UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Técnica Particular de Loja

ESCUELA DE CIENCIAS DE LA COMPUTACIÓN

MODALIDAD A DISTANCIA

DISEÑO DE UNA GUÍA DE AUDITORÍA PARA EVALUAR EL CONTROL INTERNO INFORMÁTICO EN LA EMPRESA HASOFINAD DE LA CIUDAD DE QUITO

TESIS DE GRADO PREVIA LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

AUTOR:

MIREYA ALEXANDRA HERRERA ORTIZ

DIRECTOR:

ING. DIANA CUENCA B.

CENTRO UNIVERSITARIO QUITO

2010

CERTIFICACIÓN

Ing. Diana Cuenca B.
DIRECTOR DE TESIS

CERTIFICA:

Que el presente trabajo de investigación, previo a la obtención del título de Ingeniero en Informática, fue revisado durante todo el proceso de desarrollo desde su inicio hasta su culminación, por lo cual autorizo su presentación.

Ing. Diana Cuenca Benítez

Loja,

CESIÓN DE DERECHOS

Yo Mireya Alexandra Herrera Ortiz, declaro ser autor del presente trabajo y eximo expresamente a la Universidad Técnica Particular de Loja y a sus representantes legales de posibles reclamos o acciones legales.

Adicionalmente declaro conocer y aceptar la disposición del Art. 67 del Estatuto Orgánico de la Universidad Técnica Particular de Loja que en su parte pertinente textualmente dice: "Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través o con el apoyo financiero, académico o institucional (operativo) de la Universidad.

……..…….

Mireya Alexandra Herrera Ortiz

AUTORÍA

Los conceptos, ideas opiniones desarrolladas en el presente trabajo son de exclusiva responsabilidad de los autores.

DEDICATORIA

Todo el esfuerzo realizado para la elaboración de este trabajo lo dedico a mis hijos Gabriel y Xavier, por ser la motivación principal para seguir adelante; a mis padres, Marco y Alicia, por el amor que me han brindado y por los valores que me inculcaron; a mi tía Myriam, que ha estado presente en cada uno de mis logros; a mis abuelitos queridos, Alberto y Carlota, que con su cariño han llenado mis días. Y un agradecimiento especial a Dios, que está siempre a mi lado y es quien me ha dado la fuerza y el coraje para superarme cada día.

AGRADECIMIENTO

Un especial agradecimiento a la Universidad Técnica Particular de Loja, a sus autoridades y directivos; de manera muy especial a mi Directora, Ing. Diana Cuenca, quien con sus vastos conocimientos e inapreciables consejos me ha guiado. A todos mis profesores, a lo largo de esta carrera, por los conocimientos impartidos, que aportaron para mi desarrollo como profesional y como mejor ser humano.

INTRODUCCIÓN

La globalización y el vertiginoso avance de la tecnología, así como la creciente importancia que se está dando a la información, como el principal activo y motor del crecimiento y sostén de una organización, han cambiado de manera sustancial la mentalidad de los tomadores de decisiones en el ámbito nacional para asumir los nuevos desafíos.

Es así que la información, es la base de la empresa del siglo XXI y son, precisamente, los nuevos administradores quienes la utilizan para la planificación y el logro los objetivos organizacionales, comprendiendo la necesidad de la aplicación y mejora de los procesos de TI, para satisfacer las necesidades y expectativas de sus clientes y las de sus negocios.

Es en este contexto, en el que la seguridad del ambiente informático, desde todos sus puntos, se ha convertido en una necesidad inherente al proceso administrativo exitoso. La falta de evaluación y actualización de los procesos de control interno ha generado una serie de complicaciones y conflictos, que ha derivado en la inconsistencia, en el menor de los casos, hasta una pérdida irreparable de información crítica, sobre la cual se basan decisiones importantes para el buen funcionamiento de una organización, por lo que se considera de suma importancia la redefinición de procesos de control eficaces y la consiguiente elaboración de políticas para poder alcanzar los objetivos de un ambiente de información eficiente y confiable.

La propuesta planteada de una guía de procedimientos estándar para evaluar las debilidades de los controles internos, ha sido desarrollada con la finalidad de diseñar los instrumentos y herramientas necesarios para que, tanto los auditores cuanto los administradores puedan contar con elementos suficientes para que sus procesos y actividades se ejecuten con eficiencia, eficacia y que sus recursos sean utilizados de manera apropiada, buscando así aportar al logro y consecución de los objetivos institucionales.

Para su propósito, la investigación se ha organizado en varios capítulos y temas que en

conjunto responden al objetivo planteado.

En el capítulo I, se presentan las consideraciones acerca de la evaluación de control interno en sistemas computarizados de información. El procesamiento computarizado somete uniformemente todas las transacciones similares a las mismas instrucciones de procesamiento, sin embargo, la posibilidad de errores, como un riesgo de los datos ingresados al computador para procesamiento, pueden tener errores o ser incompletos. La guía contendrá las características diferenciales de los sistemas de control interno informático

En el capítulo II, se describe la evaluación de los controles generales y de aplicación. Su importancia radica en el tratamiento de un ambiente de control adecuado, fundamentado en la actitud asumida con respecto al control interno por todos los funcionarios de una organización, así como de la Dirección Superior, y el personal informático. Se definirán los procedimientos de cumplimiento de las normas éticas, de seguridad y de control interno.

En el capítulo III, se detalla el Desarrollo de una base de información. El proceso de una evaluación de control interno comienza con el conocimiento de la estructura global de toda la organización, partes del negocio, sistemas de transacciones, u otros componentes que deban ser evaluados. Una parte importante de este proceso consistirá en obtener una comprensión global del Sistema de Información Computarizado de una organización. En este contexto, los sistemas de control interno serán considerados globalmente, incluyendo los siguientes aspectos: (1) estructura y administración del sistema y (2) hardware, software, y métodos de comunicaciones de datos utilizados.

En el capítulo IV, se dan a conocer las consideraciones de riesgo. Se considerará las características especiales de los sistemas computarizados y sus riesgos asociados, así como el análisis específico de la implantación de los controles y la evaluación de su funcionamiento.

En el capítulo V, se describen pruebas de controles. Se incluirá los procedimientos de evaluación a los procesos informáticos considerando la segregación de tareas en ambientes informáticos, controles de acceso a los programas, así como de los datos de ingreso, procesamiento y salida.

En el capítulo VI, se explicará la aplicación del modelo COBIT, que fue desarrollado como un estándar para las buenas prácticas de seguridad y control en tecnología de información, este modelo será utilizado para evaluar los riesgos existentes, a través de los 34 objetivos de control de alto nivel de este modelo y operar a un nivel superior a los estándares de tecnología para la administración de los sistemas de información.

En el capítulo VII se presenta la Aplicación práctica de la evaluación de control interno. Una vez concluida la Guía de Auditoría, esta será aplicada en la evaluación del ambiente de control interno informático en la empresa.

Finalmente, el capítulo VIII recoge un seguimiento de recomendaciones. Las Recomendaciones son acciones correctivas que se presentan en los informes de auditoria o en informes especiales de carácter preventivo, como producto de las deficiencias encontradas en la evaluación del control interno en ambientes informáticos y son dirigidas a las autoridades competentes que tienen la facultad de implementarlas. La tesis presentará como una actividad de retroalimentación el seguimiento de las recomendaciones planteadas a fin de conocer la efectividad de su implementación.

Esta Guía de Auditoría podrá ser aplicada en la evaluación del ambiente de control interno informático en empresas reales, considerando además en lo pertinente, los estándares de ISACA ((Information Systems Audit and Control Association) que contienen principios básicos y procedimientos esenciales de auditoría, que el auditor de Sistemas Informáticos debe tener en cuenta durante un proceso de auditoría.

ÍNDICE GENERAL

CAPITULO I

CONSIDERACIONES ACERCA DE LA EVALUACIÓN DE CONTROL INTERNO EN SISTEMAS DE INFORMACIÓN

1.1 CONTROL INTERNO. GENERALIDADES.

Actualmente, la información y la tecnología son consideradas como activos valiosos dentro de las organizaciones, ya que las decisiones apropiadas que tomen los directivos se basan en datos precisos y veraces. Para lograr una administración efectiva, se debe tener un conocimiento suficiente sobre los riesgos que implica la tecnología de la información, para poder aplicar los controles necesarios dentro de la organización.

Es en este contexto que, es ineludible contar con un ambiente de control conveniente, en donde exista un marco de control interno que regule y asegure procesos internos eficaces, así como las debidas políticas y procedimientos organizacionales, en donde todos los miembros de la empresa que operan los sistemas informáticos sean partícipes de sus deberes y responsabilidades de forma que, sean sus acciones las más adecuadas para la obtención conjunta de los objetivos organizacionales.

El control, según la metodología COBIT se define como: "Las Políticas, Procedimientos, Prácticas y Estructura Organizacional, diseñadas para proveer una razonable seguridad de que los objetivos del negocio serán alcanzados y los eventos indeseados serán prevenidos o detectados y corregidos [1]."

El informe COSO define al control interno como: "Proceso diseñado para entregar seguridad en: Efectividad y eficiencia en las operaciones, seguridad en reportes financieros y cumplimiento de leyes y regulaciones. [2]"

Es así que, el principal objetivo del control interno en el ambiente de TI, que es el que nos compete, es salvaguardar uno de los activos más importantes de las organizaciones, la información. Precisamente, para que un control interno sea fiable, deberá asegurar la integridad y exactitud de los datos.

1.2 OBJETIVOS DEL CONTROL INTERNO EN AMBIENTES TI

En ambientes de la Tecnología de Información, los objetivos de control interno [3] son los

siguientes:

- La protección de los activos de información, como datos, software y hardware.
- Observancia de normas legales e internas de la organización.
- Mantener integridad y precisión en los datos.
- Fiabilidad de procesos y eficacia en la utilización de recursos organizacionales.

Entonces, el objetivo integral de control en un ambiente informatizado es asegurar la consistencia y fiabilidad de los datos procesados y de actividades que se desempeñan, a través de buenas prácticas y procedimientos eficaces.

1.3 RELACIÓN DEL CONTROL INTERNO CON LA MISIÓN Y OBJETIVOS DEL NEGOCIO

Estos últimos años, las organizaciones explotan los beneficios del desarrollo de la TI, dependiendo cada vez más de ella y utilizándola como un recurso óptimo para planificación estratégica para lograr los objetivos institucionales. Es así que, el uso apropiado de funciones automatizadas en la empresa, ha determinado una evolución de las estructuras de los controles internos, lo que a su vez, implica un cambio sobre la planificación y aplicación de los procesos de control administrativo y operacional. En este contexto, la evaluación de los objetivos de control en TI está íntimamente ligada a los objetivos organizacionales.

Ahora bien, dado que la declaración de la misión suministra el contexto para formular la línea de negocios específica en la que actuará la empresa y las estrategias mediante las cuales operará, establece el campo en el que va a competir, determina la manera cómo se asignarán los recursos y cuál es el modelo general del crecimiento y dirección para el futuro, el control interno deberá formar parte de esas estrategias, para asegurar el cumplimiento de esa misión.

Los controles internos viabilizan los procesos, no sólo administrativos sino también operativos, pues posibilita la superación de riesgos para poder alcanzar las metas y objetivos trazados por los directivos de la organización. De ahí que, una evaluación de controles planificada con cuidado, permitirá descubrir ineficiencias o insuficiencias que

pudieran poner en peligro la gestión eficiente del negocio. Es en este contexto, en el que los controles internos deben ser responsabilidad de todo el personal directivo, administrativo y operativo de la empresa.

Según COBIT 4.1 [4], el Sistema de Control Interno impacta en TI en lo siguientes tres niveles:

"• Al nivel de dirección ejecutiva, se fijan los objetivos de negocio, se establecen políticas y se toman decisiones de cómo aplicar y administrar los recursos empresariales para ejecutar la estrategia de la compañía. El enfoque genérico hacia el gobierno y el control se establece por parte del consejo y se comunica a todo lo largo de la empresa. El ambiente de control de TI es guiado por este conjunto de objetivos y políticas de alto nivel.

• Al nivel de procesos de negocio, se aplican controles para actividades específicas del negocio. La mayoría de los procesos de negocio están automatizados e integrados con los sistemas aplicativos de TI, dando como resultado que muchos de los controles a este nivel estén automatizados. Estos se conocen como controles de las aplicaciones. Sin embargo, algunos controles dentro del proceso de negocios permanecen como procedimientos manuales, como la autorización de transacciones, la separación de funciones y las conciliaciones manuales. Los controles al nivel de procesos de negocio son, por lo tanto, una combinación de controles manuales operados por el negocio, controles de negocio y controles de aplicación automatizados. Ambos son responsabilidad del negocio en cuanto a su definición y administración aunque los controles de aplicación requieren que la función de TI dé soporte a su diseño y desarrollo.

• Para soportar los procesos de negocio, TI proporciona servicios, por lo general de forma compartida, por varios procesos de negocio, así como procesos operativos y de desarrollo de TI que se proporcionan a toda la empresa, y mucha de la infraestructura de TI provee un servicio común (es decir, redes, bases de datos, sistemas operativos y almacenamiento). Los controles aplicados a todas las actividades de servicio de TI se conocen como controles generales de TI. La operación formal de estos controles generales es necesaria para que dé confiabilidad a los controles en aplicación. Por ejemplo, una deficiente administración de cambios podría poner en riesgo (por accidente o de forma deliberada) la confiabilidad de los chequeos automáticos de integridad."

1.4 COMPONENTES DEL CONTROL INTERNO

Según el Informe COSO, primera parte, los componentes del control interno son cinco, interrelacionados e interactuantes [5], que deben estar presentes en cualquier sistema de control interno en cualquier organización, siempre de la mano con evaluaciones periódicas de dichos controles. Estos componentes son:

1.4.1 Ambiente de Control

El entorno de control es el lugar en el que el personal de una empresa desarrolla sus actividades y tareas diarias, cumpliendo con sus responsabilidades de control, siendo este el fundamento de todos los demás componentes, pues desde aquí parte la estructura y funcionamiento de una empresa.

Los factores que determinan el ambiente de control encierran la integridad y los valores éticos, tales como la aplicación de códigos de conducta y políticas para regular las prácticas profesionales plausibles, así como la ética y estilo de la dirección, pues la cultura de la organización, y por tanto, el ambiente de control, suelen ser influidos por la experiencia, calidad y acciones de los directivos o altos ejecutivos, determinando la eficacia o ineficacia en la implantación y aplicación del control interno.

En lo que concierne al ambiente de control en ambientes de TI, es la jefatura del Departamento de Sistemas junto con la administración de la organización, la responsable de la planificación, organización, recurso humano, dirección y control del departamento. Es así que, establecer y mantener un apropiado ambiente de control, es una de sus funciones más importantes. Quien está dirigiendo el departamento de TI, influye directamente en el ambiente de control, pues si no asume un verdadero compromiso con las actividades de control delineadas, lo más factible es que los empleados no le den la importancia suficiente a las políticas y normativas existentes, poniendo en riesgo la confiabilidad de la información de la empresa.

Así mismo, los funcionarios deben tener un nivel de capacidad apropiado para los distintos niveles y puestos del departamento, con suficientes y actualizados conocimientos y habilidades, de tal manera que puedan entender adecuadamente el valor del significado de un ambiente de control propicio relacionado con sus

responsabilidades.

Es así que, los procesos de evaluación de desempeño, capacitación, remuneración y promoción, deben asegurar el establecimiento de procedimientos que reconozcan y valoricen la contribución de la competitividad profesional del personal del departamento de TI.

Es en este contexto, en el que el ambiente de control suficientemente fuerte y bien establecido, permite obtener un mayor grado de confianza en los controles implantados, así como una reducción de la cantidad de evidencia que se requiere para lograr el objetivo de auditoría.

1.4.2 Evaluación de riesgos

El control interno, básicamente, contribuye a la mitigación de los riesgos que afectan la gestión del negocio. En toda organización existen riesgos, tanto internos como externos, que deben ser evaluados y esta evaluación del riesgo consiste en la identificación y análisis de dichos factores que afectarían el logro de los objetivos planteados. Basados en esta evaluación, se podrá determinar la mejor manera para administrar y controlar esos riesgos.

La vulnerabilidad de un sistema puede ser evaluado mediante una investigación y análisis de los riesgos más relevantes y hasta qué punto el control implantado puede neutralizarlos. Para realizar una evaluación de riesgos adecuada, se debe tener un conocimiento suficiente de la organización y de sus estructuras, para poder identificar las debilidades y gestionar los controles necesarios para corregirlas, de tal manera que los riesgos asociados sean mitigados. Generalmente, se analizan los riesgos asociados a:

- Confidencialidad, el riesgo que personal no autorizado modifique información sensible.
- Disponibilidad, el riesgo de no disponer de la información cuando el proceso de negocio la requiere y no proteger convenientemente los recursos y capacidades asociadas.
- Integridad, el riesgo de no garantizar precisión, suficiencia y validez de la información, acorde con los valores y expectativas del negocio.

1.4.3 Actividades de control

Las actividades de control son procedimientos que permiten asegurar que las políticas de la dirección se ejecutan apropiadamente. Las actividades de control deben tomar en cuenta los riesgos que fueron determinados en el estudio anterior y ser asumidas por la dirección.

Los controles se seleccionan de acuerdo a un estudio costo-beneficio, de tal manera que el costo de su implementación justifique una reducción real de los riesgos, con su consecuente valor adicional, es decir, una disminución en posibles pérdidas potenciales. La importancia de una selección e implementación de controles adecuados, consiste en que los riesgos que se han detectado sean mitigados, de tal manera que estos sean reducidos a un nivel aceptable.

1.4.4 Información y comunicación

En un ambiente informatizado, lo más importante es que la información relevante que se encausa y se almacena, sea recibida, procesada y divulgada, para que sea distribuida de forma segura a toda la organización. Es así, la información debe ser transmitida a través de canales efectivos y multidireccionales para obtener una comunicación realmente eficaz. Los datos de salida deberán ser validados en un sistema, de tal manera que el procesamiento sea el correcto. Es decir, para que la información sea confiable, íntegra y esté disponible en cualquier momento, se deben tener en cuenta ciertos controles que aseguren estas características, que determinan la seguridad de un sistema de información.

1.4.5 Monitorización

La monitorización de sistemas es uno de los cimientos en los que se apoya la seguridad, dado que permite conocer con certeza si las medidas de seguridad implementadas a través de controles están activadas para la detección de incidentes.

Las actividades de monitoreo deben ser permanentes e incluir acciones de supervisión constante por parte del personal asignado en un departamento de TI. Estos profesionales serán los responsables del mantenimiento y revisión de las actividades de supervisión, que estarán enmarcadas en un proceso de revisión definido por la jefatura.

Este proceso debe asegurar que las revisiones sean hechas en respuesta a

cambios que pudieran afectar el análisis de riesgos para la organización. Además, facilita las auditorías informáticas que pudieran requerirse, pues a través del monitoreo permanente y constante, se van guardando registros, de donde se pueden obtener evidencias de desvíos a los controles establecidos, así como incidentes de seguridad detectados en los sistemas.

Las actividades de monitorización se diferencian con las auditorías internas periódicas porque las primeras son realizadas en forma rutinaria, diaria.

Posteriormente se emitió la Segunda Parte del Coso, denominado ERM (Enterprise Risk Management) [6] con los siguientes tres componentes adicionales:

- Establecimiento de objetivos
- Identificación de eventos
- Respuesta a los riesgos

1.4.6 Establecimiento de objetivos

Este componente es aplicado cuando la administración de la organización considera la estrategia de riesgos en la formulación de los objetivo, formalizando su cuantificación a nivel de entidad, es decir, una visión a alto nivel, de cuánto riesgo están dispuestos a aceptar quienes están en alta dirección, estableciendo además, una tolerancia al riesgo respecto al nivel aceptable de variación de cumplimiento de los objetivos.

1.4.7 Identificación de eventos

En este componente se distinguen los riesgos y las oportunidades. Los riesgos, considerados como sucesos que pueden tener un impacto negativo, y las oportunidades que son los eventos que pueden tener un impacto positivo. Consiste entonces, en identificar los incidentes que pueden afectar la estrategia y el logro de los objetivos. Determina además, cómo los factores internos y externos se combinan e interactúan para influenciar su perfil en los riesgos.

1.4.8 Respuesta al riesgo

Identifica y evalúa las posibles respuestas al riesgo, es decir, transfiriendo, compartiendo, reduciendo o aceptando determinados riesgos existentes en la organización y evaluando a su vez, la relación costo – beneficio de cada potencial respuesta, y el grado en que ésta reducirá el impacto y/o la probabilidad de ocurrencia.

1.5 TIPOS DE CONTROLES

Los controles internos para sistemas informáticos han ido evolucionando conforme la tecnología ha seguido avanzando. Los controles que se utilizaban hace unos diez años, hoy en día son insuficientes, pues el entorno informático es totalmente diferente, dado el creciente uso de todo tipo de transacciones y comunicaciones a través de Internet, medios de almacenamiento nuevo, cambios en la cultura informática, implementación de redes sociales, entre otros cambios tecnológicos. Desde los más simples controles manuales hasta mecanismos complejos de control automatizado, el fin es el mismo: asegurar la integridad, disponibilidad y eficacia de los sistemas. Es así, que desde el punto de vista de los objetivos de los controles informáticos, se puede hablar de tres grupos generales:

1.5.1 Controles Preventivos

Controles diseñados para prevenir y disuadir eventos indeseables, antes de que suceda una intrusión en el sistema. Por ejemplo, mediante el uso de software de seguridad que impida accesos no autorizados a un sistema.

1.5.2 Controles Detectivos

Cuando está sucediendo una intrusión, los sistemas activados alertan la existencia de un intruso, basándose en los eventos que han sido disparados. Es en esta situación, en la que actúan los controles detectivos, durante la intrusión, cuando los controles preventivos han fallado. Por ejemplo, una reconfiguración dinámica de las reglas del firewall, un bloqueo de cuenta de usuario después de varios intentos de inicio de sesión fallidos, registros de actividad diaria para detectar errores u omisiones.

1.5.3 Controles Correctivos

Los controles correctivos facilitan la recuperación de un sistema a su estado anterior, es decir, retornar al sistema al estado que tenía antes del ataque o intrusión, en el menor tiempo posible. Por ejemplo, utilizar estrategias de copia de seguridad y planes de recuperación. También se pueden implementar controles correctivos en base a la experiencia de intrusiones ya ocurridas, al analizar las causas y debilidades que las ocasionaron.

1.6 IMPORTANCIA DE LA EVALUACIÓN DE LOS CONTROLES INTERNOS

En el contexto de ambientes informatizados, se puede afirmar con seguridad que el control interno es todo un sistema, utilizado por las organizaciones, establecido por la dirección, para realizar con confianza los procesos, con el fin de salvaguardar sus activos, protegerlos y asegurarlos en la medida de lo posible, para conservar la exactitud y la veracidad de la información que utilizan en todas las operaciones y actividades en los distintos departamentos de la organización, de tal manera que dicha información pueda fluir en todos los niveles con la mayor confiabilidad y eficiencia.

Si se hace un recuento de todas las ventajas que se desprenden de la implantación de controles internos adecuados, se concluye en la importancia de evaluar al sistema de control interno en ambientes informatizados, pues resulta práctico la medición de la eficiencia y la productividad al momento de implantarlos en su operación cotidiana, lo que facilita el conocimiento de la situación real en la entrada, procesamiento y salida de la información. Es también relevante en la práctica, el realizar una planificación conveniente a los objetivos de seguridad que se desean obtener, tal que permita verificar que dichos controles sean cumplidos, tal como se especifica en el plan, de tal manera que se pueda tener una mejor perspectiva sobre su gestión.

Un plan de evaluación del control interno que esté correctamente dirigido para conseguir los objetivos propuestos, es una base real sobre la que descansa la confiabilidad y exactitud de la información circulante, que a su vez, sirve como fundamento a los directivos para la toma de decisiones puntuales, a tiempo y acertadas. El nivel de fortaleza de un sistema informatizado establecerá si existe una seguridad razonable de

las operaciones y procesos sistematizados. En el caso contrario, un sistema de control interno poco confiable, será un aspecto negativo, que pone en peligro la precisión en la información procesada dentro de una organización.

Si no se aplican controles internos apropiados, el sistema informatizado corre el riesgo de tener desviaciones en sus procesos, consecuentemente, las decisiones que se tomen en base a información incorrecta no serán las más apropiadas para su cometido, así podría acarrear una conflictos operativos, derivándose una serie de efectos negativos que podrían poner en peligro la consecución de los objetivos organizacionales, pues los controles se establecen con el fin de reducir el riesgo de pérdidas o por lo menos, mitigarlas o reducirlas al máximo [7].

Es así que, para valorar la eficiencia de un sistema de control, es de vital importancia definir los objetivos que se quieran obtener al ser implementados y que estos procedimientos de control sean aplicados en forma organizada, en el orden establecido e interrelacionados entre ellos, lo que configura un sistema más fuerte y confiable. Cuando el sistema está operando, es necesaria la aplicación de pruebas para determinar si los controles implementados están funcionando tal como estaba previsto en el plan, pues los controles, lo que realizan es un trabajo de comprobación para asegurar que el sistema informatizado está desempeñando efectivamente las funciones que se le asignaron y que está cumpliendo los objetivos definidos.

1.7 GUÍA DE EVALUACIÓN DEL CONTROL INTERNO

CONSIDERACIONES PRELIMINARES ACERCA DE LA EVALUACIÓN DE LOS CONTROLES INTERNOS INFORMÁTICOS

El proceso de evaluación involucra la identificación de las debilidades potenciales, así como el diseño e implantación de los controles adecuados que las mitigan. La evaluación de los controles existentes en entornos informáticos dentro de una organización, normalmente suele realizarse para determinar la eficacia o ineficacia de esos controles. Habitualmente, si los controles generales o de aplicación no son confiables o no han sido evaluados, las pruebas necesarias para determinar el grado de confiabilidad de los datos procesados se amplían.

Aún si los controles del sistema han sido bien planeados y programados y son aplicados de manera inconsistente o incorrecta, entonces esos controles serán ineficaces. Existen muchos motivos para que los controles no sean considerados o sean ignorados por el personal, tales como resistencia al cambio por comodidad, falta de atención, inercia o simplemente eluden los controles para no perder tiempo. Así mismo, si no existe documentación suficiente acerca de los controles implementados, puede ser un indicio de que no existen controles adecuados, que no son entendidos o que son aplicados de manera impropia.

Una estrategia para conocer y comprender los controles existentes en el ambiente informático en una organización es entrevistar al personal usuario del sistema, pues son quienes tienen mayor conocimiento de las operaciones que se realizan a diario. Esta evidencia testimonial deberá ser ratificada a través de observación directa y otras pruebas.

Por todas estas razones, el auditor informático debe ser capaz de distinguir y escoger los procedimientos de control más significativos que serán evaluados y confirmar su eficacia. Así, podrá determinar si el sistema de control implementado en la organización está capacitado para prevenir, detectar y corregir cualquier error, así como encontrar deficiencias en los controles o la ausencia o ineficacia de los mismos.

Después de efectuada la evaluación de los controles del sistema, el auditor tiene que emitir una opinión sobre la eficacia, uso y capacidad de prevenir, detectar y corregir errores, así como el desempeño de los mismos. Esta opinión emitida en cuanto al grado de eficacia de los controles existentes, va a depender de la evidencia encontrada, que deberá ser relevante y confiable.

1.8 ESTUDIO INICIAL: CONOCER LAS CARACTERÍSTICAS DIFERENCIALES DE LOS SISTEMAS INFORMÁTICOS

Un sistema de información (SI) es un conjunto organizado de elementos, los cuales formarán parte de alguna de las siguientes categorías: personas, datos y actividades o técnicas de trabajo [8]. Todos estos elementos interactúan entre sí para procesar la información y distribuirla de la mejor manera a través de todos los niveles de la organización, en función de sus objetivos.

Un sistema informático, como cualquier otro sistema, es el conjunto de

hardware, software y de recursos humanos, todos estos componentes relacionados e interactuando entre sí. Si se describiera un sistema informático típico, se diría que lo compone un computador que usa dispositivos programables para capturar, almacenar y procesar datos, una persona que lo maneja y los periféricos que reciben y exteriorizan el resultado del procesamiento realizado. Pero, para que sea un verdadero sistema informático, deberían existir varios sistemas interconectados entre sí, que se comunican unos con otros a través de un grupo de reglas y condiciones: los protocolos. Estos definen la comunicación entre sistemas informáticos distintos que se encuentran conectados entre sí. Si dos sistemas informáticos usan el mismo protocolo, pueden interconectarse y ser parte de un sistema mayor.

El auditor informático, para iniciar su trabajo de evaluación en una empresa que usa computadores para el procesamiento de su información, debe tener en cuenta las características diferenciales de los sistemas informáticos, que, a saber, son las siguientes:

1.8.1 Procesamiento uniforme de transacciones

Los procesos realizados por un computador someten uniformemente todas las transacciones relacionadas a idénticas instrucciones de procesamiento. Por tanto, el evento de ocurrencia de que se produzcan errores al azar, un problema de control frecuente en entornos manuales, queda reducido. Sin embargo, los datos ingresados al computador por personas, para su procesamiento, de hecho si podrían tener errores o estar incompletos.

1.8.2 Posibilidad de errores e irregularidades no detectadas

En sistemas computarizados, el riesgo de que haya accesos no autorizados a los datos o de alteración de los mismos sin dejar evidencias perceptibles, puede ser mayor que en los sistemas manuales. Esto es porque la información es almacenada en forma electrónica, en donde la participación del hombre en el procesamiento es mínima, por lo tanto, se reduce la oportunidad de detectar manualmente los accesos no autorizados. Generalmente, en los entornos informáticos los recursos de información tienden a centralizarse.

1.8.3 Posibilidad de mayor supervisión gerencial

Los sistemas informáticos permiten que la gerencia pueda utilizar una extensa variedad de herramientas analíticas para revisar y supervisar las operaciones rutinarias de la empresa.

1.8.4 Rastreo de las transacciones

El diseño de algunos sistemas permite la conservación por un tiempo, en medios magnéticos, del rastreo de las transacciones con propósitos de auditoría.

1.8.5 Segregación de funciones incompatibles

La existencia de algunos controles internos, realizados por varios sujetos en los sistemas manuales, que podrían ser concentrados en sistemas informatizados.

1.8.6 Iniciación automática o ejecución de transacciones

Un computador es capaz de realizar automáticamente ciertas funciones, tal como la iniciación de algunas transacciones o los procesos que son necesarios para ejecutarlas, por lo que podrían o no existir evidencias visibles de estos procesos automáticos.

1.8.7 Los controles manuales dependen de la confiabilidad del procesamiento de datos

El procesamiento por computadora permite la obtención de informes y otros documentos que podrían ser usados para realizar controles manuales. La efectividad de los procedimientos de control manual puede depender de la efectividad de los controles sobre la integridad y exactitud del procesamiento realizado por un computador.

1.8.8 Los controles de aplicación dependen de los controles generales

Si no han sido establecidos controles generales apropiados sobre las actividades computarizadas, la efectividad de los controles automatizados, incluidos en el

software de aplicación, podría quedar disminuida.

1.9 CONOCIMIENTO DE LOS CONTROLES INTERNOS EN LOS SISTEMAS DE INFORMACIÓN

El auditor ha de conocer que en un entorno informático, se pueden tener tres tipos de controles y en cada uno de ellos se encontrarán controles específicos. Los controles más representativos de cada tipo, que el auditor deberá tomar en cuenta antes de planificar una evaluación, se describen a continuación.

1.9.1 Controles Preventivos

Son mecanismos específicos de control cuyo objetivo es anticiparse ante el evento de que se presenten situaciones no deseadas o inesperadas que pudieran afectar al logro de los objetivos y metas, por lo que se consideran más efectivos que los detectivos y los correctivos.

1.9.1.1 Sistemas de seguridad lógica

La seguridad lógica, se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información. Consiste en aplicar defensas y asegurar procedimientos para resguardar el acceso a los datos, de tal manera que sólo las personas con autorización puedan acceder a ellos.

La evaluación se debe realizar en los siguientes controles:

- Restricción del acceso a los programas y archivos.
- Identificación y autentificación. Se denomina Identificación al momento en que el usuario se da a conocer en el sistema; y Autenticación a la verificación que realiza el sistema sobre esta identificación.
- Definición de roles de usuario, donde se agrupan los derechos de acceso de acuerdo con el rol de los usuarios.
- Control de las transacciones, a través de accesos autorizados.
- Limitaciones a los servicios, existencia de restricciones para utilización de aplicaciones, ya sean establecidas por el administrador del sistema o por las

propiedades preestablecidas de la aplicación.

- Formas de acceso, es decir, los permisos otorgados al usuario sobre los recursos y a la información, tales como: lectura, escritura, ejecución, borrado, creación y búsqueda.
- Ubicación y horarios de uso de recursos. El administrador puede otorgar permisos de acceso a los usuarios dependiendo de la ubicación física o lógica de los datos o de las personas. Los controles en cuanto a horarios, limita el acceso de los usuarios a intervalos de tiempo determinados a los recursos disponibles.
- Controles de acceso interno, utilizados para efectuar la autenticación del usuario. Se implementan para proteger los datos y aplicaciones. Generalmente, se utilizan claves, encriptación, listas de control de acceso, límites a la interfaz de usuario.
- Control de acceso externo, tales como dispositivos de control de puertos, firewall, perfiles de acceso públicos.

1.9.1.2 Controles de validación y razonabilidad

Los controles de validación detectan los errores cometidos al ingresar información a un sistema. Los controles de razonabilidad verifican si el contenido de un campo ingresado corresponde a un rango determinado.

1.9.1.3 Segregación de funciones

La segregación de funciones para el acceso a los recursos de los sistemas de información, se aplicará para los usuarios del sistema, la entrada de datos, explotación, administración de redes y sistema, administración de cambios y seguridad.

1.9.2 Controles Detectivos

Son mecanismos específicos de control que actúan en el momento en que los eventos o acontecimientos están sucediendo e identifican las omisiones o desviaciones antes de que concluya un proceso determinado.

1.9.2.1 Pistas de auditoría

Una pista de auditoría es una lista de entradas de auditoría, que describen la vida útil de un objeto, archivos o eventos. Es una serie de registros sobre las actividades del sistema, de procesos o aplicaciones y de los usuarios del sistema e incluye información suficiente para determinar los eventos que han ocurrido en un sistema y quién o qué los disparó. Estas pistas de auditoría, de hecho, sirven para cumplir algunos objetivos, tales como: seguimiento de las acciones de los usuarios en el sistema, de eventos del sistema, detección de intrusiones e identificación de problemas. Entonces, estos datos almacenados de suceso/eventos, sean normales o anormales (errores, irregulares, ilegales, ilícitos, o fraudes), deberían tener una supervisión rutinaria para que sean detectados a tiempo, de tal manera que pasen de ser solo controles detectivos y constituirse en controles preventivos.

1.9.2.2 Informes de excepción

Los informes de excepción destacan las desviaciones en las operaciones normales de un sistema. Un informe de excepción tiene como finalidad avisar de los comportamientos anormales o desencadenar una acción determinada cuando se presentan, es decir, es un sistema de alerta o alarma, al realizar comprobaciones de la información captada con un estándar. Estos informes de excepción serán útiles si el estándar escogido es apropiado y si la desviación frente a él recoge realmente la excepción que ha de desencadenar la acción correctora.

1.9.2.3 Técnicas de backup y de recuperación

El backup es un sistema de respaldo y se refiere a realizar copias de archivos almacenados originalmente en discos rígidos, que almacenan información importante que una organización desea conservar en el tiempo. Dado que los sistemas están expuestos a fallas por distintas causas, ya sean naturales o provocadas, esta técnica es muy útil, de tal manera que el sistema pueda retornar a la normalidad en un corto tiempo. El respaldo de archivos es importante para asegurar la disponibilidad e integridad de los datos.

Hay tres tipos de técnicas de backup: Una completa, en donde se guarda una réplica exacta de los archivos que se van a proteger en un dispositivo de almacenamiento de respaldo. Otra, llamada incremental, en la que se almacenan solo aquellos archivos que han sido modificados desde la última copia de seguridad completa o incremental. Y la última, la diferencial, en la que se almacenan sólo los archivos que han sido modificados desde la última copia de seguridad completa.

Ahora bien, la recuperación de datos es el proceso de recuperar datos de los medios de almacenamiento dañados por cualquier causa. Estos daños pueden ser físicos o lógicos.

Actualmente, la recuperación de datos es una tarea menos complicada, pues con el avance de la tecnología y técnicas nuevas se lo puede hacer más sencillamente. Las técnicas más conocidas para recuperación de datos son las siguientes:

- Uso de herramientas que ofrecen los sistemas operativos, tales como la realización de copias de respaldo y recuperación de datos en los discos duros internos y externos.
- Uso de programas externos de recuperación de datos, que pueden obtenerse gratuitamente en el Internet o pagados.
- Transporte del disco duro que contiene los datos y el sistema operativo a otro equipo, configurándolo como esclavo, para obtener la recuperación de los archivos.
- Uso de cintas de respaldo, para hacer copias utilizando servidores de datos en plataformas Windows NT o Server, Linux, por ejemplo. Las empresas grandes utilizan comúnmente esta técnica.
- Uso de discos de respaldo, ya sean estos discos duros externos o cualquier tipo de disco óptico, como Cd/Dvd-Rom's o blue ray.

Para garantizar una recuperación eficiente y lo más rápida posible, hay que comprobar que existan los controles necesarios que aseguren que se mantienen copias de seguridad de la información del usuario, que es lo más crítico y en menor grado, un respaldo de la información del sistema, para lo cual deberían

existir políticas de respaldo. Las políticas de respaldo son una serie de normas que adoptan las empresas para almacenar su información, debido a la existencia de gran cantidad de datos y su importancia para la gestión del negocio. Estas normas rigen el ámbito de: seguridad, secuencia de utilización de dispositivos, estrategias de respaldo, y periodicidad del respaldo.

1.9.2.4 Batch totals

Es la suma de un campo determinado en una colección de artículos utilizados como control total para garantizar que todos los datos han sido introducidos en el computador. Por ejemplo, utilizando el número de cuenta como un batch (lote) total, todos los números de cuenta se suman manualmente antes de la entrada en el computador. Después de la entrada, el total es comparado con la suma de los números en el computador. Si no coinciden, los documentos fuente se deben cotejar manualmente con la lista del computador [9].

1.9.2.5 Hash totals

Es un método para garantizar la exactitud de los datos procesados. Se trata de un total de varios campos de datos en un archivo, incluidos los campos que no suelen utilizarse en los cálculos, tales como número de cuenta. En diversas etapas en la tramitación, el total de hash se vuelve a calcular y se compara con el original. Si alguno de los datos se ha perdido o cambiado, un desajuste señala un error [10].

1.9.3 Controles Correctivos

Son mecanismos específicos de control que poseen el menor grado de efectividad y operan en la etapa final de un proceso, el cual permite identificar y corregir o subsanar en algún grado omisiones o desviaciones.

1.9.3.1 Modificación de sistemas y programas

Según la descripción del Informe COSO, con respecto a la actividad de Tecnología de la información, el objetivo 2 [11] es: “Obtener, procesar y obtener la información de manera completa y exacta y entregársela a las personas para permitirles cumplir sus responsabilidades” y uno de los riesgos descritos es el de una

incorrecta implantación de las modificaciones de sistemas y programas, por lo que recomienda prácticas y actividades de control que deben tomarse en cuenta:

- Aprobación debida de solicitudes de cambio de programas y/o sistemas.
- Seguimiento de los cambios aprobados durante el proceso de cambio.
- Revisión y aprobación de los cambios por los usuarios del diseño definitivo de los cambios.
- Todos los cambios deben estar sujetos a pruebas, revisión y resultados por parte de los usuarios y de la dirección de SI.
- Aprobación por quien solicita la implementación de cambios sometidos a pruebas.
- Notificación a los departamentos de procesamiento de datos afectados por los cambios.
- Preparación y actualización de documentos como libro de gestión de operaciones, manuales del usuario, descripciones de programas y del sistema.

1.9.3.2 Restauración de ficheros

Las copias de seguridad protegen la continuidad del negocio en caso de pérdidas de archivos, ya sea por error humano, por ataques de virus, falla inesperada del software e inclusive por fallas en el servicio eléctrico. La finalidad del procedimiento de respaldo es proteger la disponibilidad e integridad de la información. Cuando los eventos indeseables ya han sucedido y si se han seguido con las políticas de respaldo y recuperación, se dispondrá de copias de seguridad de los archivos importantes para la organización. Es entonces, que se aplicará este control correctivo: la restauración de archivos, a partir de esas copias de archivos que podrán ser restaurados si se pierden o dañan los archivos originales, en el menor tiempo posible, para asegurar que las actividades y procesos de la empresa continúen.

Para restaurar archivos de forma segura y efectiva, en el caso de eliminación, modificación o corrupción, existen herramientas específicas en cada sistema operativo, así como también herramientas comerciales. Para lograrlo, se debe asegurar que las copias de seguridad sean programadas, ya sea diario, semanal o mensualmente, así como determinación de medios de almacenamiento más convenientes, ya sean dispositivos externos o en red. Sin embargo, no sólo es

recomendable mantener copias de seguridad para restauración de ficheros sino también de controladores y estados del sistema.

CAPITULO II

EVALUACIÓN DE LOS CONTROLES GENERALES Y DE APLICACIÓN

Dado que los sistemas informáticos de cualquier organización son fundamentales para la gestión del negocio, deben ser controlados apropiadamente. Según ISACA, los procedimientos de control de SI, incluyen políticas y prácticas establecidas por la gerencia para proveer seguridad razonable de que los objetivos específicos serán alcanzados [12]. Es así que se han determinado estos procedimientos de control, que se agrupan en dos categorías principales: Los controles generales, que se aplican a todos los procesos u operaciones que se aplican en un entorno informatizado, con el objetivo de garantizar que éste sea seguro y confiable; y, los controles de aplicación, incorporados directamente en aplicaciones individuales, cuya finalidad es la de garantizar un procesamiento confiable y exacto.

Los procedimientos de control, para que sean efectivos, deberán ser apropiados, es decir, que se debe aplicar el control correcto en el lugar correcto y que sea conforme al riesgo que se quiera mitigar. Así mismo, deberán funcionar en consistencia al plan determinado, es decir, deben ser cumplidos al pie de la letra y de forma cuidadosa por todo el personal. El costo de su implementación y ejecución no debe exceder de los beneficios que pudieran resultar del proceso y deberán ser entendibles, razonables y ser congruentes con los objetivos de control que hubieren sido determinados.

