que se dé una detallada revisión de los login, procesos de autenticación, perfiles de usuario y roles y privilegios</p> <p>g) Que exista un reporte sobre los usuarios que acceden a la base de datos y los tipos de operaciones que están realizando</p>			
7	<p>Solicitar la logística de las claves de acceso y verificar:</p> <p>a) Que todos los usuarios representan un usuario válido y autenticado</p> <p>b) Que el passwords por defecto en las cuentas de administración del sistema han sido cambiadas</p> <p>c) Que están definidos los procedimientos para cambios de claves periódicamente y que los passwords son seguros. Estos cambios se pueden hacer al menos trimestralmente</p> <p>d) Que la clave dada a los usuarios este compuesta por combinaciones números, letras y símbolos, evitando que contengan números secuenciales,</p>			

	<p>nombres o fechas significativas</p> <p>e) Que la clave dada al usuario sea individual ya que eso permite, al momento de efectuar transacciones, registrar a los responsables de cualquier tipo de cambio o en su defecto se controle a través de la función o rol del usuario que requiere dicho acceso. En este último caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios</p> <p>f) Que las instrucciones sobre las claves a los diferentes usuarios sea dada de forma confidencial</p>			
8	Examinar si se ha establecido horarios, de modo que limite el acceso de los usuarios a determinadas horas de día o a determinados días de la semana			
9	Solicite una impresión de la bitácora de sesiones de usuarios y examine que todas los intentos de conexión no exitosos son almacenados, revisados y se les hecho seguimiento			
10	Revisar si se ha establecido un numero máximo de violaciones en sucesión para que la computadora cierre esa Terminal y se de aviso al responsable de ella.			
11	Registrar cada violación a los procedimientos con el fin e llevar estadísticas y frenar las tendencias mayores			
12	<p>Solicite un el informe de excepciones y verifique si se ha realizado un análisis que cubra los siguientes aspectos:</p> <p>a) Separar aquellos fallos que son importante de los que no tienen trascendencia</p> <p>b) Separar los que son accidentales de los que no lo</p>			

	son c) Clasificarlos por fallos de acceso al sistema, intento de acceso a ficheros protegidos, intentos de uso de comandos sobre los que el usuario no tiene permiso, etc.			
	<u>Flujo</u>			
13	<u>CAPTURA</u> Verifica que existan rutinas que verifiquen la compatibilidad de los datos, validando el tipo de datos que contienen los campos o verificando si se encuentran dentro de un rango			
14	Examinar si se lleva a cabo un conteo de registros, creando campos de memoria para ir acumulando cada registro que se ingresa y verificar con los totales ya registrados			
15	Determinar si se realiza una separación de aquellos formularios o registros que poseen diferencias y cual es el proceso para reingresarlos al sistema de forma correcta			
16	<u>PROCESO</u> Determinar que las funciones aritméticas se ejecuten correctamente			
17	Establecer que todas las transacciones se asienten en el registro indicado			
18	Asegurar que los errores descubiertos en el procesamiento de datos se corrijan satisfactoriamente.			
19	Revisar que los programas de aplicación contengan condiciones que verifiquen rutinariamente el trabajo			

	realizado durante el procesamiento de datos para promover la integridad de estos			
20	<p>Realizar pruebas de actividades de control programadas por medio de programas controlados, y asegurarse:</p> <p>a) Que las pruebas reflejan condiciones validas y no validas</p> <p>b) Que los resultados de las pruebas se comparan con los resultados predeterminados manualmente para tener la seguridad de que se proceso de manera apropiada la información de prueba</p> <p>c) Que las operaciones válidas fueron procesadas con propiedad y que las operaciones no válidas son reconocidas por los controles programados y se producen los adecuados mensajes de aviso de error</p> <p>d) Que los datos de prueba procesados en la entidad han sido eliminados de los registros</p>			
21	<p><u>DISEMINACIÓN</u></p> <p>Verificar las cifras totales y cálculos para comprobar la exactitud de los reportes de salida producidos por el departamento de informática, de la información enviada por medios de comunicación y de la información almacenada.</p>			
	<u>Almacenamiento y conservación</u>			
22	Verificar que la información esta almacenada por largos periodos de tiempo en medios de fácil acceso, como discos duros.			

23	Identifique espacios de almacenamientos críticos.			
24	Verifique que los archivos de <i>logs</i> y los archivos de control son montados en diferentes discos y de estos se tienen copias.			
25	Asegúrese que cada disco usa un controlador independiente para minimizar le efecto en una falla del controlador			
26	Asegúrese que los requerimientos de espacio de almacenamiento, en el momento del diseño tuvieron en cuenta las proyecciones a futuro			
27	Evaluar los medios de almacenamiento, los procedimientos usados, la revisión de las copias, la correcta etiquetada (interna y externa), la seguridad del sitio de almacenamiento y la correcta rotación de las copias			
28	<p>Verificar los procedimientos que utilizan para minimizar la cantidad de redundancia en los datos almacenados, asegurando que estos eviten:</p> <p>a) Incremento del trabajo, ya que un dato se encuentra almacenado en dos o más lugares, y deben grabarse o actualizarse en todos los lugares a la vez.</p> <p>b) Desperdicio de espacio de almacenamiento, ya que los mismos datos están almacenados en varios lugares distintos.</p> <p>c) Inconsistencia de datos, porque se actualiza el dato en un lugar pero en otro no es actualizado</p>			

	<u>Información y comunicación</u>			
29	Elabore cédula de hallazgos.			
30	Comunique cualquier situación observada que afecte los controles de datos.			
31	Concluya sobre el área examinada.			
Elaborador por:		Revisado por:		Supervisado por:
Fecha:		Fecha:		Fecha:

PROGRAMA DE TRABAJO CONTROLES DE APLICACION		REF: CA		
INSTITUTO DEL CAFÉ				
UNIDAD DE AUDITORÍA INTERNA				
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS				
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)				
Periodo a examinar del 01 de enero al 31 de marzo de 2009				
Objetivos:				
a. Verificar la existencia y aplicación de controles lógicos de aplicación referentes al sistema de información computarizado				
b. Evaluar la idoneidad y suficiencia de los controles de aplicación establecidos				
c. Detectar desviaciones en la aplicación de las actividades de control de aplicación				
d. Recomendar mejoras que permitan detectar y/o corregir las desviaciones de control de aplicación detectadas				
No.	Procedimiento	Ref. PT's	Hecho por	Fecha
1	Elabore Cédula Sumaria de Controles de Aplicación			
	<u>Diseños de pistas de auditoría</u>			
2	Verifique en las pistas de auditoría: Que existan pistas de auditoría y cumplan las siguientes características: a) Registro histórico <ul style="list-style-type: none"> • Fecha • Hora • Usuario • Revisión 			

	<ul style="list-style-type: none"> • Autorización • Equipo desde el cual se realizaron los registros <p>b) Seguridad de la información</p> <ul style="list-style-type: none"> • Procesamiento de datos • Daños a la seguridad del sistema • Modificaciones no autorizadas • Datos borrados que son parte de la información • Registro de accesos al sistema • Que no existan interrupciones del servicio • Registro de violaciones de autoridad <p>c) Análisis</p> <ul style="list-style-type: none"> • Registro de datos dañados o destruidos <p>d) Monitoreo</p> <ul style="list-style-type: none"> • Que se hayan auditado las áreas de informática • Que existan registros de los sucesos encontrados anteriormente <p>Que procedimientos aplicaron</p>			
	<u>Mecanismos de autorización</u>			
3	<p>Revise los siguientes aspectos en los mecanismos de autorización:</p> <p>a) Definición de niveles de autorización</p> <p>b) Registro de accesos al servidor</p> <p>c) Autenticación de usuarios</p> <p>d) Mantenimientos de perfiles de usuarios</p>			