Para realizar una evaluación de los controles, se presentarán conceptos generales acerca de los dos grupos de controles y luego se establecerán los elementos que determinan la eficacia de esos controles, así como guías para las evaluaciones, que pueden ser extensivas, moderadas o reducidas. Las revisiones serán propuestas como una guía de referencia, por lo que, en cada caso particular, se deberá decidir cuales de ellas son aplicables a cada circunstancia específica.

2.1 CONTROLES GENERALES

Los controles generales tienen como fin el asegurar las operaciones de la organización y su continuidad apropiada. Básicamente, se fundamentan en la estructura, políticas y procedimientos que se aplican a las operaciones del sistema informático de toda la

organización. Estos controles preparan el entorno adecuado para que operen con seguridad los sistemas de aplicación. El objetivo final de los controles generales es suministrar un nivel razonable de seguridad sobre el logro de los objetivos globales del control interno: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información

Cuando se considera necesario evaluar un sistema informatizado, se deben evaluar inicialmente los controles generales que operan sobre el sistema de una empresa. Si estos son deficientes o insuficientes, la confiabilidad disminuye, es por esto que dichos controles generales deben ser evaluados por separado y antes de evaluar los controles de las aplicaciones.

Para iniciar la evaluación a los procedimientos de control existentes en una organización, se deben considerar las siguientes categorías de controles:

- **Controles de organización y administración.-** Se refiere a las políticas, procedimientos y estructura organizacional establecidos para organizar las responsabilidades de todos los involucrados en las actividades relacionadas al área de informática.

- **Controles de desarrollo y mantenimiento de software de aplicación.-** Estos controles ayudan a la prevención de implementaciones o modificaciones no autorizadas de programas, así como también establecen control sobre cambios a sistemas, acceso a la documentación de sistemas y adquisición de sistemas de aplicación de terceros.

- **Controles de operación de cómputo y de seguridad.**- Estos controles se aplican para vigilar la operación de los sistemas y proporcionar seguridad razonable de que los sistemas son usados sólo para propósitos autorizados, que el acceso a las operaciones esté restringido a personal autorizado, así como garantizar que sólo se utilizan programas autorizados y que los errores de procesamiento son detectados y corregidos.

- **Controles de software.-** Estos controles permiten restringir y supervisar el acceso a personal autorizado a los programas y archivos críticos para el sistema y que el software (sistema operativo) se adquiere o desarrolla de manera autorizada y eficiente

- **Controles de acceso.-** Los controles de acceso limitan o detectan el acceso a recursos, tales como datos, programas, equipamientos e instalaciones, protegiéndolos contra modificaciones no autorizadas, pérdida y divulgación de información confidencial.

- **Continuidad del servicio.-** Son controles que garantizan que, en caso de que ocurran eventos inesperados, las operaciones críticas no sean interrumpidas y que puedan ser retomadas prontamente y que los datos críticos sean protegidos.

Para cada categoría, se identificarán los elementos críticos así como procedimientos adecuados para realizar la evaluación de estos controles.

2.1.1 Controles de Organización y Administración

2.1.1.1 Organización del Departamento de Sistemas

Antes llamado Centro de Procesamiento de Datos, es el departamento o unidad responsable por administrar y proveer todos los servicios relacionados al área de informática, como redes de computadoras, servicios de mantenimiento, etc.

Es necesario que el Departamento de Sistemas tenga una estructura organizacional bien definida, en donde las responsabilidades de todos sus integrantes estén claramente instituidas, documentadas y divulgadas, así como contar con políticas de personal apropiadas sobre selección, segregación de funciones, entrenamiento y evaluación del desempeño. Es, entonces, indispensable que el auditor informático verifique, en la entidad que está auditando, la existencia de una estructura organizada que administre razonablemente todos los recursos computacionales de la empresa, de tal manera que se puedan satisfacer las necesidades de información de forma eficiente y económica.

2.1.1.2 Segregación de Funciones

La finalidad de segregar funciones es, básicamente, evitar que una sola persona controle todos los estados críticos de un proceso. Esta segregación se logra por medio de la división de responsabilidades entre dos o más grupos o personas y es este proceso, que permite aumentar la detección de errores o acciones indebidas,

pues las actividades de un grupo o sujeto servirán para verificar las actividades de otro.

La forma en la que se aplique la segregación de funciones dependerá del tamaño y del riesgo asociado a las instalaciones y actividades de cada empresa en particular. En una organización grande, se podrán separar funciones clave con más flexibilidad, en cambio, en una empresa pequeña, hay pocas personas que ejecutan sus operaciones. Así mismo, actividades que involucran recursos económicos importantes o que presentan mucho más riesgo, tienen que ser distribuidas entre diversas personas y ser supervisadas más rigurosamente.

Si no existe o se aplica inadecuadamente esta importante función, se acrecienta la posibilidad de riesgo de que ocurran transacciones o procesos erróneos o dolosos, modificaciones incorrectas de programas y daños en los recursos informáticos.

En el entorno informático, sin embargo, la sola aplicación o implementación de esta función no garantiza que los empleados realicen sólo actividades autorizadas, entonces es necesario tomar en cuenta también ciertos procedimientos formales de operación así como una adecuada supervisión.

Para realizar la evaluación de los controles organizacionales, se deben analizar los elementos críticos más relevantes:

- **Unidades organizacionales bien definidas**

  Cada unidad organizacional de la Unidad de Sistemas (US):

  - Debe precisar niveles claros de autoridad, responsabilidades y habilidades técnicas necesarias para desempeñar el trabajo;
  - Definir sus objetivos primordiales y pautas de desempeño;

  Los funcionarios de US:

  - Deben realizar actividades compatibles con aquéllas que han sido instituidas formalmente por la empresa;
  - Deben tener capacidad técnica conforme con la establecida en los perfiles descritos para el desempeño de cargos.

- **Actividades de los funcionarios controladas y políticas claras de selección, entrenamiento y evaluación de desempeño**

  Se debe verificar que se cumplan las siguientes pautas:

  - Existencia de instrucciones documentadas para el ejercicio de las actividades y si los empleados las siguen;
  - Existencia de manuales de operación del sistema operativo y de software de aplicación.
  - Hay una supervisión apropiada sobre el personal;
  - Todas las actividades de quienes operan el sistema son automáticamente almacenadas en registros históricos y si estos registros son analizados periódicamente en busca de cualquier anormalidad;
  - Se supervisa el inicio del sistema y es ejecutada sólo por el personal autorizado;
  - Existencia de políticas definidas, métodos y criterios para llenar las vacantes, de tal manera que se precisen las habilidades técnicas que satisfagan un perfil;
  - Hay un programa de entrenamiento y capacitación del personal y se cuenta con los recursos suficientes para hacerlo;
  - Existe un esquema eficaz para evaluar el desempeño del personal.

- **Política de segregación de funciones y controles de acceso**

  Las políticas de una empresa son aquellas normas que deben de seguirse con la finalidad de tener un orden y un control en las actividades que se dan dentro de la misma. No obstante, rara vez estas políticas están claramente definidas y generalmente no son comunicadas al personal de la Unidad, o en otros casos, no son entendidas por los integrantes de la empresa, adicionalmente y con frecuencia, estas no están alineadas con la visión de la empresa y no siempre se desprenden de ellas objetivos claros, en la mayoría de los casos no son revisadas periódicamente para adecuarlas a los cambios tanto internos como del contexto nacional e internacional. Sin embargo, conociendo estas limitaciones, es necesario que el auditor informático, considere las siguientes técnicas de verificación:

- Que las funciones distintas son ejecutadas por diferentes personas, tales como administración de SI, proyectos de sistemas, de aplicaciones, programación, prueba y garantía de calidad, cambios, operación de terminales y servidores, control, seguridad y administración de datos.
- Que ningún funcionario tenga el control completo sobre funciones de procesamiento incompatibles, como por ejemplo, entrada de datos y verificación de validez de los mismos o comparación de los datos de salida.
- Observar si las actividades que realizan los funcionarios están en conformidad con la segregación de funciones dispuesta.
- Que sólo el personal autorizado para ingresar datos o ejecutar transacciones en los sistemas de información, sean quienes atiendan a las áreas informatizadas de la empresa.
- Que los procedimientos normales de operación del DS están apropiadamente documentados y que las acciones indebidas se identifican oportunamente.
- Que exista una política referente a rotaciones periódicas de personal y de reemplazos.
- Que las descripciones de las atribuciones de los cargos asignados reflejen los principios de segregación de funciones.
- Verificar, mediante entrevistas, que todos los funcionarios están conscientes de sus funciones y responsabilidades y que desempeñan sus obligaciones de acuerdo con los objetivos del cargo y con las responsabilidades y actividades que están formalmente establecidas.
- Que la responsabilidad de limitar el acceso de funcionarios a actividades críticas de operación está claramente definida, divulgada e implementada.
- Verificar la existencia de controles lógicos y físicos de acceso que restringen las actividades de los empleados a las acciones autorizadas según sea su cargo.
- Constatar que el desempeño de los funcionarios es supervisado periódicamente y controlado para garantizar que las actividades sean compatibles con las atribuciones de los respectivos cargos.
- Constatar la realización de evaluaciones periódicas del riesgo, para establecer si

los procedimientos de control para la división de funciones están actuando como se espera y manteniendo el riesgo en niveles razonables.

- **Recursos informáticos administrados eficiente y económicamente**

Según COBIT, los recursos de TI [13] se pueden definir como sigue:

- "Las aplicaciones incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.
- La información son los datos en todas sus formas de entrada, procesados y generados por los sistemas de información, en cualquier forma en que son utilizados por el negocio.
- La infraestructura es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.
- Las personas son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing [14] o contratadas, de acuerdo a como se requieran."

En este contexto, el auditor informático deberá realizar las siguientes consideraciones:

- Las actividades que se ejecutan por parte del DS se encuentran, normalmente, dentro de un cronograma que se cumple apropiadamente, de modo que posibilita que los recursos informáticos sean utilizados con eficiencia y simplifica la atención más eficaz de las solicitudes de usuario. Entonces, la actividad de evaluación consiste en la entrevista a usuarios y propietarios de los recursos informáticos para detectar distorsiones en la localización de recursos y/o conflictos originados por fallas en la planificación de la distribución de la carga de trabajo.
- La capacidad de hardware instalada debe ser suficiente, de tal forma que se pueda atender la demanda en las horas pico y, consecuentemente, mantener la calidad del servicio a los usuarios. La actividad de evaluación consiste en entrevistar usuarios y examinar los registros de uso del hardware para detectar las deficiencias en la configuración del sistema, a través de la identificación de dispositivos que no están

siendo usados o que se encuentran sobrecargados.

- Verificar la existencia de un plan concreto destinado a los grupos de usuarios, referente a la disponibilidad de los recursos informáticos, con características de procesamiento adecuadas a las necesidades de la empresa.
- Verificar si hay el establecimiento de políticas referente a la disponibilidad del procesamiento de datos y utilización de servicios de Internet.

Dentro del marco de referencia de COBIT, acerca de la adquisición de recursos de TI, refiere que: "Se deben suministrar recursos TI, incluyendo personas, hardware, software y servicios. Esto requiere los procedimientos de adquisición, la selección de proveedores, el ajuste de arreglos contractuales y la adquisición en sí. El hacerlo así garantiza que la organización tenga todos los recursos de TI que se requieren de una manera oportuna y rentable". Estas actividades ayudan a la reducción del riesgo en adquisición de recursos de TI así como la obtención de valor monetario por las adquisiciones de TI, por tanto, el auditor las debe tener en cuenta para realizar una evaluación más cuidadosa:

- Conseguir asesoría profesional, legal y contractual.
- Que se hayan definido procedimientos y estándares de adquisición.
- Que, cuando se necesite realizar una adquisición de hardware, software y/o servicios, se lo haga de acuerdo con los procedimientos definidos.

2.1.2 Controles de Desarrollo y Mantenimiento de Software de Aplicación

Los paquetes de software de aplicación ejecutan determinado tipo de operación y normalmente, varias aplicaciones pueden funcionar dentro de un mismo conjunto de software de sistema, conocido como sistema operativo. Es en este contexto en el que los controles sobre la modificación de programas de aplicación pueden, de cierto modo, garantizar que se efectúen solo programas y modificaciones autorizadas. De otro modo, la omisión de características de seguridad, sea intencional o no, se manifiesta en un alto riesgo de ocurrencia de eventos indeseables y peligrosos, como el ingreso de procesos erróneos o códigos maliciosos, ingreso de virus al sistema que puede paralizar la operación del mismo, así como accesos no autorizados a información confidencial o sensible para el mantenimiento del negocio.

Entonces, es primordial ejercer un control sobre el software disponible en los equipos computacionales de la empresa, que están expuestos a alteraciones y modificaciones, así como también los riesgos que tiene el software en desarrollo. Es así que, se determinarán los elementos críticos para la evaluación de los controles de cambios y desarrollo de software.

2.1.2.1 Características de procesamiento y modificaciones en el programa están debidamente autorizadas

Constatar que existe una metodología de desarrollo de software que:

- Tiene una estructura de desarrollo compatible con los conceptos y buenas prácticas y que el usuario participa de forma activa durante el proceso.
- Tiene documentación suficiente, de tal manera que sirva como orientación y referencia para personal con diferentes niveles de conocimiento y experiencia, así como también si incluye los requerimientos de documentación
- Contiene medios para el control de cambios de los requerimientos del proyecto a lo largo del ciclo de vida del software.
- Verificar si el personal involucrado en el desarrollo y prueba ha sido capacitado para llevar a cabo la metodología de desarrollo escogida para aplicarla en la empresa.
- Constatar el uso de formularios de solicitud de cambios de software para documentar pedidos y autorizaciones de cambio.
- Verificar si las solicitudes de cambio pasan por la aprobación tanto de los usuarios del sistema como del DS.
- Verificar la existencia de políticas claras con respecto al uso e instalación de sólo software autorizado.

2.1.2.2 Todo el software nuevo o alterado es probado y aprobado

Verificar que:

- Existe un reglamento para realizar las pruebas de software, en donde se disponen las responsabilidades de cada parte involucrada en el proyecto.

- Los planes de prueba siempre se documentan y aprueban.
- Se usa una muestra suficiente de datos de prueba para representar las actividades y condiciones que se presentan durante el procesamiento.
- El entorno de pruebas es distinto al ambiente de producción y los datos reales no son usados en la prueba de cambios de programas, excepto para construir archivos de datos de prueba.
- Se revisan y documentan los resultados de las pruebas.
- Los cambios de un programa se ponen en producción sólo después de que han sido formalmente aprobados por los usuarios y por la Gerencia de desarrollo de sistemas.
- La documentación es actualizada con respecto a software, hardware, personal de operación y usuarios, cuando el sistema nuevo o modificado es puesto en operación.
- Se revisan periódicamente las modificaciones introducidas en el software para comprobar si se respetaron los controles de acceso y de cambio.

2.1.2.3 Biblioteca de control de software

- **Identificación e inventario de programas.-** Verificar la existencia de una aplicación de administración de biblioteca para:
  - Producir pistas de auditoría de cambios en un programa.
  - Mantener números de versión de los programas.
  - Registrar e informar cambios de programa.
  - Mantener informaciones sobre fechas de creación de módulos en uso.
  - Mantener copias de versiones anteriores.
  - Controlar actualizaciones paralelas.

- **Restricciones de acceso a biblioteca.-** Verificar si:
  - Se dispone de bibliotecas separadas para programas en desarrollo y mantenimiento, programas en prueba y programas en producción.

- Los códigos fuente tienen su biblioteca propia.
- El código en uso, código fuente y las copias adicionales de los programas son protegidos por software de control de acceso y por características de seguridad del sistema operativo.

2.1.3 Controles de Operación de Cómputo y de Seguridad

Un programa de seguridad para una entidad debe contener políticas de seguridad y formas para implantarlas. Debe constituir una estructura adecuada para evaluar el riesgo, desarrollar e implementar procedimientos de seguridad efectivos, así como también contar con una supervisión para comprobar si son eficientes esos procedimientos. Si estos controles fueran inadecuados, a pesar de tener un programa bien elaborado, es posible que las responsabilidades no estén lo suficientemente claras, no comprendidas o implementadas de forma impropia, así que si se aplicaran estos controles, pudieran resultar inconsistentes e ineficaces. De ser así, la protección brindada a los recursos críticos o sensibles sería insuficiente, lo que conllevaría a un desperdicio de recursos para la implantación de controles en situaciones de bajo riesgo.

2.1.3.1 Políticas de gestión de seguridad

Las políticas de seguridad son un conjunto de normas, reglamentos y protocolos, que especifican distintas medidas que hay que tomar para proteger la seguridad del sistema, las funciones y responsabilidades de todos los componentes de la organización y los mecanismos para controlar su funcionamiento apropiado. Para que sea eficiente, la política de seguridad de una empresa debe cubrir todos los aspectos relacionados con el sistema y los principios básicos que deben tomarse en cuenta para su elaboración se listan a continuación:

- El primer principio para una seguridad eficiente es la protección del sistema en todos los aspectos de protección: elemento humano, factores físicos, prácticas y procedimientos, hardware, software, aplicaciones y elementos de apoyo a la seguridad, así como también la interacción entre ellos. También se debe considerar el entorno del sistema, es decir, en qué tipo de organización se van a implantar las políticas de seguridad.

- El segundo principio básico dice que una política de seguridad debe ajustarse a las necesidades y recursos, al valor que tiene la información en ese entorno y al uso que se da a los equipos de cómputo Deben evaluarse los riesgos, el valor del sistema protegido y el costo de implementarlo. Las medidas de seguridad tomadas deben ser proporcionales a estos valores.
- Y por último, toda política de seguridad debe asentarse primordialmente en el sentido común. Así que es necesario tener un conocimiento del sistema que se va a proteger así como de su entorno, experiencia y conocimiento respecto a evaluación de riesgos y establecimiento de medidas de seguridad, así como una comprensión acerca de la naturaleza humana, de los usuarios y de sus posibles motivaciones.

Estos principios deben ponerse en práctica determinando además el grado de vulnerabilidad de los datos, desde el punto de vista de su integridad, confidencialidad y disponibilidad.

2.1.3.2 Evaluación del riesgo

Para la elaboración o modificación de un plan y políticas de seguridad, se debe partir de una evaluación completa del riesgo, que es primordial porque a través de esta evaluación se pueden identificar todas las amenazas y vulnerabilidades del sistema y se puede decidir aquellos riesgos que serán aceptados y aquellos riesgos que deberán ser reducidos a través de controles de seguridad.

La evaluación del riesgo debe considerar la vulnerabilidad propia de los datos, es decir, la susceptibilidad a errores causados por omisión o inserción incorrecta o indebida de datos, así como el riesgo adicional que se deriva del uso de sistemas o equipos por parte de usuarios internos y externos, y eventuales intentos de acceso por usuarios no autorizados.

Al realizar este estudio, hay que tomar en cuenta las revisiones de la configuración del sistema y de la red, además de la observación y prueba de los controles de seguridad implantados. Aunque el personal involucrado en actividades de seguridad puede dar una visión apreciable sobre las vulnerabilidades existentes, la evaluación general del riesgo debe ser hecha por personal independiente, de tal modo que se garantice su objetividad.

La evaluación general de riesgo puede ser efectuada de forma más espaciada, cada año o dos, dependiendo de la necesidad particular de una empresa, pero el riesgo debe ser reevaluado cada vez que haya un cambio en la operación de la empresa o en influencias externas que afecten esa operación.

2.1.3.3 Políticas de seguridad eficaces

- Se debe verificar que hay un programa de entrenamiento inicial de todos los nuevos funcionarios y usuarios, así como un entrenamiento periódico de actualización, y que está siendo seguido, por tanto, hay que examinar los registros de las actividades de entrenamiento.
- Verificar las políticas de acuerdo con la confidencialidad y examinar una muestra de registros para constatar si los usuarios y funcionarios con acceso a información confidencial han firmado una declaración de confidencialidad.
- Verificar que los procesos de transferencia y dimisión incluyen procedimientos de seguridad tales como:
    - Devolución de llaves, claves, pases de identificación, etc.
    - Notificación a la administración para la desactivación inmediata de claves de acceso.
    - Retiro inmediato del funcionario del local de trabajo.
    - Definición del periodo en que el funcionario saliente deberá guardar el sigilo de la información confidencial a la que tuvo acceso.

2.1.4 Controles de Software

Un software de sistema, conocido como sistema operativo, suele utilizarse para dar soporte y controlar una diversidad de aplicaciones que pueden ser ejecutadas en un mismo computador. Este software del sistema ayuda a controlar y coordinar la entrada, procesamiento, salida y almacenamiento de los datos de todas las aplicaciones ejecutadas en el sistema.

Existen algunos paquetes de software de sistema que pueden alterar datos y códigos de programa en archivos, sin dejar una pista de auditoría, por tanto, el control sobre el

acceso y la alteración del software de sistema son fundamentales para ofrecer una garantía razonable de que los controles de seguridad basados en el sistema operacional no están comprometidos, lo que podría afectar el buen funcionamiento del sistema computacional como un todo.

Si los controles aplicados al software de sistema son ineficaces o inadecuados, usuarios no autorizados podrían utilizarlo para evadir los controles de seguridad, con el consiguiente peligro de que pudieran acceder a programas críticos o información sensible para borrarlos o modificarlos, con lo que aumentaría el riesgo de dolo y sabotaje.

Para evaluar los controles aplicados al software de sistema es necesario que el auditor considere los siguientes elementos críticos:

2.1.4.1 Acceso limitado al software de sistema

Las políticas y procedimientos que la unidad de Sistemas debe aplicar para la restricción del acceso al software del sistema, son las siguientes:

- El acceso al software del sistema debe ser restringido sólo a usuarios cuyas responsabilidades así lo requieran y debe ser limitado a un número de personas. Por ejemplo, programadores o usuarios comunes no deben tener autorización al software del sistema.
- Toda aprobación y justificación para el acceso al software del sistema debe ser documentada y almacenada en archivo.
- El nivel de acceso que se les ha permitido a los programadores del sistema debe ser evaluado constantemente, de tal modo que se verifique que este permiso de acceso aún es necesario. Constatar siempre la última fecha en la que el nivel de acceso fue revisado.

2.1.4.2 Acceso y uso supervisado de software de sistema

Las políticas y procedimientos documentados y actualizados, que deben estar aplicados para el buen uso de programas utilitarios [15] del software de sistema.

- Verificar que las responsabilidades en el uso de programas utilitarios del sistema son claramente definidas y comprendidas por los programadores del sistema.

- Constatar que las responsabilidades para ejecutar una supervisión del uso de programas utilitarios del sistema están definidas y son realizadas por la gerencia del DS.
- Verificar si se registra en informes producidos por el software de control de acceso u otro mecanismo de registro de acceso, el uso de programas utilitarios del sistema.
- Constatar si se examinan periódicamente los registros de acceso al software de sistema y a sus programas utilitarios son periódicamente examinados, así como también si las actividades sospechosas o no habituales son indagadas.
- Verificar si se realizan revisiones necesarias para comprobar si las técnicas de supervisión del uso del software del sistema funcionan como está previsto y si los riesgos se mantienen dentro de niveles aceptables, a través de evaluaciones periódicas de riesgo.

2.1.4.3 Control de las alteraciones del software de sistema.

Verificar la existencia de políticas y procedimientos actualizados para identificar, seleccionar, instalar y modificar software de sistema, así como también para identificar, documentar y solucionar problemas con este software. El establecimiento de nuevas versiones de software de sistema o sus programas utilitarios deben observar ciertos procedimientos de seguridad:

- Justificación documentada para el cambio.
- Ejecución de pruebas conducidas en un ambiente propio para pruebas.
- Informe técnico sobre los resultados de las pruebas.
- Revisión de los resultados de las pruebas y de las opiniones documentadas, por parte del gerente de DS.
- Autorización del gerente de DS para instalar la nueva versión del software del sistema en uso.
- Verificar la existencia de procedimientos para controlar cambios de emergencia, que debe incluir el modo de uso y su correspondiente documentación.

2.1.5 Controles de Acceso

El objetivo de implantar controles de acceso es brindar una garantía razonable de que los recursos informáticos, tales como los archivos de datos, aplicaciones, instalaciones y equipamientos computacionales, son adecuadamente protegidos contra modificaciones, daño, pérdida o divulgación no autorizada. Estos incluyen controles físicos, como por ejemplo el mantenimiento de los computadores en sitios cerrados para restringir el acceso físico, y controles lógicos, que no son más que implementación de software de seguridad que trabajan para prevenir o detectar acceso no autorizado a información crítica o sensible.

Si se aplican o implementan controles de acceso no apropiados, la confiabilidad de los datos procesados por el sistema disminuye, por consiguiente, el riesgo de destrucción o divulgación indebida de datos aumenta. Algunas de las posibles consecuencias de la no observancia o pobre aplicación de dichos controles son las siguientes:

- Si se tiene el acceso absoluto a archivos, cualquier usuario pudiera hacer cambios no autorizados para lograr su propia conveniencia, conseguir información confidencial o alteración de información sensible.
- Si se puede acceder fácilmente a las aplicaciones que procesan datos críticos, se puede modificar o alterar la información que se procesa, lo que permitiría el uso doloso de datos y perpetrar delitos de fraude o hurto, con el consiguiente perjuicio para una empresa.
- Si no existen controles de acceso en los terminales que permiten la entrada en la red de una organización, cualquier persona podría obtener acceso a información confidencial o de uso controlado, que estuvieren almacenados en medios magnéticos o impresos, suplantar datos o programas o dañar/robar intencionalmente equipos y aplicaciones software.

He aquí que la restricción de acceso y la limitación al acceso de recursos de alto riesgo, tales como software de seguridad, garantiza que los usuarios puedan acceder solo a los recursos necesarios para realizar sus tareas y que los funcionarios no puedan ejecutar funciones incompatibles o que vayan más allá de su responsabilidad.

Es entonces, necesario, obtener un equilibrio apropiado entre las necesidades del usuario y los requerimientos de seguridad, así como también un análisis minucioso de las

vulnerabilidades e importancia de cada recurso de información disponible, comprobándolos con las tareas que ejecutan los usuarios. Si estos objetivos de seguridad se alcanzan, el riesgo de modificación o divulgación indebida de información se puede reducir sin interferir mayormente en las reales necesidades de los usuarios.

Para implementar controles de acceso adecuados, se debe determinar el nivel y tipo de protección convenientes a cada recurso, así como la identificación de los usuarios que necesitan tener acceso a esos recursos. Quienes deben determinar estas características deben ser los propietarios de los recursos [16]. Por ejemplo, los jefes de departamentos deben determinar la importancia de los programas que usan y de la información que guardan, así como del nivel de acceso que es apropiado para el personal que usa el sistema para ejecutar sus operaciones cotidianas.

A continuación, se presentan los principales elementos críticos que el auditor debe considerar para evaluar una apropiada administración de los controles de acceso.

2.1.5.1 Clasificación de los recursos de información de acuerdo con su importancia y vulnerabilidad

Verificar que:

- Los propietarios de los recursos saben y aceptan los criterios de clasificación determinados y que han hecho o harán la clasificación de los principales recursos que se encuentran bajo su responsabilidad.
- La clasificación de los recursos estuvo basada en evaluaciones de riesgo, documentada y aprobada por la administración y que ésta es habitualmente revisada.

2.1.5.2 Mantenimiento de una lista actualizada de usuarios autorizados y niveles de acceso

Las autorizaciones de acceso deben estar:

- Documentadas en formularios estandarizados y almacenadas en un archivo organizado.
- Aprobadas por el propietario del recurso informático.

- Transmitidas para los administradores de seguridad de forma protegida.

Se debe verificar que:

- Los propietarios de los recursos informáticos deben revisar habitualmente las autorizaciones de acceso, de tal modo que se pueda para comprobar si todavía son necesarias y adecuadas.
- La autorización al acceso remoto de los sistemas debe ser otorgada a un número limitado de usuarios y deben documentarse y aprobarse las justificaciones para dicho acceso.
- De existir administradores de seguridad, estos deben revisar las autorizaciones de acceso y cualquier autorización que no esté clara o justificada, debe ser consultada con los propietarios de los recursos.
- Cualquier cambio que se realice en el perfil de seguridad debe ser automáticamente registrado y revisado periódicamente por la administración.
- Cualquier actividad que sea poco usual o fuera de lo normal debe ser investigada.
- La administración del DS debe ser notificada de inmediato cuando usuarios del sistema han salido de la empresa o han sido transferidos.
- Las autorizaciones de acceso temporales están documentadas en formularios estandarizados y almacenadas en archivo, comunicadas de forma protegida a los responsables de la seguridad, aprobada por la gerencia de DS y automáticamente desactivadas cuando se ha cumplido un determinado período.
- Deben tener formularios estandarizados para documentar la aprobación para compartir información con otras organizaciones. Se debe examinar dichos formularios y entrevistar a los responsables del mantenimiento de los datos.
- Antes de compartir los datos o programas con otras empresas, se deben formalizar acuerdos que definirán la forma en que estos serán protegidos. Así que se deben examinar los documentos de autorización para compartir información así como los acuerdos de seguridad.

2.1.5.3 Controles lógicos y físicos para la prevención y detección de acceso no autorizado

a. Controles de acceso físico

Es primordial verificar que, en la organización:

- Se identifican todas las amenazas relevantes para la seguridad física de los recursos más sensibles, para lo que se verifica la disposición física de los recursos.
- El acceso físico está restringido únicamente a los usuarios que necesitan acceder frecuentemente a los recursos informáticos, a través de claves de identificación, tarjetas magnéticas para ingresar, por ejemplo. Así que se debe observar los puntos de acceso a las instalaciones durante las horas de trabajo, contrastar la lista de personal que tiene acceso autorizado.
- La revisión regular de la lista de personas que tienen acceso físico a las instalaciones críticas.
- La existencia de obstáculos físicos para el acceso a sala de cómputo, archivos y otras instalaciones críticas.
- Todas las entregas y retiros de medios de almacenamiento de datos son autorizados y registrados y a los responsables de esta actividad.
- La gerencia o los responsables de seguridad deben mantener de forma protegida los dispositivos de acceso tales como llaves, tarjetas magnéticas, entre otros.
- La entrada de visitantes al centro de cómputo debe ser registrada y siempre deben estar acompañados por algún funcionario del DS. Se debe, entonces, entrevistar a quien registra la entrada de visitantes, a los guardias y responsables por la seguridad así como realizar una observación acuciosa del tránsito de personas por las áreas críticas en los períodos dentro y fuera del horario de trabajo.
- La existencia de procedimientos adecuados para la salida del personal del área que estuviere en riesgo en situaciones de emergencia, así como del retorno del personal cuando la situación vuelva a su estado normal.

- Las contraseñas deben ser únicas para cada usuario, no para grupos; deben ser controladas por los usuarios y no ser compartidas por nadie; deben ser cambiadas de forma periódica, por ejemplo, cada mes o cada trimestre; no se deben mostrar en pantalla cuando sean ingresadas y deben constar de por lo menos seis caracteres alfanuméricos e impedidas de repetirse, por lo menos, en los posteriores cinco o seis cambios.
- La existencia de restricciones al escoger la contraseña, para que no sea posible usar nombres y palabras fáciles de descubrir, para lo cual se debe analizar una lista generada por el sistema de claves en uso.
- Cuando se entregan claves para el acceso por primera vez, estas son inmediatamente cambiadas por los usuarios. Debe existir algún texto que indique que la clave entregada expirará automáticamente al primer ingreso, por lo que es necesario que ésta sea cambiada.
- No se pueda compartir códigos de identificación y claves de uso entre usuarios.
- El acceso al sistema restringe a pocos intentos el ingreso de claves inválidas, por ejemplo, lo más adecuado es que después de tres intentos, se bloquee el sistema.
- Se actualiza de forma periódica la lista del personal, para que en caso de dimisión o transferencia, se elimine la autorización al acceso al sistema.
- Las cuentas de acceso inactivas son supervisadas y removidas cuando ya no son necesarias. Para esto, se debe verificar las especificaciones del software de seguridad, examinar una lista de usuarios inactivos generada por el sistema y determinar por qué el acceso de dichos usuarios no fue revocado.
- Los usuarios de otros dispositivos de acceso, tales como códigos y tarjetas magnéticas, comprenden de que se deben resguardar cuidadosamente, no ser prestados ni compartidos y de que, en caso de pérdida debe ser comunicado inmediatamente a los responsables.
- Identificación de caminos de acceso: se realiza un análisis de los caminos lógicos [17] de acceso todas las veces que ocurren cambios en el sistema.

b. Controles lógicos sobre archivos de datos y programas de software

Verificar que:

- Se utiliza software de seguridad para limitar el acceso a los archivos de datos y programas.
- El acceso al software de seguridad está restringido solo a los administradores del sistema.
- Las sesiones de acceso a redes son finalizadas automáticamente después de un periodo de inactividad del usuario.
- Los responsables por la administración del sistema han configurado el software de seguridad para restringir el acceso no autorizado a archivos de datos, bibliotecas de datos, procedimientos de operación en lote, bibliotecas de código fuente, archivos de seguridad y archivos de sistema operativo. Se deben probar los controles intentando conseguir acceso a varios archivos restringidos.

c. Controles lógicos sobre la base de datos

- Se debe constatar que los controles sobre los sistemas administradores de bases de datos (DBMS) [18] y el diccionario de datos [19] se implementaron para:
- Restringir el acceso a archivos de datos para lectura de datos, modificaciones o borrado de campos.
- Controlar el acceso al diccionario de datos usando perfiles de seguridad y contraseñas.
- Mantener pistas de auditoría, para determinar los cambios en los que se hayan hecho en los diccionarios de datos.
- El acceso al sistema del DBMS está restringido únicamente a personal cuyas facultades requieren del acceso.

d. Controles lógicos sobre el acceso remoto

Verificar que se implementó un software de comunicación (software de red) [20] para:

- Identificar el terminal en uso, para poder restringir el acceso mediante terminales específicos.
- Verificar los códigos de identificación del usuario y contraseñas para el acceso a las aplicaciones específicas.
- Controlar el acceso mediante conexiones entre sistemas y terminales.
- Restringir el uso de facilidades de red en aplicaciones específicas.
- Interrumpir automáticamente la conexión cuando se finalice una sesión.
- Mantener registros de actividad en la red.
- Restringir el acceso a definiciones de opciones de red, recursos y perfiles de operador.
- Permitir que solo usuarios autorizados desconecten componentes de la red.
- Restringir el acceso interno y controlar cambios al software de comunicaciones.
- Garantizar que los datos no puedan ser accedidos o modificados por un usuario no autorizado, durante su transmisión o cuando son almacenados temporalmente.
- Restringir y supervisar el acceso al hardware de comunicaciones (routers, switches) o instalaciones.
- Verificar la existencia de procedimientos para eliminar datos confidenciales y programas instalados en recursos que van a ser dados de baja en la organización, ya sea por venta, donación, etc.

2.1.5.4 Supervisión del acceso, investigación de evidencias de violaciones de seguridad y adopción de medidas correctivas

Se debe constatar que:

- Se conservan pistas de auditoría y se registran todas las actividades que implican el acceso y modificación de archivos vulnerables o críticos.
- Se informa a la administración y se indagan las violaciones a la seguridad a través del análisis de informes sobre actividades sospechosas, tales como intentos para entrar al sistema que no hayan sido exitosos.

- Se toman medidas de disciplina para corregir las violaciones de seguridad que hayan sido detectadas.
- Se cambian las políticas de control de acceso cuando las violaciones de seguridad han sucedido.

2.1.6 Controles de Continuidad del Servicio

Una organización que depende en gran proporción de la disponibilidad de la información, al perder la capacidad de procesar, recuperar y proteger dicha información, podría detener las actividades normales de operación, causando un impacto significativo en la consecución de los objetivos del negocio. Es así que, las empresas necesitan establecer procedimientos para proteger sus recursos de información, minimizar el riesgo de sufrir interrupciones y a la vez, permitir una recuperación eficiente y rápida de operaciones críticas. Estos planes de recuperación deben ser probados periódicamente, simulando desastres, para garantizar que son eficaces y que van a funcionar como se previó.

Es en este contexto, que los controles para garantizar la continuidad del servicio deben prever todas las probabilidades de interrupción del servicio que existen, sin importar si son leves, como el corte de energía o destrucción eventual de un archivo, hasta las más relevantes, tales como incendios o desastres naturales que requieran el recuperación de las operaciones en un lugar físico alterno.

Para esto, se debe asegurar que los controles a implementarse sean adecuados, en cualquier nivel de riesgo, pues si es muy alto, como en terapia intensiva en una clínica, por ejemplo, una interrupción de energía eléctrica podría resultar en daños personales o pérdida de vidas. También es importante que estos controles sean conocidos, adoptados y aplicados por la gerencia y por todo el personal involucrado. Es así, que la gestión de la administración es de vital importancia, pues ellos pueden garantizar los recursos necesarios para emprender planificaciones de riesgos, entrenamientos y pruebas. En cuanto al personal responsable de las actividades de mantenimiento de la continuidad del servicio, como por ejemplo, de la elaboración de copias de seguridad de archivos, debe estar bien informado de los riesgos a los que se expone si no se aplican correctamente esas actividades de control.

A continuación se hace una revisión de los elementos críticos, que el auditor informático deberá considerar para la evaluación de la continuidad del servicio y de las actividades de

control.

2.1.6.1 Evaluación de vulnerabilidades de las operaciones por computador e identificación de los recursos que las apoyan

Se debe constatar que:

- Se tiene elaborada una lista de datos, operaciones y sistemas críticos que indica la prioridad de cada ítem, que ha sido aprobada por los administradores responsables y que muestra la situación actual de los recursos informáticos.
- Los recursos que dan soporte a las operaciones críticas se encuentran inventariados, incluyendo hardware, software, proveedores, documentación del sistema, instalaciones y mobiliario y recursos humanos.
- Las prioridades de los procedimientos de emergencia se encuentran documentadas y aprobadas por la administración y la gerencia de DS.

2.1.6.2 Adopción de medidas para prevenir y minimizar daños e interrupciones potenciales

El aplicar las medidas adecuadas capaces de prevenir y minimizar los daños e interrupciones potenciales se relacionan con procedimientos de copia de seguridad (backup), controles del ambiente informático, entrenamiento del personal para responder a incidencias y medidas de prevención de interrupciones inesperadas.

2.1.6.3 Desarrollo y documentación de un plan general de contingencia

Este tema se relaciona con tener un plan de contingencia documentado, contar con alternativas de procesamiento de datos y comunicación, así como prever pruebas periódicas del plan de contingencia y elaboración de los ajustes que sean necesarios.

2.2 CONTROLES DE APLICACIÓN

Los controles de aplicación están relacionados con el uso de controles en los diferentes

programas instalados en un computador. El uso de estos controles, garantizan que el procesamiento sea confiable y exacto, a partir de controles incorporados de forma directa en programas de aplicación, en las tres áreas de operación: Entrada, proceso y salida de datos.

El objetivo principal de la aplicación e implementación de los controles de aplicación es salvaguardar la confidencialidad, integridad y disponibilidad de la información que se procesa, almacena y/o genera, es decir, conservar la totalidad, exactitud, autorización, mantenimiento y actualización.

Según COBIT [21], "los procesos de TI de COBIT abarcan a los controles generales de TI, pero sólo los aspectos de desarrollo de los controles de aplicación; la responsabilidad de definir y el uso operativo es de la empresa.

Los controles incluidos en las aplicaciones de los procesos del negocio se conocen por lo general como controles de aplicación. COBIT asume que el diseño e implementación de los controles de aplicación automatizados son responsabilidad de TI, y están cubiertos en el dominio de Adquirir e Implementar, con base en los requerimientos de negocio definidos, usando los criterios de información de COBIT. La responsabilidad operativa de administrar y controlar los controles de aplicación no es de TI, sino del dueño del proceso de negocio.
Por lo tanto, la responsabilidad de los controles de aplicación es una responsabilidad conjunta, fin a fin, entre el negocio y TI, pero la naturaleza de la responsabilidad cambia de la siguiente manera:

- La empresa es responsable de:
  - Definir apropiadamente los requisitos funcionales y de control
  - Uso adecuadamente los servicios automatizados

- TI es responsable de:
  - Automatizar e implementar los requisitos de las funciones de negocio y de control
  - Establecer controles para mantener la integridad de controles de aplicación. "

Según el Informe COSO [22] dentro del apartado "Controles sobre los Sistemas de Información", se encuentra el segundo grupo de controles, llamados de aplicación, y que son "diseñados para el control del funcionamiento de las aplicaciones, asegurando la

totalidad y exactitud en el proceso de transacciones, su autorización y validez, como por ejemplo: Comprobaciones de formato, existencia y razonabilidad de los datos".

Al realizar una evaluación de los controles de aplicación, se debe siempre ejecutar junto con la verificación de los controles generales del sistema y comprobar conjuntamente la legalidad del proceso efectuado, es decir, si un producto final está de acuerdo con las leyes vigentes.

Para que los controles de aplicación existentes sean adecuados, se debe disponer de procedimientos que garanticen que los programas de aplicación y sus modificaciones sean autorizados y probados antes de su implementación, así como también procedimientos adecuados de revisión, aprobación, control y edición de datos de entrada, para garantizar su integridad y prevenir errores. También deben existir procedimientos de detección y corrección de errores, así como contar con la opinión de los usuarios sobre la confiabilidad de los datos.

Para iniciar la evaluación a los procedimientos de control existentes en una organización, se deben considerar las siguientes categorías de controles:

- **Controles de entrada de datos:** Diseñados para garantizar que los datos son convertidos a un formato estándar y que son insertados en la aplicación de forma precisa, completa y a tiempo.
- **Controles de procesamiento de datos:** Deben asegurar que todos los datos de ingreso sean procesados y que la aplicación sea ejecutada con éxito, usando los archivos de datos, las rutinas de operación y la lógica de procesamiento correctos.
- **Controles de salida de datos:** Utilizados para garantizar la integridad y la correcta distribución de los datos de salida, en el momento preciso.

Para cada categoría, se identificarán los elementos críticos así como procedimientos adecuados para realizar la evaluación de estos controles.

2.2.1 Controles de Entrada de Datos

Ingresar los datos también puede resultar riesgoso. Podría ingresarse equivocadamente los datos o estos pueden duplicarse. También puede suceder que los datos no estén actualizados y hasta que se ingresen datos no autorizados, lo que conlleva consecuencias, desde la más leve como errores de sintaxis hasta las más graves como la realización de transacciones no autorizadas. A continuación se listarán los controles de

entrada de datos más comunes. Estos controles se implementan para detectar transacciones no autorizadas, incompletas, duplicadas o erróneas, de tal manera que puedan ser controladas hasta ser corregidas.

2.2.1.1 Documentos o Pantallas de Entrada de Datos

El auditor deberá verificar, para la evaluación, la existencia de los siguientes procedimientos:

- Que los documentos o pantallas de entrada aseguren la entrada de datos de manera exacta y consistente.
- Que los campos de datos de llenado obligatorio puedan ser identificados fácilmente.
- Que existen estándares para las pantallas de entrada, referentes a su presentación, ubicación de los campos y accionamiento de teclas.

2.2.1.2 Rutinas de Preparación de los Datos

- El auditor deberá comprobar la existencia de ciertas buenas prácticas que se deben seguir para la preparación de los datos a ser llenados en cada documento.
- Que hay funcionarios responsables para la preparación, revisión y autorización de entrada de datos y que están bien identificados.
- Que existen rutinas escritas por cada actividad en la preparación de datos, con instrucciones claras y apropiadas.

2.2.1.3 Autorización para Entrada de Datos

Cuando se ingresan datos en línea, se deben implementar rutinas de validación de datos, pues en esta modalidad de ingreso no se puede autorizar. El sistema debe comprobar de forma automática si el usuario está registrado para usar una aplicación y si los datos enviados satisfacen ciertas condiciones. Es así que no siempre se pueden adecuar procedimientos de autorización antes de la entrada de datos. Dentro de este contexto, una empresa deberá implantar prácticas para impedir el uso no autorizado o el mal uso de terminales mientras se ingresen

datos.

El auditor deberá hacer las siguientes verificaciones para la entrada de datos on-line:

- En el caso de aplicaciones en que se ingresan datos en terminales, hay procedimientos de seguridad para el uso, mantenimiento y control de claves de identificación del usuario y del terminal o estación de trabajo.
- Que las claves para identificar al usuario y al terminal son verificadas para autorizar el ingreso de datos.
- Que hay procedimientos documentados para que, en caso de transmisión electrónica de documentos, la ruta utilizada y los procedimientos de autorización sean registrados.
- Que los computadores y/o terminales que tiene una empresa para el ingreso de datos están localizados en salas físicamente seguras.
- Que los procedimientos para el ingreso de datos aseguren que esta actividad solo sea ejecutada por funcionarios con determinado nivel de acceso y que se utilizan claves para prevenir el uso no autorizado de los equipos.
- Que hay claves de identificación, únicas e individuales, de tal manera que sea posible el control de acceso a los datos.
- También, el auditor debe verificar las aplicaciones con ingreso de datos batch [23]:
- Que la aprobación de ingreso de datos esté limitada a las personas definidas por la institución en un documento escrito.
- Que las personas que son responsables de la autorización del ingreso de datos, no realizan otras tareas incompatibles, por el principio de segregación de funciones [Segregación de funciones incompatibles. CAPÍTULO 1, APARTADO 1.8.5].

En el ingreso de datos on-line, el auditor debe verificar si se cumple con:

- La existencia de controles lógicos y físicos en los terminales y computadores, que previenen y detectan el ingreso de datos no autorizados.

- La implementación de mecanismos de seguridad, para administrar la autorización de acceso a las transacciones on-line y a los registros históricos asociados.
- La garantía que ofrecen los mecanismos de seguridad de que todas las tentativas de acceso, con o sin éxito, son grabados en logs, que registran fecha y hora del acceso e identifican al usuario.

2.2.1.4 Retención de Documentos de Entrada

Generalmente, una entidad suele retener los documentos originales por un determinado tiempo, para facilitar la recuperación o reconstrucción de datos, en caso de sucesos indeseables. El auditor deberá constatar la existencia de procedimientos documentados para dicha retención:

- Que los documentos se retienen por un período suficiente para permitir la recuperación de datos, en el caso que se pierdan durante la fase de procesamiento.
- Que los documentos están archivados de manera organizada, para facilitar su recuperación.
- Que el departamento que originó los documentos conserva copias de estos.
- Que tan solo las personas formalmente autorizadas tienen acceso a los documentos archivados.
- Que existen procedimientos documentados para borrar y destruir los documentos cuando ha terminado el período de retención, y que estos procedimientos se aplican.

2.2.1.5 Validación de los Datos de Entrada

La empresa debe implantar prácticas que aseguren que los datos de ingreso son validados y editados de manera que reflejen cabalmente los documentos originales. Es así que, el auditor deberá constatar la existencia de procedimientos documentados que especifican el formato de los datos para asegurar el ingreso de datos en el campo correcto y con el formato correcto:

- Que existe información de apoyo para facilitar el ingreso de datos y reducir el número de errores en las rutinas de ingreso de datos.

- Que se cuenta con mecanismos para la validación, edición y control del ingreso de datos, ya sea mediante terminales inteligentes o software dedicado a esa función.
- Que los campos principales para el correcto procesamiento posterior de los datos son de llenado obligatorio.
- Que existen rutinas para detectar, rechazar e impedir el ingreso de datos incorrectos en el sistema.
- Que se ejecuta la validación de los datos en todos los campos principales del registro o pantalla de ingreso.
- Que las rutinas de validación de datos prueban la presencia de:
    - Códigos de aprobación y autorización;
    - Dígitos de verificación en todas las claves de identificación;
    - Dígitos de verificación al final de una secuencia de datos numéricos;
    - Códigos válidos;
    - Valores alfanuméricos o numéricos válidos;
    - Tamaños válidos de campo;
    - Campos combinados;
    - Límites válidos, razonabilidad de los valores o banda de valores válidos;
    - Campos obligatorios llenados;
    - Símbolos;
    - Registros de entrada completos;
    - Campos repetitivos, eliminando la necesidad de ingreso de los mismos datos más de una vez.
- Que la rutina de ingreso de datos establece un registro histórico de los datos, suministrando una pista de auditoría.

2.2.1.6 Tratamiento de Errores

Una empresa debe implantar rutinas para corrección y reenvío de datos de

entrada incorrectos. El auditor debe verificar la existencia de rutinas para la identificación, corrección y reenvío de datos incorrectos.

- Que la rutina de ingreso de datos tiene procedimientos automáticos o manuales que permiten que los datos errados sean corregidos y reenviados de forma rápida.
- Que hay control sobre los errores que pudieran suceder al ingresar datos y que permita identificarlos, conjuntamente con las medidas que se hayan dispuesto para corregirlos y el tiempo transcurrido entre su ocurrencia y su corrección.
- Que cuando se generen mensajes de error al ingreso de datos, estos sean claros y fáciles de entender para el usuario, lo que facilita la corrección y el reenvío de los datos.

2.2.1.7 Mecanismos de Soporte para el Ingreso de los Datos

El auditor debe comprobar que en la entidad exista un grupo de control responsable por las siguientes actividades:

- Indagar sobre cualquier problema operacional en el terminal u otro dispositivo de ingreso de datos y corregir.
- Asegurar que los procedimientos de reinicio son realizados de manera adecuada.
- Monitorear las actividades de ingreso de datos en el terminal u otro dispositivo similar.
- Cuando se detecte cualquier desvío de los procedimientos de ingreso de datos preestablecidos, el grupo debe investigar.
- Los recursos informáticos y humanos disponibles para el ingreso de datos garantizan que estos sean insertados a tiempo.

2.2.2 Controles de Procesamiento de Datos

La finalidad de estos controles es asegurar que todos los datos de ingreso sean procesados y que la aplicación sea ejecutada exitosamente, usando los archivos, las rutinas de operación y la lógica de procesamiento correctos.

2.2.2.1 Integridad del Procesamiento

En este aspecto, el auditor debe verificar la existencia de procedimientos documentados que exponen la manera en cómo los datos son procesados por una aplicación en particular.

- Que los sistemas en red se encuentren protegidos contra la actualización paralela de archivos, por diferentes usuarios.
- Que se han generado registros históricos (logs) [24] que almacenan eventos producidos por el computador y sus usuarios durante el procesamiento de la aplicación, proporcionando una pista de auditoría de las transacciones que fueron procesadas.
- Que las claves de identificación del usuario, del terminal o del computador, así como datos de fecha, hora e información anterior a un cambio (si se justifica la relevancia) se conservan en registros históricos.

2.2.2.2 Validación del Procesamiento

En este apartado, el auditor debe verificar que:

- Los datos incorrectos son rechazados por la aplicación.
- Se ejecutan procedimientos de validación en todos los campos importantes o de llenado obligatorio, antes de grabar los datos.

2.2.2.3 Tratamiento de Errores del Procesamiento

La finalidad de las rutinas de tratamiento de error es identificar las transacciones erróneas y suspender su procesamiento sin afectar la ejecución de otras transacciones válidas. El auditor deberá constatar que se han determinado procedimientos documentados para la identificación, corrección y reinserción de datos rechazados:

- Que los mensajes que producen las rutinas de tratamiento de error de procesamiento son claros y objetivos.
- Que se controlan adecuadamente los archivos temporales de datos rechazados por el sistema y que se generan mensajes de alerta para que estos datos

puedan ser revisados y corregidos.

- Que hay control sobre los errores ocurridos durante el procesamiento de datos, de tal manera que puedan ser identificados, así como la existencia de medidas para corregirlos y registros del tiempo transcurrido entre su ocurrencia y su corrección.

2.2.3 Controles de Salida de Datos

La finalidad de este tipo de controles es garantizar la integridad y la distribución correcta y a tiempo de los datos de salida.

2.2.3.1 Revisión de los Datos de Salida

Se realizan revisiones de los informes de los datos de salida con relación a su integridad y exactitud antes de ser dispuestos a los usuarios.

En relación a este ítem, el auditor deberá constatar la existencia de procedimientos documentados para informar, corregir y rehacer informes de salida con errores. La revisión de los informes de salida consiste en una comparación de la cuenta de los registros con los totales de control, de tal manera que se pueda garantizar que se ingresaron todos los datos apropiadamente.

2.2.3.2 Distribución de los Datos de Salida

El auditor, en este apartado, deberá verificar la existencia de los controles siguientes:

- Los informes impresos son etiquetados, identificando nombre del producto, nombre del destinatario, fecha y hora de generación, y que son entregados a su destino dentro de los plazos determinados.
- La presencia de procedimientos escritos que refieren el proceso de distribución de los datos de salida, sea en informes impresos o en línea.
- La existencia de listas de distribución prefijadas para todos los datos creados por la aplicación. Estas listas pueden ser cambiadas de acuerdo con las necesidades de la empresa.

- Si se aplican cuestionarios periódicos para los usuarios, para determinar si los datos producidos continúan siendo necesarios o útiles.
- La existencia de controles sobre los datos que se presentan a los usuarios en pantalla, para impedir adulteraciones.
- La presencia de registros históricos de las informaciones sobre los datos de salida.
- La existencia de procedimientos documentados para reportar y controlar los errores que hayan ocurrido en el procesamiento de los datos de salida, así como aquellos ocurridos en procesos batch o en línea.
- La conservación de los registros de los informes con errores y la comunicación de estos informes a los usuarios.

2.2.3.3 Seguridad de los Datos de Salida

Una empresa debe disponer de procedimientos para limitar el acceso a los informes tan solo a personas autorizadas. Así que, el auditor debe constatar que:

- Se disponen de procedimientos documentados para catalogar los informes como confidenciales, críticos o de acceso público.
- Se hayan implementado procedimientos adecuados para salvaguardar los informes considerados confidenciales por la institución.
- Existen procedimientos que restringen el acceso a datos e informes confidenciales (impresos o en línea) solo a personal autorizado y que estos conocen y aceptan mantenerlos confidencialmente y que se toman las medidas apropiadas para protegerlos.
- Se identifican o marcan los informes y que cuando ya no son útiles a la organización, se destruyen apropiadamente.

2.3 EVALUACIÓN DE CONTROLES EN EMPRESAS PYMES

Generalmente, las empresas pequeñas y medianas suelen ser familiares o de grupos de amigos y no suele existir, mayormente, una cultura de la seguridad. En muchos casos no

están conscientes de los riesgos a los que están expuestos sus sistemas informáticos, hoy más que nunca, por el avance de la tecnología en la red. Así mismo, muchas de estas empresas no tienen un mínimo de procedimientos establecidos y políticas para el control y seguridad de sus sistemas, y por lo tanto, de la información que estos generan y almacenan. El entorno informático en el que se mueve la pequeña empresa, en su mayoría, en nuestro país, puede describirse como incipiente y básico: Suelen adquirir equipos avanzados y, en algunos casos, sistemas de información más complejos, pero no invierten en capacitación para su personal, que suele ser limitado, por tanto, muchos empleados suelen utilizar la información de forma impersonal, accediendo a todo tipo de archivos, sin límites ni restricciones, lo cual puede llevar a una situación comprometedora si se accede a información confidencial. Como no hay políticas de control, los empleados con poco carácter ético, pueden robar o alterar información crítica, lo que trae consecuencias graves para una empresa. Si tampoco tienen procedimientos para la realización de copias de seguridad, se corre el riesgo de una paralización de las actividades computarizadas en caso de fallas de cualquier tipo en el sistema, lo que causa un gasto económico, que puede ser considerable, así como la pérdida de tiempo valioso para el negocio. Es así, que los directivos de empresas pequeñas y medianas deberían realizar una comparación entre el costo de la implementación de controles para garantizar una seguridad razonable y el costo de la paralización de su negocio.

2.3.1 Riesgos en las PYMES

En empresas pequeñas suelen utilizarse frecuentemente computadores de escritorio, que ofrecen eficiencia y flexibilidad, así como precios que las hacen accesibles para todo tipo de negocios. Y, en muchas de ellas, suelen estar conectadas a una red que permite compartir datos o periféricos.

Este tipo de empresas necesitan mecanismos de seguridad propios, que difieren de aquellos implantados típicamente en un centro de procesamiento de datos de una empresa grande, sea pública o privada, pues estas organizaciones también están expuestas a riesgos importantes, asociados al uso de Pc's, tales como:

- **Familiaridad:** Como estos equipos son aparentemente simples y fáciles de utilizar, existe el riesgo de que el uso inadecuado sea minimizado por los usuarios y por la administración.

- **Costo:** Los Pc's suelen ser considerados de bajo costo, pero no se toma en cuenta también el costo del software que se va a utilizar, de los periféricos que se necesitan y del mantenimiento que se les debe dar, lo que puede elevar significativamente el costo de un equipo.
- **Ubicación física:** Los Pc's, generalmente, se instalan sobre escritorios comunes, con poca o ninguna protección contra el robo, acceso no autorizado o daño accidental.
- **Software propietario:** Se suele adquirir software disponible en el mercado, que no tienen mecanismos de seguridad suficientes o adecuados, pues son más baratos que desarrollar programas a la medida de las necesidades de la empresa.
- **Conexiones en redes:** Cuando los pc's se utilizan como terminales o forman parte de una red de comunicación, su uso no autorizado puede llevar al acceso indebido a datos y programas de toda la empresa.

Para resguardarse de estos riesgos, las empresas pequeñas necesitan adoptar políticas y procedimientos determinados para adecuar el uso de los computadores por parte de sus empleados y directivos, utilizando principalmente estándares de hardware, software, adquisición, capacitación y soporte, además de los controles generales y de aplicación.

2.3.2 Controles Aplicables a las PYMES

Los conceptos básicos de control interno son aplicables a todo tipo de organización, sin importancia de su tamaño, pero la aplicación práctica es más directa, flexible e informal en las pequeñas empresas. En este tipo de entidades, generalmente, no es posible mantener todos los mecanismos de control que se implantan en las grandes organizaciones. La dirección debe apoyarse en sus empleados, acudir a los terceros y otros asesores externos, en cuestiones de informática. . Los Pc´s necesitan de controles específicos para protegerlos contra la pérdida de datos y programas, ya sea por robo o accidente, tales como restricciones físicas de acceso a los equipos; controles aplicados al software, tales como claves de acceso y realización periódica de copias de seguridad; protección contra el robo de equipos por medio de mecanismos convenientes de seguridad en el lugar donde están instaladas las máquinas.

El auditor, para realizar una evaluación de los controles en empresas pequeñas, debe

tener en cuenta los siguientes elementos críticos:

- **Controles de software en uso:** Tienen como fin garantizar la consistencia de la operación del software instalado en los Pc´s, de tal forma que se pueda impedir la instalación de programas no autorizados, la modificación indebida del software instalado, entre otros riesgos.
- **Seguridad:** Se utilizan para controlar el acceso a los recursos informáticos, datos y programas. Así se protegen contra modificaciones indebidas, robo, divulgación de documentos confidenciales, entre otros riesgos.
- **Controles sobre la operación:** El objetivo de su implantación es proteger los recursos de información contra perjuicios y daños causados por falta de capacitación o conocimiento del personal y de mantenimiento apropiado.

A continuación, se presentan procedimientos que el auditor deberá comprender para realizar una evaluación de controles en este tipo de empresa, que debe ser complementado por las guías sobre controles generales y de aplicaciones. [2.1 CONTROLES GENERALES 2.1y 2.2 CONTROLES DE APLICACIÓN. CAPITULO 2].

2.3.2.1 Controles de software en uso

El auditor debe constatar la existencia de:

- Políticas, estándares y procedimientos debidamente documentados para adquisición y uso de computadores y del software asociado, incluyendo también datos sobre desarrollo y prueba de aplicaciones; documentación; controles de entrada, salida y procesamiento; backup y recuperación de datos y programas; autorización para el uso de software, hardware y datos.
- Un inventario actualizado de los recursos informáticos, incluyendo hardware y software, su ubicación física, los usuarios, software en uso.
- Un análisis costo/beneficio y de la compatibilidad de los recursos informáticos con el ambiente ya instalado previo a la adquisición de recursos nuevos.
- Supervisión periódica de los equipos de cómputo y de su uso.
- Normas que prohíben la instalación de programas personales de los empleados en los computadores de la empresa, así como mecanismos para prevenir y

detectar el uso o instalación de programas sin licencia (software pirata).

- La documentación del software de cada equipo se mantiene actualizada y en un lugar seguro.
- Procedimientos documentados para que los usuarios cataloguen, almacenen y realicen copias de seguridad de archivos de datos y programas, y que estos procedimientos se cumplen.

2.3.2.2 Controles de Seguridad

En lo que respecta a la seguridad el auditor deberá constatar que:

- Los recursos informáticos se encuentran catalogados u organizados de acuerdo con su importancia y vulnerabilidad, con lo que se permite que los mecanismos de control estén encaminados a la protección de los recursos que representen mayores riesgos.
- Se dispone de mecanismos de identificación de usuarios y verificación del nivel de acceso a los equipos, ya sea por códigos o claves de identificación, por ejemplo, y que no se permite su uso compartido.
- Los equipos conectados a la red pública tienen mecanismos de protección contra acceso externo indebido.
- Los procedimientos para documentación y respaldo de programas, archivos de datos y aplicaciones son adecuados y que estos se cumplen.
- Los respaldos de datos críticos o confidenciales están resguardados en un lugar seguro.
- Se ha elaborado un plan de contingencias también para el entorno informático.
- Los programas de aplicación son protegidos contra actualizaciones indebidas.
- Los recursos físicos de informática contienen identificación única y son inventariados.
- Se utilizan reguladores de voltaje, como mínimo, u otros dispositivos similares para protección de los equipos de cómputo.
- En todos los equipos se han instalado, como medida mínima de seguridad, programas antivirus en versiones actualizadas.

- Se disponen de procedimientos para que los usuarios pasen las unidades externas, como memorias usb y discos externos, por el programa antivirus.
- Se ha capacitado al personal en el uso seguro y adecuado de equipos computarizados, así como sobre la concientización acerca de la importancia de la seguridad en ambientes informáticos.
- El personal y la administración están conscientes de los riesgos que implican el uso de equipos de computación y que ellos actúan de forma adecuada, siguiendo los procedimientos establecidos para minimizarlos.

2.3.2.3 Controles sobre la operación

En este apartado, el auditor deberá constatar que:

- Los usuarios reciben entrenamiento y capacitación adecuados.
- Se programan mantenimientos periódicos preventivos en todos los equipos de cómputo.
- El contenido de los discos rígidos es supervisado y controlado.
- Existe un centro de soporte al usuario capaz de dar informaciones, deshacer de dudas de utilización y registrar problemas con el procesamiento.

Existen también requisitos mínimos identificados con la seguridad en las empresas pequeñas, más simples, que también el auditor, según su criterio, pudiera examinar, para determinar si al menos se cuenta con estos requisitos:

- Comprobación de contraseña segura, asegurándose que todas ellas deben tener algún grado de complejidad, con al menos ocho caracteres alfanuméricos y símbolos combinados.
- Las contraseñas se encuentran guardadas en un lugar seguro, no son compartidas entre funcionarios y no están escritas en un lugar visible en el entorno de trabajo.
- La información confidencial de la red de la empresa se encuentra restringida sólo a los usuarios autorizados y dentro del perímetro del local donde funciona la empresa. Que solo puede acceder a la información crítica y confidencial, el personal designado con esta responsabilidad.
- Cada Pc debe tener asignada una contraseña y debe estar activada la opción para

que la contraseña de protección se habilite de forma automática si el equipo no está siendo utilizado en un período de tiempo corto, por ejemplo, la iniciación del protector de pantalla o hibernación que sólo se puede desbloquear mediante la contraseña.

- La presencia de software antivirus, como mínimo, en todos los equipos, y que este software esté actualizado, con la opción automática de actualización activada. También debería, de ser posible, existir software anti-spyware instalado y actualizado en todos los equipos.
- Los sistemas operativos se mantienen actualizados, con los parches de seguridad instalados y que la opción de descarga e instalación automática de estos paquetes esté activada y programada.
- La disponibilidad de un firewall, ya sea basado en software o en hardware. En empresas pequeñas con pocos terminales, se suele utilizar el primero.
- Que las unidades para discos Usb estén deshabilitados para reproducción automática, así como tener instalado un software que realice un análisis de virus apenas se conecte uno de estos dispositivos.

CAPÍTULO III

DESARROLLO DE UNA BASE DE INFORMACIÓN

Cuando se va a iniciar un proceso de auditoría, el auditor debe empezar por conocer la estructura general de la empresa en la que va a realizar su trabajo, así como el ámbito del negocio en el que se desenvuelve, cómo se procesan las transacciones, entre otros componentes que deben ser analizados por el profesional, para obtener un conocimiento cierto del entorno en el que va a desarrollar su labor.

Entre los componentes que deberá analizar el auditor informático, se encuentra la obtención de una comprensión global del sistema informático que está implementado en la organización. En este contexto, se incluyen los siguientes elementos de estudio, que deberán ser considerados por el auditor en su evaluación: estructura y administración del sistema informático; hardware y software; bases de datos y procedimientos de comunicaciones de datos que se usan en el entorno informático.

3.1 ESTRUCTURA Y ADMINISTRACIÓN DE SI

El conocimiento de cómo se estructura y administra un sistema informático en una organización se hace indispensable para poder ejecutar una evaluación más completa de la segregación de tareas [Segregación de funciones, CAPÍTULO 1. APARTADO 1.9.1.3] y otros controles dentro del Departamento de Sistemas. De igual manera, este procedimiento suministra las bases para formar una relación de trabajo positiva con el personal responsable de la empresa.

La información que se va a recabar debe contemplar datos importantes tales como, quién es el responsable del Departamento de Sistemas, quién es su jefe inmediato, nombres de el o los gerentes, así como el número de personal y líneas de dependencia por cada una de las funciones relevantes de operación dentro de este departamento.

Tales funciones son: Sistema y programación, grupo de desarrollo de software, administración de base de datos, software de recuperación de datos, software de seguridad en uso y cómo se realiza el ingreso de datos (en el sitio de procesamiento o de forma remota). Esta información recogida se puede documentar como una lista o como una tabla si existiera más de un sitio físico donde se realiza el procesamiento (centro de procesamiento de datos).

En el caso de que la información se transmite electrónicamente entre los centros de procesamiento y sitios remotos, se debe realizar una descripción gráfica de la red que se utiliza. Este bosquejo de la red debe referir de manera clara, todos los medios de comunicación de datos que se usan en una organización, tales como:

- **Redes privadas:** Red constituida por computadoras y líneas alquiladas, generalmente funcionan bien y suelen ser seguras, pues el tráfico no sale del perímetro de la organización y los intrusos tendrían que intervenir las líneas físicamente para infiltrarse.
- **Redes públicas:** Una red pública es una red que cualquier persona puede usar, sin necesidad de una clave de acceso personal para ingresar. Es una red de hosts interconectados por medio de una subred de comunicación, capaz de compartir información y que abarca una gran área geográfica. Se conoce también como WAN (red de área amplia). Los hosts son los computadores personales de los usuarios y los proveedores de servicios de Internet son quienes operan la subred de comunicación.
- **Redes locales, LAN (Local Area Network):** Redes de área local, son redes de propiedad privada que interconectan hosts en el perímetro de un edificio o un campus de pocos kilómetros de longitud. Suelen utilizarse para conectar pc's, estaciones de trabajo para compartir recursos e intercambiar información.
- **Redes VPN (Virtual Private Network):** Es un canal seguro a través de Internet u otras redes públicas para conectar dos redes locales a través de Internet, donde el host remoto se conecta a otra LAN como si estuviera conectada físicamente a ella. El contenido de la conexión se cifra, por lo que la información es inaccesible al público, pero no para la red privada a la que se conecta.
- **Redes VAN (Value Added Networks):** Redes de valor agregado, son redes que usan los servicios de comunicación de otras compañías comerciales, utilizando el hardware y software que permiten mejorar los servicios de comunicación que se ofrecerán.

3.2 HARDWARE Y SOFTWARE

Respecto a un conocimiento global en cuanto a hardware y software del que dispone una organización, COBIT le da al auditor una guía aplicable a este apartado, en la sección AI3, Adquirir y Mantener Infraestructura Tecnológica [25] , refiere que las organizaciones deben contar con procesos para adquirir, implementar y actualizar la infraestructura

tecnológica, lo que refiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas. Cuando se habla de infraestructura tecnológica, se está refiriendo a recursos hardware y software. Los objetivos de control de alto nivel correspondientes a este proceso, que el auditor deberá considerar en su proceso de evaluación son:

- **Plan de Adquisición de Infraestructura Tecnológica:** La empresa deberá generar un plan para adquirir, implementar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio y que esté de acuerdo con la dirección tecnológica de la organización.
- **Protección y Disponibilidad del Recurso de Infraestructura: Implementar** medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad.
- **Mantenimiento de la infraestructura:** Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo al procedimiento de administración de cambios de la organización.
- **Ambiente de prueba de Factibilidad:** Establecer el ambiente de desarrollo y pruebas para soportar la efectividad y eficiencia de las pruebas de factibilidad e integración de aplicaciones e infraestructura, en las primeras fases del proceso de adquisición y desarrollo.

El auditor, basándose en estos objetivos, deberá evaluar, adicionalmente, la presencia o pertinencia de políticas y procedimientos, sobre recursos hardware y software, que aseguren que:

- Se ha determinado un plan que permite la evaluación del hardware y software que se adquiere, en relación a su impacto sobre la infraestructura tecnológica existente y el desempeño del sistema.
- El software es instalado y mantenido de acuerdo a los procesos referidos en el apartado de adquisición y mantenimiento de la infraestructura tecnológica.
- Si se ha desarrollado software, este debe ser probado exhaustivamente antes de ponerlo en producción.

- En el software están incluidos procesos de aseguramiento de la integridad como parte del mismo.
- Se han establecido parámetros de software, de tal manera que la integridad de datos y programas del sistema esté asegurada.
- Cuando se prepare, instale y mantenga el software existente, no exista amenaza para los datos y programas ya instalados.
- La posibilidad de acceso al software esté limitada y restringida sólo a personal autorizado.
- Las contraseñas provistas por el proveedor de software para instalar en las máquinas, son cambiadas en ese momento y que los cambios al software y actualización de versiones, son supervisados por los responsables de esta actividad.

En cuanto al mantenimiento preventivo de hardware, tanto del existente en el/los centros de procesamiento como los instalados en los equipos usuarios, el auditor deberá consultar sobre la existencia de programaciones, en cuanto a pasos a seguir y frecuencia para mantenimiento preventivo, servicio que es prestado comúnmente por los proveedores de cada dispositivo de hardware, de la siguiente manera:

- El mantenimiento de hardware que ha sido programado en la agenda elaborada para esta actividad, no tendrá impacto sobre aplicaciones críticas.

- El mantenimiento programado no se planeó para fechas consideradas como de gran carga de trabajo y que, en caso contrario, se pudiera flexibilizar la agenda para que no coincida en estas fechas el mantenimiento planificado.

En cuanto al software, el auditor basará su evaluación en los siguientes puntos importantes:

- Realizar una comparación del software instalado, por lo menos de aquél que procesa la información sensible o crítica, con los requerimientos del sistema, para determinar su real desempeño, así como la compatibilidad con los recursos disponibles.

- Realizar una evaluación de los parámetros del software del sistema, para conocer si son aptos, suficientes y adecuados para el aseguramiento de la integridad de la información y aplicaciones instaladas.

- Probar el acceso al sistema y a aplicaciones críticas, para determinar si éste se

encuentra restringido para sólo personas autorizadas o si está abierto para cualquier usuario.

- Sobre el software del sistema (sistema operativo), si está instalado adecuadamente y si se encuentran activadas las opciones de actualizaciones automáticas y si se cuenta con puntos de seguridad. El decir que está instalado adecuadamente, incluye las licencias de permiso de uso determinado por el proveedor y los parámetros adecuados para limitar el acceso a personal autorizado que necesite acceder, por sus responsabilidades, a las funciones de administración del sistema.

3.3 BASES DE DATOS

Cuando recién aparecieron las bases de datos, estas se referían a un archivo que contenía una colección de datos que podían ser accesados de forma predeterminada por una o más aplicaciones de usuario diseñadas para esa base de datos específica. Esta modalidad funcionaba bien, hasta que se necesitaba realizar modificaciones a los datos que contenía. Es así, que surgió la necesidad de nuevas aplicaciones que pudieran sobrepasar estas dificultades. Aparecieron, entonces, los DBMS (Data Base Management System, sistema administrador de bases de datos), que resolvieron los problemas referentes a datos duplicados y deficiencias en la integridad y seguridad de los datos.

El papel del DBMS es mantener y organizar los datos, para que estén siempre disponibles para programas de aplicación, cuando son requeridos. El administrador de base de datos es un software complicado, cuya responsabilidad es mantener la seguridad e integridad de los datos.

En este contexto, el auditor ha de tomar en cuenta los siguientes componentes, que suelen estar presentes cuando una organización maneja bases de datos a través de software especializado o software de propósito general.

3.3.1 Diccionarios de datos

Los diccionarios de datos almacenan todos los elementos de datos disponibles en el sistema, sus características y cómo son usados por los programas de aplicación. Cuando los datos se comparten entre dos o más aplicaciones, como ocurre con las bases de datos, es necesario que se mantenga un registro esa información por cada elemento de

datos.

En este apartado, el auditor debe realizar un análisis de los procedimientos y normas existentes para el acceso, contenido y cambios al diccionario de datos, considerando los siguientes puntos:

- Se restringe el uso de las herramientas administrativas de la base datos solo al personal que tenga las atribuciones compatibles con el acceso, designados como administradores de la base de datos, así como a los archivos de datos y diccionario de datos.
- Se ha limitado el acceso al software y a las tablas de seguridad del DBMS y a los perfiles de seguridad del diccionario de datos.
- Disponibilidad de registros históricos de acceso y actualización a los elementos de la base de datos, así como habilitación de pistas de auditoría.
- Presencia de elementos necesarios en el diccionario de datos, tales como: Fecha de creación y última actualización, descripción de cada elemento de datos, claves utilizadas.
- La disponibilidad de una lista de aplicaciones y sistemas que utilizan cada elemento de datos y en qué manera.
- Existen o no procedimientos para producción de copias de seguridad (backup) y recuperación del diccionario de datos.
- Existe control de cambios y sobre la creación de nuevos nombres de archivos y descripción de datos.

3.3.2 Acceso a la base de datos

El acceso a la base de datos suele ser necesario para los programadores, administradores y usuarios del sistema. La mayoría de software de gestión de base de datos permite distintos medios de acceso a los datos que almacena, trabajando dentro de un esquema de control de acceso muy riguroso.

Generalmente, la base de datos se almacena en un solo sistema y se pone a disposición para usuarios directamente conectados a ese sistema o con acceso mediante una red. Esta base de datos centralizada, muchas veces, satisface las necesidades de una empresa. Sin embargo, en otras organizaciones, hay una necesidad de acceder a los

mismos datos en diferentes lugares, para lo que suelen utilizar un software de administración de base datos que permita una base de datos distribuida. Así, en cada lugar se ejecuta una copia del DBMS, que interactúa con las demás por medio de la red y, de este modo, forma un sistema único. Los datos así compartidos, son tratados por el DBMS como una base de datos única y completa. Los datos son distribuidos por la red de acuerdo con las solicitudes de cada lugar, aumentando la velocidad de acceso.

En este contexto, el auditor deberá preparar una lista para comprobar la existencia o no de procedimientos que aseguren la integridad y disponibilidad de los datos, que entre otros podría incluir los siguientes puntos:

- Existencia de procedimientos para garantizar la disponibilidad de la base de datos, así como su recuperación, lo más pronto posible, después de que ocurren fallas de operación o eventos indeseables o desastrosos. Si estos procedimientos de recuperación se prueban y actualizan periódicamente y con qué frecuencia.
- Disponibilidad de procedimientos de respaldo de hardware (en cuanto a drivers) y software, para asegurar la disponibilidad de la base de datos para las aplicaciones que sean prioritarias, en caso de que se vea disminuida la capacidad de funcionamiento.
- Se han habilitado o no caminos alternativos de ingreso a bases de datos que son accesadas vía red.
- Disponibilidad y cumplimiento de procedimientos recuperación lógica y física de las bases de datos.
- Disponibilidad de procedimientos para evaluar el desempeño de la base de datos.
- Presencia en el sistema administrador de base de datos de elementos de control sobre la organización, el acceso y el compartimiento de datos.
- Disponibilidad, en el sistema administrador de base de datos, de control sobre los cambios que se realicen en la base de datos, actualización de aplicaciones, funciones de DBMS y diccionario de datos.

3.3.3 Administración de Datos

Debido al tamaño y la complejidad de las bases de datos, las organizaciones, generalmente, tienen personal que se designa para atender las actividades de administración de bases de datos, que incluyen el mantenimiento de estructuras de datos,

del software de DBMS y aplicaciones relacionadas, documentación de la base de datos, procedimientos de copias de seguridad, recuperación de fallas de la base de datos, entre otras.

En este sentido, el auditor deberá observar los siguientes procedimientos, a fin de verificar cuáles están disponibles en la empresa en la que va a realizar su evaluación:

- Se encuentran definidas y documentadas las responsabilidades relativas a la administración de bases de datos, tales como:
  - Proyecto y mantenimiento de la estructura de base de datos.
  - Revisión y evaluación de la confiabilidad del sistema administrador de base de datos y la seguridad de datos.
  - Evaluación del personal que opera la base de datos.
  - Capacitación del personal responsable de la administración de base de datos.
  - Cumplen con el perfil para administrar una base de datos.
- Las actividades de administración de base de datos son almacenadas en registros históricos y periódicamente analizadas por un supervisor.

3.4 REDES

En la actualidad, los usuarios de un sistema pueden encontrarse en un lugar diferente de donde están físicamente los recursos informáticos de una empresa, utilizando redes de comunicación entre computadores para permitirles el acceso instantáneo a información y a otros usuarios en diferentes lugares de la institución. Es así, que las redes ofrecen facilidades tales como acceso compartido a datos, aplicaciones, impresoras y otros dispositivos; correo electrónico; acceso a usuarios y dispositivos remotos; reducción del costo de software, por medio de licencias multiusuario; acceso y ejecución de procesos en sistemas remotos.

Para que todo este sistema de comunicación de datos funcione correctamente, se utilizan:

- Registros (logs) de comunicaciones, donde se registran todos los bloques transmitidos, correcta o incorrectamente, que se usan como estadísticas y para intento de recuperación de datos transmitidos.
- Software de comunicación de datos, para comprobaciones de protocolo de transmisión,

grabación de registros de transacciones y para codificación y decodificación de señales de comunicación.

- Protocolo de transmisión, que garantiza la recepción correcta del bloque de informaciones transmitido.
- Software o hardware para la realización de codificación y decodificación de la información transmitida.

El riesgo más común en el uso de redes es el de acceso no autorizado a información y a aplicaciones que se corren en una organización, lo que puede causar daños o prejuicios intencionales o accidentales.

Actualmente, se ofrece en el mercado software y hardware especializado en limitar el acceso de usuarios o sistemas externos a una red de comunicación, tales como gateways o firewalls, que son dispositivos que restringen el acceso entre redes, importantes para reducir el riesgo asociado al uso de la Internet; monitores de teleprocesamiento que son aplicaciones incorporadas al sistema operativo para limitar el acceso y dispositivos de protección de los canales de comunicación.

El mejor medio para proteger la información al ser transportada por redes es el cifrado, pues no es suficiente la autorización o la autenticación cuando no se sabe exactamente cuál es la ruta por la que viajarán los datos. En cualquier salto intermedio, un atacante podría interceptarlos. Si esta información no fue cifrada, se podrán obtener datos confidenciales, caso contrario, no podrá tener ninguna información válida, pues no sabrá cuál es la clave de cifrado utilizada. En este contexto, se cuenta con la criptografía, que utiliza algoritmos (fórmulas matemáticas) y combinaciones de claves (secuencias de bits) que transforman un mensaje en códigos complicados para quienes no tienen una clave secreta, que es necesaria para descifrarlos, por lo que el contenido de un archivo o mensaje se mantiene en forma confidencial. Sirven también para proporcionar una firma electrónica, que puede revelar si hubo alguna modificación en el archivo, por lo que garantiza su integridad y además permite la identificación cierta del autor del mensaje.

Cuando el auditor, durante su evaluación, necesita conocer más a fondo el funcionamiento de las redes de comunicación de una empresa, debe tomar en cuenta los siguientes elementos críticos, que le permitirá definir la confianza en los controles:

- Administración de la red: En una organización que utiliza redes para su

comunicación, tanto interna como externa, deben existir procedimientos y políticas para ayudar la administración del ambiente de red y estándares definidos para control del hardware y del software involucrados.

- Seguridad de los datos y de la red: deben haber mecanismos de control de hardware y software que garanticen la seguridad e integridad de los datos mantenidos en el ambiente de red y de los recursos físicos que la componen, que limiten y controlen el acceso a programas y datos.
- Operación de la red: la organización debe ofrecer condiciones para una operación eficiente de la red, incluyendo normas y procedimientos de entrenamiento y capacitación del personal, realización de copias de seguridad, evaluación de la eficiencia del servicio y rutinas de recuperación de la red después de interrupciones inesperadas.
- Software de red: Debe existir monitoreo y control del software de comunicación y el sistema operativo instalado.

3.4.1 Administración de la red

Con el propósito de identificar los posibles riesgos que podrían existir en la administración de la red, el auditor deberá considerar para su evaluación los siguientes elementos:

- Existen objetivos de corto y mediano plazos para el procesamiento de datos distribuidos de la organización.
- Se han definido con claridad las configuraciones de hardware, base de datos, topología de red e interfases de red de comunicaciones.
- Se realizaron análisis de costo/beneficio para la elección de la plataforma de red, que justifique la alternativa escogida.
- Existen procedimientos de control para el procesamiento en red, que prueban y evalúan periódicamente la red de comunicaciones.
- Los procedimientos de operación de la red se distribuyen a los usuarios de cada departamento y se encuentran debidamente documentados.
- Existen mecanismos que pueden garantizar la compatibilidad de archivos entre las aplicaciones, a medida que la red crece en tamaño y complejidad.

- Se estableció una política de auditoría y de respaldo para la red.
- La Unidad de Sistemas ha definido políticas, procedimientos y estándares documentados, actualizados y divulgados al personal responsable.
- Se han implantado controles para garantizar que la integridad de los datos se mantenga durante la transferencia de datos en la red, es decir, procedimientos de autenticación de mensajes.

3.4.2 Seguridad de la red

El auditor, en este apartado, deberá analizar si existen procedimientos tales como:

- Se tiene un inventario de todos los equipos de red pertenecientes a cada departamento de la organización y que se revisan periódicamente la eficacia de las prácticas de seguridad adoptadas.
- Que se protegen los recursos físicos de la red y la integridad del software de aplicación y de los datos almacenados, mediante procedimientos de seguridad adecuados y que éstos se revisan de forma periódica.
- Que se mantiene actualizada la documentación de seguridad y que se reevalúa con frecuencia la adecuación de los controles de seguridad del hardware de comunicación y estaciones de trabajo, del sistema operativo, de las aplicaciones relevantes, de los datos que se consideran confidenciales.

3.4.3 Control de acceso

El auditor se basará en los siguientes procedimientos, para realizar una lista acerca de este apartado:

- Las pistas de auditoría se encuentran disponibles por periodos razonables y permiten revisar las actividades tales como: Login/out, indicando lugar, hora y fecha, identificación de usuario; tipo de acceso e intentos de acceso inválidos, que indiquen local, hora y fecha, e identificación de usuario.
- Autorización de acceso por cada usuario o grupo de usuarios, para discos, volúmenes, directorios y archivos.
- Qué controles de acceso se han determinado para los terminales o estaciones de trabajo y si hay un registro de claves individuales de todos los usuarios para su

identificación en el sistema.

- Existe inhabilitación de terminales y estaciones de trabajo después de un determinado número de intentos de acceso no autorizado.
- Se ha establecido perfiles de acceso para los usuarios, definiendo los recursos, datos, aplicaciones, transacciones y comandos autorizados, de acuerdo con las responsabilidades de los respectivos cargos.
- La seguridad física de servidores y equipos de comunicación y conexión en red es adecuada. Los servidores se encuentran en un área con acceso restringido para solo el personal autorizado.
- Los terminales y estaciones de trabajo poseen mecanismos de seguridad física que previenen su eliminación no autorizada.

3.4.4 Plan de contingencia

El auditor investigará y observará si existe un plan de contingencia adecuado para la recuperación de la red y si éste es probado periódicamente mediante simulaciones. Se debe considerar si están considerados en este plan los siguientes puntos:

- Protección de archivos de datos.
- Procedimientos para varios niveles de interrupciones y emergencias.
- Procedimientos de recuperación de aplicaciones del sistema.
- Lista de documentos y archivos con copias a ser mantenidas en otro lugar.