	<u>Simulación paralela</u>			
4	Realizar pruebas en paralelo a fin de verificar la confiabilidad en los resultados del sistema. a) Utilice las mismas operaciones b) Procesos de información c) Secuencias iguales			
	<u>Informes de excepción</u>			
5	Determine en el informe de excepción los siguientes aspectos: a) Informe de errores inesperados b) Datos que expliquen el suceso ocurrido c) Notificación de problemas internos d) Intento de entrar a ficheros protegidos y no autorizados			
	<u>Evaluaciones periódicas al software</u>			
6	Revise las evaluaciones periódicas aplicadas al software			
	<u>Registro de actividades de cada terminal</u>			
7	Verifique el registro de actividades de cada Terminal, como las siguientes: a) Actividades realizadas en cada computadora b) Accesos a programas c) Errores de procesamiento d) Procesos realizados			
	<u>Balanceo</u>			
8	Determine el balanceo por medio de las siguientes características: a) Controles durante y después del procesamiento de datos			

	<ul style="list-style-type: none"> b) Transferencia de datos completos c) Rutinas automatizadas del programa 			
	<u>Control de archivos</u>			
9	<p>Verifique el control de datos de archivos:</p> <ul style="list-style-type: none"> a) Archivo de datos sea correcto, b) Procesamiento en línea de diferentes terminales, c) Procesamiento en tiempo real 			
	<u>Control de archivos maestros</u>			
10	<p>Revise que el control de archivos maestros contenga lo siguiente:</p> <ul style="list-style-type: none"> a) Almacenamiento de la información b) Información este integrada c) Datos se encuentren consolidados d) Que tenga una sola base de datos 			
	<u>Procedimientos de corte</u>			
11	<p>Verifique que los procedimientos de corte se procesan en un periodo apropiado</p>			
	<u>Integridad de la configuración</u>			
12	<p>Determine la integridad de la configuración, evaluando:</p> <ul style="list-style-type: none"> a) Permisos asignados b) Última fecha de modificación c) Fecha de acceso d) Tamaño del archivo e) Firma del archivo 			
	<u>Programación de tareas en secuencia eficiente</u>			
13	<p>Determinar la programación de tareas en secuencia eficiente:</p> <ul style="list-style-type: none"> a) Programación de trabajos b) Revisar cambios autorizados al sistema 			

	<u>Automatización del monitoreo de cambios a sistemas aplicativos</u>			
14	<p>Revise si existe automatización del monitoreo de cambios a sistemas aplicativos:</p> <ul style="list-style-type: none"> a) Rastreo de cambios hechos en aplicaciones b) La inclusión de módulos al sistema c) Nuevas funciones al software d) Modificación perfiles de usuarios e) Sistemas y parámetros de servicios 			
	<u>Administración de incidentes</u>			
15	<p>Confirme en la administración de incidentes:</p> <ul style="list-style-type: none"> a) Registro consulta de clientes b) Registro de causa de incidentes c) Confirmar la resolución 			
	<u>Control de versiones</u>			
16	<p>Revise los control de versiones lo siguiente:</p> <ul style="list-style-type: none"> a) La versión del software, b) Especializaciones aplicadas, c) Mecanismos de almacenamiento de los elementos, d) Cambios sobre los elementos almacenados, e) Registro histórico de acciones de los elementos 			
	<u>Integridad de transacciones</u>			
17	<p>Revise la integridad de las transacciones:</p> <ul style="list-style-type: none"> a) De cambios b) De configuración c) De problemas d) Mejoras e) Minimización de problemas 			

	<u>Pruebas de regresión</u>			
18	Verifique las pruebas de regresión: a) Los cambios introducen nuevos errores b) Cambios revelan errores previos c) Los cambios vinculan alguna otra parte del programa			
	<u>Información y comunicación</u>			
19	Elabore cédula de hallazgos.			
20	Comunique cualquier situación observada que afecte los controles de aplicación.			
21	Concluya sobre el área examinada.			
Elaborador por:		Revisado por:		Supervisado por:
Fecha:		Fecha:		Fecha:

ANEXO 4

Ejecución de una sección de un programa
para evaluación del control interno de los sistemas de
información computarizados

PROGRAMA DE TRABAJO CONTROLES GENERALES		CG		
INSTITUTO DEL CAFÉ				
UNIDAD DE AUDITORÍA INTERNA				
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS				
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)				
Periodo a examinar del 01 de enero al 31 de marzo de 2009				
<u>Objetivos:</u>				
a. Verificar la existencia y aplicación de controles lógicos generales referentes al sistema de información computarizado.				
b. Evaluar la idoneidad y suficiencia de los controles establecidos.				
c. Detectar desviaciones en la aplicación de las actividades de control.				
d. Recomendar mejoras que permitan detectar y/o corregir las desviaciones de control detectadas.				
No.	Procedimiento	Ref. P/T	Hecho por	Fecha
	<u>Tecnología contra software malicioso</u>			
1	Elabore Hoja de Trabajo para revisión de controles.	H/T	ACSG	23Abr09
2	Elabore Cédula Sumaria de Controles Generales.	CG1	ACSG	23Abr09
4	Verifique que se encuentre instalado el siguiente software y evalúe en base a características mínimas, que se encuentren vigentes las licencias respectivas y activadas las actualizaciones automáticas:	CG2	ACSG	23Abr09
	e) Firewall:			
	• Que proteja de accesos no autorizados.	CG3	ACSG	23Abr09
	• Capacidad de alertar sobre intentos de intrusión.	CG4	ACSG	23Abr09
	b) Mantener registro para seguir pistas.	CG5	ACSG	23Abr09
	c) Bloqueo de applets Java, controles ActiveX,	CG6/CG7	ACSG	23Abr09

	cookies.			
	d) Filtrado a nivel de aplicación para conexiones hacia el exterior (usadas para troyanos).	CG8	ACSG	23Abr09
	e) Cierta facilidad de instalación, configuración y uso.	CG9/CG11	ACSG	23Abr09
	f) Antivirus:			
	• Que actualice los patrones o firmas por lo menos una vez por día.	CG12	ACSG	23Abr09
	• Que la empresa proveedora cuente con un equipo de soporte técnico con acceso a un laboratorio especializado en códigos maliciosos y un tiempo de respuesta no mayor a 48 horas con orientación en español, en caso de infección.	CG13	CSG	23Abr09
	• Contar con distintos métodos de verificación y análisis de posibles códigos maliciosos, incluyendo el heurístico.	CG14	ACSG	23Abr09
	• Adaptable a las necesidades de diferentes usuarios.	CG15	ACSG	23Abr09
	• Poderse realizar la instalación remota tanto en red LAN como WAN.	CG16	ACSG	23Abr09
	• Que cuente con una consola central donde se reciba reporte de virus, mandar actualizaciones y personalizar a distintos usuarios.	CG17	ACSG	23Abr09
	• Que permitan la creación de discos de emergencia o rescate.	CG18	ACSG	23Abr09
	• Que no afecte el rendimiento o desempeño normal de los equipos (residente en memoria de lo más pequeño posible).	CG19	ACSG	23Abr09