3.4.5 Operación de la red

El auditor deberá tomar en cuenta los siguientes procedimientos para ser incluidos en su lista de verificación:

- Se documentan y actualizan con una frecuencia apropiada los procedimientos de administración y operación de la red.
- Se han definido con claridad las responsabilidades de operación para todos los terminales y estaciones de trabajo.
- Se han establecido procedimientos para evaluar de forma periódica el desempeño, tiempo de respuesta y recuperación después de fallos de la red.

3.4.6 Fallas e interrupciones de servicio

El auditor deberá realizar una observación acerca de la configuración de red, a fin de verificar algún riesgo que posibilite la ocurrencia de un fallo en uno de sus puntos que induzca la caída de toda la red. Así mismo, deberá determinar con qué mecanismos se cuenta para minimizar el impacto provocado por un fallo del sistema y si se documentan los procedimientos utilizados para el retorno a la operación, en caso de que haya una interrupción inesperada del servicio y si estos se prueban y actualizan con cierta periodicidad, así como acerca del personal responsable, si está debidamente capacitado para ejecutar las actividades necesarias de manera eficiente y rápida.

3.4.7 Software de red

Sobre este apartado, el auditor debe tomar en cuenta los siguientes puntos para realizar su lista de verificación:

- Qué mecanismos se han dispuesto sobre el software de comunicación de red para almacenar temporalmente mensajes destinados a usuarios que no se encuentran conectados y retransmitirlos automáticamente cuando la conexión sea restituida.
- Se documentan procedimientos sobre el mantenimiento de rutas de comunicaciones normales y alternativas.
- Qué rutinas de de tratamiento de errores y de supervisión de desempeño se encuentran disponibles en el software de red.
- En el contrato constan explícitamente los mantenimientos preventivos y correctivos de la red.
- Qué mecanismos de control y registro se disponen para los cambios que se efectúen en el software de red.
- Se han previsto mecanismos de supervisión y autorización para los procedimientos de cambio de software de red, incluyendo la disponibilidad del sistema, impacto para los usuarios, eficiencia del sistema y actualización de la documentación y manuales.
- Qué procedimientos se han dispuesto para informar, entrenar y auxiliar al personal de operaciones en la implementación y soporte de cambios en el software de red.

CAPÍTULO IV

CONSIDERACIONES DE RIESGO

4.1 EL RIESGO EN AMBIENTES DE TI

Generalmente, cuando el auditor realiza evaluaciones del ambiente de control de TI, descubre que, en la mayoría de empresas pequeñas o medianas, no existe una cultura acerca del riesgo, por lo tanto, no disponen de planes sistemáticos de evaluación de riesgo y no se pueden establecer medidas acerca del riesgo, que contribuya, de algún modo, a alcanzar los objetivos de la empresa.

Si no se han establecido medidas de control basadas en un análisis de riesgo, no es posible detectar fácilmente las debilidades de los controles que se implantan a dedo en muchas empresas, por lo que el riesgo de operación suele ser bastante alto y puede resultar muy costoso si sucedieran eventos inesperados. Generalmente, no se cuenta con un enfoque adecuado para la evaluación de riesgos, que pueda definir un plan de acción que establezca los controles necesarios y las medidas de seguridad apropiadas para los recursos informáticos de una organización, y por lo tanto, tampoco se definen políticas para mitigar los riesgos inherentes a la operación de sistemas informáticos en la empresa.

En este contexto, se podría asegurar que no existen niveles de seguridad adecuados, aprobados y seguidos de manera formal. El panorama antes mencionado nos permite asegurar que la poca capacidad gerencial existente en los ambientes de tecnología de información, no permite acreditar niveles de seguridad adecuados y aprobados formalmente, que contribuyan a satisfacer plenamente los requerimientos de información de organizaciones pequeñas y medianas.

4.2 LA EVALUACIÓN DEL RIESGO Y LOS CONTROLES EN LA TECNOLOGÍA DE INFORMACIÓN

Para poder contar con un entorno de control conveniente, la actitud de los directivos con respecto al control interno es fundamental. Es precisamente, ese compromiso de la dirección, el que constituye un marco de referencia para la actitud que tomará el personal

de la organización. Es así que, son ellos quienes establecen y orientan con su ejemplo, los mecanismos de cumplimiento de las normas éticas y de seguridad. Es en estas condiciones, en el que el control interno asegura que la relación organizacional esté acorde con las políticas de la dirección.

Esta guía continúa con las consideraciones del riesgo, basándose en los referidos controles generales y controles de aplicación.

4.3 RIESGOS Y CONTROLES GENERALES

Dado que los controles generales se implementan para asegurar que el procesamiento de la información se realice en un ambiente razonablemente seguro, el auditor deberá concentrar su atención en los riesgos más relevantes, que conciernen a la operación de sistemas informáticos y analizar los controles adecuados que se deben aplicar para reducir o minimizar dichos riesgos.

Generalmente, el auditor puede enfocarse en la reducción de los siguientes riesgos a niveles razonables, a través de la implantación de controles generales:

4.3.1 Riesgo sobre Estructura Organizacional y Operación de Sistemas Informáticos

La ausencia de una estructura organizacional y de los procedimientos de operación de los sistemas informáticos, ocasiona un ambiente poco seguro para el procesamiento de los datos, lo que puede dificultar la preparación de información de acuerdo a los requerimientos de la empresa.

a. Control sobre la Segregación de Tareas en la Unidad de Sistemas

El auditor debe constatar que las actividades estén organizadas de tal forma que exista una segregación de tareas apropiada entre las funciones, tales como: El uso de los sistemas informáticos, ingreso de datos, operación de terminales y servidores, administración de redes, administración de sistemas, desarrollo y mantenimiento de sistemas, administración de cambios, administración de seguridad y auditoría de la seguridad.

En empresas pequeñas o medianas, son los usuarios quienes realizan las operaciones informáticas, entonces, se debe compensar la falta de segregación de

funciones, implantando controles tales como: Mantener registros por tipo de transacción, los totales de control del archivo de datos permanentes, conciliar los datos ingresados y considerados significativos, con la información de salida del sistema, supervisión directa del uso del equipo y retiro de software sensitivo de los terminales de usuario.

b. Control sobre los Procedimientos de Operación del Sistema Informático

- **Desarrollo de programas.**
  - El desarrollo de cualquier aplicación se debe hacer en base a un requerimiento formal de los usuarios.
  - Se debe tener la aprobación de los usuarios en cada uno de los puntos clave del proceso de desarrollo: Estudio de factibilidad, incluyendo el presupuesto; propuesta de desarrollo del sistema; diseño del sistema; prueba de aceptación del sistema.
  - Los usuarios deberán aprobar cualquier tipo de modificación antes de que el producto final sea implantado.

- **Prueba**

  Los procedimientos de prueba deben ser prefijados y documentados de manera formal.
  - Deben haber planes de prueba que especifiquen datos de prueba, resultados previstos y procedimientos del usuario, y, se debe verificar que se siguen dichos pasos planeados.
  - Para nuevos sistemas se llevan a cabo pruebas de corridas piloto [26] o en paralelo.
  - Los usuarios deben aprobar formalmente los resultados de las pruebas.

- **Implantación**
  - Antes de la implantación del nuevo software, la gerencia deberá revisar la documentación del sistema y de los programas.
  - La documentación se debe modificar y actualizar cada vez que se introducen cambios en el sistema.
  - Se debe obtener una autorización formal para trasladar a la biblioteca de

producción un nuevo programa.

- Los datos transferidos al nuevo sistema deben ser conciliados con los totales de control del sistema anterior.
- Luego de la conversión, los departamentos usuarios hacen pruebas de las funciones principales del nuevo programa.

- **Controles sobre software disponible en el mercado**
  - Los paquetes de software se escogen a partir de un requerimiento formal de los usuarios.
  - La selección final del software se debe realizar después de investigar la trayectoria de los proveedores; analizar varios paquetes de software similares; consultar sobre la experiencia de uso del software escogido a otros usuarios; realizar consultas con los usuarios y obtener su aprobación.
  - El software deberá ser aprobado antes de decidir la compra o antes de que expire el período de garantía.
  - Los contratos con los proveedores cubren las necesidades relativas a la documentación y mantenimiento del software adquirido.

4.3.2 Riesgo sobre el Acceso General a los Datos o Programas de Aplicación

Personas no autorizadas, sean parte del personal o terceras personas, podrían tener acceso directo a los archivos de datos o programa de aplicación que se utilizan para procesar transacciones, lo que podría resultar en modificaciones no autorizadas a los datos o programas.

4.3.2.1 Control sobre el acceso restringido a los datos o programas de aplicación

Las personas que pueden acceder al sistema informático de una empresa, sea cual fuere el motivo, podrían evitar las prácticas normales de control de procesamiento de transacciones, generando errores o anomalías. Es indispensable que el auditor pueda identificar las posibles vías de acceso no autorizados, con la finalidad de poder considerar el impacto de estos accesos no autorizados sobre la información de la empresa.

Generalmente, se suele restringir el acceso mediante la identificación de los

usuarios y el uso de contraseñas. De este modo, el acceso al sistema se permitirá si se ingresa la combinación correcta de identificación y la contraseña correspondiente. Sin embargo, para que este mecanismo sea eficaz, se debe usar software para interactuar con las solicitudes de acceso y, permitir o negar el acceso, tomando en cuenta si la identificación o contraseña ha sido definida en el sistema y si el usuario está autorizado para ejecutar la función solicitada.

Los procedimientos de control que, generalmente, suelen usarse para evaluar los riesgos existentes son:

- Identificación del usuario junto con las contraseñas correspondientes.
- Software de control de acceso.
- Registro de operaciones.
- Restricción del acceso físico.

4.3.2.2 Controles sobre el acceso físico

- Las terminales deben estar instaladas en lugares protegidos por cerraduras o por dispositivos de reconocimiento de huellas digitales o de voz.
- Las terminales deben estar en áreas supervisadas.
- El acceso a las terminales sólo se permite a los operadores autorizados y a usuarios previamente autorizados.
- El acceso a los centros de procesamiento de datos se debe controlar con tarjetas de acceso y códigos de combinación.
- Las tarjetas y llaves deben entregarse solo al personal autorizado y deben definirse procedimientos para controlar la devolución de estos dispositivos de acceso.
- Deben definirse disposiciones especiales para el acceso de visitantes y personal de limpieza al centro de cómputo.
- Se debe informar inmediatamente a la gerencia del DS y al personal a cargo de la seguridad cuando un empleado se retira de la empresa.
- La documentación concerniente a sistemas y programas solo debe estar a disposición de los analistas y programadores.

4.3.2.3 Funciones de control del software de seguridad

- El acceso debe ser limitado, en base a perfiles de seguridad incorporados al software de seguridad, a los elementos del sistema que van a ser controlados, como: archivos de datos, terminales, programas, tablas de claves de acceso, editores on-line [27] y utilitarios del sistema operativo.
- Se deben definir las rutas de acceso autorizadas que pueden ser usadas, como por ejemplo, se permite el ingreso de información contable sólo desde ciertas terminales.
- Las funciones que puede realizar un usuario deben estar definidas, como por ejemplo, un usuario puede estar autorizado a leer información, pero no para modificarla o puede tener acceso, pero sólo desde un terminal específico.
- Se deben monitorear y registrar actividades determinadas, así como generar informes de seguridad, como por ejemplo, emisión de un listado cada vez que un usuario privilegiado accede al sistema o cuando se ha tratado de obtener acceso fallido.
- El control de los sistemas de claves de acceso se debe realizar a través de la generación de informes de mantenimiento, identificando períodos en los que se deben hacer cambios de las claves; la interrupción de la conexión de terminales luego de transcurrido un tiempo definido de inactividad y la individualización de combinaciones identificación y contraseña de acceso implicadas en actividades inusuales o en intentos de acceso no autorizados.

4.3.2.4 Registro de operaciones

En general, todos los sistemas operativos generan registros de operación, que consiste en un registro completo de cada actividad de procesamiento realizada en un computador. Dichos registros pueden ser examinados por el personal de DS para descubrir actividades no usuales de procesamiento.

Sin embargo, los registros pueden ser muy voluminosos como para ser revisado en la práctica y cualquier revisión podría ser hecha a la ligera y en forma ineficiente por el personal responsable. Para solucionar este inconveniente, se suele utilizar software de generación de informes, de manera que solo se listen

determinadas actividades de procesamiento, que sean relevantes en el funcionamiento de la organización.

4.3.3 Riesgos y Controles para cambios a los programas

Al igual que la tecnología ha ido evolucionando continuamente, también lo ha hecho la estructura funcional de las unidades de sistemas, por lo que, el auditor deberá tomar en cuenta algunos conceptos importantes, que pudieran ser significativos dentro de un proceso evaluativo:

- Actualmente, el entorno sistema-usuario es interactivo, en el que los usuarios participan de forma activa y directa.
- El hardware ha reducido notablemente de precio y se pueden encontrar computadores pequeños de gran capacidad de procesamiento, por lo que, muchas organizaciones se han equipado con microcomputadores, más baratos que los típicos terminales de antes. Se ha invertido en redes conformadas por una cantidad considerable de unidades y el uso de aplicaciones independientes, lo que incide directamente en la estructura organizativa de la mayoría de los sistemas.

Es entonces, que, debido esta permanente evolución de la tecnología, los sistemas también están pasando por estados de cambio continuo. Es por estas razones que en muchas organizaciones se han formado grupos de trabajo dedicado especialmente al desarrollo de sistemas nuevos o a realizar cambios a los que ya se encuentran en los sistemas. Es así que, es importante un control y supervisión permanente de las modificaciones que se hacen a los sistemas.

El riesgo dentro de este contexto es la reducción notable de la confiabilidad de la información que se procesa en los sistemas cuando los programadores realicen cambios incorrectos o no autorizados en el software de aplicación.

Control: Procedimientos para cambios a los programas

Las actividades de mantenimiento incluyen las tareas necesarias para que las aplicaciones sigan siendo operativas y que se adapten a los requerimientos variables de los usuarios y de la empresa. En muchas organizaciones grandes, se invierte mucho tiempo de programación para realizar las modificaciones a los programas, que se suelen hacer por algunas razones importantes:

- Para adecuar las aplicaciones cuando se dan cambios del hardware y/o software de

base.

- Para obtener mayor efectividad y eficiencia.
- Para corregir errores.

Estos procedimientos para modificar programas deben ser administrados de manera apropiada y ser documentados, para asegurar que sigan operando adecuadamente y que, mientras dure este proceso de mantenimiento, el software no sea maniobrado para fines no autorizados.

Para realizar modificaciones a cualquier programa se debe tomar en cuenta que:

- Cualquier solicitud de modificación debe estar documentada y aprobada por un nivel directivo conveniente, para que se constituya en un respaldo válido.
- Los cambios deben ser hechos solamente en las versiones de prueba de los programas y no en las que se encuentran en producción. Además, sólo los deben realizar el personal de la Unidad de Sistemas, no por operadores ni usuarios.
- Cualquier cambio debe ser examinado y probado por personal distinto de los programadores que hicieron las modificaciones.
- Se debe guardar un registro permanente de todas las modificaciones. Este proceso lo hace normalmente el software de bibliotecas de manera automática.
- Los resultados de las pruebas deben ser aprobados en conjunto con la jefatura del área o departamento que solicitó la modificación, antes de pasar el programa ya modificado a la biblioteca de producción.

4.4 RIESGOS Y CONTROLES DE APLICACIONES

Los controles de aplicación incluyen procedimientos computarizados y manuales, por parte del usuario. Los primeros implican ingresos de datos por medio de un terminal, realizados por usuarios y un proceso computarizado que controla el flujo de datos dentro del computador. Los procedimientos manuales se realizan para cerciorarse de que las transacciones procesadas sean correctamente preparadas, autorizadas y enviadas al centro de cómputo.

El que los controles de aplicación sean efectivos, depende de los riesgos que hay en el ambiente de control de cada empresa, de la naturaleza de los controles que se han implantado, de cómo se implementaron y de su vinculación con otros controles.

En este contexto, se van a estudiar los riesgos más comunes que son evaluados en la implantación de controles de aplicación:

- Acceso a las funciones de procesamiento de transacciones de los programas de aplicación, a personas no autorizadas, lo que permite la lectura, modificación, agregación o eliminación de información existente en los archivos de datos o ingreso de transacciones no autorizadas para ser procesadas.

- Los datos ingresados para ser procesados en el sistema pueden ser erróneos, incompletos o ser ingresados por duplicado.

- Los datos rechazados y las partidas en suspenso pueden no ser identificados, analizados y corregidos debidamente.

- Las transacciones reales que han sido ingresadas para su procesamiento o generadas por el sistema pueden perderse, ser procesadas o informadas de manera incompleta o inexacta.

4.4.1 ACCESO A FUNCIONES PROGRAMADAS DE PROCESAMIENTO

4.4.1.1 Controles sobre el Acceso del Usuario

El auditor debe verificar que se cumpla con la mayor parte de los siguientes controles:

a. Técnicas de control físico

- Las terminales deben estar ubicadas en sectores asegurados mediante cerraduras, o dispositivos de reconocimiento de la voz o de análisis de huellas digitales.
- Las terminales son ubicadas en sectores bajo supervisión directa.
- Se adquieren dispositivos de identificación física (por ejemplo, tarjetas o llaves) para operar la terminal.
- Las tarjetas o llaves sólo se entregan a personal autorizado.
- El acceso desde determinadas terminales se restringe sólo a funciones específicas.

b. Controles de claves de acceso (contraseñas)

- Dar acceso limitado a actividades y aplicaciones, de acuerdo a un nivel establecido según sea la segregación de funciones.
- Identificar a los usuarios autorizados mediante identificaciones individuales de usuario.
- Las contraseñas deben ser conocidas por los usuarios autorizados solamente.
- Se deben guardar registros de las tentativas de acceso con claves erróneas y los mismos deben ser examinados, de tal modo que puedan ser identificados los intentos de acceso no autorizado.
- Se debe restringir el acceso a los datos en un sistema de administración de base de datos.
- Tienen que existir controles sobre la identificación del usuario (nombre de usuario / contraseña).
- Cuando se da acceso a una aplicación a través de terminales, se debe asignar a cada usuario autorizado una identificación única que lo identifica en el sistema y que sea un requisito para acceder al sistema, junto con la contraseña que se le debe asignar, antes de que sea autorizado a leer, modificar o eliminar datos.
- El uso de una contraseña ratifica que, quien ha accedido a un sistema es el propietario de la identificación autorizada, a la vez que suministra control sobre el acceso cuando un usuario no autorizado intente acceder al sistema utilizando una identificación válida y una terminal autorizada.
- Se debe evitar el compartir la dupla usuario/contraseña entre varias usuarios relacionados, pues la probabilidad de vulnerar la integridad de la contraseña se ve comprometida. Esta práctica suele ser muy usual en empresas pequeñas, práctica que debe ser desterrada.
- Las contraseñas e identificaciones de usuarios podrían no ser eficaces por sí solos. Muchas veces se guardan en archivos de datos, por lo que, el acceso a estos archivos debe ser restringido mediante una contraseña también.

c. Seguridad sobre claves de acceso

- Los archivos que guardan contraseñas deben ser codificados o protegidos por medio de contraseñas a su vez.
- La responsabilidad por la asignación de las contraseñas debe estar claramente definida.
- No se debe permitir ver los caracteres de las contraseñas en las pantallas de las terminales.
- Las contraseñas deben expirar cada cierto periodo de tiempo, por ejemplo, cada 60 días, para obligar al usuario a que la cambie.
- Las contraseñas, cuando son cortas, se pueden obtener mediante ataques de fuerza bruta o ataques de diccionario, por tanto deben estar formadas por una combinación alfanumérica de por lo menos 8 caracteres para limitar eficazmente las oportunidades de descifrar al azar su contenido.
- Se debe configurar un límite de intentos de inicio de sesión errados, para que, pasado ese número de intentos, se bloquee la cuenta durante un tiempo previamente configurado, para evitar accesos no autorizados.
- Debe prohibirse la reutilización de contraseñas antiguas al cambiarlas.

d. Monitores de Teleproceso

Se requiere de los monitores de teleproceso (TP) [28] para que sea posible la comunicación entre las terminales y el software de aplicación del servidor central. También tienen mecanismos de seguridad, lo que permite la restricción del acceso a las funciones de procesamiento individuales mediante el uso de un sistema de identificación del nombre de usuario/contraseña. El software de TP puede definir:

- Las terminales desde las cuales los usuarios están autorizados a acceder a los programas de un sistema.
- Los usuarios autorizados de cada sistema o programa.
- Las contraseñas que se utilizan para validar la autenticidad de los usuarios.
- Las transacciones que los usuarios están autorizados a realizar.

Cuando se accede a una función, los usuarios podrán acceder a cualquier función de ese programa, pues el TP no puede restringir el acceso a otras funciones de procesamiento dentro de una misma aplicación.

Si el monitor de teleproceso fue implantado de manera apropiada, el acceso y uso de las funciones de procesamiento de una aplicación se restringe solo a los usuarios cuyas contraseñas hayan sido definidas al sistema mediante las correspondientes tablas de autorización de seguridad. Esto quiere decir que, el TP debe trabajar en conjunto con todo el software de sistemas que use la empresa y que sus dispositivos de limitación de acceso no pueden ser invalidados.

e. Software de seguridad

Algunas organizaciones suelen restringir aún más el acceso a las funciones de los programas de aplicación, por lo que suelen combinar un TP con software de seguridad o con rutinas dentro de los sistemas operativos, para proveer un mayor nivel de seguridad, restringiendo así las posibilidades del usuario de acceder a cierto software significativo para las operaciones de la empresa.

El software de seguridad filtra los accesos a un usuario, limitando dicho acceso para actividades no autorizadas, según sean las responsabilidades de trabajo de cada usuario en la organización. Por ejemplo, en un departamento de venta de autos, se les permitirá a los asesores a leer la información necesaria para cumplir con su trabajo, pero no se le permitirá el acceso para realizar modificaciones o eliminar esa información.

Además de la capacidad de controlar el acceso a los archivos de datos, los paquetes de software de seguridad poseen otros eficaces mecanismos de seguridad que pueden ser utilizados para controlar los riesgos del acceso general y monitorear el acceso al sistema de manera tal que se facilite el control y supervisión por parte de la gerencia. Algunos paquetes de seguridad son: RACF (Resource Access Control Facility) [29], de IBM, que es un compendio de reglas de seguridad que se crean en base a clases, controla todo el sistema internamente (procesos, subprocesos, schedulers, dispatchers, el núcleo, etc.), controla los usuarios, el acceso de los usuarios a los datos, el acceso de los mecanismos de acceso a los datos, la interacción de los mecanismos de acceso

con los procesos. O el ACF2 [30], que es un producto de seguridad para entornos z/OS (sistemas operativos IBM para mainframes) y z/VM (sistemas operativos virtuales para un mismo mainframe físico) , incluyendo sistemas operativos UNIX y Linux for zSeries (término colectivo preferido para el sistema operativo Linux compilado para correr en mainframes de IBM), que permite fortalecer la seguridad y agilizar la administración, y brinda capacidades mejoradas de auditoría, para ayudarlo a: administrar eficientemente las identidades de los usuarios y el acceso a los activos, monitorear proactivamente los accesos y reportes, ejecutar políticas de negocio, cumplir con la regulaciones y alcanzar la administración integral de la seguridad.

f. Software de administración de base de datos (DBMS)

Cuando el acceso a las funciones de procesamiento es otorgado a través de terminales, generalmente se utiliza software de administración de base de datos (DBMS) para que el usuario pueda leer, actualizar, agregar o eliminar datos almacenados en una base de datos. El software de administración de bases de datos [31] es la herramienta principal de software del enfoque de la administración de base de datos, dado que controla la creación, el mantenimiento y el uso de la base de datos de una organización y de sus usuarios finales.

El software DBMS contiene tablas de seguridad que son verificadas antes de que se puedan acceder o modificar los registros de datos. El software DBMS puede controlar elementos de datos específicos o "vistas lógicas" de datos. Sin esta particularidad, los datos que se comparten entre las aplicaciones estarían expuestos a ser modificados por un usuario no autorizado.

En este contexto, los controles que pueden restringir el acceso a los sistemas de base de datos para mitigar el riego descrito se listan a continuación:

- Las tentativas de acceso no autorizados al sistema deben ser informados.
- Se deben implantar de manera adecuada los controles de acceso, limitando el tipo de acceso a una o más de las operaciones, tales como leer, actualizar, agregar y eliminar.
- Algunos sistemas de bases de datos admiten el uso de otras medidas de

seguridad tales como protección por contraseñas y registros de los accesos a los datos o al sistema.

- El sistema de base de datos debe controlar todos las solicitudes de lectura, modificación o de eliminación de un campo de datos, en este último caso, se asegura de que, por esta operación no se pierda el acceso a otro campo dependiente de este.
- Los utilitarios de los sistemas de bases de datos, usados para su mantenimiento, deben ser controlados por el administrador de la base de datos, para asegurar de que todo mantenimiento requerido sea bien realizado y autorizado.
- Se debe contar con procedimientos preestablecidos para autorizar el uso del sistema de bases de datos fuera del horario de trabajo.
- Todos los cambios al sistema de bases de datos o a su biblioteca deben ser aprobados y regularizados por el administrador de la base de datos.
- Deben existir procedimientos para que no se pueda acceder a la base de datos a través de medios que no estén bajo el control del software del sistema de base de datos.
- Deben mantenerse archivos de registros de transacciones y de recuperación de la base de datos, separados de la misma, tanto física como lógicamente.
- Deben restringirse y controlarse el uso de los utilitarios de consulta para actualizar la base de datos, con registro del uso y sus resultados.
- Debe limitarse el uso ciertos comandos del lenguaje de manejo de datos, tales como insertar, reemplazar o eliminar.

4.4.2 DATOS INGRESADOS PARA PROCESAMIENTO

El riesgo más común es que los datos de transacciones o los datos fijos ingresados para ser procesados pueden se imprecisos, incompletos o haber sido ingresados más de una vez.

4.4.2.1 Controles de Edición y Validación

En este contexto, el auditor debe conocer los controles más comunes, que son

utilizados para reducir el riesgo asociado.

a. **Controles de formato.** Los controles de formato de datos numéricos, alfabéticos o alfanuméricos, aseguran que tienen una cantidad apropiada de caracteres y una longitud específica, es decir, que no sea muy pequeña para que se pueda ver todo el contenido del campo. Comprobar qué tipo de datos contienen los campos y si estos están dentro del rango permitido de valores, es una condición muy importante para que este tipo de control sea efectivo.

b. **Control de campo faltante.** Los controles de campos faltantes se implementan para asegurar que los campos de datos importantes o sensibles hayan sido completados. No debe ser permitido que estos campos sean omitidos al realizar un proceso relevante. Los controles de combinación se utilizan en forma similar para requerir que se ingresen datos en un campo específico cuando se ingresan datos en campos relacionados o dependientes.

c. **Controles de límite o razonabilidad.** Los controles de límite se implementan para asegurar que los datos se ajustan o que no exceden el procesamiento de una transacción. Los controles de razonabilidad incluyen controles de campo cruzados, por ejemplo, las facturas de proveedores de servicios no se pueden cargar en la cuenta de inventarios. Así también, considera la comprobación automática de tablas, códigos, límites mínimos y máximos o de ciertas condiciones establecidas previamente

d. **Controles de validación.** Los controles de validación aseguran que los datos ingresados sean consistentes con datos fijos en archivos maestros [32]. Por ejemplo, después de pasar por el control de formato de los datos, códigos de proveedores, números de cuenta, se contrastan con registros de los archivos maestros para determinar su validez.

e. **Controles de procesamiento duplicado.** Los controles de procesamiento duplicado identifican los números de documento o lotes que son ingresados para su proceso más de una vez.

f. **Pruebas de correlación o combinación de campos de datos.** Estos controles comparan los datos de diferentes campos para probar su razonabilidad en base a criterios especificados por una aplicación. Por ejemplo, un sistema de roles de pagos puede controlar que no se hagan

pagos por horas extras al personal ejecutivo.

g. **Códigos de integridad de campo.** Estos controles se aplican para verificar la exactitud de los datos durante el proceso de ingreso, incluyéndose también durante su transmisión por las redes.

h. **Controles de balanceo.** Estos controles aseguran que transacciones específicas, tales como cuentas de débitos y créditos en asientos de diario, por ejemplo, se balanceen a cero, para que no se produzcan errores al acumulara esas cuentas.

i. **Dígitos de verificación.** Los dígitos de verificación son un código de integridad de campo muy utilizado. Se trata del uso de un dígito adicional incluido en los campos numéricos. Durante el proceso de validación de datos, se hace un cálculo con los otros dígitos que debe ser igual al dígito de verificación. Este procedimiento se usa generalmente para asegurar el ingreso de números o códigos válidos en los campos correspondientes.

4.4.3 TRANSACCIONES RECHAZADAS Y PARTIDAS EN SUSPENSO

Riesgo: Los datos rechazados y las partidas en suspenso pueden no ser identificados, analizados y corregidos adecuadamente.

Una aplicación bien diseñada controla cada transacción rechazada y mantiene un registro en un archivo separado hasta que esta transacción sea corregida. Este archivo se conoce como archivo en suspenso. Las partidas que contienen errores deben ser incluidas en todos los informes de excepciones posteriores hasta que el grupo de control de datos o el usuario tomen las medidas correctivas que consideren necesarias. Cuando las transacciones rechazadas se reingresan, deben ser sometidas a los mismos controles de edición y validación que se aplican a las transacciones originales.

Cuando los datos se ingresan interactivamente, el usuario que comete el error, es advertido de forma inmediata de que existe una condición de error o excepción, para que sea corregido enseguida. De forma alternativa, la transacción se puede incluir en un archivo en suspenso para su corrección y reprocesamiento posterior, proceso que lo realizará la persona responsable de este proceso.

A continuación, se presentan algunos de los controles más utilizados para mitigar este riesgo y que el auditor deberá tener en cuenta para su estudio de evaluación.

4.4.3.1 Controles programados sobre las partidas en suspenso.

- Se deben implementar controles programados para asegurar la correspondencia de partidas en suspenso con los registros maestros en ciclos posteriores de procesamiento y remoción del archivo de partidas en suspenso de aquellas partidas igualadas.
- Se debe imprimir todos los movimientos, hacia y desde los registros en suspenso, para proporcionar un rastro de auditoría completo.
- Los movimientos iniciados por medios manuales y los generados por el sistema de computación deben ser separados en los archivos y en los listados impresos.
- Se deben realizar análisis regulares de todas las partidas pendientes.
- Se pueden usar programas de consulta para listar todas o parte de las partidas en suspenso.
- La efectividad de estos controles programados dependerá de lo apropiado de los procedimientos de seguimiento del grupo usuario.

4.4.3.2 Controles del usuario sobre partidas en suspenso

- Conciliación del movimiento de partidas en suspenso con los informes de actualización del archivo para cada ciclo de procesamiento.
- Control de todos los ajustes iniciados por los usuarios con documentos de ingreso autorizado.
- Investigación de las excepciones notificadas por el sistema para comprobar si se han tomado las medidas correctivas adecuadas.
- Los documentos usados para asignar, transferir o cancelar partidas en suspenso deben ser sometidos, por lo menos, a los mismos controles aplicables a todos los demás documentos de ingreso.

Estos documentos deben ser correctamente autorizados y controlados por el responsable de cada departamento usuario.

4.4.3.3 Controles del usuario sobre transacciones rechazadas no incluidas en archivos del computador.

En algunos casos, los sistemas rechazan totalmente algunos datos y no guarda ningún registro en un archivo. Cuando esto sucede, el auditor debe evaluar si los procedimientos de seguimiento que el grupo usuario ha realizado, son adecuados. Estos controles, comúnmente aplicados por el grupo usuario sobre las transacciones rechazadas, incluyen los siguientes:

- Mantenimiento de un registro manual de partidas rechazadas y su procesamiento posterior.
- Preparación de los rechazos corregidos, lo que permite asegurar que todos estos sean investigados y corregidos.
- Corrección de los rechazos originados en errores en los documentos fuente, a cargo del departamento usuario de donde proceden, y devolución de los documentos corregidos para su procesamiento, verificando los controles normales de ingreso, incluyendo su autorización.
- Análisis periódicos de rechazos, por relevancia, causa, antigüedad y corte, lo que ayuda a determinar si estos son ocasionados por procedimientos de ingreso no adecuados y a evaluar el impacto de esos errores.
- Procesamiento manual de datos rechazados, como por ejemplo, llenar una factura manualmente. Por lo general, un control de este tipo es ineficiente, pero puede servir cuando los volúmenes de rechazo son bajos. Si se aplica este tipo de control, los archivos de datos deben ser actualizados de inmediato con las transacciones manuales autorizadas apropiadamente.

4.4.4 TRANSACCIONES PROCESADAS E INFORMADAS

Riesgo: Las transacciones reales que han sido ingresadas para su procesamiento o generadas por el sistema pueden perderse, ser procesadas o informadas de manera incompleta o inexacta.

Los medios de control que usualmente se aplican para mitigar este riesgo y que el auditor deberá conocer, se describen a continuación.

4.4.4.1 Controles de Procesamiento por Lotes

Los controles de procesamiento garantizan que los datos que se ingresen, sean procesados en forma exacta y confiable. La recopilación de datos constituye el subsistema significativo de las operaciones generales de un SI. Para reducir al mínimo la pérdida de datos cuando se transportan de un lugar a otro, lo mismo que para comprobar los resultados de diferentes procesos, se preparan totales de control para cada lote de datos [33]. Los controles de procesamiento por lotes que deben estar presentes en un sistema son los siguientes:

- Preparación de totales de lote o totales de control ciegos de los campos considerados críticos. Los totales de control ciegos son totales de control generados mediante la suma de campos numéricos en los lotes de documentos. Si carecen de sentido por sí mismos, estos totales pueden ayudar a identificar errores u omisiones. Un ejemplo es el total matemático de los códigos de cuenta utilizados en un lote de asientos de diario. Si uno o más de los códigos de cuenta son incorrectamente ingresados, el total de los códigos ingresados no coincidirá con el total ciego.
- Preparación y aprobación de formatos de control de lote y formularios de control de envíos, que incluyan totales de control para realizar balances.
- Control numérico de los lotes, que ayuda a detectar lotes no autorizados e identificar lotes faltantes.
- Registro diario de control de información de lotes, mantenido por el departamento usuario, para facilitar el seguimiento de los lotes, cuando estos salen de él.
- Los usuarios deben hacer una conciliación de los totales de control con los totales de salida, para establecer que no se hayan perdido o agregado datos durante el proceso y para asegurar la exactitud del ingreso y procesamiento de datos.
- Los usuarios deben realizar un registro del número de lotes que contiene, registro que sirve como indicador de que los errores frecuentes o recurrentes son una llamada de atención de que no se están siguiendo los procedimientos adecuados.
- Se deben aplicar procesamientos de control para el ingreso en líneas de transacciones individuales, tales como generación por el computador de totales

de control periódicos de los datos ingresados, para su informe y conciliación por los departamentos usuarios.

- Mantenimiento de un registro diario de transacciones, impresión periódica de las transacciones procesadas y comparación con documentos fuente realizada por los departamentos usuarios.

Ocasionalmente, en reemplazo de los controles de lote, pueden aplicarse controles posteriores al procesamiento, los totales de control de salida deben coincidir con los totales de control de entrada. Los procedimientos de control posteriores [34] se establecen como una comprobación final de la precisión e integridad de la información procesada. Estos procedimientos son los siguientes:

- Una inspección inicial, para detectar los errores más obvios.
- La comunicación de los resultados se debe controlar, para asegurarse de que sólo los reciben las personas autorizadas.
- Los totales de control de salida se deben conciliar con los totales de control de entrada, para asegurarse de que no se han perdido ni agregado datos durante el procesamiento o la comunicación.
- Todas las formas fundamentales (cheques de pago, registros de acciones, etc.) se deben numerar previamente y controlar.

A pesar de tomar precauciones, es probable que se filtren algunos errores, por lo que, el punto de control principal para detectarlos es el usuario, así que debe haber un canal de comunicación abierto entre los usuarios y quien(es) realiza el control, para que reporten un error apenas este ocurra, para que se tome la acción necesaria para corregirlos.

4.4.4.2 Controles de Sesión

El software de aplicación es el encargado de realizar los controles de sesión, que han sido diseñados para emular un procedimiento de control por lotes. Los totales de campos críticos, por tipo de transacción, se acumulan automáticamente durante el ingreso de datos y se guardan para poder ser comparados con totales actualizados. Los controles de sesión que se aplican usualmente son los siguientes:

- Se acumulan totales de control separados, por cada terminal y por cada tipo de transacción, a medida que los datos se van ingresando.
- Generación de un registro e informe del total de partidas acumuladas en el archivo de transacciones, al finalizar una jornada de trabajo.
- Actualización de los registros de control del archivo maestro en base al registro de control del archivo de transacciones.
- Una vez actualizado el archivo maestro, se hace una acumulación programada de los registros individuales de este, para conciliación con el registro de control del archivo maestro. Generación de informe de actualización.

4.4.4.3 Controles de etiquetas internas de archivos

Estos controles son mecanismos automáticos de organización, de tareas del software de administración de operaciones y/o software de administración de archivos de datos, que pueden emplearse para asegurar de que se están utilizando las versiones correctas de archivos de datos y programas en producción.

4.4.4.4 Controles de transmisión de datos

Los controles que contribuyen a la exactitud e integridad del proceso de transmisión de datos y que se usan comúnmente, se listan a continuación:

- Los mecanismos estándar del software de comunicaciones generan un dígito de verificación (utilizando un algoritmo previamente establecido) con la información incluida en la transmisión. El resultado de dicho algoritmo es registrado en un segmento del mensaje del encabezamiento previo a la transmisión. El mismo cálculo es realizado nuevamente al recibirse el mensaje y el resultado comparado con la información registrada en el encabezamiento. Si en este proceso anterior se identifican diferencias, la información debe ser retransmitida.
- Registro y recálculo de los dígitos de verificación en los mensajes de encabezamiento.
- Confirmación de partidas individuales o de grupos de partidas ingresadas al sistema que son retransmitidas a las terminales para salida en pantalla o impresión.

- Numeración secuencial de las partidas, realizada por el sistema, con códigos de identificación específicos para cada transacción ingresada desde cada terminal.
- Información de los números de secuencia faltantes o duplicados.
- Utilización de registros de final de transmisión para verificar que todas las partidas hayan sido correctamente transmitidas.

4.4.4.5 Procedimientos de reenganche y recuperación

Cuando ocurre intempestivamente una interrupción del procesamiento, se pueden perder las transacciones que se están procesando en ese momento, evento que es particularmente delicado cuando los datos son ingresados en modo interactivo y en sistemas que utilizan procesamiento de actualización inmediata. Cuando estos sucesos ocurren, generalmente no se dispone de documentos o salidas impresas como respaldo, por lo que es difícil determinar a posteriori si la transacción fue totalmente procesada antes de la interrupción. A continuación se describen los procedimientos de back-up de reenganche y recuperaciones más comunes, que el auditor debe tomar en cuenta para su estudio:

- Se debe mantener un registro diario de transacciones, de tal modo que se facilite la recuperación automática de transacciones parcialmente procesadas.
- Se debe imprimir de forma periódica, según se requiera, registros diarios de transacciones para identificar los pasos de procesamiento que han sido completados para las partidas individuales.

Existen algunos procedimientos para la recuperación de los datos del archivo maestro, en caso de destrucción o pérdida:

- Copiado o vuelco cíclico (dumping) de los archivos maestros a cintas o discos. A intervalos establecidos se copia el contenido de los archivos que han sido creados o modificados desde el vuelco anterior. La frecuencia se puede determinar por el volumen, sensibilidad de los datos, frecuencia de procesamiento, entre otros parámetros.
- Retención de todos los archivos de transacciones y documentos de ingreso posteriores a la copia más reciente del archivo maestro.

- Definición de los períodos de retención para los duplicados de archivos maestros y archivos de transacciones.
- Prueba periódica de los procedimientos de recuperación automáticos.
- Actualización de un duplicado de archivo maestro simultáneamente con el archivo principal.

En los sistemas de base de datos, existen procedimientos adicionales, tales como:

- Mantener un registro de imágenes, antes y después de actualizar los elementos de datos.
- Uso de programas utilitarios para controlar la relación de los indicadores internos de la base de datos u otros vínculos entre los elementos de datos.
- Prevención y/o detección de situaciones de bloqueo [35] durante el procesamiento.
- Se deben mantener registros diarios de transacciones separados físicamente de la base de datos.

4.4.4.6 Controles sobre datos generados automáticamente y cálculos programados

- Recuento de todos los registros leídos en la generación de datos.
- Actualización de archivos y controles de balance para las transacciones generadas.
- Conciliación de los recuentos de registros y actualizaciones de archivos.
- Revisión de la autorización y razonabilidad de las transacciones y cálculos con posterioridad al procesamiento.
- Numeración secuencial de las transacciones generadas.
- Registro diario de transacciones generadas por el sistema (rastro de auditoría).
- Emisión de una copia impresa de los datos generados para su posterior autorización, revisión y conciliación por el usuario.
- Revisión y seguimiento de los informes de excepción significativos.

- Controles sobre los cambios a los datos fijos utilizados para la generación de datos.

CAPÍTULO V

PRUEBAS DE CONTROLES

Cuando se han detectado debilidades en alguna área, y en ellas si se habían implementado controles, no se requiere aplicar muchas pruebas, por lo que el auditor podría sugerir implantar los controles necesarios que corregirían dichas debilidades. Por otra parte, aquellas áreas que aparentan tener controles débiles deben ser sometidas a prueba, ya que, el objetivo de la evaluación de controles es que el control exista, funcione apropiadamente y sea efectivo. Es así, que, por experiencia, el auditor querrá probar un control que, tal vez, no indique una debilidad pero que fue implementado para mitigar un riesgo en particular. Entonces, los controles que se van a probar suelen ser identificados en base al juicio del auditor, en base a la información que recabó en los pasos anteriores. Ciertas pruebas de efectividad del control suelen ser complejas y necesitan de un proceso detallado de planificación y del uso de técnicas de datos de prueba. Generalmente, el proceso no es detallado y se suelen aplicar pruebas más cortas que garanticen suficientemente de que el control es el adecuado y está funcionando apropiadamente. Sin embargo, es recomendable planificar los procesos de prueba, sean estos complejos o no.

Un plan de pruebas de los controles seleccionados debe incluir aspectos tales como el método de prueba que se va a usar, el responsable de aplicar la prueba, decidir cuándo se debe realizar y elegir el proceso de prueba determinado.

Por lo general, las pruebas de los controles se pueden ejecutar de forma estática o dinámica. Una prueba estática consiste en la evaluación de un procedimiento o programa y, dependiendo del objetivo para el que fue diseñado el control, se debe analizar si las instrucciones del programa que implementa el control, alcanzan o no ese objetivo. Una prueba dinámica, en cambio, consiste en la ejecución del control y examinar los resultados. Para un control manual, las transacciones sujetas a ese control deberían ser examinadas. En cambio, en un sistema computarizado, se deben preparar datos de prueba [36].

5.1 PRUEBAS DE CUMPLIMIENTO

Una prueba de cumplimiento es una prueba que reúne evidencia de auditoría para indicar si un control funciona efectivamente y logra sus objetivos [37]. El auditor obtiene evidencia de auditoría mediante pruebas de cumplimiento [38] de:

- Existencia, que el control existe
- Efectividad, que el control está funcionando con eficiencia
- Continuidad, que el control ha estado funcionando durante todo el periodo.

Las pruebas de cumplimiento son aquellas que determinarán la naturaleza, el alcance y oportunidad de los procedimientos de auditoría a aplicar en la información almacenada en el sistema de información. El auditor deberá verificar los siguientes puntos:

- La existencia de una estructura organizativa adecuada, mediante inspección de manuales, perfiles de usuario, entrevistas, entre otras herramientas.
- La existencia escrita y correcta actualización de normas y procedimientos.
- La continuidad del procesamiento (planes de contingencia, políticas de respaldo).
- Los controles del teleprocesamiento (funciones del administrador de red, criptografía).

Los controles en las aplicaciones pueden verificarse a través de medidas de documentación, niveles medios de fallas, calidad de diseño, cantidad de usuarios, complejidad, cantidad de transacciones, modalidades del procesamiento, estabilidad, escalabilidad. Para reflejar estas medidas se podría usar una matriz de riesgo con sus respectivas ponderaciones.

Para llevar a cabo las pruebas de cumplimiento de un sistema puede o no utilizarse una computadora. Las pruebas de cumplimiento, usando una computadora, pueden clasificarse en:

- **Post-operación.-** Si se verifican los controles luego del procesamiento:
  - Puede usarse el sistema real con transacciones reales: se comparan resultados predeterminados con resultados reales
  - Puede usarse el sistema real con transacciones simuladas: en este caso se comparan resultados predeterminados con resultados simulados. La técnica se denomina lote de prueba. Se podrá utilizar el mismo lote para probar todas las

funcionalidades del sistema pero el mismo tendrá que estar actualizado y debe ser pensado de tal forma que represente todas las condiciones de posible ocurrencia

- Puede usarse un sistema simulado construyendo un sistema paralelo al real con las funcionalidades que se desean probar. La técnica se denomina simulación en paralelo y se comparan resultados de transacciones reales en el sistema real con resultados de transacciones reales en el sistema simulado. Este método permite saber si la información resultante del sistema real fue modificada "por el costado" del sistema pero tiene como desventaja que sólo se pueden realizar pruebas parciales y que requiere la suficiente pericia técnica para construir el sistema simulado.

- **En la operación**.- Aplicación de pruebas concurrentes:
  - En el sistema real se ingresan transacciones reales y transacciones simuladas. La técnica se denomina ITF (integrated test facilities o mini compañía).
  - Se generan registros especiales de auditoría dentro de los registros principales del procesamiento (debiendo estar debidamente identificados).

  La técnica sólo es aplicable en organizaciones que cuentan con organismos de supervisión que lo permiten, de otro modo podría ser considerada como fraude.

  Requiere baja pericia técnica y le aporta al auditor el factor sorpresa pero puede tener inconvenientes en su implementación o en su control si las transacciones simuladas no son debidamente identificadas

5.1.1. Segregación de Tareas

El auditor debe tomar en cuenta para la prueba de la segregación de tarea, incluir los siguientes aspectos:

- Realizar un análisis de las responsabilidades asignadas a empleados que son encargados de partes más significativas del procesamiento de información. Así, se determinará si la responsabilidad por la iniciación de las transacciones está apartada de las responsabilidades por la aprobación, procesamiento y registro de ellas. Hay que asegurar que todos los procedimientos realizados para iniciar o ingresar las transacciones para su procesamiento, hayan sido evaluados,

inclusive si hubieren reingresos de transacciones rechazadas.

- Se debe determinar si los usuarios autorizados revisan periódicamente los informes de excepción de transacciones rechazadas y si realmente se toman medidas apropiadas para resolverlas.
- El auditor observará a los empleados en su entorno de trabajo para establecer si están cumpliendo con las responsabilidades asignadas.

5.1.2 Controles de Acceso a los Programas

Las pruebas de códigos de identificación, contraseñas y dispositivos de seguridad de los monitores de teleprocesamiento, software de seguridad y software de DBMS probablemente requieran coordinación con un especialista en auditoría de sistemas. Sin embargo, el auditor podrá utilizar uno o más de los siguientes procedimientos:

- Observar cómo los usuarios acceden al sistema, de tal manera que se confirme su comprensión de los mismos.
- Obtener, revisar y analizar los perfiles de seguridad o tablas de autorización de seguridad del monitor de teleprocesamiento, software de seguridad o software de DBMS. El propósito de esta prueba es determinar si los usuarios no autorizados y aquellos a quienes se hayan asignado funciones incompatibles, están limitados de forma apropiada en su acceso a las funciones de procesamiento del software de aplicación.
- En el caso de sistemas de DB, se puede obtener una copia del diccionario de datos para comparar los perfiles de seguridad, contraseñas, identificaciones de usuario y funciones que los usuarios están autorizados a llevar a cabo, para determinar que sean consistentes. El auditor puede intentar conectarse con el sistema e intentar violar intencionalmente (junto con el personal apropiado del cliente) los niveles de seguridad autorizados y tratar de eludir los dispositivos de seguridad de las terminales. Esta prueba tiene como fin la confirmación de la existencia de los controles de acceso, así como de una mejor comprensión de los mismos. Las violaciones deben ser rastreadas hasta los informes de seguridad, si dichos informes se van a utilizar para propósitos de auditoría.

Cuando se terminan de aplicar las pruebas, el auditor debe estar en condición de determinar si el uso del paquete de software de sistemas es el adecuado y si,

conjuntamente con el sistema de identificaciones/contraseñas, restringe eficazmente el acceso no autorizado a las funciones de procesamiento del software de aplicación.

5.1.3 Pruebas para los Controles de Edición y Validación

En el caso de las pruebas de los controles de edición y validación, el auditor deberá incluir los siguientes pasos:

- Comprobar si las rutinas de procesamiento programadas que contienen los controles de edición y validación funcionan de la manera esperada.
- Determinar que los controles programados que aseguran que las transacciones rechazadas sean identificadas y mantenidas en archivos en suspenso, funcionen de la forma que se espera y que no puedan ser eludidos.
- Establecer si los empleados autorizados de los departamentos usuarios han tomado las medidas adecuadas con respecto a las excepciones o errores incluidos en los listados de errores y transacciones rechazadas, generados por el computador.
- Así mismo, si se considera que las funciones y controles programados son importantes a fines de la evaluación del riesgo o si se estima que son funciones de procesamiento y controles clave, el auditor debe asegurarse de que los controles sobre los programas de aplicación pertinentes también sean adecuados.

A menudo, el uso de transacciones de prueba es el método más directo y eficiente para probar funciones de procesamiento y controles programados. El auditor deberá probar cada función de procesamiento y control programado que sea relevante. Se requieren transacciones de prueba para determinar que las rutinas programadas funcionan de la manera esperada. Sólo es necesario probar cada función una vez, a menos que esa característica del programa sea posteriormente cambiada. Una vez que se confirma la validez de las instrucciones programadas, puede confiarse en el computador procese las transacciones uniformemente.

Pueden desarrollarse otros enfoques distintos de la utilización de transacciones de prueba, para determinar que las transacciones sean adecuadamente procesadas por las rutinas programadas. Por ejemplo, una muestra de transacciones puede ser reprocesada manualmente, para confirmar que las funciones de procesamiento trabajaron adecuadamente para dichas transacciones.

Cuando se utiliza este enfoque, deberán diseñarse otras pruebas para asegurarse de que las transacciones no autorizadas efectivamente no sean aceptadas y de que las transacciones rechazadas o parcialmente procesadas sean adecuadamente aisladas, analizadas y corregidas. Estos factores también deberán ser considerados en el diseño de las transacciones de prueba.

En el caso de que se utilicen transacciones de prueba, deben ser diseñadas de forma tal de determinar que los controles clave realmente existen y asegurar que las transacciones son procesadas en la forma prevista. Las rutinas programadas son probadas mediante el intento de ingreso de datos específicamente seleccionados o preparados para confirmar la existencia de las funciones de procesamiento y controles.

Las transacciones válidas son adecuadamente procesadas a través del software de aplicación y las salidas son representaciones exactas de las transacciones procesadas.

Las transacciones inválidas son rechazadas e incluidas en archivos de ítems en suspenso para su control, así como también en informes de excepciones que deberán ser analizados posteriormente.

Los criterios de edición y validación y otras funciones de procesamiento y controles importantes, existen realmente y funcionan apropiadamente y los informes de excepción son generados cuando se presentan condiciones de excepción.

El desarrollo de transacciones de prueba lo suficientemente amplias para probar controles y funciones de procesamiento programadas requiere bastante tiempo cuando se utiliza esta técnica por primera vez. Sin embargo, en períodos futuros puede lograrse un significativo ahorro de tiempo si el software de aplicación del cliente no es modificado frecuentemente. Se podrá volver a utilizar el mismo conjunto de transacciones en exámenes posteriores, en tanto los programas o la naturaleza de las transacciones ingresadas a la aplicación no se modifiquen.

Alternativamente, puede tomarse como punto de partida el uso de transacciones auténticas elegidas al azar o datos de prueba desarrollados y utilizados por el cliente durante la etapa de prueba del proceso de desarrollo de programas (si así fuera el caso). Así, el tiempo requerido para el desarrollo de las transacciones de prueba puede reducirse. Sin embargo, aún así el auditor deberá evaluar la corrección e integridad de las transacciones de prueba utilizadas para alcanzar los objetivos de la prueba. La selección al azar de transacciones auténticas no proporciona usualmente un lote de

transacciones de prueba que cubra todas las posibles condiciones de error, dado que una selección previa de dichas transacciones predispone el universo hacia aquellas transacciones que serían aceptadas por el sistema.

Los principales tipos de técnicas de transacciones de prueba son la utilización de datos de prueba o lotes de prueba, instalaciones de prueba integradas (ITF) y pruebas on-line.

5.2 DISEÑO DE PRUEBAS DE CUMPLIMIENTO

Esta actividad consiste en diseñar las condiciones que van a permitir la verificación del funcionamiento de un control específico.

El auditor deberá diseñar cada prueba en base a la identificación del objetivo del control que va a ser probado, la condición de la prueba y los resultados esperados. Para que el diseño de las pruebas sea el apropiado, el auditor podría elaborar condiciones de prueba en base a algunas preguntas, tales como: Se rechazan los valores y códigos no autorizados; se aplica consistentemente el control; si el control cubre una gran variedad de condiciones, se deberían probar todas ellas; si el control bajo prueba, está relacionado con otro control, deberían ser evaluados conjuntamente.

El auditor, al seleccionar pruebas de control, puede escoger de entre posibles pruebas que pueden ser realizadas para cada una de las áreas de control, de entre varias alternativas relacionadas con los controles considerados en los capítulos anteriores. Cada una de las pruebas deberá ser aplicada a controles determinados y no a un control no relacionado.

5. 3 REALIZACIÓN DE LAS PRUEBAS DE CUMPLIMIENTO

Se deben preparar las pruebas identificadas y ejecutarlas adecuadamente para alcanzar resultados correctos. El auditor puede realizar, como prueba dinámica:

- Seleccionar la evidencia para verificar el funcionamiento del control.
- Solicitar la evidencia al responsable del control en la entidad
- Evaluar el funcionamiento del control examinando la evidencia seleccionada mediante datos de prueba.

Como prueba estática:

- Identificar el procedimiento a ser seguido para obtener el control deseado
- Crear una o dos transacciones de prueba, típicas o regulares
- Caminar a través del programa para asegurarse que siguiendo el proceso, se obtiene el resultado deseado.

5.4 PRUEBAS SUSTANTIVAS

Después que el auditor ha aplicado las pruebas de cumplimiento, deberá analizar la información almacenada en el sistema informático. Si dicha información se encuentra en soportes informáticos puede ser analizada en su totalidad, pues está disponible y se puede analizar de manera rápida. Caso contrario, si la información no está almacenada digitalmente puede ser muestreada según el diagnóstico hecho sobre los controles.

El objetivo de la fase de pruebas sustantivas es adquirir suficiente evidencia, de tal manera que el auditor pueda tomar una decisión final sobre si han ocurrido pérdidas sustanciales o podrían ocurrir durante el procesamiento. Esta decisión es expresada por los auditores externos en la forma de una opinión.

Generalmente, se sugieren cinco tipos diferentes de pruebas sustantivas para un auditor informático:

- Pruebas de identificación de procesamiento erróneo.
- Pruebas de estudio de calidad de datos.
- Pruebas para comparar datos con las cuentas físicas.
- Pruebas para identificar datos inconsistentes.
- Confirmación de datos con fuentes externas.

La mayoría de estas pruebas requieren un soporte computarizado. Se pueden utilizar Técnicas de Auditoría Computarizada (TAC) para obtener evidencias de auditoría.

5.5 TECNICAS DE AUDITORIA COMPUTARIZADA

La expresión “Técnicas de Auditoría Computarizadas, (TAC)” se utiliza para referirse a todas las técnicas que utilizan computadoras, software y datos de computación para obtener evidencia de auditoría.

Al desarrollar un plan de auditoría, el auditor informático se debe plantear cuestiones tales como:

- ¿Existen oportunidades para usar técnicas computarizadas?
- ¿Cuál es la evidencia de auditoría específica que puede ser obtenida a través del uso de técnicas computarizadas?
- ¿Qué tipo de técnica computarizada debería utilizarse?

Las decisiones de planificación que se tomen respecto a las respuestas, deberán ser documentadas, especialmente en la relación entre las técnicas a ser utilizadas y la evidencia de auditoría que se desea alcanzar.

Las técnicas que se utilizan generalmente son las siguientes:

- Técnicas que utilizan programas de recuperación y análisis de información, conocidas como programas de recuperación y análisis.
- Técnicas que utilizan microcomputadoras.
- Técnicas que utilizan transacciones de prueba.

La elección entre estas técnicas depende primordialmente de la evidencia que se desea obtener. Normalmente, los programas de recuperación y análisis ayudan al auditor informático a obtener evidencia sustantiva, donde lo que se busca es seleccionar datos, calcular montos y obtener totales de archivos. Las técnicas que utilizan microcomputadoras también suelen usarse para obtener evidencia sustantiva, utilizando datos transferidos del sistema central de la empresa a un microcomputador, técnica también conocida como downloading. Las técnicas de transacciones de prueba, generalmente, se utilizan para obtener evidencia de que los controles de aplicación operan en forma efectiva.

El uso de cualquiera de estas técnicas para la obtención de evidencia sustantiva deberá considerar la efectividad de las técnicas disponibles y alternas, en relación con su costo beneficio. En este contexto, deben considerarse las siguientes observaciones, que pueden afectar las decisiones, tales como:

- Software disponible en la empresa u organización.
- La disponibilidad del personal del departamento de TI de la entidad y su capacidad técnica.
- La experiencia y disponibilidad del personal.
- Los controles sobre los sistemas informáticos de la organización.
- La eventualidad de reutilizar los mismos programas en auditorías futuras y otras áreas similares
- Si la organización dispone de programas que requieran modificaciones menores para adaptarse a las necesidades de auditoría.

Con respecto a la relación costo/beneficio de las técnicas disponibles, se deberán seleccionar los procedimientos más efectivos y eficientes para cada organización. Las siguientes recomendaciones podrían ser útiles para una elección apropiada:

- Considerar si es conveniente que el personal de la entidad desarrolle programas utilizando su propio software de recuperación y análisis
- Considerar la relación costo/beneficio de que el personal desarrolle los programas de recuperación y análisis utilizando el software de la entidad o bien paquetes de software de auditoría.

La decisión para escoger entre una u otra técnica estará influida por la necesidad de análisis posteriores de la información. Para propósitos de recuperación de información, informes y utilización de rutinas, el procesamiento a través del computador central puede ser más eficiente. La conveniencia de utilizar downloading puede estar influida por la necesidad de elaborar información, realizar análisis "what if" [39] y procedimientos de revisión analítica que son adecuados para efectuarse en un microcomputador.

La transferencia de los datos de la organización a un microcomputador y el desarrollo de su revisión mediante software, es generalmente la forma más eficiente de obtener evidencia de auditoría. Esta técnica tiene la ventaja de que, una vez que los datos han sido transferidos al microcomputador, se podrán realizar selecciones y cálculos adicionales con facilidad.

Si los datos no pueden ser transferidos, la alternativa más conveniente puede ser la de escribir un programa de recuperación y análisis.

Si la institución no cuenta en su instalación con una conexión micro-computadores/computador central, debe evaluarse cuidadosamente la conveniencia económica (relación costo/beneficio) de su incorporación. La implantación, sin una adecuada planificación previa, puede resultar costosa. Si el ambiente no es propicio, es difícil que se pueda implantar con éxito.

CAPÍTULO VI

APLICACIÓN DEL MODELO COBIT

El marco de trabajo COBIT define las mejores prácticas para la administración del área de Tecnología de la Información. COBIT fue desarrollado por ISACA (Information Systems Audit and Control Association) y el IT Governance Institute (ITGI) en 1992.

La misión [40] de COBIT es “investigar, desarrollar, publicar y promover internacionalmente los objetivos aceptados del control de la tecnología de información para el uso cotidiano de los delegados del negocio y el área de TI”. El marco de trabajo de COBIT entrega la información necesaria a través de una metodología de medidas generalmente aceptadas, así como procesos y mejores prácticas para la aplicación más efectiva de controles en una organización.

COBIT está basado en los Objetivos de Control existentes de la Information Systems Audit and Control Foundation (ISACF), mejorados con los estándares internacionales existentes y emergentes técnicos, profesionales, regulatorios y específicos de la industria. Los Objetivos de Control resultantes, aplicables y aceptados en forma generalizada, han sido desarrollados para ser aplicados a los sistemas de información de toda la empresa.

El término "generalmente aplicables y aceptados" es explícitamente utilizado en el mismo sentido que los Principios Contables Generalmente Aceptados (GAAP). Para los propósitos del proyecto, "buenas prácticas" significan el consenso de los expertos. [41].

COBIT proporciona ventajas a los delegados, usuarios, y a los auditores. Los delegados se benefician de COBIT, porque provee un repositorio de información sobre el cual, las decisiones y las inversiones relacionadas puedan ser evaluadas. La toma de decisión se vuelve más eficaz porque COBIT, ayuda a la Gerencia en la definición de un plan estratégico, definiendo la arquitectura de la información, adquiriendo lo necesario en el área, relacionado el hardware y software, asegurando un servicio continuo y la supervisión del funcionamiento del los sistemas del negocio. Los usuarios se benefician de COBIT, debido al aseguramiento proporcionado en el área de T.I. ya que provee controles de seguridad, y el manejo de procesos definidos por el negocio. COBIT beneficia a los auditores porque además les ayuda a administrar y manejar los activos de la infraestructura. También les da el servicio de corroborar sus resultados de la intervención.

6.1 ESTRUCTURA DE COBIT

El argumento de fondo de COBIT es la orientación hacia los negocios, es así que la forma en que se ha estructurado, es en respuesta a la necesidad de las organizaciones de mantener un sistema de control interno adecuado. La estructura se diseñó pensando en los usuarios y los auditores, pero también para que pueda ser utilizado como un amplio "checklist" para los propietarios del proceso del negocio, pues la amplia competitividad exige un involucramiento y responsabilidad total sobre todos los aspectos del proceso del negocio por parte de los propietarios. Es dentro de este contexto, que la estructura COBIT provee una herramienta para el propietario del proceso del negocio, lo que le permite facilitar el descargo de su responsabilidad.

Los componentes del COBIT son: Un Resumen Ejecutivo (Executive Summary), un Marco Referencial (Framework), Objetivos de Control (Control Objectives), Guías de Auditoría (Audit Guidelines), Conjunto de Herramientas de Implementación (Implementation Tools Set) y un Cd Rom. [42]

- El Resumen Ejecutivo (Executive Sumary) contiene una síntesis ejecutiva que suministra a la alta gerencia entendimiento y conciencia sobre los conceptos clave y principios del COBIT.
- El Marco Referencial (Framework), provee a la alta gerencia un entendimiento más detallado de los conceptos clave y principios del COBIT, e identifica los cuatro dominios de COBIT describiendo en detalle, además, los 34 objetivos de control de alto nivel e identificando los requerimientos de negocio para la información y los recursos de las Tecnologías de la Información que son impactados en forma primaria por cada objetivo de control.
- Los Objetivos de Control (Control Objetives), que contienen declaraciones de los resultados deseados o propósitos a ser alcanzados mediante la implementación de 302 objetivos de control detallados y específicos a través de los 34 procesos de las Tecnologías de la Información.
- Las Guías de Auditoría (Audit Guidelines) contienen los pasos de auditoría correspondientes a cada uno de los 34 objetivos de control de TI de alto nivel para proporcionar asistencia a los auditores de sistemas en la revisión de los procesos de TI con respecto a los 302 objetivos detallados de control recomendados para proporcionar a la gerencia, certeza o unas recomendaciones para mejorar.

- Un Conjunto de Herramientas de Implementación (Implementation Tool Set), el cual proporciona las lecciones aprendidas por organizaciones que han aplicado COBIT rápida y exitosamente en sus ambientes de trabajo. Este conjunto de herramientas de implementación incluye la Síntesis Ejecutiva, proporcionando a la alta gerencia conciencia y entendimiento del COBIT. También incluye una guía de implementación con dos útiles herramientas: Diagnóstico de la Conciencia de la Gerencia y el Diagnóstico de Control de TI, para proporcionar asistencia en el análisis del ambiente de control en TI de una organización. También se incluyen varios casos de estudio que detallan como organizaciones en todo el mundo han implementado COBIT exitosamente. Adicionalmente, se incluyen respuestas a las 25 preguntas mas frecuentes acerca del COBIT, así como varias presentaciones para distintos niveles jerárquicos y audiencias dentro de las organizaciones.
- Un completo CD-ROM en el cual se puede encontrar toda la información detallada en los manuales descritos anteriormente.

En la estructura COBIT se enfatiza el impacto sobre los recursos de Tecnología Informática junto con los requerimientos del negocio que necesitan ser satisfechos, en cuanto a efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. Adicionalmente, la estructura brinda definiciones para los requerimientos del negocio que son destilados de niveles más altos de objetivos para calidad, seguridad e información financiera según se relacionan con Tecnología Informática.

6.2 RESUMEN EJECUTIVO [43]

Para proporcionar la información que la empresa necesita para lograr sus objetivos, los recursos de TI deben ser administrados por un conjunto de procesos agrupados de forma natural. Las decisiones económicas se basan en la información oportuna, relevante y real. Diseñado específicamente para ejecutivos y los encargados, el resumen ejecutivo de COBIT consisten en una descripción ejecutiva que proporcione un conocimiento y entendimiento de los conceptos dominantes y de los principios de COBIT.

Para muchas empresas, la información y la tecnología que las soportan representan sus más valiosos activos, aunque con frecuencia son poco entendidos. Las empresas exitosas reconocen los beneficios de la tecnología de información y la utilizan para impulsar el

valor de sus interesados (stakeholders). Estas empresas también entienden y administran los riesgos asociados, tales como el aumento en requerimientos regulatorios, así como la dependencia crítica de muchos procesos de negocio en TI.

La necesidad del aseguramiento del valor de TI, la administración de los riesgos asociados a TI, así como el incremento de requerimientos para controlar la información, se entienden ahora como elementos clave del Gobierno Corporativo. El valor, el riesgo y el control constituyen la esencia del gobierno de TI.

El gobierno de TI es responsabilidad de los ejecutivos, del consejo de directores y consta de liderazgo, estructuras y procesos organizacionales que garantizan que TI en la empresa sostiene y extiende las estrategias y objetivos organizacionales.

Más aún, el gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que TI en la empresa soporta los objetivos del negocio. De esta manera, el gobierno de TI facilita que la empresa aproveche al máximo su información, maximizando así los beneficios, capitalizando las oportunidades y ganando ventajas competitivas. Estos resultados requieren un marco de referencia para controlar la TI, que se ajuste y sirva como soporte a COSO (Committee Of Sponsoring Organisations Of The Treadway Commission), el marco de referencia de control ampliamente aceptado para gobierno corporativo y para la administración de riesgos, así como a marcos compatibles similares.

Las organizaciones deben satisfacer la calidad, los requerimientos fiduciarios y de seguridad de su información, así como de todos sus activos. La dirección también debe optimizar el uso de los recursos disponibles de TI, incluyendo aplicaciones, información, infraestructura y personas. Para descargar estas responsabilidades, así como para lograr sus objetivos, la dirección debe entender el estatus de su arquitectura empresarial para TI y decidir qué tipo de gobierno y de control debe aplicar.

Las áreas de enfoque del gobierno de TI, son las siguientes:

- **Alineación Estratégica.-** Se enfoca en garantizar la alineación entre los planes del negocio y de TI. Define, mantiene y valida la propuesta de valor de TI y alinea las operaciones de TI con las operaciones de la empresa.

- **Entrega de Valor.**- Se refiere a la ejecución de la propuesta de valor a lo largo de todo el ciclo de entrega, asegurando que TI entregue todos los beneficios prometidos en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de la

TI.

- **Administración de Recursos.**- Se refiere a la inversión óptima, así como la administración apropiada de los recursos críticos de TI, como lo son: aplicaciones, información, infraestructura y personas. Los temas claves tratan acerca de la optimización de conocimiento e infraestructura.

- **Administración de Riesgos.-** Requiere que los altos ejecutivos de la empresa estén concientes de los riesgos, un claro entendimiento acerca del riesgo que tiene la organización, comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos y la inclusión de las responsabilidades de administración de riesgos de la organización.

- **Medición del Desempeño.**- Rastrear y monitorear la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio.

6.3 MARCO REFERENCIAL [44]

COBIT incluye una sinopsis del marco, que proporciona una comprensión más detallada de estos conceptos y principios, mientras que identifica los dominios de COBIT en cuatro áreas: Planeamiento y organización, adquisición e implementación, entrega y soporte, monitoreo. En estas áreas hay 34 objetivos.

COBIT proporciona ventajas a los delegados, usuarios, y a los auditores. Los delegados se benefician de COBIT, porque provee un repositorio de información sobre el cual, las decisiones y las inversiones relacionadas puedan ser evaluadas. La toma de decisión se vuelve más eficaz porque COBIT, ayuda a la Gerencia en la definición de un plan estratégico, definiendo la arquitectura de la información, adquiriendo lo necesario en el área, relacionado el hardware y software, asegurando un servicio continuo y la supervisión del funcionamiento del los sistemas del negocio. Los usuarios se benefician de COBIT, debido al aseguramiento proporcionado en el área de TI. ya que provee controles de seguridad, y el manejo de procesos definidos por el negocio. COBIT beneficia a los auditores porque además les ayuda a administrar y manejar los activos de la infraestructura. También les da el servicio de corroborar sus resultados de la

intervención.

Como respuesta a las necesidades descritas en la sección anterior, el marco de trabajo COBIT se creó como respuesta a las necesidades críticas de la organización, con las características principales de ser orientado a negocios, orientado a procesos, basado en controles e impulsado por mediciones.

- **Orientado al negocio**

  La orientación a negocios es el tema principal de COBIT. Está diseñado para ser utilizado no sólo por proveedores de servicios, usuarios y auditores de TI, sino también como guía integral para la Gerencia y para los dueños de los procesos de negocio.
  El marco de trabajo COBIT se basa en el siguiente principio: Para proporcionar la información que la empresa requiere para lograr sus objetivos, la empresa necesita invertir, administrar y controlar los recursos de TI, usando un conjunto estructurado de procesos que provean los servicios que entregan la información empresarial requerida.

  El marco de trabajo COBIT ofrece herramientas para garantizar la alineación con los requerimientos del negocio.

  Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos más amplios de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

  - La efectividad tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.
  - La eficiencia consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos.
  - La confidencialidad se refiere a la protección de información sensitiva contra revelación no autorizada.
  - La integridad está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.
  - La disponibilidad se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la

protección de los recursos y las capacidades necesarias asociadas.

- El cumplimiento tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.
- La confiabilidad se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.

- **Orientado a Procesos**

COBIT define las actividades de TI en un modelo genérico de procesos, que se encuentra organizado en cuatro dominios: Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y, Monitorear y Evaluar. Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear.

El marco de trabajo de COBIT proporciona un modelo de procesos de referencia y un lenguaje común para que todos en la empresa visualicen y administren las actividades de TI. La incorporación de un modelo operativo y un lenguaje común para todas las partes de un negocio involucradas en TI es uno de los pasos iniciales más importantes hacia un buen gobierno. También brinda un marco de trabajo para la medición y monitoreo del desempeño de TI, comunicándose con los proveedores de servicios e integrando las mejores prácticas de administración. Un modelo de procesos fomenta la propiedad de los procesos, permitiendo que se definan las responsabilidades.

Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Normalmente se ordenan dentro de dominios de responsabilidad de plan, construir, ejecutar y Monitorear. Dentro del marco de COBIT, estos dominios se llaman:

- **Planear y Organizar (PO)**.- Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS).
- **Adquirir e Implementar (AI).-** Proporciona las soluciones y las pasa para convertirlas en servicios.
- **Entregar y Dar Soporte (DS).-** Recibe las soluciones y las hace utilizables por los usuarios finales.

- **Monitorear y Evaluar (ME).-** Monitorear todos los procesos para asegurar que se sigue la dirección provista.

- **Basado en controles**

COBIT define objetivos de control para los 34 procesos, así como para el proceso general y los controles de aplicación. Los procesos requieren controles.

Control se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos.

Los objetivos de control de TI proporcionan un conjunto completo de requerimientos de alto nivel, que la gerencia debe considerar a fin de obtener un control efectivo de cada proceso de TI. Los controles:

- Son sentencias de acciones de gerencia para aumentar el valor o reducir el riesgo
- Consisten en políticas, procedimientos, prácticas y estructuras organizacionales.
- Están diseñadas para proporcionar un aseguramiento razonable de que los objetivos de negocio se conseguirán y que los eventos no deseables se prevendrán, detectarán y corregirán.

La gerencia de la empresa necesita tomar decisiones relativas a estos objetivos de control:

- Seleccionando aquellos aplicables.
- Decidir aquellos que deben implementarse.
- Elegir como implementarlos (frecuencia, extensión, automatización, etc.)
- Aceptar el riesgo de no implementar aquellos que podrían aplicar.

6.4 OBJETIVOS DE CONTROL [45]

La llave a lo productivo se mantiene en un ambiente tecnológico cambiante, es así como el dueño o dueños del negocio mantienen el control. Los objetivos del control de COBIT proporcionan la información crítica necesaria para suministrar una política clara y tener un

control en las prácticas. Así mismo se incluyen las demandas de resultados o los propósitos que se tienen por alcanzar, poniendo los 215 objetivos en ejecución del control a través de los 34 procesos de TI.

Los Objetivos de Control para la Información y la Tecnología relacionada (COBIT) brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones habilitadas por TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien.

Cada uno de los procesos de TI de COBIT tiene un objetivo de control de alto nivel y varios de objetivos de control detallados. Como un todo, representan las características de un proceso bien administrado.

Los objetivos de control detallados se identifican por dos caracteres que representan el dominio (PO, AI, DS y ME) más un número de proceso y un número de objetivo de control. Además de los objetivos de control detallados, cada proceso COBIT tiene requerimientos de control genéricos que se identifican con PCn, que significa Control de Proceso número. Se deben tomar como un todo junto con los objetivos de control del proceso para tener una visión completa de los requerimientos de control.

- **PC1 Metas y Objetivos del Proceso**

  Definir y comunicar procesos, metas y objetivos específicos, medibles, accionables, reales, orientados a resultado y en tiempo (SMARRT) para la ejecución efectiva de cada proceso de TI. Asegurando que están enlazados a las metas de negocio y se soportan por métricas adecuadas.

- **PC2 Propiedad del Proceso**

  Asignar un dueño para cada proceso de TI, y definir claramente los roles y responsabilidades del dueño del proceso. Incluye, por ejemplo, responsabilidad del diseño del proceso, interacción con otros procesos, rendición de cuentas de los resultados finales, medición del desempeño del proceso y la identificación de mejora de las oportunidades.

- **PC3 Proceso Repetible**

  Diseñar y establecer cada proceso clave de TI de tal manera que sea repetible y consecuentemente produzca los resultados esperados. Proveer una secuencia lógica pero flexible y escalable de actividades que lleve a los resultados deseados y que sea lo suficientemente ágil para manejar las excepciones y emergencias. Usar procesos consistentes, cuando sea posible, y ajustarlos sólo cuando no se pueda evitar.

- **PC4 Roles y Responsabilidades**

  Definir las actividades clave y entregables finales del proceso. Asignar y comunicar roles y responsabilidades no ambiguas para la ejecución efectiva y eficiente de las actividades clave y su documentación, así como la rendición de cuentas para los entregables finales del proceso.

- **PC5 Políticas, Planes y Procedimientos**

  Definir y comunicar cómo todas las políticas, planes y procedimientos que dirigen los procesos de TI están documentados, revisados, mantenidos, aprobados, almacenados, comunicados y usados para el entrenamiento. Asignar responsabilidades para cada una de estas actividades y en momentos oportunos, revisar si se ejecutan correctamente. Asegurar que las políticas, planes y procedimientos son accesibles, correctos, entendidos y actualizados

- **PC6 Desempeño del Proceso**

  Identificar un conjunto de métricas que proporcionen visión de las salidas y el desempeño del proceso. Establecer objetivos que se reflejen en las metas del proceso y los indicadores de desempeño de tal manera que permitan el logro de las metas de los procesos. Definir como los datos son obtenidos. Comparar las medidas actuales con los objetivos y tomar las acciones sobre las desviaciones cuando sea necesario. Alinear métricas, objetivos y métodos con el enfoque de monitoreo global del desempeño de TI.

Los controles efectivos reducen el riesgo, aumentan la probabilidad de la entrega de valor y aumentan la eficiencia, debido a que habrá menos errores y un enfoque de administración más consistente.

6.5 DISEÑO DE HERRAMIENTAS Y PLANTILLAS PARA LA APLICACIÓN DE COBIT Y EVALUACIÓN DE CONTROLES [46]

En este apartado, se definirán y diseñarán las herramientas que el auditor deberá utilizar en la evaluación que realizará. Las plantillas estarán disponibles en los anexos presentados al final de este trabajo.

6.5.1 DIAGNÓSTICO PRELIMINAR

En primer lugar, el auditor debe conocer en detalle qué es lo que desea obtener con la evaluación. Debe saber más detalles acerca de los requerimientos del cliente para tener un horizonte definido en cuanto a objetivos y metas que desea alcanzar. Para lograrlo, deberá tener en cuenta los siguientes puntos, con lo que se elaborará la primera plantilla para iniciar la evaluación de los controles (ANEXO 1: [Plantilla DIAGNÓSTICO PRELIMINAR]):

- **Antecedentes generales**: El auditor debe empezar por el nombre de la empresa, su denominación y la actividad en la que está enmarcada.
- **Misión:** Definir el tipo de negocio en el que la compañía está inmersa, exponer el por qué de la existencia de la organización, qué funciones tiene la empresa, para quién las desempeña, de qué forma se desempeñan dichas funciones y el propósito de la organización.
- **Visión:** Cuál es la condición futura de la organización, qué es lo que la empresa desea lograr a un determinado plazo.
- **Objetivos estratégicos:** Cuáles son las metas que quiere alcanzar mediante su actividad.
- **Conocimiento general del área de sistemas:** Si en la empresa hay un departamento especializado para sistemas, el auditor deberá describir el entorno en el que desarrollará su trabajo de evaluación, tal como es el conocimiento de la organización, mediante el análisis del organigrama de esta área y cuáles son los objetivos que el departamento tiene en relación a los sistemas informáticos.
- **Definir un plan estratégico** para la evaluación de los controles, incluyendo el contexto en el que se desempeña la empresa.
- **Definir los objetivos de evaluación**, tanto de los sistemas informáticos disponibles y

de las aplicaciones en uso; objetivos de evaluación de la arquitectura de la información, es decir, la verificación de políticas de seguridad, uso de recursos, instalaciones físicas.

6.5.2 DISEÑO DE CUESTIONARIOS

A continuación, el auditor deberá identificar los objetivos de control de alto nivel necesarios, desde COBIT, específicamente para la evaluación actual en particular.

Se utilizarán cuestionarios, debido a la facilidad de su uso. Se diseñarán preguntas en base los controles a nivel de detalle, lo que facilitará la evaluación de los procesos de control relacionados y el consecuente seguimiento de los pasos dispuestos en la guía propuesta.

Debe aclararse que el auditor deberá tomar en cuenta únicamente los objetivos de control relacionados con esta evaluación en particular.

De acuerdo a COBIT, se dividirá el trabajo en cuatro dominios: Planificación y Organización, Adquisición e Implementación, Entrega de Servicio y de Soporte y, Monitoreo.

En el Anexo No. 2 se encuentra el cuestionario elaborado para el caso práctico realizado en una empresa en particular. En este apartado, se incluirán los objetivos de alto nivel escogidos en base al análisis realizado con los correspondientes vínculos a las plantillas generadas en este caso en particular.

Como es de conocimiento del auditor, cada dominio consta de varios objetivos de alto nivel y de cada dominio, deberá saber seleccionar los más apropiados para cada empresa en particular, siempre acorde al análisis previo que realizará.

DOMINIO: PLANIFICACIÓN Y ORGANIZACIÓN [plantilla DOMINIO: PLANIFICACIÓN Y ORGANIZACIÓN]		
Objetivo de alto nivel	**Descripción**	**Objetivo**
Evaluación de riesgos	Controla el proceso de TI para evaluar los riesgos. Apoya las decisiones de la administración para lograr los objetivos de TI y responder a las amenazas, de tal manera que se reduzca la complejidad, la objetividad creciente e identificando factores importantes de decisión.	Identificación de riesgos y análisis de impactos de TI, que involucran funciones disciplinarias. Permite la toma de medidas de eficiencia de costos para mitigar los riesgos.

DOMINIO: ADQUISICIÓN E IMPLEMENTACIÓN [plantilla DOMINIO: ADQUISICIÓN E IMPLEMENTACIÓN]		
Objetivo de alto nivel	**Descripción**	**Objetivo**
Evaluación para la adquisición y mantenimiento de infraestructura tecnológica	Controla el proceso de TI de Adquisición y Mantenimiento de la Infraestructura de Tecnología, cuyo objetivo de control es mantener las plataformas apropiadas y las aplicaciones comerciales de apoyo.	Asegurar la entrega de información a la organización que se orienta al criterio de información requerido y es medido por los Indicadores Claves de Objetivos, referente a adquisición apropiada de hardware, la normalización en el software, la valoración de hardware, ejecución del software y la administración consistente del sistema.
Evaluación para el desarrollo y mantenimiento de procedimientos de TI	Controla el proceso de TI para desarrollar y mantener procedimientos relacionados con la TI con el objetivo del negocio de asegurar el debido uso de las aplicaciones y de las soluciones tecnológicas establecidas	Enfoque estructurado del desarrollo de manuales de procedimiento de usuario y de operaciones, requerimientos de servicio y materiales de entrenamiento.
Evaluación para la instalación y acreditación de sistemas	Controla el proceso de TI que instala y acredita los sistemas. El objetivo de control es verificar y confirmar que la solución sea apropiada para el propósito planeado.	Asegurar la entrega de información a la organización, orientada al criterio de información requerida. Es medido por los Indicadores Claves de Objetivos, referentes al logro de una instalación bien establecida, movimiento, conversión y plan de aceptación.
Evaluación para la administración de la capacidad y desempeño de TI	Controla el proceso de TI que administra el desempeño y la capacidad con el objetivo del negocio de asegurar que la capacidad adecuada esté disponible y que se haga el mejor y el óptimo uso de ésta para satisfacer las necesidades requeridas de desempeño	Recolección de datos, análisis y reporte sobre el desempeño de los recursos, el dimensionamiento de la aplicación y la demanda de carga de trabajo.

DOMINIO: ENTREGA Y SERVICIO DE SOPORTE [plantillas DOMINIO: ENTREGA DE SERVICIO Y DE SOPORTE]		
Objetivo de alto nivel	**Descripción**	**Objetivo**
Evaluación para la garantía de un servicio continuo	Controla el proceso de TI para asegurar el servicio continuo.	Garantizar que se cuente con los servicios de TI que se requieran y asegurar un impacto mínimo en el negocio en el caso de una interrupción importante. Se consigue el objetivo a través de un plan operativo y de probada continuidad de TI que esté en línea con el plan general de continuidad del negocio y con sus requerimientos de negocio relacionados.
Evaluación para la garantía de la seguridad de los sistemas	Controla el proceso de TI para asegurar la seguridad de los sistemas.	Salvaguardar información contra el uso, revelación o modificación no autorizada, daño o pérdida. A través de verificación de controles de acceso lógico que aseguran que el acceso a los sistemas, datos y programas esté restringido a los usuarios autorizados.
Evaluación para la educación y capacitación de los usuarios	Controla el proceso de TI para educar y entrenar a los usuarios.	Asegurar que los usuarios estén haciendo uso efectivo de la tecnología y que estén concientes de los riesgos y responsabilidades que involucra. Se consigue mediante un extenso plan de entrenamiento y desarrollo.
Evaluación para la asistencia y asesoramiento de los usuarios de TI	Controla el proceso de TI para dar apoyo y asistencia a los clientes de TI. .	Asegurar que cualquier problema experimentado por el usuario sea resuelto apropiadamente. Otorga una opción de ayuda, que proporciona apoyo a usuarios del sistema.
Evaluación para la administración de la configuración	Controla el proceso de TI que administra la configuración. Asegura entrega de información a la organización.	Responder a todos los componentes de TI, previniendo la alteración no autorizada, verificando la existencia física y manteniendo una base para administración confiable de cambio. Se consigue a través de controles que identifican y almacenan todos los Recursos de TI y su situación física, y un programa de comprobación regular que confirma su existencia.