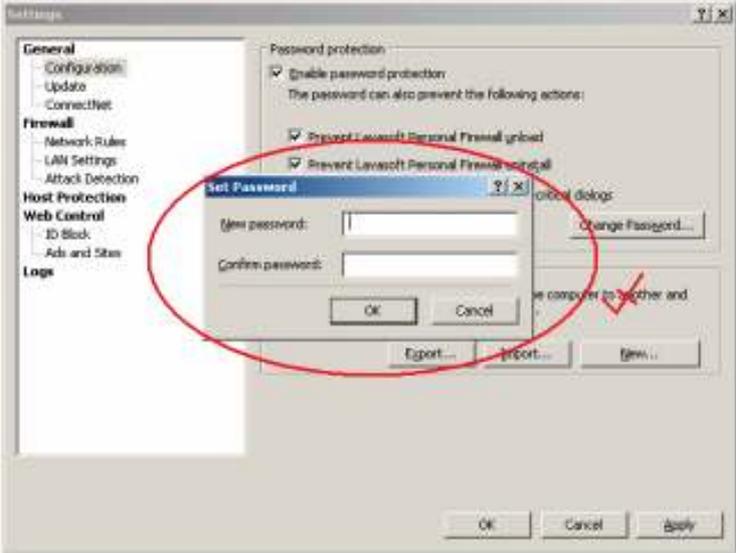
<ul style="list-style-type: none"> • Número de falsos positivos que se den en rastreo normal como heurístico sean el mínimo posible. • Mecanismo de auto protección que alerte de posibles infecciones por distintas vías: Internet, correo electrónico, red, etc. • Posibilidad de chequear el arranque así como los posibles cambios en el registro de aplicaciones. 		CG20	ACSG	23Abr09
		CG21	ACSG	23Abr09
		CG22	ACSG	23Abr09
	g) Anti-espías:			
	• Que permita seleccionar las unidades y carpetas a analizar.	CG23	ACSG	23Abr09
	• Que posea opciones de análisis (escanear registro, memoria, uso de heurística, etc.).	CG24	ACSG	23Abr09
	• Detección y bloqueo de aplicaciones que intenten escribir en el registro del sistema operativo sin autorización.	CG25	ACSG	23Abr09
	• Capacidad de evitar el secuestro del navegador.	CG26	ACSG	23Abr09
	• Eliminación de spyware encontrado.	CG27	ACSG	23Abr09
	• Eliminación del contenido del caché, cookies, historial, etc.	CG27	ACSG	23Abr09
• Posibilidad de crear copia de seguridad.	CG27	ACSG	23Abr09	
• Escaneo en tiempo real y protección durante las descargas desde internet.	CG28	ACSG	23Abr09	
• Restauración de ficheros previamente eliminados.	CG29	ACSG	23Abr09	
• Bloqueo de instalación de barras de herramientas o ayudantes de navegador no	CG30	ACSG	23Abr09	

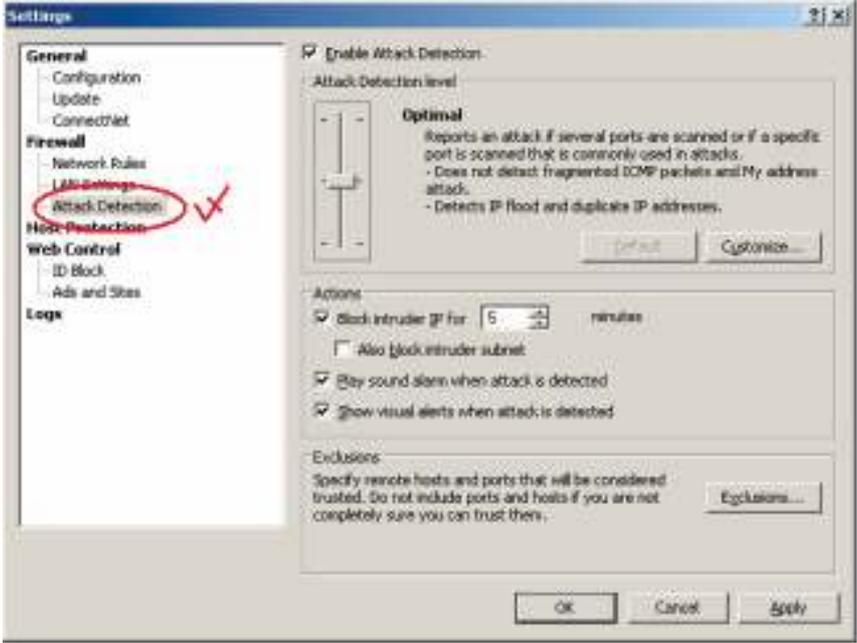
	deseados. h) Filtrado de IP: <ul style="list-style-type: none"> • Bloqueo de programas y sitios. 	CG31/CG33	ACSG	23Abr09
<u>Información y comunicación</u>				
13	Elabore cédula de hallazgos.	CGn1	ACSG	24Abr09
14	Comunique cualquier situación observada que afecte los controles generales.	CGn2	ACSG	27Abr09
15	Concluya sobre el área examinada.	CG1	ACSG	29Abr09
Elaborador por: ACSG		Revisado por: MRPM		Supervisado por: AGR
Fecha: 15Abr09		Fecha: 16Abr09		Fecha: 16Abr09

HOJA DE TRABAJO		H/T
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 1 del Programa CG	
	<u>Evaluación del control interno del sistema SMC v2.1:</u>	
CG	Controles generales	
CD	Controles de datos	
CA	Controles de aplicación	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

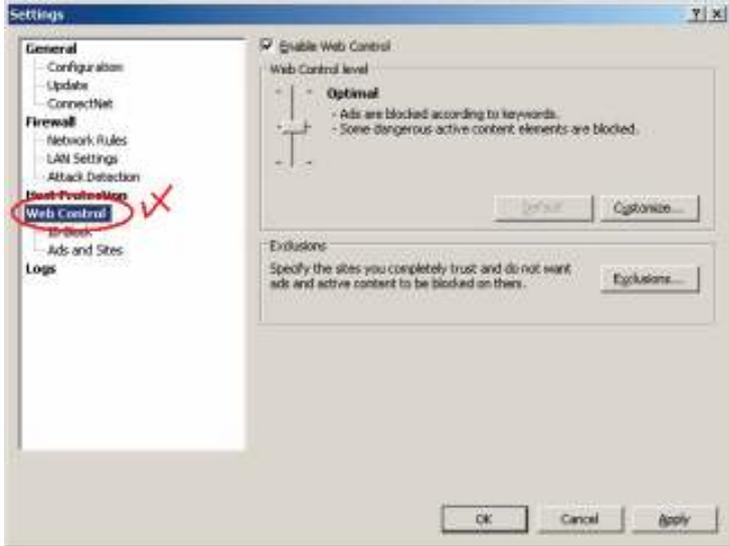
CONTROLES GENERALES CÉDULA SUMARIA		CG1
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 2 del Programa CG	
CGn	Integridad de la información	
CG2-CG31	Tecnología contra software malicioso	
CGn	Administración de privilegios	
CGn	Detección de intrusos	
CGn	Protección de información sensible	
CGn	Administración de acceso	
CGn	Identidades de usuario	
	CONCLUSIÓN:	
	En base a la evaluación realizada a los controles lógicos generales, concluimos, que excepto por las situaciones reportables contenidas en el PT CGn1 , la institución cuenta con controles que presentan un grado de seguridad razonable.	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