Evaluación para la administración de problemas e incidentes	Controla el proceso de TI para administrar los problemas y los incidentes, cuyo objetivo es asegurar que los problemas y los incidentes sean resueltos y que se investigue la causa para prevenir cualquier recurrencia.	Habilita un sistema de administración de problemas que registra y procesa todos los incidentes.
Evaluación para la administración de datos	Controla el proceso de TI para administrar los datos.	Asegurar que los datos sigan siendo completos, precisos y válidos durante su ingreso, actualización y almacenamiento. Se logra mediante una combinación efectiva de controles de aplicación y generales sobre las operaciones de TI.
Evaluación para la administración de instalaciones	Controla el proceso de la administración de las instalaciones	Proporcionar un entorno físico conveniente que proteja a las personas contra los riesgos artificiales y naturales. Se logra mediante la instalación de controles medioambientales y físicos convenientes que se revisan regularmente para su funcionamiento apropiado.

DOMINIO: MONITOREO [Plantilla DOMINIO: MONITOREO]		
Objetivo de alto nivel	**Descripción**	**Objetivo**
Evaluación para el monitoreo de los procesos	Controla el proceso de TI para monitorear los procesos,	Asegurar el logro de los objetivos de desempeño fijados para los procesos de TI. Se logra mediante la definición de indicadores relevantes de desempeño, el reporte sistemático y oportuno del desempeño y la pronta acción frente a las desviaciones.
Evaluación de la idoneidad del control interno	Controla el proceso para la evaluación adecuada de control interno.	Asegurar el cumplimiento de los logros del control interno. Se obtiene a través del compromiso de supervisar el control interno, evaluando su efectividad, sobre una base regular.

6.5.3 DISEÑO DE PLANTILLAS PARA EVALUACIÓN DE APLICACIONES CRÍTICAS [47]

- **DATOS GENERALES DE LA APLICACIÓN** [PLANTILLA PARA AUDITORÍA A APLICACIONES CRÍTICAS]**:**

  Descripción de aspectos generales de la aplicación, donde constan una descripción de la misma, funciones generales, si tiene módulos se debe hacer una breve descripción de cada uno y, por último, un promedio de usuarios.

  Describir las características del diseño tales como: Arquitectura utilizada en el desarrollo del software, tiempo en producción, lenguaje de programación base, bases de datos (si hubieren) que la aplicación utiliza y marcar si es que el desarrollo es interno, externo, mixto o de terceros.

  Anotar las características de la documentación, tales como: manual de usuario, de instalación y si se dispone de un diccionario de datos (en caso de desarrollo interno o mixto).

  Indicar sobre la existencia o no de un historial o log de errores, incluir en esta plantilla dicha información, si hubiere.

- **EVALUACIÓN DEL NIVEL DE RIESGO DE LAS APLICACIONES**

  Después de que el auditor realiza un reconocimiento general de las aplicaciones sensibles disponibles en la empresa, deberá realizar una evaluación y calificación de riesgo de cada una de ellas. El objetivo principal de este procedimiento es identificar a las aplicaciones críticas y que son prioritarias para el buen desempeño del negocio.

  Esta evaluación se hará basada en la importancia, características, desarrollo y mantenimiento y, extensión y complejidad de la aplicación.

  Los resultados se tabularán de acuerdo a factores de riesgo que serán establecidos en cada plantilla.

- **CALIFICACIÓN DEL NIVEL DE RIESGO DE LA APLICACIÓN** [PLANTILLA PARA LA EVALUACIÓN DEL NIVEL DE RIESGO DE APLICACIONES]

  Después de haber evaluado la aplicación, se debe organizar las aplicaciones en forma ascendente-descendente, empezando por la más crítica o importante. Esta

clasificación se la hará de acuerdo al puntaje tabulado en la parte correspondiente a nivel de riesgos, por lo que las aplicaciones más críticas (las que obtuvieron más alto puntaje) serán evaluadas en primer lugar, lo que asegura una evaluación más minuciosa, en tanto que las que no lo son, pueden ser evaluadas en un tiempo posterior y de manera parcial. Se utilizará una matriz de calificación de riesgos.

- **IDENTIFICACIÓN DE CONTROLES EXISTENTES**

  En base a los riesgos identificados, el auditor debe encontrar los controles actuales aplicados a las aplicaciones, buscando en cada área. Solo se enlistarán los controles existentes al momento de la evaluación más no los controles que debería tener.

  El auditor ya dispone de cuestionarios, realizados en una etapa anterior, lo que facilita el trabajo de identificación. Otras evidencias de la existencia de controles, de ser necesario, puede conseguirlas en base a la observación de los procedimientos, como una tarea adicional.

  Ahora bien, pueden existir muchos controles y haber sido aplicados, pero esto no garantiza su efectividad. Es por esta razón, que el auditor debe aplicar pruebas de cumplimiento para los controles para asegurar si el control realmente existe y si funciona como se espera. Sin embargo, el auditor deberá aplicar dichas pruebas solo para los controles que considere sean importantes y tengan un impacto significativo sobre riesgos, de tal manera que el trabajo sea efectivo y de buena calidad. Hay que aclarar que no es necesario aplicar las pruebas de cumplimiento si el auditor ha conseguido suficiente evidencia del funcionamiento del control en las etapas anteriores.

  Después de la aplicación de esta etapa, el auditor deberá consignar sus datos en la matriz de riesgos y controles [PLANTILLA PARA IDENTIFICACIÓN DE CONTROLES EXISTENTES EN EL ENTORNO FÍSICO Y LÓGICO], lo que facilitará la realización de los informes finales y conclusiones y recomendaciones.

- **REALIZACIÓN DE INFORMES, CONCLUSIONES Y RECOMENDACIONES**

  CARTA DE PRESENTACIÓN O RESUMEN [7.5 INFORME DE EVALUACIÓN DEL CONTROL INTERNO]

  En este documento, el auditor va a hacer un resumen de la evaluación realizada y va dirigida al Gerente de la empresa. Dicho documento debe incluir: naturaleza,

objetivos y alcance de la evaluación de controles; una conclusión general, en donde se abordarán las áreas más débiles así como también se incluirán las observaciones más críticas, ordenadas según su prioridad.

INFORME FINAL [7.6 INFORME FINAL]

En este documento, el auditor deberá incluir los objetivos de la evaluación, el alcance y los aspectos que incidieron de forma negativa en el desarrollo de la evaluación. Hay que destacar que este informe sólo incluirá los hallazgos importantes y que tengan un alto impacto en el desempeño eficiente del negocio, por tanto, dichos hechos deberán ser relevantes, exactos y no repetidos. El informe debe ser redactado de tal manera que sea fácilmente entendido por sí solo y de forma concreta.

En el cuerpo del informe se incluirán los comentarios relevantes que se concluyen basados en el trabajo realizado. Se deben presentar de la siguiente manera:

Observaciones

- **Antecedentes:** Descripción de acontecimientos pasados relevantes para la evaluación actual.
- **Situación actual:** Todos los controles encontrados, cómo están implementados, si funcionan como se esperaba cuando se los diseñó, si se están cumpliendo adecuadamente o no. Se puede incluir una descripción de cómo debería funcionar para poder describir mejor la desviación.
- **Efectos:** Las consecuencias que habrían si se produciera el riesgo.
- **Causas:** El por qué se produce la situación planteada.

Recomendaciones

En un informe final, las recomendaciones deben orientarse hacia una solución a los problemas detectados. El objetivo de dichas recomendaciones es dar una solución adecuada a las deficiencias encontradas. La decisión de implementarlas o no corren a cargo de los directivos de cada organización, ya que no todas ellas podrían ser viables, ya sea porque no existe la logística necesaria o el

presupuesto no es suficiente para llevarlas a cabo.

Anexos

Se puede incluir información adicional, de ser necesario, para complementar el contenido de los hallazgos o presentar resultados del reprocesamiento de datos.

CAPÍTULO VII

APLICACIÓN PRÁCTICA DE LAS GUÍAS DE EVALUACIÓN DE CONTROL INTERNO BASADAS EN COBIT

7.1 DIAGNÓSTICO PRELIMINAR

ANTECEDENTES GENERALES:

Nombre Empresa: HASOFINAD

Actividad: Consultora de auditoría, asesoría gerencial y servicios financieros

MISION

HASOFINAD es una empresa dedicada a proporcionar servicios de auditoría, asesoría gerencial, financiera, administrativa, contable y de recursos humanos, basados en la correcta optimización de sus recursos, de manera personalizada y con excelencia de calidad, para contribuir al desarrollo y éxito de sus clientes.

VISIÓN

Ser una empresa líder al brindar un servicio de la más alta calidad y seriedad a sus clientes.

OBJETIVOS ESTRATÉGICOS

Brindar a los clientes la mejor alternativa, no solamente orientada al cumplimiento de las obligaciones, sino en un efectivo y seguro servicio al cliente.

Establecer relaciones a largo plazo con los clientes, incorporando un equipo humano de trabajo comprometido con las políticas de la empresa.

HASOFINAD CIA. LTDA., debe siempre mantenerse orientada a la satisfacción de las necesidades de los clientes.

CONOCIMIENTO GENERAL DEL ÁREA DE SISTEMAS: Es una empresa dedicada a la asesoría financiera y gerencial, no tiene un área de sistemas.

DEFINICIÓN DE UN PLAN ESTRATÉGICO DE EVALUACIÓN DE CONTROLES

Contexto:

Como principio, la empresa HASOFINAD CIA. LTDA., se desempeña en tres áreas principales de servicios:

- De contabilidad gerencial, procesando información financiera de forma clara, confiable y adecuada.
- De asesoría gerencial, referente a la administración del riesgo de la información, para asesorar a empresas en la administración de riesgos relacionados con el uso de la tecnología de la información, colaborando con la implantación de controles y seguridad.
- De asesoría financiera en tres áreas principales: Finanzas corporativas, servicios transaccionales, recuperación corporativa

La empresa dispone de un computador principal, en donde se guardan los trabajos contables, organizados en hojas de cálculo, los informes de auditoría y los informes gerenciales y financieros por cada una de las empresas cliente. Tienen un software especializado para llevar los estados financieros de las empresas clientes. También cada asesor dispone de su computador portátil en donde guardan igualmente sus trabajos contables e informes, dispuestos de la misma forma que en el computador principal, cada computador sólo contiene el trabajo de cada asesor. Además, se cuenta con otro computador destinado para la secretaria de la empresa. Ahora, el problema radica justamente en que, como cada asesor almacena todo su trabajo, el correspondiente trabajo para pasar toda esta información al computador principal recae sobre éste. Esta forma actual de manejar la información, provoca una pérdida de tiempo y trabajo, sobre todo en lo que se refiere a información contable, lo que provoca, en numerosas ocasiones, errores en la entrada de datos en la computadora principal, duplicación de datos contables, con la consecuente salida equivocada, errores que son difíciles de localizar, pues se tiene que hacer una revisión en dos máquinas, la principal y la que contiene la información de x asesor, lo que trae como consecuencia, el retraso en la entrega de los informes necesarios. Los equipos están conectados en una pequeña red, los dos pc's conectados a través de cables y los portátiles, a través de wi-fi, conectados a través de un router.

En cuanto a hardware, el equipo principal posee procesador Pentium IV a 3.4 Ghz, tarjeta

de red (en el caso del equipo principal) y, además de ésta, puerto para red inalámbrica (en el caso de las portátiles), tiene un disco duro de 160 G, 1 G en RAM (los datos dados son de los componentes principales y que van a estar involucrados en la aplicación principal). En cuanto a software, la plataforma sobre la que se trabaja es el sistema operativo Windows Xp (service pack 2), sin actualizaciones al día y con licencia de operación, solo en el caso de las portátiles. No posee ninguna aplicación para gestión de base de datos.

HASOFINAD tiene un equipamiento acorde a su tamaño y a su ámbito de negocio, pero tiene problemas logísticos debido a la ineficiencia del mal uso de sus recursos. No disponen de políticas de seguridad mínimas y los recursos son mal administrados.

OBJETIVOS DE EVALUACIÓN DE SISTEMAS Y APLICACIONES

- Comprobar existencia de niveles de seguridad de los equipos.
- Comprobar seguridad en aplicaciones en su uso.
- Verificar existencia políticas de acceso y protección de las aplicaciones.
- Verificar si los usuarios tienen correctamente asignado el software correspondiente.
- Analizar operaciones y funciones de la red.
- Analizar existencia de manuales de los sistemas y aplicaciones.

OBJETIVOS DE EVALUACIÓN DE LA ARQUITECTURA DE LA INFORMACIÓN

- Evaluación equipamiento computacional
- Verificar políticas de mantenimiento y características de los equipos.
- Verificar planes de contingencia.
- Verificar políticas de seguridad para todos los equipos disponibles.
- Verificar responsabilidad del uso adecuado de los equipos.
- Verificar políticas en el uso apropiado de las comunicaciones.
- Evaluación de las instalaciones
- Verificar estado, seguridad, distribución de las instalaciones eléctricas.
- Verificar estado en que se encuentra la oficina.

7.2 CUESTIONARIOS DE EVALUACIÓN DE CONTROLES (COBIT Y GUÍA DE EVALUACIÓN DE CONTROLES)

Fecha realización:10 de diciembre de 2009

Auditor: Alexandra Herrera

DOMINIO: PLANIFICACIÓN Y ORGANIZACIÓN

OBJETIVO: Evaluación de riesgos

No.	Ítem	N/A	SI	NO
1.1	Existe un marco de evaluación sistemático de riesgos que se relacione con el logro de los objetivos de la Entidad? Comentarios: no se cuenta con un plan de riesgos.			X
1.2	El enfoque de evaluación de riesgos, comprende el ámbito de aplicación, la metodología de evaluación, las responsabilidades y las habilidades requeridas? Comentarios: no hay evaluación de riesgos	X		
1.3	El enfoque de evaluación está enfocado principalmente a los bienes, las amenazas y los puntos vulnerables? Comentarios:...no hay evaluación de riesgos	X		
1.4	La dirección ha cuantificado y calificado los riesgos a fin de medir el grado de aceptación? Comentarios: han cuantificado pero no han sido expuestos al personal, ni han sido medidos			X
1.5	Existe un plan de acción para mitigar los riesgos? Comentarios: no hay ningún plan establecido			X
1.6	Existe definido un riego residual capaz de compensarlo con la contratación de un seguro? Comentarios:..no han pensado en seguros comerciales			X
1.7	Se ha considerado a los sistemas de control para equilibrar la prevención, la detección, corrección y medidas de control? Comentarios: no lo han considerado, porque piensan que esto es un gasto y sería oneroso para ellos, no han tomado conciencia de este apartado			X

RESULTADOS DE TABULACIÓN DE DATOS: PLANIFICACIÓN Y ORGANIZACIÓN		**2**	**0**	**5**

DOMINIO: ADQUISICIÓN E IMPLEMENTACIÓN

OBJETIVO: Evaluación para la Adquisición y mantenimiento de infraestructura tecnológica

No.	Ítem	N/A	SI	NO
2.1	Se ha implementado procedimientos de evaluación de hardware y software para detectar defectos del sistema? Comentarios: no se disponen de dichos procedimientos			X
2.2	Se ha programado un mantenimiento rutinario del hardware para reducir los riesgos de falla? Comentarios: se da mantenimiento a los equipos dos veces al año, se contratan servicios de terceros		X	
2.3	La configuración y mantenimiento de los parámetros del software se encuentra debidamente protegida? Comentarios: no saben cómo hacerlo ni de qué se trata			X
2.4	El software de sistemas se ha instalado de acuerdo con el marco de adquisición y mantenimiento? Comentarios: no se lo ha hecho			X
2.5	El mantenimiento se efectúa de acuerdo al marco de adquisición y mantenimiento? Comentarios: no, de acuerdo al calendario que la gerencia tiene previsto			X
2.6	Son controlados los cambios del software de acuerdo con los procesos de cambio de la Entidad? Comentarios:...no saben a qué se refiere	X		

Objetivo: Evaluación para el Desarrollo y mantenimiento de procedimientos de TI

No.	Ítem	N/A	SI	NO
3.1	Se han definido con oportunidad los requerimientos operativos y los niveles de servicio futuros? Comentarios: no se han definido			X
3.2	Se prepara y se mantiene actualizado los manuales de procedimientos de los usuarios? Comentarios: no existen manuales de procedimientos de usuario	X		
3.3	Se prepara y se mantiene actualizado los manuales de operaciones? Comentarios:..no hay manuales de operaciones	X		
3.4	Se han desarrollado materiales de capacitación de los sistemas desarrollados? Comentarios: no se desarrollan sistemas, solo se adquieren aplicaciones comerciales	X		

OBJETIVO: Evaluación para la instalación y acreditación de sistemas

No.	Ítem	N/A	SI	NO
4.1	Se ha entrenado debidamente a los usuarios y al personal de acuerdo a un plan definido? Comentarios: en el caso de los sistemas de información, no existe ningún plan de entrenamiento para usuarios	X		
4.2	Se ha establecido optimizar los sistemas previendo los recursos requeridos para operar software nuevo o con cambios importantes? Comentarios: no se ha hablado al respecto			X
4.3	La implementación de los planes, que se relaciona con la preparación del sitio, adquisición e instalación de equipos, entrenamiento a usuarios, se han preparado revisando y aprobando las partes relevantes? Comentarios: no hay planes al respecto	X		

4.4	Ha existido o existe un plan pre-establecido para la conversión de datos de un antiguo sistema? Comentarios: no existe			X
4.5	Existe una constancia por escrito en la que indique que el producto está completo?		X	
	Comentarios: si hay constancia por escrito, después de que instalan algún nuevo software se aseguran del producto			
4.6	Se han revisado los requerimientos del sistema operativo que aseguren las necesidades del usuario? Comentarios: para nada, no saben exactamente qué necesidades tiene cada uno de los usuarios			X

Objetivo: Evaluación para la Administración de la capacidad y desempeño de TI

No.	Ítem	N/A	SI	NO
5.1	Se encuentran identificadas y convertidas en requerimientos y términos de disponibilidad, el desempeño y la disponibilidad de TI? Comentarios: no se ha tomado en cuenta este aspecto	X		
5.2	Existe un plan para obtener, monitorear y controlar la disponibilidad de los servicios de información? Comentarios: no existe			X
5.3	Existe un procedimiento que asegure el monitoreo del desempeño de los recursos de tecnología información y que las excepciones sean reportadas en forma oportuna y completa? Comentarios: no hay procedimientos de este tipo			X
5.4	Existen herramientas apropiadas para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de la configuración, desempeño y disponibilidad de mecanismos de tolerancia de fallas, mecanismos de asignación de recursos y definición de prioridades de tareas? Comentarios: no existen			X

5.5	El proceso establecido, incluye la capacidad de pronóstico que permita que los problemas se solucionen antes de que afecten al sistema? Comentarios: no hay ningún proceso contemplado en este aspecto	X		
5.6	Existen controles que aseguren la preparación de pronósticos de carga de trabajo que permitan identificar tendencias y proporcionar la información necesaria para el plan de capacidad? Comentarios: no saben de que se trata	X		
5.7	Existen procedimientos para la revisión del hardware que asegure una capacidad justificable económicamente para procesar las cargas de trabajo y proporcionar la cantidad y calidad de desempeño requeridos prescritos en los acuerdos de servicio? Comentarios:..no existe ningún procedimiento al respecto, me informaron que, si falla algo en cualquiera de los equipos, llaman a técnicos para que lo reparen, pero no tienen un presupuesto establecido para estas contingencias.			X
5.8	Se ha implementado mecanismos de tolerancia de fallas, de asignación equitativa de recursos y definición de prioridades de tareas a fin de utilizar en forma adecuada la disponibilidad de los recursos? Comentarios: no saben de qué se trata	X		
5.9	Se ha considerado aspectos tales como: contingencia, cargas de trabajo y planes almacenamiento en el aseguramiento de la capacidad requerida? Comentarios: no saben de qué se trata	X		
RESULTADOS DE TABULACIÓN DE DATOS POR DOMINIO: ADQUISICIÓN E IMPLEMENTACIÓN		**11**	**2**	**12**

DOMINIO: ENTREGA DE SERVICIO Y DE SOPORTE

OBJETIVO: Evaluación para la Garantía de un servicio continuo

No.	Ítem	N/A	SI	NO
6.1	Existe un marco de referencia de continuidad que defina los roles, responsabilidades, las reglas y estructura para documentar el plan y los procedimientos? Comentarios: no se ha hablado al respecto dentro de la empresa			X
6.2	El plan de continuidad es consistente con el plan de la entidad y toma en consideración el plan a mediano y largo plazo que asegure su consistencia? Comentarios: no existe plan de continuidad	X		
6.3	Existe un plan escrito que asegure la continuidad de, por lo menos, los servicios básicos? Comentarios: no han realizado ningún plan de continuidad			X
6.4	Existen procedimientos y guías que minimicen los requerimientos de continuidad con respecto a personal, instalaciones, hardware, software, equipo, formatos materiales de consumo y mobiliario? Comentarios:....no existen procedimientos al respecto			X
6.5	Existen procedimientos de control de cambios que aseguren la actualización del plan de continuidad con requerimientos actuales? Comentarios: no saben de qué se trate, no hay plan de continuidad.	X		
6.6	El plan de continuidad es evaluado en forma regular con base a un plan de acción de acuerdo a los resultados reportados? Comentarios: no existe un plan de continuidad	X		
6.7	La metodología de continuidad para desastres, incluye sesiones de entrenamiento regulares? Comentarios:....no existe ninguna metodología relacionada con el punto	X		
6.8	El plan de continuidad está distribuido solo entre el personal autorizado y cuenta con las seguridades respectivas para evitar su divulgación?	X		

	Comentarios: no hay ningún plan de continuidad			
6.9	Cuentan los usuarios con procedimientos alternativos en caso de emergencias o desastres? Comentarios: no hay procedimientos para emergencias	X		
6.10	El plan de continuidad identifica los programas de aplicación, servicio de terceros, sistemas operativos, personal, insumos, archivos críticos así como los tiempos necesarios para la recuperación después de un desastre? Comentarios: no hay ningún plan de continuidad	X		
6.11	La metodología de continuidad, incluye la identificación de alternativas relativas al centro de cómputo y al hardware de respaldo así como una selección de alternativa final?			
6.11.1	Existe un contrato formal para este tipo de servicios? Comentarios: no hay ninguna metodología disponible	X		
6.12	Se han establecido sitios de almacenamiento seguros para las copias de la información, documentos y otros recursos que soporten su recuperación y la continuidad del plan de la organización? Comentarios: se tienen almacenados ciertos documentos y cierta información, pero el sitio no es adecuado ni seguro			X
6.13	Existen establecidos procedimientos para evaluar un plan de continuidad y su actualización, después de un desastre ocurrido? Comentarios: No hay procedimientos ni plan de continuidad	X		

Objetivo: Evaluación para la Garantía de la seguridad de los sistemas

No.	Ítem	N/A	SI	NO
7.1	La seguridad de tecnología de información es administrada considerando los elementos que aseguren una adecuada seguridad? Comentarios: no existe ningún tipo de seguridad al ingreso a los sistemas y su administración	X		

7.2	Se encuentran restringidos el acceso lógico y el uso de los recursos a través de un mecanismo de autenticación de los usuarios y de recursos asociados con las reglas de acceso? Comentarios: no hay reglas de acceso, en cada máquina se tiene una cuenta de usuario sin administrar			X
7.3	Se han considerado la necesidades individuales para visualizar, agregar, modificar o eliminar datos para garantizar el control de la seguridad de acceso? Comentarios:....no han considerado nada al respecto			X
7.4	Se han establecido procedimientos que aseguren acciones oportunas relacionadas con los requerimientos, establecimiento, emisión y suspensión de cuentas de usuario			
7.4.1	Existe un procedimiento formal que indique el propietario de los datos o del sistema que otorga los privilegios de acceso? Comentarios: no saben de qué se trata	X		
7.5	Existe un proceso de control establecido para revisar y confirmar periódicamente los derechos de accesos? Comentarios: no saben de qué se trata	X		
7.6	Controlan los usuarios, en forma sistemática, la actividad de sus propias cuentas			
7.6.1	Existen mecanismos de información que permitan supervisar la actividad normal, así como, alertar sobre actividades inusuales? Comentarios: no suelen controlar sus cuentas, ni centralizados ni individualmente			X
7.7	La administración de seguridad tiene asegurado la actividad de control para que una inminente violación de seguridad sea notificada inmediatamente al administrador y que las acciones subsecuentes sean consideradas en forma automática? Comentarios: no hay administración de seguridad	X		
7.8	Existe una decisión explícita del dueño de los datos para asegurar que todos los datos se encuentren clasificados en términos de sensitividad de acuerdo con un esquema de clasificación? Comentarios: no saben de qué se trata	X		
7.9	Existen controles para asegurar que la identificación y los derechos de acceso de los usuarios estén establecidos y	X		

	administrados de forma única y centralizada? Comentarios: no saben de qué se trata			
7.10	Todas las actividades de seguridad se encuentran reportadas y revisadas apropiadamente en forma regular para identificar actividades no autorizadas? Comentarios: no se realizan actividades de seguridad	X		
7.11	Existe una plataforma centralizada con instalaciones de comunicación rápidas y seguras que manejen los incidentes de seguridad computacional?			
7.11.1	Se han establecido entre los funcionarios, los responsables para el manejo de incidentes, que aseguren una respuesta apropiada, efectiva y oportuna? Comentarios: no se manejan incidentes de seguridad			X
7.12	Se realiza en forma periódica una reacreditación de seguridad, para conservar al día el nivel de seguridad? Comentarios: no conocen acerca del tema	X		
7.13	Dentro de las políticas de la entidad se incluye prácticas de control que permitan verificar la autenticidad de las contrapartes que proporcionan transacciones electrónicas? Comentarios: no se encuentran controles de este tipo			X
7.14	Las políticas de la entidad, aseguran que se instrumenten controles que proporcionen autenticidad a las transacciones? Comentarios: no hay ningún control relacionado en las políticas de la empresa			X
7.15	Las políticas de la entidad, incluyen controles que no permitan que las transacciones pueda ser negadas por ninguna de las partes, por ejemplo a través de firmas digitales y registros de tiempos? Comentarios: no incluyen ningún control de este tipo	X		
7.16	Las políticas de la entidad, aseguran que la información de transacciones confidenciales es enviada por canales seguros? Comentarios: no existen políticas referentes	X		
7.17	El hardware y software relacionado con seguridad, se encuentra permanentemente protegido para asegurar su integridad y evitar la divulgación de claves secretas?			X

	Comentarios: el único software de seguridad del que disponen los equipos es antivirus, pero desactualizado, pues el tiempo de prueba caducó hace mucho tiempo			
7.18	Existe un marco de referencia con adecuadas medidas de control preventivas, detectivas y correctivas para evitar virus computacionales? Comentarios: no existe			X
7.19	Se cuenta con sistemas firewall para conexiones a Internet? Comentarios: no se dispone de firewall, más que el del S.O			X
7.20	Existe protección consistente a la integridad de todas las tarjetas que son utilizadas para autenticación o almacenamiento de información financiera u otra información sensitiva? Comentarios: no se dispone de tarjetas magnéticas para el fin correspondiente	X		

Objetivo: Evaluación para la Educación y capacitación de los usuarios

No.	Ítem	N/A	SI	NO
8.1	Existan procedimientos que permitan identificar y documentar las necesidades de entrenamiento de personal que hace uso de los servicios de información? Comentarios: no hay procedimientos para entrenamiento			X
8.2	Se han definido los grupos, objetivos, entrenadores de las sesiones de entrenamiento de acuerdo a las necesidades establecidas? Comentarios: no existe nada al respecto	X		
8.3	Se encuentra todo el personal capacitado y entrenado en los principios de seguridad de sistemas? Comentarios: no hay principios de seguridad de sistemas, no se les ha hablado respecto a la seguridad	X		

Objetivo: Evaluación para la Asistencia y asesoramiento a los usuarios de TI

No.	Ítem	N/A	SI	NO
9.1	Existe un soporte para usuarios para que interactúen con el personal de manejo de problemas? Comentarios: no hay soporte de usuarios	X		
9.2	Existen procedimientos que aseguren que todas las preguntas de los usuarios sean registradas por el grupo de ayuda? Comentarios: no existe un grupo de ayuda	X		
9.3	Existen niveles adecuados de atención, a las preguntas de los usuarios que pueden resultar complejas? Comentarios: no se receptan preguntas, ni simples ni complejas			X
9.4	Existen procedimientos que permitan monitorear las preguntas planteadas por los usuarios? Comentarios: no existe ningún procedimiento al respecto			X
9.5	Existen procedimientos que aseguren el reporte adecuado de las preguntas de los usuarios y su solución? Comentarios: no hay ninguno			X

Objetivo: Evaluación para la Administración de la configuración

No.	Ítem	N/A	SI	NO
10.1	Existen procedimientos que aseguren el registro único de los elementos de la configuración autorizados e identificables en el inventario al momento de la adquisición? Comentarios: no saben de qué se trata	X		
10.2	Existe una configuración base, de elementos como punto de verificación, que permita regresar después de las modificaciones? Comentarios: no existe			X
10.3	Los procedimientos establecidos aseguran que la existencia y consistencia del registro de la configuración sean revisados en forma periódica? Comentarios:...no saben de qué se trata	X		

10.4	Se revisa en forma periódica la existencia de software no autorizado en las computadoras de la entidad? Comentarios: no se ha hecho ninguna revisión			X
10.5	Se han establecido procedimientos de administración para la configuración, que aseguren los componentes críticos de los recursos de la organización hayan sido propiamente identificados y mantenidos? Comentarios: no existen procedimientos para este punto			X
10.6	Todo el software de la organización se encuentra debidamente etiquetado, inventariado y con las respectivas licencias?. Se han realizado pruebas de auditoría al respecto? Comentarios: no se inventariado ni se han realizado auditorías			X

Objetivo: Evaluación para la Administración de problemas e incidentes

No.	Ítem	N/A	SI	NO
11.1	Se encuentra implementado un sistema de administración de problemas que aseguren el registro, análisis y soluciones de todos los incidentes, problemas o errores?			
11.1.1	Se emiten reportes sobre problemas significativos? Comentarios: no se ha implementado ningún sistema de administración de problemas			X
11.2	Los problemas identificados son resueltos de la forma más oportuna y eficiente? Comentarios: no suelen identificarse problemas relacionados a los sistemas disponibles, se necesitan servicios de terceros cuando se requiere			X
11.3	Las prioridades para los procesos emergentes se encuentran documentados y aprobados debidamente por la administración? Comentarios: no existen procesos emergentes			X

Objetivo: Evaluación para la Administración de datos

No.	Ítem	N/A	SI	NO
12.1	Existen procedimientos de preparación de datos a ser seguidos por los usuarios a fin de minimizar los errores u omisiones?			
12.1.1	Estos procedimientos aseguran que los errores e irregularidades sean detectados, reportados y corregidos? Comentarios: existen procedimientos manuales para este fin		X	
12.2	Existen procedimientos de manejo de errores, de ser así, estos aseguran que los errores y las irregularidades puedan ser detectados, corregidos y reportados? Comentarios:...todo error se detecta mediante trabajo manual y se reporta de la misma forma			X
12.3	Existen procedimientos que aseguren que la entidad pueda retener o reproducir los documentos fuente originales durante un tiempo razonable? Comentarios:....no existen procedimientos para este punto			X
12.4	Existen procedimientos apropiados que aseguren que la entrada de datos es llevada a cabo solo por personal autorizado? Comentarios: no se ha tomado en cuenta este punto			X
12.5	Existen controles suficientes que verifiquen la exactitud, suficiencia y validez de los datos sobre transacciones capturados para su procesamiento? Comentarios: no hay controles automatizados, toda verificación se la hace manualmente			X
12.6	Existen procedimientos para la corrección y reenvío de datos que hayan sido capturados en forma errónea? Comentarios: se lo hace manualmente, antes de ingresar al sistema		X	
12.7	Existen procedimientos para el procesamiento de datos que aseguren una adecuada división de funciones y que el trabajo sea verificado en forma rutinaria? Comentarios: se han determinado procedimientos para división de		X	

	funciones y el trabajo se verifica rutinariamente en forma manual			
12.8	Se encuentran establecidos procedimientos de manejo de errores que permitan la identificación de las transacciones erróneas sin que estas sean aun procesadas y sin interrumpir el procesamiento normal? Comentarios: se verifica manualmente antes de ingresar los datos al sistema		X	
12.9	Existen procedimientos establecidos que permitan el manejo y la retención de los datos de salida de los programas de aplicación? Comentarios: no existen			X
12.10	Existen procedimientos por escrito para comunicar la distribución de datos de salida? Comentarios: existen procedimientos en el reglamento interno para revisión de datos de salida en reportes, se lo hace manualmente		X	
12.11	Existen procedimientos que aseguren la precisión de los reportes de los datos de salida sean revisadas por los usuarios? Comentarios: se lo hace manualmente		X	
12.12	Existe una adecuada protección contra el acceso o modificación no autorizado durante la transmisión y transporte de información sensible? Comentarios: no hay la debida protección en cuanto a este punto			X
12.13	Existen procedimientos establecidos que impidan la divulgación indebida o desecho de información delicada de la entidad? Comentarios: se ha tomado en cuenta este punto dentro del reglamento interno de la empresa		X	
12.14	Existen procedimientos para el almacenamiento de datos que consideren requerimientos de recuperación, economía y políticas de seguridad? Comentarios: no existen procedimientos para documentar requerimientos de seguridad			X

12.15	Se han definido periodos de retención y términos de almacenamiento para documentos, datos, programas, reportes y mensajes de entrada y salida? Comentarios: no existen procedimientos para estas tareas			X
12.16	Existen procedimientos que aseguren un inventario sistemático del contenido de la librería de medios magnéticos? Comentarios: no hay una librería, no hay inventario actualizado		X	
12.17	Se han establecido procedimientos para establecer protección a la librería de medios magnéticos? Comentarios: no existe ningún procedimiento para proteger librerías de medios magnéticos			X
12.18	Se ha establecido una estrategia apropiada de respaldo y restauración que asegure una revisión de los requerimientos de la organización, así como el desarrollo, prueba y documentación del plan de recuperación? Comentarios: no existe un plan de recuperación de sistema ni de datos			X
12.19	Existen procedimientos que aseguren que los respaldos se realicen de acuerdo con la estrategia de respaldos definida y que su utilidad sea verificada regularmente? Comentarios: no aplica, no hay procedimientos para respaldos	X		
12.20	Los procedimientos de respaldo incluyen el almacenamiento apropiado para el archivo de los datos y de la documentación relacionada dentro y fuera de las instalaciones? Comentarios: no hay políticas relacionadas con el respaldo de archivos, me comentaban que, como se guarda la información en cada computadora, siempre hacen una copia en la computadora principal			X
12.21	Se ha implementado una política y procedimientos para asegurar que el archivo cumple con los requerimientos legales y de la entidad y se encuentran protegidos y registrados adecuadamente? Comentarios: no han tomado en cuenta estos requisitos			X

12.22	Se encuentran implementados procedimientos y protocolos que aseguren la integridad, confidencialidad y la no negación de mensajes sensitivos cuando se transmiten datos a través de Internet o una red pública? Comentarios: no hay ningún procedimiento de seguridad			X
12.23	Se verifica la autenticidad e integridad de la información sobre la información electrónica que se origina externamente? Comentarios: no entienden este punto			X
12.24	Existen procedimientos apropiados para que aseguren la integridad y autenticidad para transacciones electrónicas sensibles? Comentarios: no entienden a qué se refiere el punto			X
12.25	Se verifica periódicamente la integridad y lo adecuado de los datos mantenidos en archivos y otros medios magnéticos? Comentarios: no han tomado en cuenta este punto, los medios archivados se encuentran en un lugar inapropiado y no se los revisa periódicamente			X

Objetivo: Evaluación para la Administración de instalaciones

No.	Ítem	N/A	SI	NO
13.1	Se han establecido apropiadas medidas de seguridad física y control de acceso para las instalaciones de acuerdo a las políticas de seguridad, incluyendo dispositivos de información fuera de las instalaciones? Comentarios: no existen políticas acerca de seguridad física, existen ciertas medidas, como mantener la puerta de acceso principal a las instalaciones con candados y ventanas con rejas en el primer piso, pero el lugar en el que se encuentran los equipos no tiene la más mínima seguridad.			X
13.2	Se ha considerado mantener un bajo perfil de las instalaciones relacionadas con TI? Comentarios:...El lugar donde están los equipos se pueden visualizar desde fuera			X

13.3	Se acostumbra acompañar a las personas que no forman parte de la empresa, cuando estas entran a las instalaciones? Comentarios: se ha tomado esta precaución		X	
13.4	Se han establecido y se mantiene las suficientes medidas para la protección contra factores ambientales?			
13.5.1	Existen equipos o dispositivos especializados para monitorear y controlar el ambiente? Comentarios: en Quito no es necesario, pero se recomendaría detectores de incendio en la oficina que alberga los equipos y la información.			X
13.6	Se ha evaluado la necesidad de contar con generadores de luz, para conservar el suministro de energía? Comentarios:..En los dos últimos meses se había considerado este recurso, pero resultaba oneroso			X

RESULTADOS DE TABULACIÓN DE DATOS POR DOMINIO: ENTREGA Y SERVICIO DE SOPORTE	**N/A**	**SI**	**NO**
TOTALES	**26**	**12**	**44**

DOMINIO: MONITOREO

Objetivo: Evaluación para el Monitoreo de los procesos

No.	Ítem	N/A	SI	NO
14.1	Existen definidos indicadores de desempeño que permitan medir las actividades internas y de terceros?			
14.1.1	Se elaboran reportes de desempeño? Comentarios: solo en relación al trabajo de asesoría que prestan, en cuanto al desempeño del sistema, no aplica			X
14.2	Los servicios proporcionados a los usuarios son comparados con los objetivos? Comentarios: no aplica	X		
14.3	Son evaluados los índices de satisfacción de los usuarios o			X

	clientes? Comentarios: la empresa tiene como política la calidad en sus servicios y siempre están atentos a la retroalimentación con sus clientes, en cuanto a usuarios del sistema interno, no se cuenta con la debida retroalimentación.			

Objetivo: Evaluación de la idoneidad del control interno

15.1	En el curso normal de las operaciones, son monitoreadas las actividades de control interno, a través de la supervisión y comparación? Comentario: no hay actividades de control interno en la empresa			X
15.2	Se reporta y se conserva toda la información relacionada con los errores, inconsistencias o excepciones? Comentarios:....Existen ciertos reportes sobre errores, cuando estos han sido informados por el mismo sistema, pero no se los ha tomado en cuenta			X
15.4	Existen auditorías independientes o auto auditorías que garanticen la seguridad operacional y el funcionamiento adecuado de control interno? Comentarios: No hay intenciones de contratar auditorías informáticas			X

RESULTADOS DE TABULACIÓN DE DATOS POR DOMINIO: MONITOREO	**N/A**	**SI**	**NO**
TOTALES	**1**	**0**	**5**

**De acuerdo a la tabulación de datos realizada en este apartado, se realizarán las observaciones y recomendaciones en el Informe Final, dirigido al Gerente de la empresa.

7.3 AUDITORÍA A APLICACIONES CRÍTICAS, CASO PRÁCTICO EN HASOFINAD

DATOS GENERALES DE LA APLICACIÓN

Preparador por: Alexandra Herrera
Fecha: 13 de diciembre de 2009
Nombre de la Aplicación: Software Contable Administrativo Latinium

A. ASPECTOS GENERALES

Breve descripción de la aplicación: El software permite ingresar la información de los clientes, pues se puede crear las bases de datos necesarias para cuantas empresas se necesite, en lo que se refiere a inventario, cuentas por cobrar, cuentas por pagar, emisión automática de estados financieros, además que incluye los anexos transaccionales y formularios 103, 104 del SRI, cálculo de impuesto a la renta, IVA, retenciones. Cuenta también con manejo de nómina, para cálculos de aportes, retenciones y provisiones de sueldos adicionales.

Funciones generales: Permite el ingreso de diferentes tipos de comprobantes de diario así como la creación de otros tipos de comprobantes que se requiera. Se pueden configurar reportes como egresos y cheques, adecuados a la impresión de formatos pre-impresos. Los informes que puede generar son: Diarios, Mayores, Balance General, Balance de Resultados y el Balance de Comprobación, así como la mayorización, que se genera automáticamente a partir de la información ingresada en las cuentas contables. Es posible realizar también conciliaciones bancarias, basada en la información registrada en los asientos. Los asientos pueden ser bloqueados para que no exista ninguna modificación y este proceso puede ser revertido desde la misma pantalla. El sistema admite, mediante perfiles de usuario, la asignación de accesos de distintos usuarios, según sea su requerimiento y autorización. También se puede generar los anexos transaccionales y los formularios 103 y 104 del SRI digitando la información solo una vez. Para el cierre de período, permite guardar copias de toda la información almacenada, por cada cliente, de tal manera que siempre se mantiene siempre un respaldo de todas las transacciones de cada cliente.

Módulos (Opcional): Se trabaja con el módulo de contabilidad, el de nómina (planillas) y el de activos fijos, anexado al primer módulo descrito.

Número promedio de usuarios que utilizan la aplicación: 6 usuarios

B. CARACTERÍSTICAS DE DISEÑO

Arquitectura: Arquitectura modular, desarrollada para trabajar sobre plataformas SQL SERVER 2005 y 2008 y Windows Vista.

Tiempo en producción: 3 años

Lenguaje de desarrollo: lenguaje de programación #C.

Base de datos que utiliza: bases de datos MSDE, SQL SERVER v. 2000, 2005 y 2008.

Desarrollo:

- Interno
- Producto o paquete de terceros **X**
- Externo
- Mixto

C. CARACTERÍSTICAS DE DOCUMENTACIÓN

DOCUMENTACIÓN DISPONIBLE NO DISPONIBLE ACTUALIZADA

Manual de usuario: Si

Manual de instalación: Si

Diccionario de datos: No entregado

D. HISTORIA DE ERRORES

No se ha reportado hasta el momento.

7.4 EVALUACIÓN DEL NIVEL DE RIESGO DE APLICACIONES

Preparador por: Alexandra Herrera

Fecha: 13 de diciembre de 2009

Nombre de la Aplicación: Software Contable Administrativo Latinium

IMPORTANCIA DE LA APLICACIÓN

a. Relación de la aplicación con los objetivos de la empresa	
1. No hay relación.	
2. Baja relación.	**X**
3. Media relación.	
4. Alta relación	

b. Impacto a los usuarios frente a eventuales caídas de la aplicación	
1. No pasa nada.	**X**
2. Opera con varios problemas.	
3. Casi se paraliza	

c. Fraudes históricos	
1. No se han presentado fraudes.	**X**
2. Un fraude	
3. Dos fraudes	
4. Más de dos fraudes.	

1. CARACTERÍSTICAS DE LA APLICACIÓN

1.1. Edad de la aplicación	
1. Aplicación instalada menos de 3 meses	
2. Aplicación instalada menos de 1 año	
3. Aplicación instalada entre 1 y 2 años	**X**
4. Aplicación instalada entre 3 y 5 años	
5. Aplicación instalada hace más de 5 años.	

1.2. Interfases con otras aplicaciones	
1. No tiene interfases	
2. Interfases con un sistema	**X**
3. Interfases con dos o tres sistemas	
4. Interfaces con más de tres sistemas	

1.3. Percepción del usuario sobre la aplicación	
1. Muy Buena.	
2. Buena	**X**
3. Regular	
4. Mala	

1.4. Documentación de la aplicación	
1. Disponible, adecuada y actualizada	
2. Disponible, adecuada y no actualizada	**X**
3. No adecuada	
4. No disponible	

2. DESARROLLO Y MANTENIMIENTO DE LA APLICACIÓN

Si la aplicación es un desarrollo interno o externo:

2.1. Participación en el desarrollo	
1. Usuarios, control de calidad, sistemas	
2. Únicamente usuarios y sistemas	
3. Sólo sistemas	

2.2. Metodología de desarrollo	
1. Existe una metodología de desarrollo formal	
2. Existe una metodología de desarrollo pero no está escrita	
3. No existe una metodología de desarrollo	

2.3. Número de cambios críticos (por errores) Anual	
1. 0 cambios	
2. De 1 a 3 cambios	
3. De 4 a 10 cambios	
4. De 10 a 20 cambios	
5. Más de 20 cambios	

Si la aplicación es un desarrollo de terceros:

2.4. Entrega/recepción de la aplicación	
1. Fue un proceso formal	
2. Se realizó informalmente	**X**
3. No se ha completado	

2.5. Contrato de mantenimiento de la aplicación	
1. Existe un contrato formal para el mantenimiento de la aplicación y se cumple a cabalidad	
2. Existe un contrato pero no se cumple	
3. No existe un contrato pero se realiza mantenimiento según se presente el requerimiento	**X**
4. No existe	

2.6. Número de cambios críticos (por errores) anual	
1. 0 cambios	
2. De 1 a 3 cambios	**X**
3. De 4 a 10 cambios	
4. De 10 a 20 cambios	
5. Más de 20 cambios	

.

|3. EXTENSIÓN Y COMPLEJIDAD DE LA APLICACIÓN

3.1. Empleados que usan la aplicación frente al total de empleados	
1. Hasta un 30%.	
2. Hasta un 60%.	
3. Más del 60%.	**X**

3.2. Volumen de transacciones procesadas en la aplicación frente al total de transacciones de la empresa	
1. Hasta un 30%.	
2. Hasta un 60%.	
3. Más del 60%.	**X**

3.3. Comunicación con sucursales, puntos de venta, clientes o proveedores	
1. Sin conexión	
2. Computador y/o controlador remoto conectado al equipo principal con hasta de 12 terminales (interno)	**X**
3. Conexión con las sucursales, clientes y/o proveedores con más de 12 terminales	

.

3.4. Complejidad de los procesos y cálculos de la aplicación	
1. Procesos y cálculos sencillos	**X**
2. Procesos y cálculos complejos	

7.4 CALIFICACIÓN DEL NIVEL DE RIESGO DE LA APLICACIÓN

MATRIZ DE CALIFICACIÓN DE RIESGOS

Elaborado por: Alexandra Herrera

Revisado por: Alexandra Herrera

Fecha: 15 de diciembre de 2009

Factores de Evaluación	Puntaje
• Relación de la aplicación con los objetivos de la empresa	4
• Impacto a los usuarios frente a eventuales caídas de la aplicación	1
• Fraudes históricos	1
• Edad de la aplicación	2
• Interfases con otras aplicaciones	2
• Percepción del usuario sobre la aplicación	1
• Documentación de la aplicación	2
• Entrega/recepción de la aplicación	2
• Contrato de mantenimiento de la aplicación.	3
• Número de cambios críticos (por errores) anual.	2
• Empleados que usan la aplicación frente al total de empleados.	3
• Volumen de transacciones procesadas en la aplicación frente al total de transacciones de la empresa.	3
• Comunicación con sucursales, puntos de venta, clientes o proveedores.	2
• Complejidad de los procesos y cálculos de la aplicación	1
Total	29

Después de llevar a cabo la observación del sistema en funcionamiento así como las conversaciones mantenidas con el personal (asesores y secretaria), se identificaron los riesgos siguientes (se incluyen también aquellos riesgos que tienen una probabilidad muy baja de suceder, pero que son comunes a todas las organizaciones):

1. Pérdida del suministro eléctrico durante cortos o largos períodos.

2. Catástrofes: terremotos.

3. Incendio en las instalaciones o en el perímetro.
4. Pérdida o robo de computadores portátiles o de escritorio.
5. Suspensión del servicio de banda ancha.
6. Infección por virus.
7. Intrusión en el sistema.
8. Fallos en el software en estudio o en la plataforma que lo soporta.
9. Escalación de privilegios.
10. Fallos en el hardware.
11. Digitación incorrecta al ingresar los datos.

Selección de riesgos críticos:

Escalas: Probabilidad ocurrencia Impacto

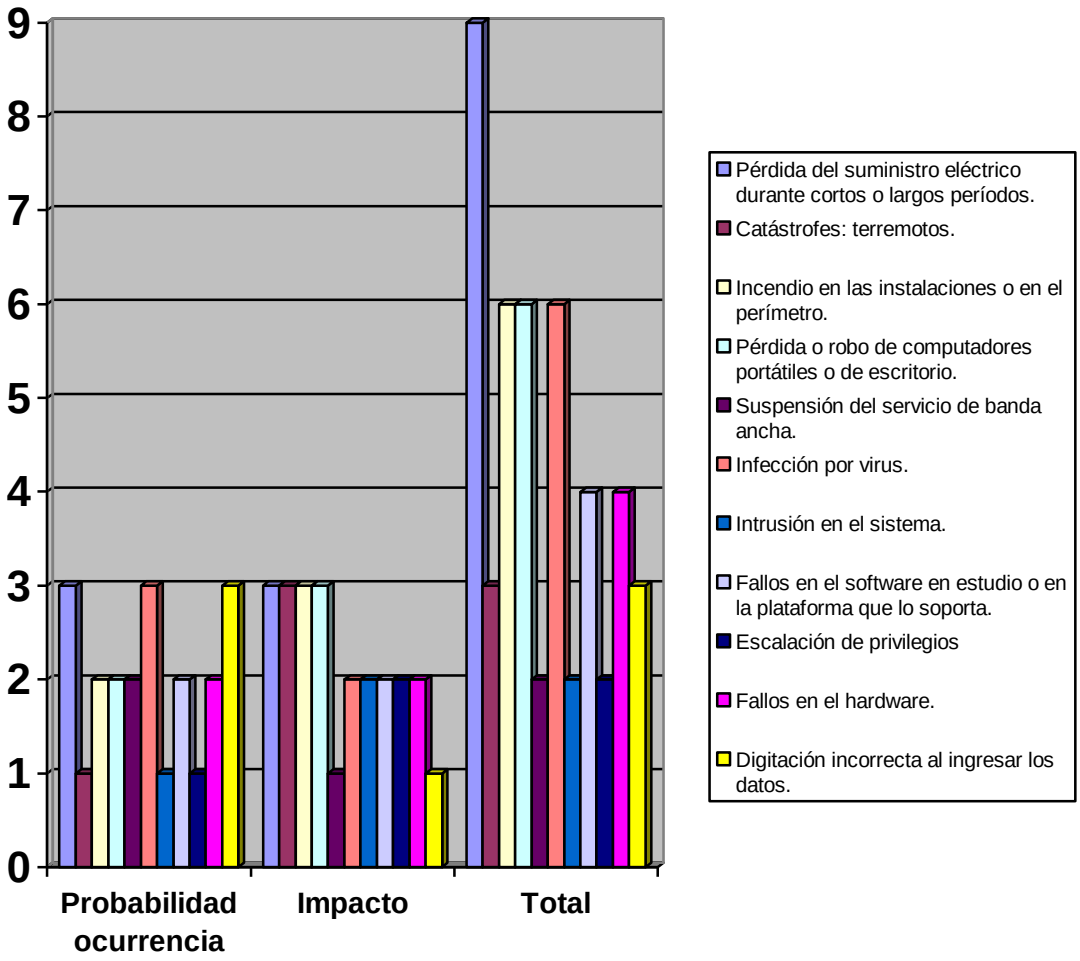
Alto (3) Alto (3)

Media (2) Medio (3)

Baja (1) Bajo (1)

MATRIZ DE CALIFICACIÓN DE RIESGOS **Elaborado por:** Alexandra Herrera **Revisado por:** Alexandra Herrera **Fecha:** 16 de diciembre de 2009			
Riesgos detectados	**Probabilidad ocurrencia**	**Impacto**	**Total**
1. Pérdida del suministro eléctrico durante cortos o largos períodos.	3	3	9
2. Catástrofes: terremotos.	1	3	3
3. Incendio en las instalaciones o en el perímetro.	2	3	6
4. Pérdida o robo de computadores portátiles	2	3	6

o de escritorio.			
5. Suspensión del servicio de banda ancha.	2	1	2
6. Infección por virus.	3	2	6
7. Intrusión en el sistema.	1	2	2
8. Fallos en el software en estudio o en la plataforma que lo soporta.	2	2	4
9. Escalación de privilegios	1	2	2
10. Fallos en el hardware.	2	2	4
11. Digitación incorrecta al ingresar los datos.	3	1	3



De acuerdo a la tabla, los riesgos más críticos, en orden descendente de su calificación final son: Riesgo 1, riesgo 3, riesgo 4, riesgo 6. Los riesgos aceptables serían riesgo 8 y riesgo 10. Los demás riesgos tienen poca probabilidad de ocurrencia, sin embargo, hay que tomarlos en cuenta al realizar planes de contingencia (que compete a los directivos de la empresa y queda fuera del alcance de nuestro trabajo).

Identificación de controles existentes en el entorno físico y lógico de HASOFINAD

Los controles aplicados actualmente en la aplicación en estudio, que han sido identificados como los más críticos y que se tomarán en cuenta para el informe final, se han organizado en la siguiente matriz de riesgos y controles:

MATRIZ DE RIESGOS Y CONTROLES

Aplica a: Entorno lógico, físico y de aplicación crítica
Área: Asesoría
Fecha: 18 de diciembre de 2009
Preparado por: Alexandra Herrera

Riesgos detectados	Control 1	Control 2	Control 3	Total Controles Existentes
1. Pérdida del suministro eléctrico durante cortos o largos períodos.	• Sistemas de alimentación ininterrumpida, UPS.	• Existencia de protectores de sobretensión, tales como regletas de enchufes con interruptor que tenga circuito protector.		1
2. Incendio en las instalaciones o en el perímetro.	• Existencia de detectores de incendio adecuados al negocio. • Contratación actualizada de seguros contra incendios.	• Contar con equipos extinguidores de incendios, cargados y en servicio.	• Existencia de plan de evacuación del personal.	2
3. Pérdida o robo de computadores portátiles o de escritorio.	Seguridad física: • Controles de acceso de personal autorizado a los equipos. • Sistemas de respaldo actualizados, guardados en lugares	• Seguridad física: • Existencia de inventario de todo el equipo informático. • Instalación de detectores de movimiento,	• Controles disuasorios incluidos en forma de cláusulas en los contratos del personal que maneja la información	2

	seguros.	alarmas, rejas de protección en ventanas y puertas. • Uso de cajas fuertes o armarios cerrados con candados, para guardar respaldos actualizados de información.	sensible.	
4. Infección por virus.	• Existencia de precauciones para minimizar la introducción potencial de algún virus • Instalación de programas de detección de virus y protección de red.	• Desactivación para lectura automática de las unidades USB y CD-ROM. • Existencia de directivas para descargas no autorizadas desde Internet.	• Permisos de archivo de sólo lectura. • Instalación de aplicaciones nuevas en una computadora de prueba no conectada a la red.	1
5. Fallos en el software en estudio o en la plataforma que lo soporta.	Copias de seguridad de datos: • Estrategias para obtener copias de seguridad y archivado de la información de los sistemas. • Tipo de medio (cinta, disco o medio óptico). • Tipo de copia de seguridad (completa, incremental y diferencial).	Recuperación de datos: • Frecuencia de prueba de las copias de seguridad.	• Existencia de un plan de continuidad: • Existencia de planes adecuados de recuperación de desastres y continuidad, basados en análisis de riesgos. • Existencia de planes de contingencia.	1

	• Agenda de rotación y archivado (tiempo real, diaria, semanal y mensual). • Existencia de registros de las copias de seguridad.			
6. Fallos en el hardware.	Copias de seguridad de datos: • Estrategias para obtener copias de seguridad y archivado de la información de los sistemas. • Tipo de medio (cinta, disco o medio óptico). • Tipo de copia de seguridad (completa, incremental y diferencial). • Agenda de rotación y archivado (tiempo real, diaria, semanal y mensual). • Existencia de registros de las copias de seguridad.	• Recuperación de datos: Frecuencia de prueba de las copias de seguridad.	• Existencia de un plan de continuidad: • Existencia de planes adecuados de recu-peración de desastres y continuidad, basados en análisis de riesgos. • Existencia de planes de contingencia.	1
TOTAL CONTROLES EXISTENTES	**5**	**3**	**0**	

7.5 INFORME DE EVALUACIÓN DEL CONTROL INTERNO

Ing.

Omar Herrera

Gerente General

HASOFINAD

Fecha: 15 de enero de 2010

Naturaleza de la auditoría

Evaluación de control interno sobre software administrativo, entornos físicos y lógicos de seguridad en uso del mismo y equipos utilizados por el personal.

Objetivos de la evaluación

- Emitir una opinión técnica relacionada con la evaluación de las especificaciones propias de la aplicación.
- Determinar riesgos, causas y efectos que pudieran poner en peligro los datos almacenados en los equipos, desde el software en uso.

Alcance

El alcance del trabajo está referido a la evaluación del control interno, si existe o no algún grado de control sobre el entorno físico y lógico de la empresa.

Importancia del área analizada

El área analizada es el entorno físico de HASOFINAD, los equipos disponibles y la aplicación crítica que se utiliza para la gestión del trabajo realizado por los asesores y secretaria. La importancia de esta aplicación evaluada, además de los entornos físicos y lógicos, radica en que esta aplicación se usa para ingresar los datos de las empresas que están siendo auditadas o evaluadas por los asesores, por tanto, es información sensible y crítica, de la que depende el éxito de los informes y balances finales.

Conclusión general

De la evaluación realizada a los controles disponibles para el uso adecuado del sistema estudiado, se desprende que existen riesgos detectados que no han sido cubiertos por el personal ni directivos de la empresa, por lo que se concluye que los datos críticos se encuentran actualmente en riesgo, pudiendo perderse sin recuperación exitosa en cualquier momento, debido a un mal uso o a un fallo crítico.

Observaciones críticas

De la evaluación realizada, se desprenden las siguientes observaciones, en cuanto a seguridad física y lógica se requiere:

- Falta de información sobre los requerimientos mínimos de seguridad de aplicaciones, de equipos, de datos y del entorno físico en general.
- No se contempla aspectos referentes a planes de contingencia.
- Falta de prevenciones para evitar pérdida de información.
- No se tienen estrategias claras para el resguardo de la información ni para la recuperación efectiva en caso de fallos de cualquier tipo.

Los aspectos mencionado podrían ocasionar que la información se pierda en cualquier momento, como efecto de un mal manejo de los equipos o fallas de hardware, software o eléctricas, lo que conllevaría a gastos onerosos y tiempo perdido, con la consiguiente pérdida de la confianza de los clientes, por retrasos en la entrega de trabajos.

Alexandra Herrera Ortiz

AUDITOR

7.6 INFORME FINAL

SEÑOR GERENTE HASOFINAD CIA. LTDA.

INFORMA:

REF: EVALUACIÓN DE CONTROL INTERNO

1. ANTECEDENTES

Mediante comunicación dirigida al Gerente de la empresa de servicios de asesoría financiera HASOFINAD, de fecha 08 de diciembre de 2009, se solicita la autorización para la evaluación del control interno en el entorno lógico, físico y de aplicaciones, respuesta obtenida el 9 de diciembre de 2009, para el inicio de dicha evaluación desde el 10 de diciembre de 2009.

2. OBJETIVOS

- Obtener evidencias sobre riesgos detectados sobre el uso de equipos, entorno y software administrativo.
- Emitir una opinión relacionada con la evaluación de las especificaciones de seguridad y operación de equipos, software, así como recomendaciones prácticas para el buen funcionamiento de dichos ítems en uso.

3. ALCANCE

El alcance del trabajo está referido a la evaluación del software administrativo Latinium, utilizado por el personal de la empresa (asesores, secretaria), para el ingreso de datos de empresas que utilizan sus servicios profesionales, así como los equipos que se utilizan para dicho fin:

DETALLE	EXISTENCIA (unidades)
Computadores Personales	2
Computador Portátil	4
Software crítico	1
Licencias de uso	6

EQUIPOS DISPONIBLES	ASPECTOS TÉCNICOS
PC 1	PIV, 3.4 GHz, disco 250 g ide, ram 500 mb, S.O. Windows XP professional
PC 2	Iguales características de PC1
Computadores Portátiles	PIV 1.6 GHz, disco 160 g, ram 1 g, S.O. Windows XP basic
Software crítico	Latinium para procesos contables
Licencias de uso	4 licencias para software S.O. en portátiles, ninguna licencia para PC's

4. LIMITACIONES

Respecto a la colaboración del personal, no hubo novedades.

Respecto a facilidades brindadas, no se encontraron novedades.

Limitación encontrada en cuanto a fechas disponibles en la investigación, pues se realizó en días cercanos a festividades de navidad y fin de año y por actividades del personal, referentes al trabajo de cierres de balances en las empresas clientes, por lo que se retrasó la entrega del informe final hacia la tercera semana laborable del mes de enero.

5. CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Después de haber realizado los análisis correspondientes, en cuanto a la información obtenida durante el trabajo de evaluación, se llegó a la conclusión de que los controles existentes son mínimos. La seguridad de la información se podría ver afectada en cualquier momento, sin capacidad de recuperación. En cuanto al entorno, se puede decir que los equipos se encuentran en un ambiente inseguro, sin mucha protección en cuanto a ciertos riesgos tales como incendio, robo o una simple falla eléctrica podría poner en peligro la continuidad del negocio.

OBSERVACIONES Y RECOMENDACIONES

a. Observación:

Falta de información sobre los requerimientos mínimos de seguridad de equipos y aplicaciones.

- **Situación Actual:** El personal desconoce, en general, las formas más adecuadas para mantener la seguridad de equipos y de los datos ingresados.
- **Efectos:** Los riesgos detectados, de ocurrir, pudieran derivar en pérdida o deterioro de la información almacenada en los equipos principales y de los asesores, con la consiguiente pérdida de tiempo y dinero, así como retrasos en entrega de informes a los clientes de la empresa.
- **Causas:** El poco conocimiento acerca de riesgos por parte del personal, es por falta de capacitación de los asesores y demás personal, así como desconocimiento mínimo de estrategias y controles que debieran ser aplicados desde la gerencia.

Recomendación:

Se recomienda la elaboración de un manual de procedimientos mínimos para resguardo de equipos y software, a cada uno de los empleados, así como una charla sobre elaboración de planes de contingencia.

b. Observación:

No se contempla aspectos referentes a planes de contingencia.

- **Situación actual:** La gerencia no ha trabajado en planes de contingencia con su personal, en el caso de que sucedieran eventos que pudieran poner en riesgo sus bases de datos de clientes. El personal no cuenta con las herramientas necesarias para implementar sistemas de respaldo de la información, que realmente funcionen adecuadamente cuando se necesite restaurar información que se perdiera en el caso de que sucediera un imprevisto.
- **Efectos:** Si sucedieran eventos que derivaran en pérdida de datos de clientes, sería muy difícil recuperarlos y de hacerlo, los costos van a ser altos para la empresa.
- **Causas:** No han existido reuniones entre la gerencia y el personal para elaborar estrategias para enfrentar los riesgos existentes.

Recomendación:

El personal, junto con la gerencia, debe reunirse para encontrar ideas que puedan servir como base para la elaboración de un plan de contingencias, que deberá ser analizado y actualizado, por lo menos, una vez cada seis meses.

c. Observación:

Falta de prevenciones para evitar pérdida de información.

- **Situación actual:** Los equipos no cuentan con las seguridades necesarias para brindar un acceso autorizado y limitado a las aplicaciones y datos contenidos en ellos. El software en análisis tampoco ha sido configurado para permitir sólo el acceso necesario a cada uno de los asesores, así como tampoco para la secretaria ni el gerente.
- **Efectos:** De suceder accesos con exceso de privilegios, la información crítica, en el caso de el software en estudio, pudiera derivar en cambios en los asientos de ingresos o egresos, que no coincidirían con los comprobantes archivados en papel, por lo que pudieran ocurrir errores críticos al emitirse automáticamente los estados financieros de cualquiera de sus clientes, lo que pudiera derivar en perjuicios civiles y hasta penales a nivel del fisco para los clientes que resultaren afectados por cambios en los datos.
- **Causas:** El exceso de confianza en los empleados puede resultar en perjuicios para el buen nombre de la empresa.

Recomendación:

Se recomienda la configuración de los equipos para brindar sólo el acceso necesario a cada miembro de la empresa, según sea su actividad, así como la configuración adecuada dentro del software administrativo, para evitar abusos de privilegios, modificaciones indeseadas y hasta errores cometidos por el personal.

d. Observación:

No se tienen estrategias claras para el resguardo de la información ni para la recuperación efectiva en caso de fallos de cualquier tipo.

- **Situación actual:** El personal no tiene por costumbre hacer respaldos continuos de la información, ni se ha contratado servicios especializados para hacerlo. Los respaldos suele hacerlos la secretaria, pero en periodos de seis meses, aproximadamente. Los respaldos no se actualizan con frecuencia y los discos en que se guarda esta información no se encuentran en un lugar seguro.
- **Efectos:** En el caso de que hubiera, por ejemplo, una alteración en el voltaje con subida y bajada del mismo en un corto instante de tiempo, que en nuestro país es bastante frecuente y común, generalmente los más afectados suelen ser los discos duros, con la consiguiente pérdida de la información. Existen herramientas adecuadas para la recuperación de datos, pero estos servicios suelen ser caros, lo que derivaría en gastos adicionales, fuera de presupuesto, y en pérdida de un tiempo valioso.
- **Causas:** No existe la concientización del personal ni de la gerencia, en lo referente al establecimiento de estrategias y acciones de respaldo, así como el desconocimiento de las herramientas que proporciona el mismo sistema operativo para la restauración de datos o de configuraciones.

Recomendación:

Se recomienda capacitar a los empleados para que aprendan a realizar respaldos y actualizaciones de la información, que el software en estudio tiene disponible las herramientas necesarias para hacerlo, así como también sobre las herramientas que tiene el sistema operativo para resguardar y recuperar información y configuraciones. La gerencia debe establecer estrategias claras sobre respaldos y recuperaciones en caso de incidentes, así

como, junto con el personal, dar ideas sobre acciones que se pudieran realizar en caso de eventos indeseables. Se recomienda contratar con personal capacitado para dictar las charlas al personal, lo que representaría una salvaguarda segura del activo más importante para la empresa: la información.

e. Observación:

No existen controles mínimos para el acceso a los equipos ni a la aplicación más importante que tiene la empresa. Tampoco hay un control acerca del software que se instala en los equipos, ni verificación de licencias así como tampoco se dispone de software de seguridad actualizado.

- **Situación actual:** Los equipos se acceden fácilmente mediante nombres comunes de usuarios, por ejemplo, si el asesor se llama Jaime, ese es su nombre de usuario y la contraseña que usan es numérica continua, por ejemplo, 12345678, por lo que cualquier empleado puede iniciar sesión en cualquiera de los equipos. En el caso de dos portátiles, se encontraron programas de compartición de archivos en línea, como el Kazaa, instalación de mensajería instantánea, carpetas con descargas de música, videos y otros archivos de uso personal. Referente a todos los equipos, se encontraban con una versión de Norton Antivirus con licencia gratuita expirada, por lo que no se realizan actualizaciones de las bases desde hace, aproximadamente, 1 año, por lo que los equipos se encuentran vulnerables, en el caso de 4 computadores se encontraron virus ingresados desde dispositivos de memoria removibles.
- **Efectos:** Se consigue entrar fácilmente en cualquier equipo y cada uno tiene su asesor responsable, si otra persona ingresa, puede acceder rápidamente y sin ninguna restricción a todos los archivos que se guardan, lo que pudiera resultar peligroso si se consigue información considerada como crítica y restringida de los clientes de cada asesor, pues pudiera ser utilizada con fines ilícitos. En el caso de la instalación de programas que no son necesarios para desempeñar el trabajo rutinario de cada asesor, se pudieran agregar aplicaciones conseguidas en línea que pudieran contener virus o espías, con el consiguiente riesgo de robo de información o daño de aplicaciones sensibles o útiles, así como daño de archivos por la acción de virus, pudiendo hasta perder la información almacenada durante mucho tiempo. Así mismo

con ninguna protección de un software de seguridad como lo es el antivirus, sería un equipo vulnerable a ataques de cualquier tipo.

- **Causas:** No se han tomado en cuenta restricciones mínimas de acceso, de administración de cuentas y aplicaciones ni se ha concientizado en la importancia de contar, por lo menos, con una protección adecuada de antivirus. Generalmente, se piensa que eso deriva en un gasto extra para la administración, no logran entender que la información es un activo importante para el buen funcionamiento de un negocio y que es válido hacer una inversión en software de seguridad.

Recomendación:

Se recomienda una reunión del personal y administración para definir acciones sobre protección de cuentas de acceso, así como de contemplar la posibilidad de adquirir software antivirus con licencia, para todos los equipos y una charla para concienciar al personal acerca de la importancia de mantener una adecuada seguridad en los equipos y su entorno, para conservar la integridad y disponibilidad de la información almacenada en ellos.

ALEXANDRA HERRERA

7.7 REUNIÓN DE CIERRE

Fecha: 15 de enero de 2010

En presencia del Gerente de HASOFINAD, la secretaria y 4 de los asesores, se llevó a cabo la presentación del informe final. Se presentaron las observaciones hechas después de llevar a cabo la evaluación de los controles. Se discutió acerca de todas las brechas de seguridad existentes en el funcionamiento dentro del ambiente informático. Se tuvo una buena acogida por parte de los funcionarios, que estuvieron atentos a las recomendaciones que se les hizo. Hubo buena disposición por parte del Gerente, quién aceptó las recomendaciones, mas no así con la implementación de todas ellas, pues comentó que no se dispone de un presupuesto adecuado para poner en marcha todas las recomendaciones hechas, sin embargo, se aceptaron las referentes al refuerzo de la seguridad en la aplicación más importante y relevante para el tipo de negocio que llevan a cabo. También se pondría énfasis en aquellas dedicadas a la seguridad de la información y todo lo relacionado con el cuidado de guardar copias de seguridad en lugares adecuados. De tal manera, que quedó el compromiso de implementarlas lo más pronto posible, poniendo como fecha límite el 28 de febrero de 2010 para empezar a realizar este trabajo. Se agradeció por el trabajo realizado y se puso fin a la reunión.

HASOFINAD
Calle de la Begonias # 91
Urb. La Primavera
QUITO - ECUADOR

Consultoría, Informática y Auditoría

Teléfonos: 1700HASOFINAD
093146799

Quito, 26 de febrero del 2010

Srta.
Alexandra Herrera
AUDITORA
Presente

Por medio del presente quiero agradecer a usted el trabajo realizado en la Firma de mi representación, relacionado con la Evaluación del Sistema de Control Informático de HASOFINAD.

Los resultados de la evaluación practicada, así como, sus recomendaciones, serán tomados muy en cuenta en el desarrollo de nuestras actividades, para fortalecer los controles y seguridades determinados con algún grado de riesgo e identificados durante su examen.

Atentamente,

Ing. Marco Herrera Balarezo
PRESIDENTE DE HASOFINAD

CAPÍTULO VIII

SEGUIMIENTO DE RECOMENDACIONES

Las recomendaciones son acciones correctivas que se presentaron en el informe de evaluación realizado, en informes de auditoría o en informes especiales de carácter preventivo, como producto de las deficiencias encontradas en la evaluación del control interno y son dirigidas a las autoridades competentes que tienen la facultad de implementarlas.

Las recomendaciones realizadas en el informe, dirigidas al Gerente de la empresa en estudio, hasta la fecha no han sido consideradas en su totalidad. Se permitió únicamente realizar cambios de contraseñas para el acceso a cuentas de usuario en cada máquina, se realizó la desinstalación del software antivirus, porque no quisieron adquirir las licencias y se instaló en cada máquina un software antivirus gratuito, Avast v.4.8, edición personal, con sus respectivas actualizaciones en línea así como la configuración para actualizaciones diarias. También se permitió la instalación de software cortafuegos, Zone Alarm, pero sólo en los dos PC's, no así en las portátiles. Se tomaron precauciones en cuanto al almacenamiento de archivos en medios magnéticos así como se permitió inventariar los medios disponibles. Se activó la restauración del sistema, disponible en las herramientas del mismo sistema operativo en todas las máquinas y se dictó una charla acerca de la importancia de hacer respaldos periódicos de la información almacenada en cada máquina. También se hicieron las correcciones debidas al acceso y restricción en el mismo, según sean las funciones y responsabilidades de cada persona que trabaja en la empresa, así como asignación de nombres de usuario y contraseñas más seguras, que se almacenaron en un archivo digital que fue entregado al Gerente. Así mismo, aceptaron realizar cambios periódicos en las contraseñas, tanto de las cuentas de acceso al S.O. así como en el acceso a la aplicación más importante que tienen, que serán asignadas por el Gerente, cada 3 meses. Por lo demás, se me hizo saber que no tienen presupuesto suficiente como para poner en práctica todas las recomendaciones, sin embargo, por lo menos, se han tomado medidas básicas y se me informó que, en poco tiempo, se van a reunir, el personal con el Gerente más un asesor, para elaborar planes de contingencia en cuanto al entorno físico, lógico y de datos.

CAPÍTULO IX

CONCLUSIONES Y RECOMENDACIONES

9.1 CONCLUSIONES

Después de haber finalizado esta investigación, se desprenden las siguientes acotaciones:

- Para empresas pequeñas, como por ejemplo HASOFINAD, los controles existentes son muy escuetos o a lo mucho, existen en su más básica forma o simplemente, no existen, esto debido a que la Gerencia desconoce, en muchos casos las estrategias mínimas y controles efectivos a ser implementados en un ambiente informatizado o porque, no tienen conciencia de que los riesgos a los que se ven abocados los sistemas informáticos, podrían afectar la continuidad del negocio.
- La evaluación periódica de controles asociados a los procesos de una organización permiten identificar en etapas tempranas de los mismos las vulnerabilidades a las que pueden ser expuestos, ayudando a la Gerencia a identificar mecanismos de solución viables y al menos con una visión previa del análisis del costo/beneficio de adoptarlo.
- Las estrategias clave para realizar una evaluación de control interno son:
  - Una observación rigurosa de los procedimientos rutinarios en los que se desenvuelve el personal cotidianamente y para conocer más a fondo el estado actual de las actividades en el ambiente informático, así como aquéllas relacionadas con el ámbito del negocio.
  - Realizar un listado de los requerimientos para una evaluación de controles específica para cada empresa, basado en las observaciones hechas.
  - Elaborar cuidadosamente un plan para la evaluación de control interno, tomando en cuenta los objetivos que se desean obtener y que éstos sean congruentes con los objetivos de la empresa.
  - Mantener una buena comunicación con la Gerencia es importante, pues de ello depende que se acepten o no las sugerencias que serán emitidas después de realizar la evaluación.
- Los resultados de la evaluación de control interno deben ser revisados por la Gerencia y aprobados por el Gerente o los altos ejecutivos para su efectiva implantación.
- No hay estrategias claras para el resguardo de la información.

- En la pequeña empresa, como es el caso de HASOFINAD, no se tiene conciencia de la importancia de una cultura organizacional, que generalmente determina la eficacia o ineficacia en la implantación y aplicación del control interno. Dada la falta de una cultura de la organización, el ambiente de control se ve afectado pues no existen los factores adecuados para ejercer control interno, tales como aplicación de códigos y políticas para regular las actividades y tareas cotidianas, pues no se cuenta con un estilo de dirección definido que influya en el ambiente de control, es decir, no existe la experiencia suficiente ni las acciones efectivas por parte de los directivos o altos ejecutivos para llevar a cabo una tarea de control adecuada.

9.2 RECOMENDACIONES

Las recomendaciones que se desprenden después del breve análisis de las conclusiones obtenidas después de poner en práctica la guía en un ambiente informatizado real, son las siguientes:

- Para una efectiva evaluación del control interno en un ambiente informatizado, el auditor debe conocer más a fondo el ambiente de negocio en el que se desempeña la empresa en la que va a realizar su trabajo. Es importante que estudie cómo funciona el entorno actual de control interno, cómo se llevan a cabo los procedimientos establecidos, para poder determinar cuáles son sus fortalezas y cuáles sus debilidades. De aquí partirá el reconocimiento de los requerimientos de la evaluación así como los objetivos que se desean obtener al finalizar el trabajo y se establecerá como línea base para la planificación adecuada de la evaluación de control interno. Además, el auditor debe tener una buena capacidad de comunicación con la Directiva o los altos ejecutivos, pues son ellos quienes tomarán la decisión de aceptar o no las sugerencias que el auditor hará al finalizar la evaluación.

- Un ambiente de control efectivo y bien establecido, necesita de una cultura organizacional bien fundamentada. El auditor debe explicar a los altos ejecutivos la importancia de un ambiente de control adecuado relacionado con las responsabilidades de todos quienes conforman la empresa. Si los directivos no asumen el compromiso con las actividades de control planteadas, los empleados no dan la suficiente importancia a las políticas y normas existentes, por lo que la confiabilidad de la información estaría en riesgo. El auditor puede trabajar en conjunto con la Directiva para instaurar una segregación de tareas adecuada, estableciendo tareas y actividades en los distintos niveles organizacionales, de acuerdo a las habilidades y

conocimientos de cada uno de los empleados que forman parte de la empresa y asegurarse de tener el compromiso de los directivos para hacerlas cumplir de manera efectiva. Para lograrlo, el auditor podría sugerir un proceso de evaluación de desempeño y posteriormente, capacitación y reconocimiento de logros para reconocer y valorizar la contribución de la competitividad de todo el personal.

- Los resultados de la evaluación del control interno deben ser presentados a la Gerencia o los altos ejecutivos, apenas el trabajo haya sido concluido, para discutir acerca de los puntos débiles encontrados, cómo abordar la situación y las recomendaciones para su solución. A partir de esta reunión. Luego de concluido el trabajo, se debe hacer un seguimiento de las recomendaciones emitidas para obtener una retroalimentación, para saber si han sido implementadas con éxito o no y cómo se están desarrollando las actividades cotidianas dentro del nuevo ambiente de control. Es interesante realizar el seguimiento, pues al auditor le sirve para posteriores evaluaciones, así como para el enriquecimiento de su experiencia.

- La presentación de los resultados de la evaluación del control interno se hará a la Directiva de la empresa, para su discusión y análisis. Al final de esta reunión, el Gerente firmará un acta de aprobación de resultados. El auditor, en base a lo obtenido en dicha reunión debe elaborar el informe final, en donde constarán las observaciones, conclusiones y recomendaciones acerca de la situación actual del ambiente de control y los cambios que se sugieren establecer. El auditor debe tener una nueva reunión con la Directiva para presentar el informe final de la evaluación realizada y explicar la importancia de la aplicación efectiva de las recomendaciones para el buen funcionamiento del negocio, de tal manera que se asegure que, al menos un gran porcentaje de ellas sean aceptadas e implementadas, de ahí que es importante la capacidad de comunicación que tenga el auditor para expresar de manera precisa los aspectos importantes, sin extenderse a tratar sobre puntos irrelevantes, así como ser claro y utilizar un lenguaje adecuado, de tal manera que pueda ser entendido fácilmente por sus interlocutores, sin utilizar términos complicados que quizás solo el auditor entienda.

- El auditor debe tratar de comunicar las recomendaciones realizadas en base a las debilidades encontradas en el actual ambiente de control de forma precisa, por cada riesgo encontrado una o varias recomendaciones, explicando la importancia de implementar cada una de manera efectiva, basándose en lo que sucedería si el riesgo encontrado llegara a ocurrir. Se puede abordar cada riesgo en la medida de costo/beneficio, que es un lenguaje que la mayoría de la administración entiende. Después de haber sido aceptadas, el trabajo del auditor concluye en

cuanto a la evaluación de control en sí misma, por lo que, es decisión de la Directiva si solicita al auditor encargarse de la implantación o si se contrata asesores que brinden este servicio para instaurarlas. El auditor deberá hacer un seguimiento de las recomendaciones, para saber si están funcionando de manera efectiva, de tal manera que obtiene una retroalimentación para posteriores evaluaciones, así como asegurarse de que se han llevado a cabo todas o parte de las recomendaciones emitidas.

ANEXOS

ANEXO 1

DIAGNÓSTICO PRELIMINAR

ANTECEDENTES GENERALES:

Nombre Empresa: ……

Actividad: ……

MISION:

……
……
……

VISIÓN:

……
……
……

OBJETIVOS ESTRATÉGICOS:

……
……
……

CONOCIMIENTO GENERAL DEL ÁREA DE SISTEMAS:

……
……
……

DEFINICIÓN DE UN PLAN ESTRATÉGICO DE EVALUACIÓN DE CONTROLES

Contexto:

……
……
……

OBJETIVOS DE EVALUACIÓN DESISTEMAS Y APLICACIONES

……
……
……

OBJETIVOS DE EVALUACIÓN DE LA ARQUITECTURA DE LA INFORMACIÓN

……
……
……

ANEXO 2

CUESTIONARIOS POR DOMINIOS DE CONTROL

DOMINIO: PLANIFICACIÓN Y ORGANIZACIÓN

OBJETIVO: Evaluación de riesgos

1.1 Existe un marco de evaluación sistemático [4.3; 4.4] de riesgos que se relacione con el logro de los objetivos de la Entidad?

N/A	SI	NO

Comentarios:

1.2 El enfoque de evaluación de riesgos, comprende el ámbito de aplicación, la metodología de evaluación, las responsabilidades y las habilidades requeridas?

N/A	SI	NO

Comentarios

1.3 El enfoque de evaluación está enfocado principalmente a los bienes, las amenazas y los puntos vulnerables?

N/A	SI	NO

Comentarios:

1.4 La dirección ha cuantificado y calificado los riesgos a fin de medir el grado de aceptación?

N/A	SI	NO

1.5 Existe un plan de acción para mitigar los riesgos?

N/A	SI	NO

Comentarios:

1.6 Existe definido un riego residual capaz de compensarlo con la contratación de un seguro?

N/A	SI	NO

Comentarios:

1.7 Se ha considerado a los sistemas de control para equilibrar la prevención, la detección, corrección y medidas de control?

N/A	SI	NO

Comentarios:

DOMINIO: ADQUISICIÓN E IMPLEMENTACIÓN

OBJETIVO: Evaluación para la adquisición y mantenimiento de Infraestructura tecnológica

2.1 Se ha implementado procedimientos [2.3 EVALUACIÓN DE CONTROLES EN EMPRESAS PYMES] de evaluación de hardware y software para detectar defectos del sistema?

N/A	SI	NO

Comentarios:

2.2 Se ha programado un mantenimiento rutinario del hardware para reducir los riesgos de falla?

N/A	SI	NO

Comentarios:

2.3 La configuración y mantenimiento de los parámetros del software se encuentra debidamente protegida?

N/A	SI	NO

Comentarios:

2.4 El software de sistemas se ha instalado de acuerdo con el marco de adquisición y mantenimiento?

N/A	SI	NO

Comentarios:

2.5 El mantenimiento se efectúa de acuerdo al marco de adquisición y mantenimiento?

N/A	SI	NO

Comentarios:

2.6 Son controlados los cambios del software de acuerdo con los procesos de cambio de la Entidad?

N/A	SI	NO

Comentarios:

Objetivo: Evaluación para el desarrollo y mantenimiento de procedimientos de TI

3.1 Se han definido con oportunidad los requerimientos operativos y los niveles de servicio futuros?

N/A	SI	NO

Comentarios:

3.2 Se prepara y se mantiene actualizado los manuales de procedimientos de los usuarios?

N/A	SI	NO

Comentarios:

3.3 Se prepara y se mantiene actualizado los manuales de operaciones?

N/A	SI	NO

Comentarios:

3.4 Se han desarrollado materiales de capacitación de los sistemas desarrollados?

N/A	SI	NO

Comentarios:

OBJETIVO: Evaluación para la Instalación y acreditación de sistemas

4.1 Se ha entrenado debidamente a los usuarios y al personal de acuerdo a un plan definido?

N/A	SI	NO

Comentarios:

4.2 Se ha establecido optimizar los sistemas previendo los recursos requeridos para operar software nuevo o con cambios importantes?

N/A	SI	NO

Comentarios:

4.3 La implementación de los planes, que se relaciona con la preparación del sitio, adquisición e instalación de equipos, entrenamiento a usuarios, se han preparado revisando y aprobando las partes relevantes?

N/A	SI	NO

Comentarios:

4.4 Ha existido o existe un plan pre-establecido para la conversión de datos de un antiguo sistema?

N/A	SI	NO

Comentarios:

4.5 Existe una constancia por escrito en la que indique que el producto está completo?

N/A	SI	NO

Comentarios:

4.6 Se han revisado los requerimientos del sistema operativo que aseguren las necesidades del usuario?

N/A	SI	NO

Comentarios:

Objetivo: Evaluación para la administración de la capacidad y desempeño de TI

5.1 Se encuentran identificadas y convertidas en requerimientos y términos de disponibilidad, el desempeño y la disponibilidad de TI?