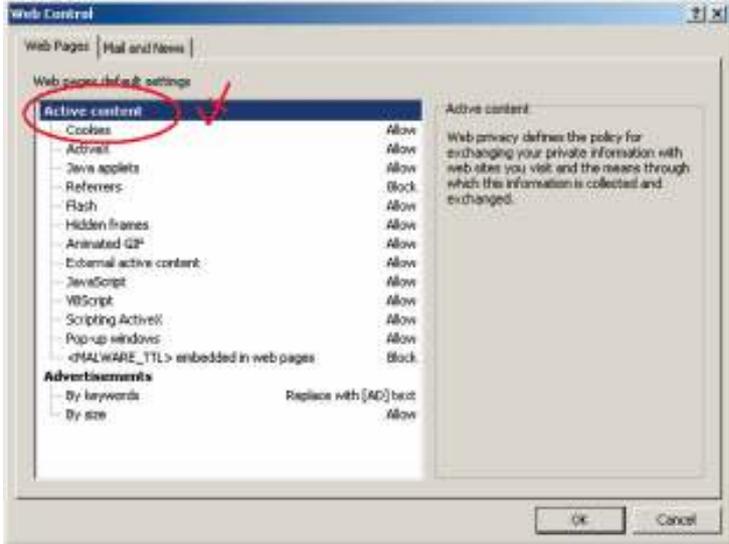
TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA FIREWALL		CG₂
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
	<ul style="list-style-type: none"> • Firewall: Lavasoft® Personal Firewall, Version 3.0 • Antivirus: McAfee® Total Protection Service, Version 4.7.0.752 Patch4 • Anti-espías: Ad-Aware® Pro, Version 2008 • Filtrado de IP. 	
	✓ = Verificado en software.	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

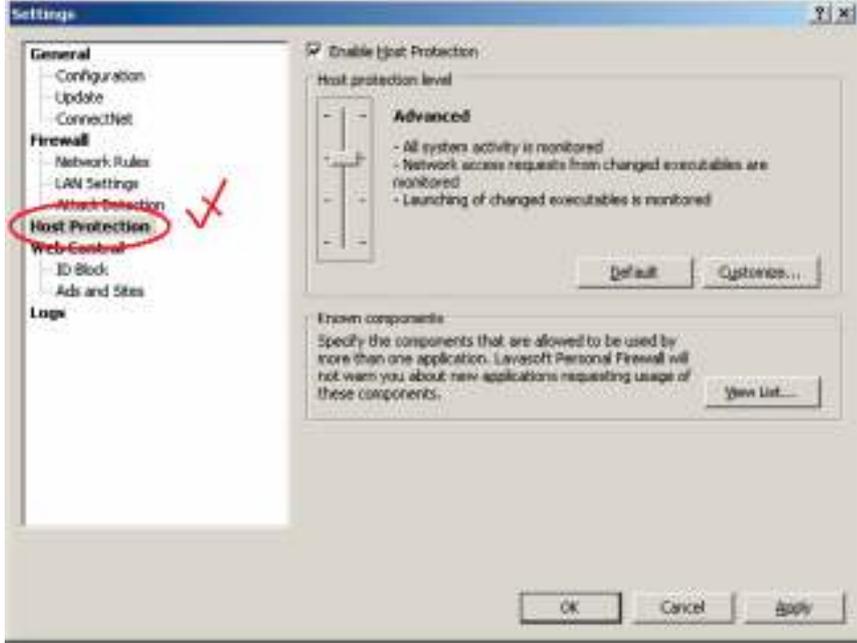
<p style="text-align: center;">TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE FIREWALL</p>	<p style="color: red; font-weight: bold; font-size: 1.2em;">CG3</p>	
<p>INSTITUTO DEL CAFÉ</p>		
<p>UNIDAD DE AUDITORÍA INTERNA</p>		
<p>EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS</p>		
<p>SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)</p>		
<p>Periodo a examinar del 01 de enero al 31 de marzo de 2009</p>		
<p>Ref.P/T</p>	<p>Procedimiento No. 4 del Programa CG</p>	
	<div style="text-align: center;">  </div> <p style="color: red; font-weight: bold; font-size: 1.2em;">✓ = Verificada la solicitud de autorización.</p>	
<p>Elaborador por: ACSG</p>	<p>Revisado por: MRPM</p>	<p>Supervisado por: AGR</p>
<p>Fecha: 23Abr09</p>	<p>Fecha: 27Abr09</p>	<p>Fecha: 27Abr09</p>

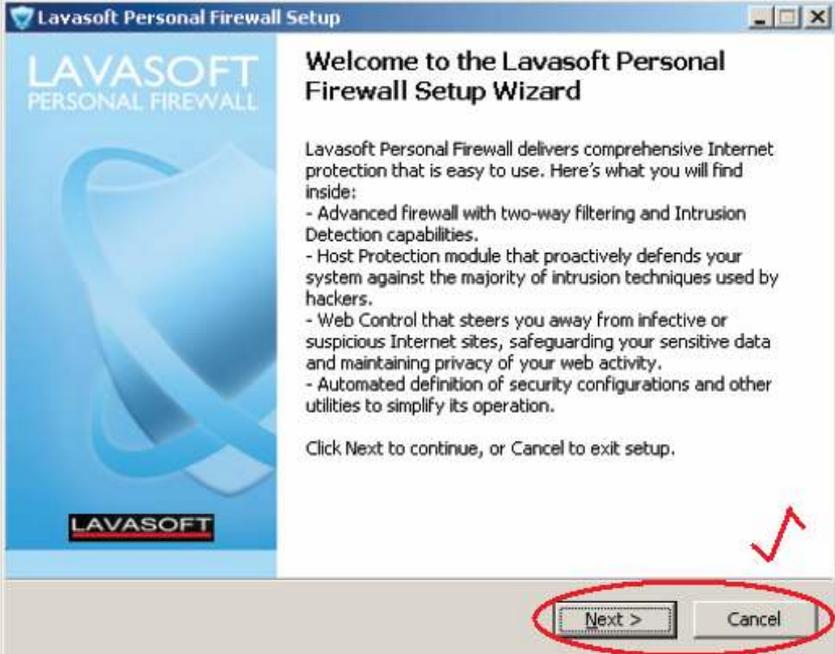
TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE FIREWALL		CG4
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
	 <p>✓ = Verificada alerta de intrusión.</p>	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

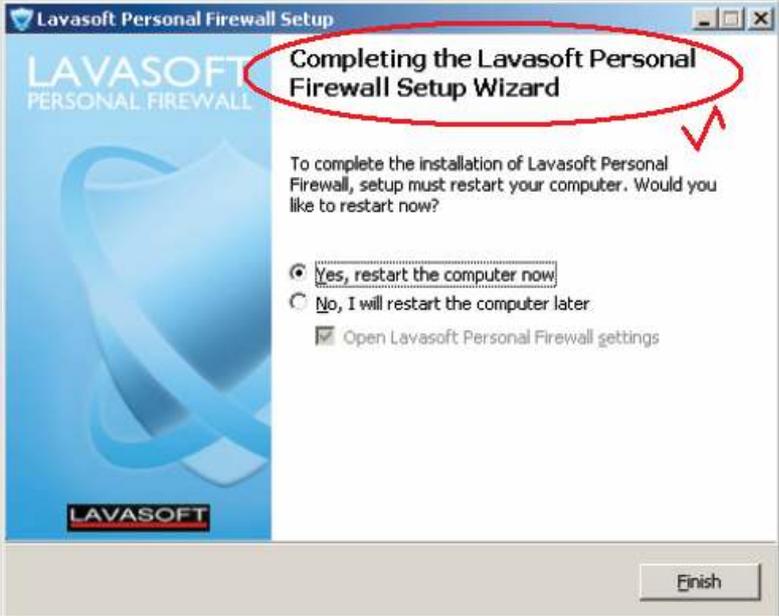
TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE FIREWALL		CG5
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
		
	 = Hallazgo 1, sin opciones de registro de pistas, ver PT CGn1	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE FIREWALL		CG6
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
	 <p>✓ = Verificado la configuración de bloqueos.</p>	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE FIREWALL		CG7
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
	 <p>Segunda pantalla de configuración de bloqueos. ✓ = Control verificado.</p>	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

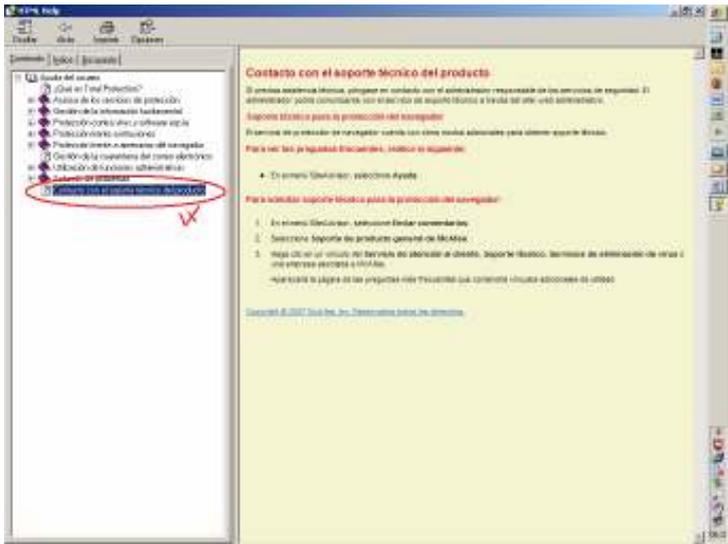
TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE FIREWALL		CG8
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
	 <p>Filtrado de aplicaciones. ✓ = Control verificado.</p>	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE FIREWALL		CG₉
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
	 <p>Instalación de software.  = Simulación realizada.</p>	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

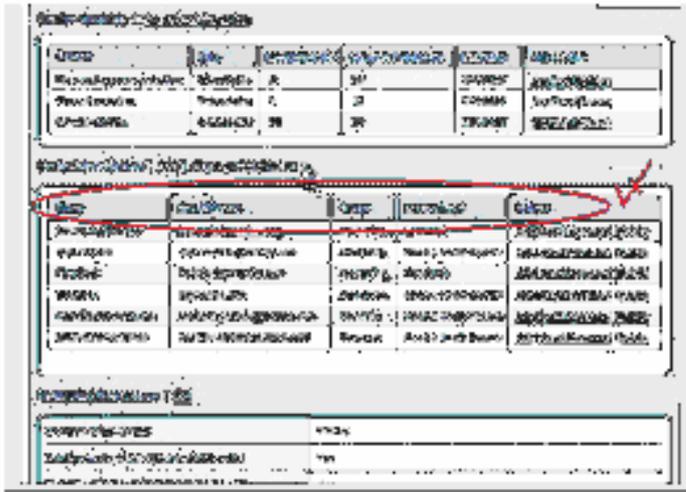
<p style="text-align: center;">TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE FIREWALL</p>	<p style="color: red; font-weight: bold; font-size: 1.2em;">CG10</p>	
<p>INSTITUTO DEL CAFÉ</p>		
<p>UNIDAD DE AUDITORÍA INTERNA</p>		
<p>EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS</p>		
<p>SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)</p>		
<p>Periodo a examinar del 01 de enero al 31 de marzo de 2009</p>		
<p>Ref.P/T</p>	<p>Procedimiento No. 4 del Programa CG</p>	
	<div style="text-align: center;">  </div> <p>Instalación de software.</p> <p>✓ = Simulación realizada.</p>	
<p>Elaborador por: ACSG</p>	<p>Revisado por: MRPM</p>	<p>Supervisado por: AGR</p>
<p>Fecha: 23Abr09</p>	<p>Fecha: 27Abr09</p>	<p>Fecha: 27Abr09</p>

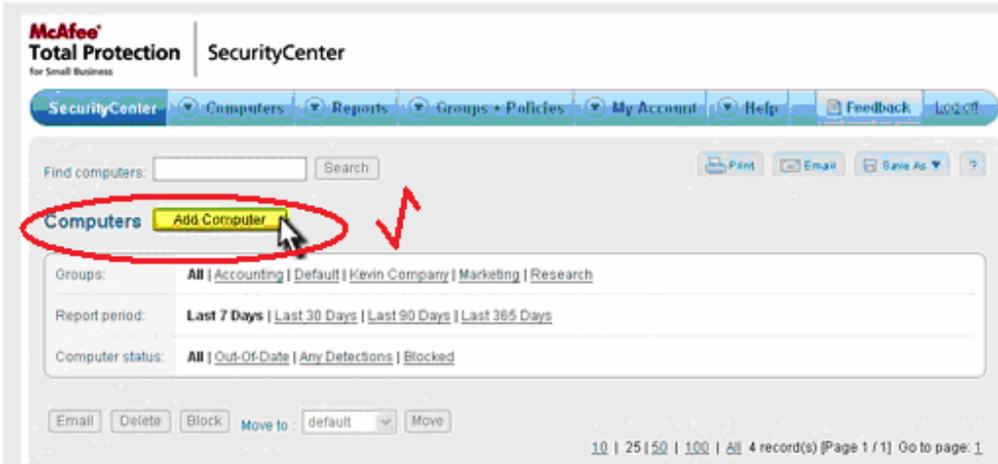
<p style="text-align: center;">TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE FIREWALL</p>	<p style="color: red; font-weight: bold; font-size: 1.2em;">CG11</p>	
<p>INSTITUTO DEL CAFÉ</p>		
<p>UNIDAD DE AUDITORÍA INTERNA</p>		
<p>EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS</p>		
<p>SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)</p>		
<p>Periodo a examinar del 01 de enero al 31 de marzo de 2009</p>		
<p>Ref.P/T</p>	<p>Procedimiento No. 4 del Programa CG</p>	
	<div style="text-align: center;">  </div> <p>Uso de software.</p> <p>✓ = Simulación realizada.</p>	
<p>Elaborador por: ACSG</p> <p>Fecha: 23Abr09</p>	<p>Revisado por: MRPM</p> <p>Fecha: 27Abr09</p>	<p>Supervisado por: AGR</p> <p>Fecha: 27Abr09</p>

TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE ANTIVIRUS		CG12
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
		
	<p>Comprobación de actualizaciones diarias.</p> <p>✓ = Verificada la actualización.</p>	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

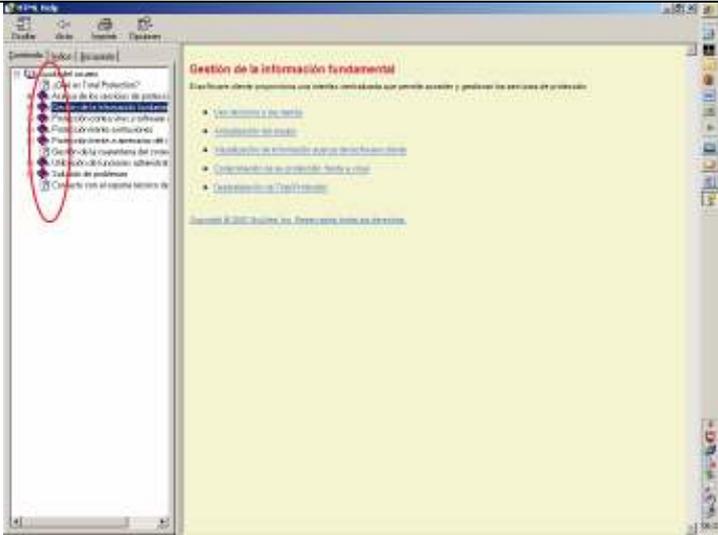
TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE ANTIVIRUS		CG13
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
		
	<p>Comprobación de apoyo técnico.</p> <p>✓ = Verificado apoyo técnico.</p>	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE ANTIVIRUS		CG14
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
	 <p>El software no presenta detección heurística integrada.</p>	
		
	 =Hallazgo.	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE ANTIVIRUS		CG15
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
	<p>SecurityCenter</p>  <p>✓ = Verificada la configuración por usuario.</p>	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE ANTIVIRUS		CG16
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
	 <p>✓ = Simulación de instalación realizada.</p>	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

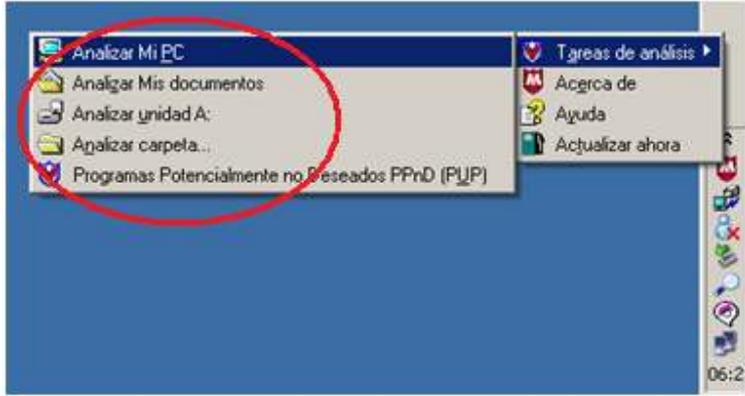
TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE ANTIVIRUS		CG17
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
	 <p>✓= Verificada pantalla de consola central.</p>	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE ANTIVIRUS		CG18
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
	 <p>No se encontraron referencias que indiquen que el software permita la creación de discos de emergencia o rescate.</p>	
		
	 = Hallazgo.	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

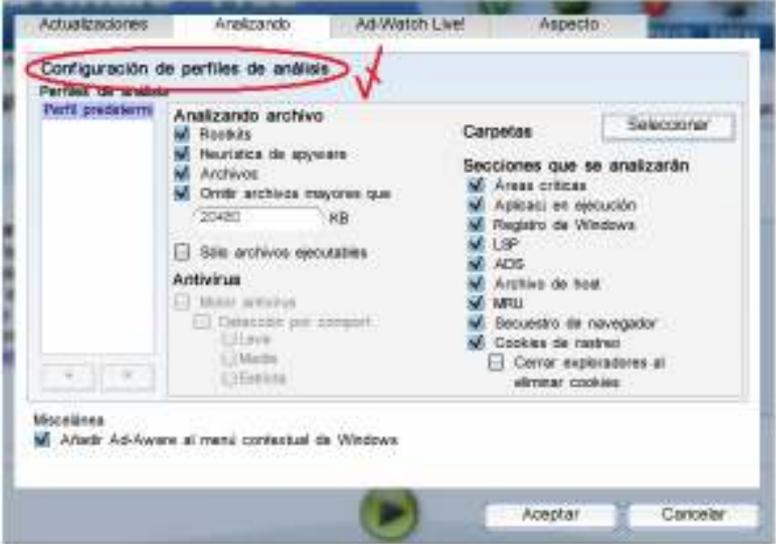
TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA NARRATIVA DE ANTIVIRUS		CG19										
INSTITUTO DEL CAFÉ												
UNIDAD DE AUDITORÍA INTERNA												
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS												
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)												
Periodo a examinar del 01 de enero al 31 de marzo de 2009												
Ref.P/T	Procedimiento No. 4 del Programa CG											
	<p>Se consultó web especializada de evaluación de antivirus (http://www.av-comparatives.org/comparativesreviews/main-tests) Mayo 2009, la cual presenta una certificación de antivirus disponibles en el mercado, para la cual utilizan varios parámetros, entre ellos: detección proactiva, falsas alarmas, rendimiento de equipo:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">CERTIFICATION LEVELS</th> <th style="text-align: center;">PRODUCTS</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">  </td> <td> Microsoft ESET NOD32 Kaspersky </td> </tr> <tr> <td style="text-align: center;">  </td> <td> AVIRA* G DATA* BitDefender* eScan* Sophos Symantec McAfee ✓ </td> </tr> <tr> <td style="text-align: center;">  </td> <td> AVG* TrustPort* Avast* F-Secure </td> </tr> <tr> <td style="text-align: center;">  </td> <td> Norman* Kingsoft* </td> </tr> </tbody> </table>		CERTIFICATION LEVELS	PRODUCTS		Microsoft ESET NOD32 Kaspersky		AVIRA* G DATA* BitDefender* eScan* Sophos Symantec McAfee ✓		AVG* TrustPort* Avast* F-Secure		Norman* Kingsoft*
CERTIFICATION LEVELS	PRODUCTS											
	Microsoft ESET NOD32 Kaspersky											
	AVIRA* G DATA* BitDefender* eScan* Sophos Symantec McAfee ✓											
	AVG* TrustPort* Avast* F-Secure											
	Norman* Kingsoft*											
	<p>De la anterior evaluación se puede determinar que el antivirus utilizado por la institución se encuentra en el segundo nivel, calificado como “avanzado” con 2 de 3 “estrellas” posibles de <i>ranking</i>.</p> <p>✓ = Verificada la evaluación.</p>											
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR										
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09										

TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA NARRATIVA DE ANTIVIRUS		CG20						
INSTITUTO DEL CAFÉ								
UNIDAD DE AUDITORÍA INTERNA								
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS								
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)								
Periodo a examinar del 01 de enero al 31 de marzo de 2009								
Ref.P/T	Procedimiento No. 4 del Programa CG							
	<p>Se consultó web especializada de evaluación de antivirus (http://www.av-comparatives.org/comparativesreviews/main-tests) a Mayo 2009, la cual evalúa el número de falsos positivos detectados por cada uno de los software analizados:</p> <table border="1"> <tr> <td>Very few false alarms (0-2):</td> <td>Microsoft</td> </tr> <tr> <td>Few false alarms (3-15):</td> <td>Sophos, Symantec, F-Secure, ESET, McAfee ✓, Kaspersky</td> </tr> <tr> <td>Many false alarms (over 15):</td> <td>AVG, eScan, Norman, AVIRA, BitDefender, TrustPort, Avast, G DATA, Kingsoft</td> </tr> </table> <p>De la anterior evaluación se puede determinar que el antivirus utilizado por la institución se encuentra en el nivel medio, en el cual se encuentran los software con detecciones de falsos positivos entre 3 y 15.</p> <p>✓ = Verificada la evaluación.</p>		Very few false alarms (0-2):	Microsoft	Few false alarms (3-15):	Sophos, Symantec, F-Secure, ESET, McAfee ✓, Kaspersky	Many false alarms (over 15):	AVG, eScan, Norman, AVIRA, BitDefender, TrustPort, Avast, G DATA, Kingsoft
Very few false alarms (0-2):	Microsoft							
Few false alarms (3-15):	Sophos, Symantec, F-Secure, ESET, McAfee ✓, Kaspersky							
Many false alarms (over 15):	AVG, eScan, Norman, AVIRA, BitDefender, TrustPort, Avast, G DATA, Kingsoft							
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR						
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09						

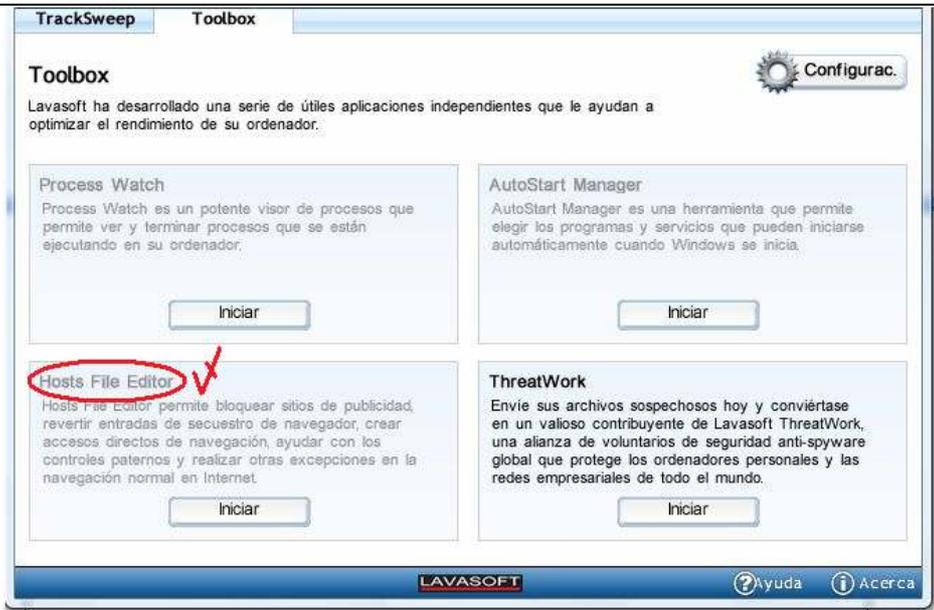
TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE ANTIVIRUS		CG21
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
	 <p>✓ = Verificados servicios de protección.</p>	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE ANTIVIRUS		CG22
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
	 <p style="text-align: right;">CG-1</p>	
	 = Hallazgo, no posee opción de análisis de arranque.	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE ANTIESPIÁS		CG23
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
	 <p>✓ Verificadas la selección de unidades.</p>	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE ANTIESPIAS		CG24
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
		
	✓ = Verificadas las opciones de análisis.	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

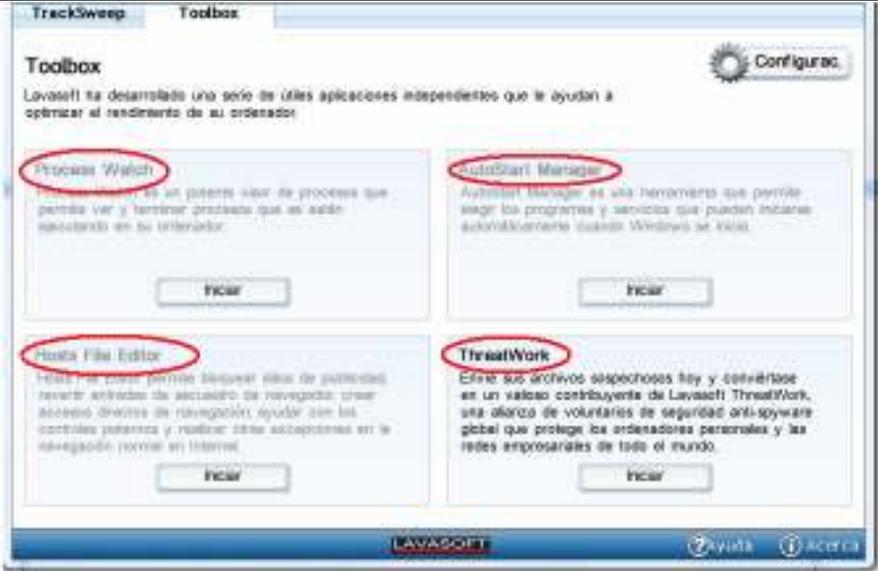
TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE ANTIESPIÁS		CG25
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
	 <p>✓ = Verificada la detección y bloqueo de aplicaciones.</p>	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

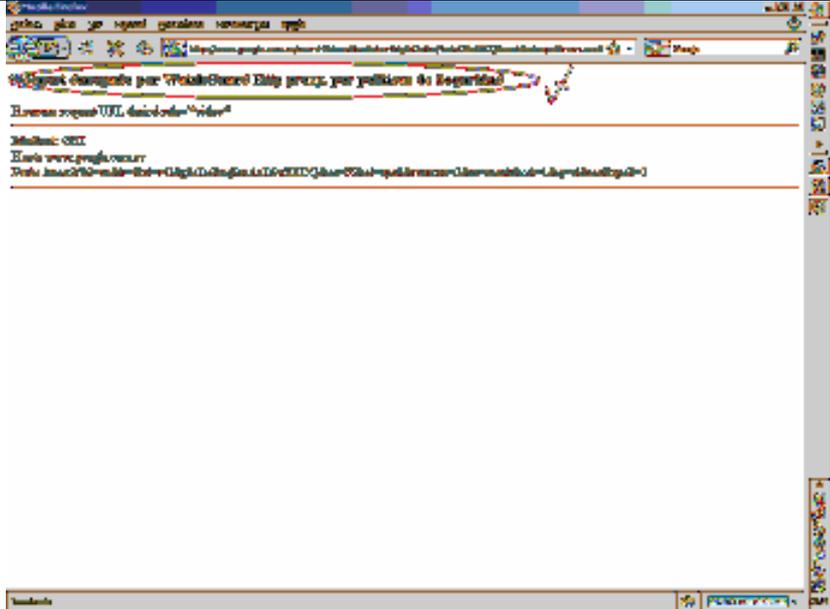
TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE ANTIESPÍAS		CG26
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
		
	<p>✓= Verificada capacidad de evitar secuestro de navegador.</p>	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

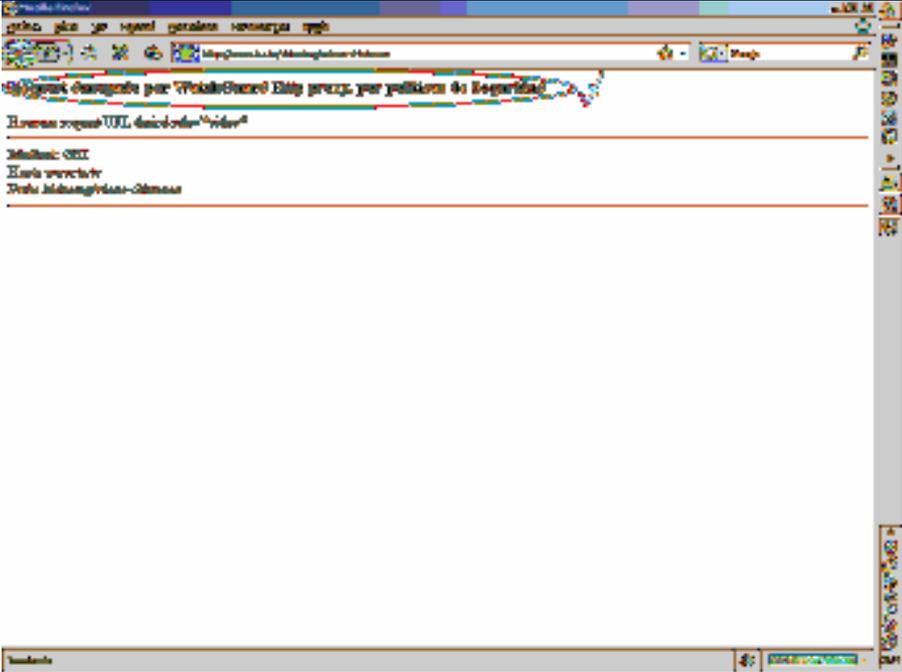
TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE ANTIESPÍAS		CG27
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
	 <p> <input type="checkbox"/> Establecer punto de restauración </p> <p> <input checked="" type="checkbox"/> = Comprobada la capacidad de copia de seguridad. <input checked="" type="checkbox"/> = Verificada la eliminación de amenazas. </p>	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE ANTIESPÍAS		CG28
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
	 <p>✓ = Verificada la protección en tiempo real.</p>	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE ANTIESPÍAS		CG29
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
	 <p>✓ = Verificada la opción de restauración de ficheros.</p>	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE ANTIESPÍAS		CG30
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
		
	 =Hallazgo, no posee bloqueo de barras.	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE FILTRADO DE IP		CG31
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
		
	<p> = Verificado bloqueo de IP para descarga de videos.</p>	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE FILTRADO DE IP		CG32
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
		
	 = Verificado bloqueo de IP sitio de ocio.	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA ANALÍTICA DE FILTRADO DE IP		CG33
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 4 del Programa CG	
		
	 =Hallazgo, no bloqueo acceso a sitio de ocio.	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

TECNOLOGÍA CONTRA SOFTWARE MALICIOSO CÉDULA DE HALLAZGOS	CGn1
INSTITUTO DEL CAFÉ	
UNIDAD DE AUDITORÍA INTERNA	
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS	
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)	
Periodo a examinar del 01 de enero al 31 de marzo de 2009	
Procedimiento No. 13 del Programa CG	
<p>TITULO: Firewall no presenta opciones de registros de pistas.</p> <p>CONDICIÓN: La protección de firewall no presenta opciones de registro de pistas que permitan darle seguimiento a las detecciones de intrusos bloqueados.</p> <p>CRITERIO: Según las normas de control interno de la institución en el artículo 42 literal f) de la sección “Software de Seguridad”, establece lo siguiente: Los software de seguridad adquiridos, deben tener una opción que permita registrar el acceso de usuarios autorizados o no, a la información del sistema.</p> <p>CAUSA: Al momento de adquirir el software de seguridad “firewall”, la decisión de compra no contemplo los requisitos establecidos en las normas de control interno de la institución, porque la obtención de un software que cumpla con todos los requisitos detallados en el Art. 42 de las normas, provocaría una inversión excesiva.</p>	

EFEECTO:

La información de la institución se encuentra vulnerable a accesos no autorizados, ya que no existen registros de pistas que permitan darle seguimiento a las detecciones de intrusos bloqueados.

RECOMENDACIÓN:

Uno de los activos más importantes que la institución posee, es la información, por lo que los software de seguridad, adquiridos deberán cumplir con todos los requisitos mínimos establecidos por la institución.

Elaborador por: **ACSG**

Revisado por: **MRPM**

Supervisado por: **AGR**

Fecha: 24Abr09

Fecha: 24Abr09

Fecha: 27Abr09

TECNOLOGÍA CONTRA SOFTWARE MALICIOSO COMUNICACIÓN DE RESULTADOS	CG_{n2}
INSTITUTO DEL CAFÉ	
UNIDAD DE AUDITORÍA INTERNA	
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS	
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)	
Periodo a examinar del 01 de enero al 31 de marzo de 2009	
Procedimiento No. 14 del Programa CG	
<p>San Salvador, 27 de abril de 2009.</p> <p>Ingeniero José Arturo Erazo Gerente de Informática Presente.</p> <p>Hemos efectuado la Evaluación del Control Interno de los Sistemas de Información Computarizados, al sistema de cuentas por cobrar (Deudores Monetarios) correspondiente al periodo comprendido del 01 de enero al 31 de marzo de 2009.</p> <p>Como resultado de nuestro examen, hemos identificado una diferencia entre los requisitos mínimos para adquirir un software de seguridad, establecidos en las normas de control interno de la institución y el firewall de seguridad que la institución está utilizando.</p> <p>Con la finalidad de cumplir con lo dispuesto en el artículo 33 de la ley de la Corte de Cuentas de la República, y obtener mayores elementos de juicio que nos permitan brindar recomendaciones adecuadas, atentamente solicitamos a usted presentar por escrito sus explicaciones o</p>	

comentarios, adjuntando la evidencia documental correspondiente, a más tardar dentro de los cinco días hábiles siguientes contados a partir de la fecha en que reciba esta nota.

Es oportuno mencionar, que la falta de respuesta a nuestra solicitud en el plazo señalado, nos indicará que las observaciones y recomendaciones planteadas han sido aceptadas por ustedes.

Aprovecho la oportunidad para expresarle las muestras de mi consideración y estima.

DIOS UNION LIBERTAD

Lic. Alexis Guillermo Rivera
Jefe de la UAI.

Elaborador por: **ACSG**

Revisado por: **MRPM**

Supervisado por: **AGR**

Fecha: 27Abr09

Fecha: 27Abr09

Fecha: 27Abr09

CONTROLES DE DATOS CÉDULA SUMARIA		CD₁
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 1 del Programa CD	
CD_n	Disponibilidad de datos	
CD_n	Integridad de datos	
CD_n	Flujos de datos	
CD_n	Almacenamiento y conservación de datos	
	<p><u>CONCLUSIÓN:</u></p> <p>En base a la evaluación realizada a los controles lógicos de datos, concluimos, que la institución cuenta con controles que presentan un grado de seguridad razonable.</p>	
Elaborador por: ACSG	Revisado por: MRPM	Supervisado por: AGR
Fecha: 23Abr09	Fecha: 27Abr09	Fecha: 27Abr09

CONTROLES DE APLICACION CÉDULA SUMARIA		CA1
INSTITUTO DEL CAFÉ		
UNIDAD DE AUDITORÍA INTERNA		
EVALUACIÓN DEL CONTROL INTERNO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS		
SISTEMA DE CUENTAS POR COBRAR (DEUDORES MONETARIOS)		
Periodo a examinar del 01 de enero al 31 de marzo de 2009		
Ref.P/T	Procedimiento No. 1 del Programa CA	
CA_n	Diseño de pistas de auditoria	
CA_n	Mecanismos de autorización	
CA_n	Simulación paralela	
CA_n	Informes de Excepción	
CA_n	Evaluaciones periódicas al software	
CA_n	Registro de actividades de cada terminal	
CA_n	Balanceo	
CA_n	Control de archivos	
CA_n	Control de archivos maestros	
CA_n	Procedimientos de corte	
CA_n	Integridad de la configuración	
CA_n	Programación de tareas en secuencia eficiente	
CA_n	Automatización del monitoreo de cambios a sistemas	
CA_n	Administración de incidentes	
CA_n	Control de versiones	
CA_n	Integridad de transacciones	
CA_n	Prueba de regresión	

	<p><u>CONCLUSIÓN:</u></p> <p>En base a la evaluación realizada a los controles lógicos de aplicación, concluimos, que la institución cuenta con controles que presentan un grado de seguridad razonable.</p>
<p>Elaborador por: ACSG</p> <p>Fecha: 23Abr09</p>	<p>Revisado por: MRPM</p> <p>Fecha: 27Abr09</p> <p>Supervisado por: AGR</p> <p>Fecha: 27Abr09</p>