N/A	SI	NO

Comentarios:

5.2 Existe un plan para obtener, monitorear y controlar la disponibilidad de los servicios de información?

N/A	SI	NO

Comentarios:

5.3 Existe un procedimiento que asegure el monitoreo del desempeño de los recursos de tecnología información y que las excepciones sean reportadas en forma oportuna y completa?

N/A	SI	NO

Comentarios:

5.4 Existen herramientas apropiadas para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de la configuración, desempeño y disponibilidad de mecanismos de tolerancia de fallas, mecanismos de asignación de recursos y definición de prioridades de tareas?

N/A	SI	NO

Comentarios:

5.5 El proceso establecido, incluye la capacidad de pronóstico que permita que los problemas se solucionen antes de que afecten al sistema?

N/A	SI	NO

Comentarios:

5.6 Existen controles que aseguren la preparación de pronósticos de carga de trabajo que permitan identificar tendencias y proporcionar la información necesaria para el plan de capacidad?

N/A	SI	NO

Comentarios:

5.7 Existen procedimientos para la revisión del hardware que asegure una capacidad justificable económicamente para procesar las cargas de trabajo y proporcionar la cantidad y calidad de desempeño requeridos prescritos en los acuerdos de servicio?

N/A	SI	NO

Comentarios:

5.8 Se ha implementado mecanismos de tolerancia de fallas, de asignación equitativa de recursos y definición de prioridades de tareas a fin de utilizar en forma adecuada la disponibilidad de los recursos?

N/A	SI	NO

Comentarios:

5.9 Se ha considerado aspectos tales como: contingencia, cargas de trabajo y planes almacenamiento en el aseguramiento de la capacidad requerida?

N/A	SI	NO

Comentarios:

DOMINIO: ENTREGA DE SERVICIO Y DE SOPORTE

OBJETIVO: Evaluación para la garantía de un servicio continuo

6.1 Existe un marco de referencia de continuidad que defina los roles, responsabilidades, las reglas y estructura para documentar el plan y los procedimientos?

N/A	SI	NO

6.2 El plan de continuidad es consistente con el plan de la entidad y toma en consideración el plan a mediano y largo plazo que asegure su consistencia?

N/A	SI	NO

Comentarios:

6.3 Existe un plan escrito que asegure la continuidad de, por lo menos, los servicios básicos?

N/A	SI	NO

Comentarios:

6.4 Existen procedimientos y guías que minimicen los requerimientos de continuidad con respecto a personal, instalaciones, hardware, software, equipo, formatos materiales de consumo y mobiliario?

N/A	SI	NO

Comentarios:

6.5 Existen procedimientos de control de cambios que aseguren la actualización del plan de continuidad con requerimientos actuales?

N/A	SI	NO

Comentarios:

6.6 El plan de continuidad es evaluado en forma regular con base a un plan de acción de acuerdo a los resultados reportados?

N/A	SI	NO

Comentarios:

6.7 La metodología de continuidad para desastres, incluye sesiones de entrenamiento regulares?

N/A	SI	NO

Comentarios:

6.8 El plan de continuidad está distribuido solo entre el personal autorizado y cuenta con las seguridades respectivas para evitar su divulgación?

N/A	SI	NO

Comentarios:

6.9 Cuentan los usuarios con procedimientos alternativos en caso de emergencias o desastres?

N/A	SI	NO

Comentarios:

6.10 El plan de continuidad identifica los programas de aplicación, servicio de terceros, sistemas operativos, personal, insumos, archivos críticos así como los tiempos necesarios para la recuperación después de un desastre?

N/A	SI	NO

Comentarios:

6.11 La metodología de continuidad, incluye la identificación de alternativas relativas al centro de cómputo y al hardware de respaldo así como una selección de alternativa final?

4.11.1 Existe un contrato formal para este tipo de servicios?

N/A	SI	NO

Comentarios:

6.12 Se han establecido sitios de almacenamiento seguros para las copias de la información, documentos y otros recursos que soporten su recuperación y la continuidad del plan de la organización?

N/A	SI	NO

Comentarios:

		N/A	SI	NO
6.13	Existen establecidos procedimientos para evaluar un plan de continuidad y su actualización, después de un desastre ocurrido?			

Comentarios:

Objetivo: Evaluación para la garantía de la seguridad de los sistemas

		N/A	SI	NO
7.1	La seguridad de tecnología de información es administrada considerando los elementos que aseguren una adecuada seguridad?			

Comentarios:

		N/A	SI	NO
7.2	Se encuentran restringidos el acceso lógico y el uso de los recursos a través de un mecanismo de autenticación de los usuarios y de recursos asociados con las reglas de acceso?			

Comentarios:

		N/A	SI	NO
7.3	Se han considerado la necesidades individuales para visualizar, agregar, modificar o eliminar datos para garantizar el control de la seguridad de acceso?			

Comentarios:

		N/A	SI	NO
7.4	Se han establecido procedimientos que aseguren acciones oportunas relacionadas con los requerimientos, establecimiento, emisión y suspensión de cuentas de usuario			
7.4.1	Existe un procedimiento formal que indique el propietario de los datos o del sistema que otorga los privilegios de acceso?			

Comentarios:

7.5 Existe un proceso de control establecido para revisar y confirmar periódicamente los derechos de accesos?

N/A	SI	NO

Comentarios:

7.6 Controlan los usuarios, en forma sistemática, la actividad de sus propias cuentas

7.6.1 Existen mecanismos de información que permitan supervisar la actividad normal, así como, alertar sobre actividades inusuales?

N/A	SI	NO

Comentarios:

7.7 La administración de seguridad tiene asegurado la actividad de control para que una inminente violación de seguridad sea notificada inmediatamente al administrador y que las acciones subsecuentes sean consideradas en forma automática?

N/A	SI	NO

Comentarios:

7.8 Existe una decisión explícita del dueño de los datos para asegurar que todos los datos se encuentren clasificados en términos de sensitividad de acuerdo con un esquema de clasificación?

N/A	SI	NO

Comentarios:

7.9 Existen controles para asegurar que la identificación y los derechos de acceso de los usuarios estén establecidos y administrados de forma única y centralizada?

N/A	SI	NO

Comentarios:

7.10 Todas las actividades de seguridad se encuentran reportadas y revisadas apropiadamente en forma regular para identificar actividades no autorizadas?

Comentarios:

N/A	SI	NO

7.11 Existe una plataforma centralizada con instalaciones de comunicación rápidas y seguras que manejen los incidentes de seguridad computacional?

7.11.1 Se han establecido entre los funcionarios, los responsables para el manejo de incidentes, que aseguren una respuesta apropiada, efectiva y oportuna?

N/A	SI	NO

Comentarios:

7.12 Se realiza en forma periódica una reacreditación de seguridad, para conservar al día el nivel de seguridad?

N/A	SI	NO

Comentarios:

7.13 Dentro de las políticas de la entidad se incluye prácticas de control que permitan verificar la autenticidad de las contrapartes que proporcionan transacciones electrónicas?

N/A	SI	NO

Comentarios:

7.14 Las políticas de la entidad, aseguran que se instrumenten controles que proporcionen autenticidad a las transacciones?

N/A	SI	NO

Comentarios:

7.15 Las políticas de la entidad, incluyen controles que no permitan que las transacciones pueda ser negadas por ninguna de las partes, por ejemplo a través de firmas digitales y registros de tiempos?

N/A	SI	NO

Comentarios:

7.16 Las políticas de la entidad, aseguran que la información de transacciones confidenciales es enviada por canales seguros?

N/A	SI	NO

Comentarios:

7.17 El hardware y software relacionado con seguridad, se encuentra permanentemente protegido para asegurar su integridad y evitar la divulgación de claves secretas?

N/A	SI	NO

Comentarios:

7.18 Existe un marco de referencia con adecuadas medidas de control preventivas, detectivas y correctivas para evitar virus computacionales?

N/A	SI	NO

Comentarios:

7.19 Se cuenta con sistemas firewall para conexiones a Internet?

N/A	SI	NO

Comentarios:

7.20 Existe protección consistente a la integridad de todas las tarjetas que son utilizadas para autenticación o almacenamiento de información financiera u otra información sensitiva?

N/A	SI	NO

Comentarios:

Objetivo: Evaluación para la Educación y capacitación de los usuarios

8.1 Existan procedimientos que permitan identificar y documentar las necesidades de entrenamiento de personal que hace uso de los servicios de información?

N/A	SI	NO

Comentarios:

8.2 Se han definido los grupos, objetivos, entrenadores de las sesiones de entrenamiento de acuerdo a las necesidades establecidas?

N/A	SI	NO

Comentarios:

8.3 Se encuentra todo el personal capacitado y entrenado en los principios de seguridad de sistemas?

N/A	SI	NO

Comentarios:

Objetivo: Evaluación para la asistencia y asesoramiento a los usuarios de TI

9.1 Existe un soporte para usuarios para que interactúen con el personal de manejo de problemas?

N/A	SI	NO

Comentarios:

9.2 Existen procedimientos que aseguren que todas las preguntas de los usuarios sean registradas por el grupo de ayuda?

N/A	SI	NO

Comentarios:

9.3 Existen niveles adecuados de atención, a las preguntas de los usuarios que pueden resultar complejas?

N/A	SI	NO

Comentarios:

9.4 Existen procedimientos que permitan monitorear las preguntas planteadas por los usuarios?

N/A	SI	NO

Comentarios:

9.5 Existen procedimientos que aseguren el reporte adecuado de las preguntas de los usuarios y su solución?

N/A	SI	NO

Comentarios:

Objetivo: Evaluación para la Administración de la configuración

10.1 Existen procedimientos que aseguren el registro único de los elementos de la configuración autorizados e identificables en el inventario al momento de la adquisición?

N/A	SI	NO

Comentarios:

10.2 Existe una configuración base, de elementos como punto de verificación, que permita regresar después de las modificaciones?

N/A	SI	NO

Comentarios:

10.3 Los procedimientos establecidos aseguran que la existencia y consistencia del registro de la configuración sean revisados en forma periódica?

N/A	SI	NO

10.4 Se revisa en forma periódica la existencia de software no autorizado en las computadoras de la entidad?

N/A	SI	NO

Comentarios:

10.5 Se han establecido procedimientos de administración para la configuración, que aseguren los componentes críticos de los recursos de la organización hayan sido propiamente identificados y mantenidos?

N/A	SI	NO

Comentarios:

10.6 Todo el software de la organización se encuentra debidamente etiquetado, inventariado y con las respectivas licencias?. Se han realizado pruebas de auditoría al respecto?

N/A	SI	NO

Comentarios:

Objetivo: Evaluación para la Administración de problemas e incidentes

11.1 Se encuentra implementado un sistema de administración de problemas que aseguren el registro, análisis y soluciones de todos los incidentes, problemas o errores?

11.1.1 Se emiten reportes sobre problemas significativos?

N/A	SI	NO

Comentarios:

11.2 Los problemas identificados son resueltos de la forma más oportuna y eficiente?

N/A	SI	NO

Comentarios:

	N/A	SI	NO
11.3 Las prioridades para los procesos emergentes se encuentran documentados y aprobados debidamente por la administración?			

Comentarios:

Objetivo: Evaluación para la Administración de datos

	N/A	SI	NO
12.1 Existen procedimientos de preparación de datos a ser seguidos por los usuarios a fin de minimizar los errores u omisiones?			
12.1.1 Estos procedimientos aseguran que los errores e irregularidades sean detectados, reportados y corregidos?			

Comentarios:

	N/A	SI	NO
12.2 Existen procedimientos de manejo de errores, de ser así, estos aseguran que los errores y las irregularidades puedan ser detectados, corregidos y reportados?			

Comentarios:

	N/A	SI	NO
12.3 Existen procedimientos que aseguren que la entidad pueda retener o reproducir los documentos fuente originales durante un tiempo razonable?			

Comentarios:

	N/A	SI	NO
12.4 Existen procedimientos apropiados que aseguren que la entrada de datos es llevada a cabo solo por personal autorizado?			

Comentarios:

12.5 Existen controles suficientes que verifiquen la exactitud, suficiencia y validez de los datos sobre transacciones capturados para su procesamiento?

N/A	SI	NO

Comentarios:

12.6 Existen procedimientos para la corrección y reenvío de datos que hayan sido capturados en forma errónea?

N/A	SI	NO

Comentarios:

12.7 Existen procedimientos para el procesamiento de datos que aseguren una adecuada división de funciones y que el trabajo sea verificado en forma rutinaria?

N/A	SI	NO

Comentarios:

12.8 Se encuentran establecidos procedimientos de manejo de errores que permitan la identificación de las transacciones erróneas sin que estas sean aun procesadas y sin interrumpir el procesamiento normal?

N/A	SI	NO

Comentarios:

12.9 Existen procedimientos establecidos que permitan el manejo y la retención de los datos de salida de los programas de aplicación?

N/A	SI	NO

Comentarios:

12.10 Existen procedimientos por escrito para comunicar la distribución de datos de salida?

N/A	SI	NO

Comentarios:

12.11 Existen procedimientos que aseguren la precisión de los reportes de los datos de salida sean revisadas por los usuarios?

N/A	SI	NO

Comentarios:

12.12 Existe una adecuada protección contra el acceso o modificación no autorizado durante la transmisión y transporte de información sensible?

N/A	SI	NO

Comentarios:

12.13 Existen procedimientos establecidos que impidan la divulgación indebida o desecho de información delicada de la entidad?

N/A	SI	NO

Comentarios:

12.14 Existen procedimientos para el almacenamiento de datos que consideren requerimientos de recuperación, economía y políticas de seguridad?

N/A	SI	NO

Comentarios:

12.15 Se han definido periodos de retención y términos de almacenamiento para documentos, datos, programas, reportes y mensajes de entrada y salida?

N/A	SI	NO

Comentarios:

12.16 Existen procedimientos que aseguren un inventario sistemático del contenido de la librería de medios magnéticos?

N/A	SI	NO

Comentarios:

12.17 Se han establecido procedimientos para establecer protección a la librería de medios magnéticos?

N/A	SI	NO

Comentarios:

12.18 Se ha establecido una estrategia apropiada de respaldo y restauración que asegure una revisión de los requerimientos de la organización, así como el desarrollo, prueba y documentación del plan de recuperación?

N/A	SI	NO

Comentarios:

12.19 Existen procedimientos que aseguren que los respaldos se realicen de acuerdo con la estrategia de respaldos definida y que su utilidad sea verificada regularmente?

N/A	SI	NO

Comentarios:

12.20 Los procedimientos de respaldo incluyen el almacenamiento apropiado para el archivo de los datos y de la documentación relacionada dentro y fuera de las instalaciones?

N/A	SI	NO

Comentarios:

12.21 Se ha implementado una política y procedimientos para asegurar que el archivo cumple con los requerimientos legales y de la entidad y se encuentran protegidos y registrados adecuadamente?

N/A	SI	NO

Comentarios:

12.22 Se encuentran implementados procedimientos y protocolos que aseguren la integridad, confidencialidad y la no negación de mensajes sensitivos cuando se transmiten datos a través de Internet o una red pública?

N/A	SI	NO

Comentarios:

12.23 Se verifica la autenticidad e integridad de la información sobre la información electrónica que se origina externamente?

N/A	SI	NO

Comentarios:

12.24 Existen procedimientos apropiados para que aseguren la integridad y autenticidad para transacciones electrónicas sensibles?

N/A	SI	NO

Comentarios:

12.25 Se verifica periódicamente la integridad y lo adecuado de los datos mantenidos en archivos y otros medios magnéticos?

N/A	SI	NO

Comentarios:

Objetivo: Evaluación para la Administración de instalaciones

13.1 Se han establecido apropiadas medidas de seguridad física y control de acceso para las instalaciones de acuerdo a las políticas de seguridad, incluyendo dispositivos de información fuera de las instalaciones?

N/A	SI	NO

Comentarios:

13.2 Se ha considerado mantener un bajo perfil de las instalaciones relacionadas con TI?

N/A	SI	NO

Comentarios:

13.3 Se acostumbra acompañar a las personas que no forman parte de la empresa, cuando estas entran a las instalaciones?

N/A	SI	NO

Comentarios:

13.4 Se han establecido y se mantiene las suficientes medidas para la protección contra factores ambientales?

13.5.1 Existen equipos o dispositivos especializados para monitorear y controlar el ambiente?

N/A	SI	NO

Comentarios:

13.6 Se ha evaluado la necesidad de contar con generadores de luz, para conservar el suministro de energía ?

N/A	SI	NO

Comentarios:

DOMINIO: MONITOREO

Objetivo: Evaluación para el Monitoreo de los procesos

14.1 Existen definidos indicadores de desempeño que permitan medir las actividades internas y de terceros?

14.1.1 Se elaboran reportes de desempeño?

N/A	SI	NO

Comentarios:

14.2 Los servicios proporcionados a los usuarios son comparados con los objetivos?

N/A	SI	NO

Comentarios:

14.3 Son evaluados los índices de satisfacción de los usuarios o clientes?

N/A	SI	NO

Comentarios:

Objetivo: Evaluación de la idoneidad del control interno

15.1 En el curso normal de las operaciones, son monitoreadas las actividades de control interno, a través de la supervisión y comparación?

N/A	SI	NO

Comentario:

15.2 Se reporta y se conserva toda la información relacionada con los errores, inconsistencias o excepciones?

N/A	SI	NO

Comentarios:

15.4 Existen auditorías independientes o auto auditorías que garanticen la seguridad operacional y el funcionamiento adecuado de control interno?

N/A	SI	NO

Comentarios:

ANEXO 3

PLANTILLA PARA AUDITORÍA A APLICACIONES CRÍTICAS

Preparador por:

Fecha:

Nombre de la Aplicación:

DATOS GENERALES DE LA APLICACIÓN

A. ASPECTOS GENERALES:

……

……

……

……

……..

B. CARACTERÍSTICAS DE DISEÑO

Arquitectura: ……..

Tiempo en producción: ……..

Lenguaje de desarrollo: ……

Base de datos que utiliza: ……

Desarrollo:

- Interno
- Producto o paquete de terceros
- Externo
- Mixto

C. CARACTERÍSTICAS DE DOCUMENTACIÓN

DOCUMENTACIÓN DISPONIBLE NO DISPONIBLE ACTUALIZADA

Manual de usuario: (S/N)

Manual de instalación: (S/N)

Diccionario de datos: (S/N)

D. HISTORIA DE ERRORES

[Errores reportados, enumerar si los hubiera] ……..

…….

ANEXO 4

PLANTILLA PARA LA EVALUACIÓN DEL NIVEL DE RIESGO DE APLICACIONES

Preparador por: …….

Fecha: …….

Nombre de la Aplicación: …….

IMPORTANCIA DE LA APLICACIÓN

a. Relación de la aplicación con los objetivos de la empresa

1. No hay relación.
2. Baja relación.
3. Media relación.
4. Alta relación.

b. Impacto a los usuarios frente a eventuales caídas de la aplicación

1. No pasa nada.
2. Opera con varios problemas.
3. Casi se paraliza.

c. Fraudes históricos

1. No se han presentado fraudes.
2. Un fraude.
3. Dos fraudes.
4. Más de dos fraudes.

1. CARACTERÍSTICAS DE LA APLICACIÓN

1.1. Edad de la aplicación

1. Aplicación instalada menos de 3 meses.

2. Aplicación instalada menos de 1 año.

3. Aplicación instalada entre 1 y 2 años.

4. Aplicación instalada entre 3 y 5 años.

5. Aplicación instalada hace más de 5 años.

1.2. Interfases con otras aplicaciones

1. No tiene interfases.

2. Interfases con un sistema.

3. Interfases con dos o tres sistemas.

4. Interfaces con más de tres sistemas.

1.3. Percepción del usuario sobre la aplicación

1. Muy Buena.

2. Buena.

3. Regular.

4. Mala.

1.4. Documentación de la aplicación

1. Disponible, adecuada y actualizada.

2. Disponible, adecuada y no actualizada.

3. No adecuada.

4. No disponible.

2. DESARROLLO Y MANTENIMIENTO DE LA APLICACIÓN

Si la aplicación es un desarrollo interno o externo:

2.1. Participación en el desarrollo

1. Usuarios, control de calidad, sistemas.

2. Únicamente usuarios y sistemas.

3. Sólo sistemas.

2.2. Metodología de desarrollo

1. Existe una metodología de desarrollo formal.

2. Existe una metodología de desarrollo pero no está escrita.

3. No existe una metodología de desarrollo.

2.3. Número de cambios críticos (por errores) Anual

1. 0 cambios.

2. De 1 a 3 cambios.

3. De 4 a 10 cambios.

4. De 10 a 20 cambios.

5. Más de 20 cambios.

Si la aplicación es un desarrollo de terceros:

2.4. Entrega/recepción de la aplicación

1. Fue un proceso formal

2. Se realizó informalmente

3. No se ha completado

2.5. Contrato de mantenimiento de la aplicación.

1. Existe un contrato formal para el mantenimiento de la aplicación y se cumple a cabalidad.

2. Existe un contrato pero no se cumple.

3. No existe un contrato pero se realiza mantenimiento según se presente el requerimiento.

4. No existe.

2.6. Número de cambios críticos (por errores) anual.

1. 0 cambios.

2. De 1 a 3 cambios.

3. De 4 a 10 cambios.

4. De 10 a 20 cambios.

5. Más de 20 cambios.

3. EXTENSIÓN Y COMPLEJIDAD DE LA APLICACIÓN

3.1. Empleados que usan la aplicación frente al total de empleados.

1. Hasta un 30%.

2. Hasta un 60%.

3. Más del 60%.

3.2. Volumen de transacciones procesadas en la aplicación frente al total de transacciones de la empresa.

1. Hasta un 30%.

2. Hasta un 60%.

3. Más del 60%.

3.3. Comunicación con sucursales, puntos de venta, clientes o proveedores.

1. Sin conexión

2. Computador y/o controlador remoto conectado al equipo principal con hasta de 12 terminales (interno)

3. Conexión con las sucursales, clientes y/o proveedores con más de 12 terminales

3.4. Complejidad de los procesos y cálculos de la aplicación

1. Procesos y cálculos sencillos

2. Procesos y cálculos complejos

2. Calificación del Nivel de Riesgo de la Aplicación

MATRIZ DE CALIFICACIÓN DE RIESGOS I	
Elaborado por:	
Revisado por:	
Fecha:	
Factores de Evaluación	**Puntaje**
Total	

Selección de riesgos críticos:

Escalas: Probabilidad ocurrencia Impacto

Alto (3) Alto (3)

Media (2) Medio (3)

Baja (1) Bajo (1)

MATRIZ DE CALIFICACIÓN DE RIESGOS II			
Elaborado por:			
Revisado por:			
Fecha:			
Riesgos detectados	**Probabilidad ocurrencia**	**Impacto**	**Total**

ANEXO 5

PLANTILLA PARA IDENTIFICACIÓN DE CONTROLES EXISTENTES EN EL ENTORNO FÍSICO Y LÓGICO

MATRIZ DE RIESGOS Y CONTROLES **Aplica a:** **Área:** **Fecha:** **Preparado por:**				
Riesgos detectados	**Control 1**	**Control 2**	**….Control n**	**Total**
Total				

ANEXO 6

MODELO INFORMES

INFORME DE EVALUACIÓN DEL CONTROL INTERNO

Nombre del Gerente

Fecha:

Naturaleza de la auditoría

……
……

Objetivos de la evaluación

……
……

Alcance

……
……

Importancia del área analizada

……
……
……
……

Conclusión general

……
……
……
……

Observaciones críticas

……

……
……
……
……
……

Firma del Auditor

INFORME FINAL

SEÑOR(a) GERENTE [Nombre del Gerente]

INFORMA:

REF: EVALUACIÓN DE CONTROL INTERNO

2. ANTECEDENTES

……
……

f. OBJETIVOS

……
……

g. ALCANCE

……
……

DETALLE	EXISTENCIA (unidades)

EQUIPOS DISPONIBLES	ASPECTOS TÉCNICOS

4. LIMITACIONES

……
……
……
……

5. COMENTARIOS

[a…x] Observación:

……

……

Situación actual:

……

……

……

……

Efectos:

……

……

……

……

Causas:

……

……

……

…….

Recomendación:

……

……

……

……

FIRMA AUDITOR

ANEXO 7

RESUMEN DEL DESARROLLO DE LA PRÁCTICA

Se solicitó la autorización al Gerente General de HASOFINAD para realizar el trabajo de evaluación de controles internos, mediante una carta. Fue aceptado y se empezaron con las actividades iniciales en el lugar donde están las instalaciones de las oficinas. Se inició con el levantamiento del inventario de los equipos informáticos disponibles así como de la identificación del software más importante.

Se solicitaron manuales y documentación disponible de cada uno de los equipos así como del software.

Hubo una reunión con el personal para tratar de conocer más a fondo qué tipo de trabajo realizan, cómo lo hacen y cómo utilizan sus equipos. Se hicieron las anotaciones correspondientes en cuanto a procedimientos de uso de los equipos y del software, realizando observaciones directas de dichos procedimientos. Esta actividad fue un poco difícil, pues los asesores no trabajan en la oficina, sino que realizan sus tareas en las empresas para las que han sido designados, por lo que fue necesario acudir en varias ocasiones a las instalaciones para poder hacer las observaciones, así como la revisión de cada equipo, pues ellos disponen de portátiles que llevan para sus actividades diarias. Fue más fácil trabajar con los equipos disponibles en la oficina, por tanto se inició el trabajo de revisión con ellos.

Se realizaron todas las anotaciones del estado actual de cada equipo para recoger todos los datos que sirvan como evidencia de la presencia de controles, así como poder hacer un análisis de riesgos basados en dicha información.

Se realizaron cuestionarios asentados en la guía elaborada en este trabajo incluyéndolos dentro de los dominios del COBIT, escogiendo los objetivos más relevantes para poder aplicarlos en esta empresa, pues no se pudieron aplicar todos ellos ya que algunos no tenían ninguna relación con el trabajo realizado en pequeñas empresas. Después, se acudió a las instalaciones de HASOFINAD y, junto con la secretaria y el Gerente, se empezaron a llenar dichos cuestionarios.

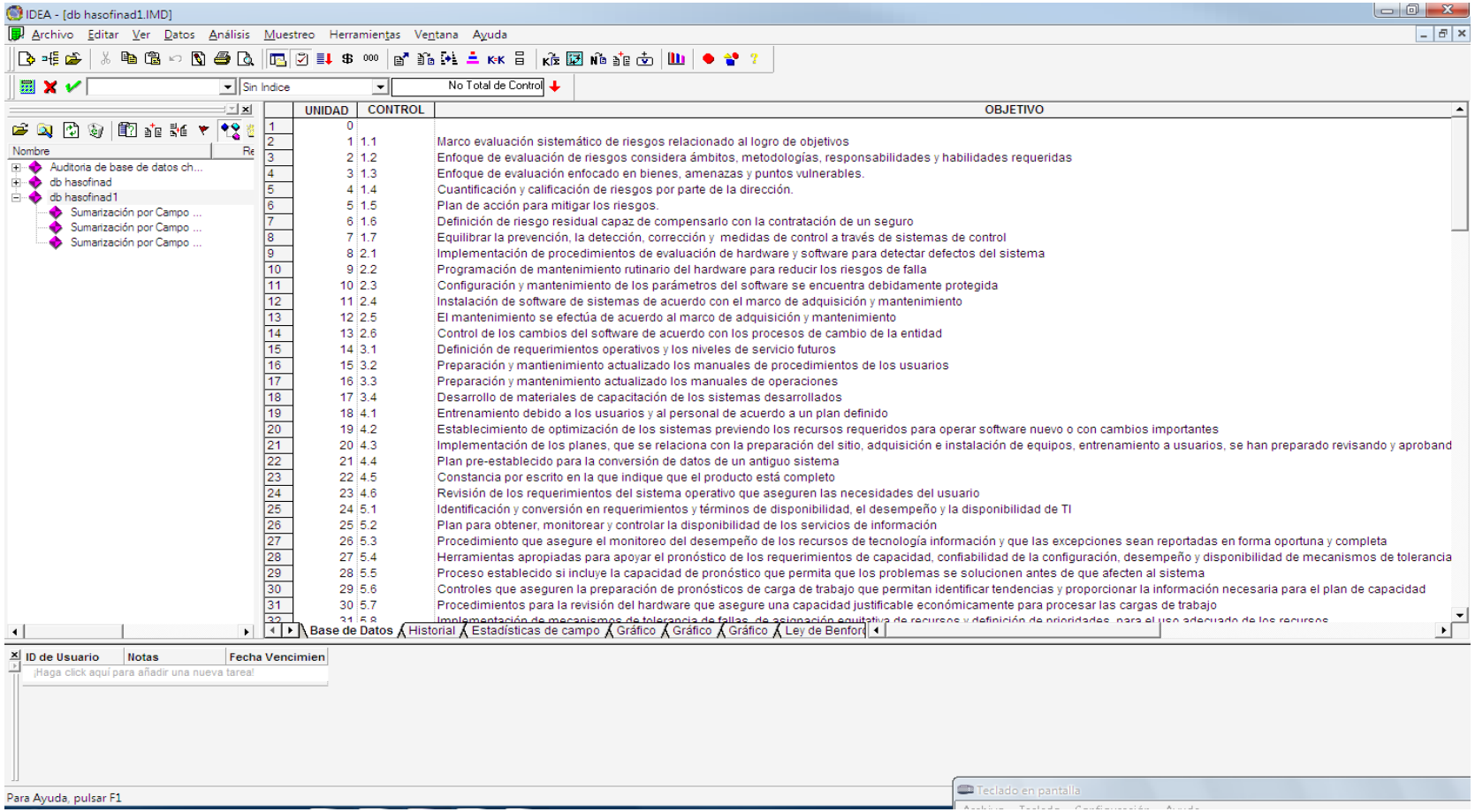
Cuando el trabajo de observación, revisión de equipos y realización de cuestionarios finalizó, se empezó ya a trabajar con toda la información obtenida, de tal manera que se hicieron los análisis necesarios para identificar los riesgos más críticos que pudieran afectar el buen funcionamiento del negocio. A partir del análisis de riesgo, se pudieron evidenciar los controles

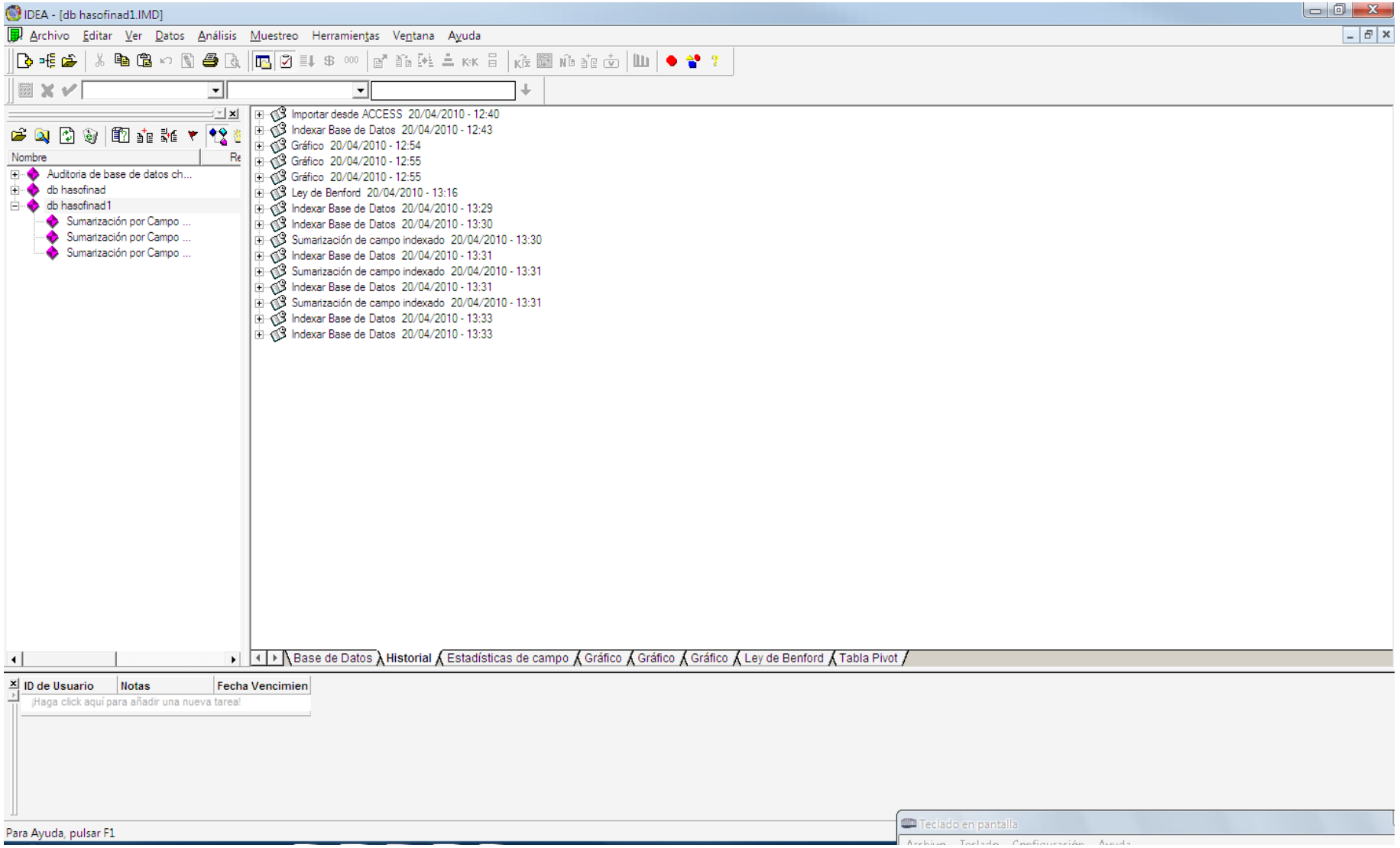
existentes, que en este caso eran muy básicos. Con toda esta información se empezó a trabajar en los informes de evaluación de controles, así como las observaciones hechas a los riesgos más relevantes con sus respectivas recomendaciones. Dichos informes fueron presentados al Gerente General y después de su aprobación, se presentó ante los asesores y la secretaria, en una reunión ligera en donde se expusieron las observaciones y recomendaciones correspondientes. Se discutieron acerca de los puntos que ellos consideraron más importantes y el Gerente aceptó las recomendaciones respecto a algunos controles que deberían ser implementados. No así con todos, pues se me hizo conocer que no se cuenta con el presupuesto necesario para llevar a cabo todas las recomendaciones, sin embargo, se vieron aquellas más prioritarias para el negocio. Se dio cierre al trabajo realizado y se recibieron los agradecimientos correspondientes por parte del Gerente y personal de la empresa.

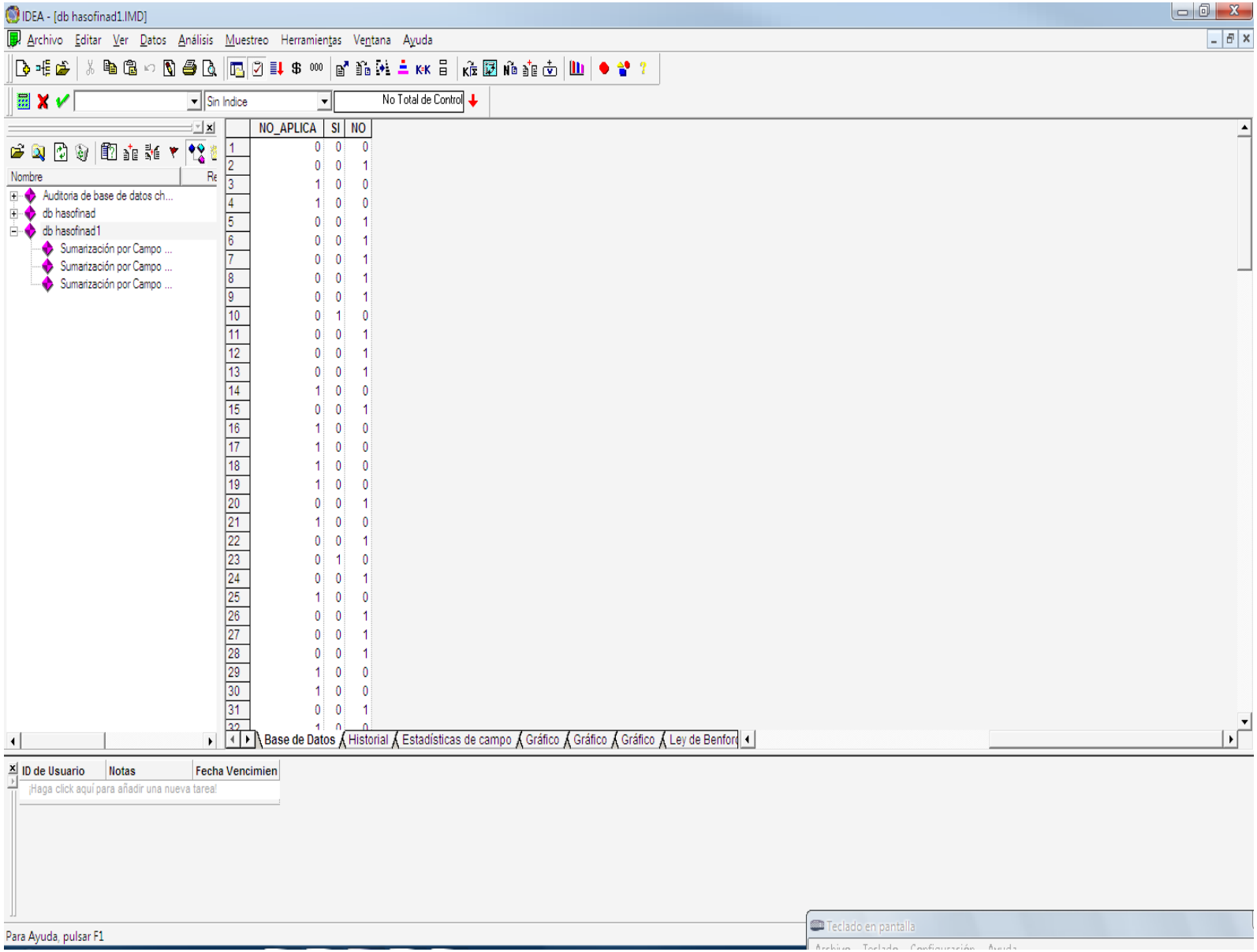
ANEXO 8

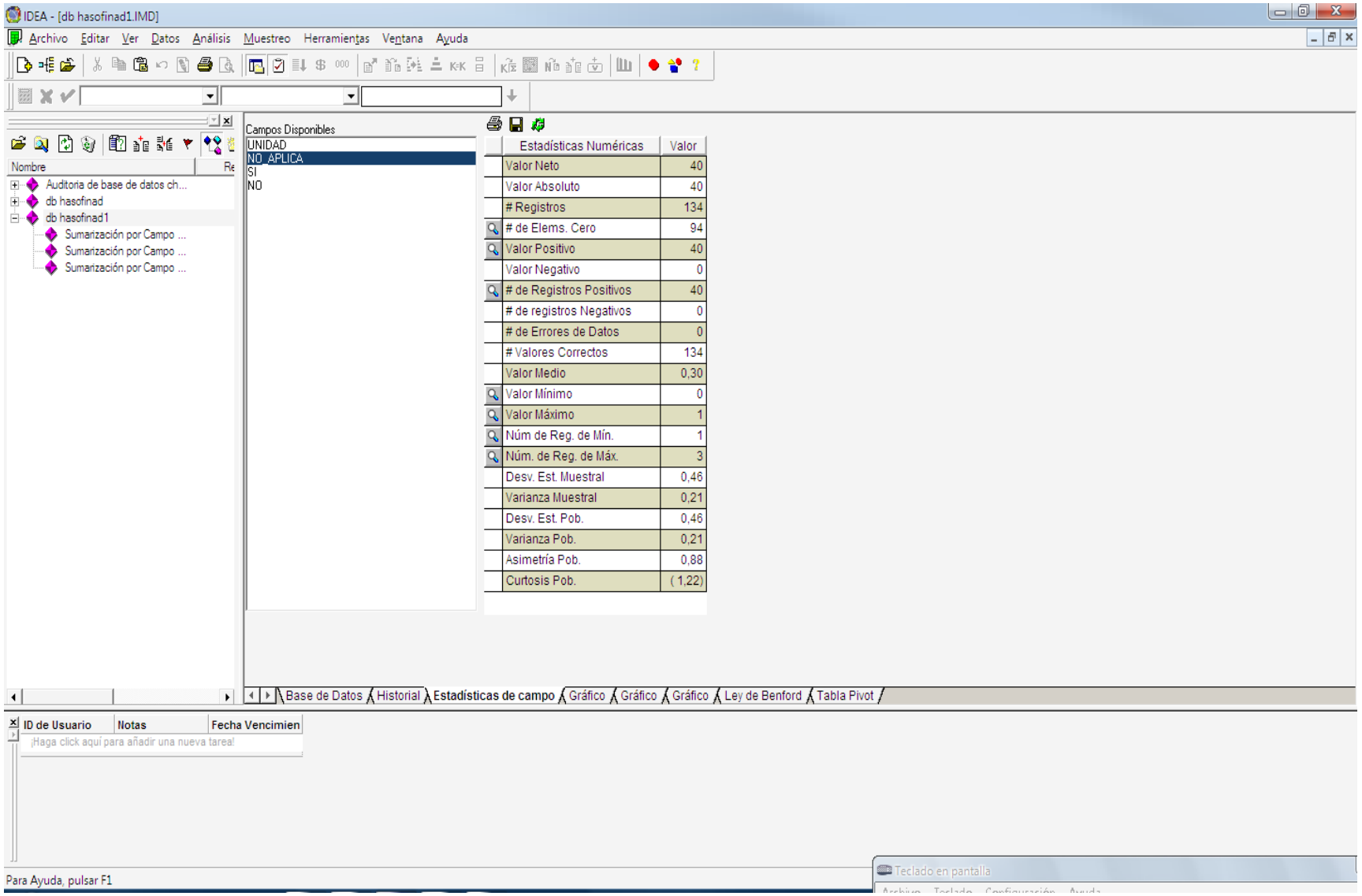
DESARROLLO DE BASE DE DATOS Y ANÁLISIS EN SOFTWARE IDEA

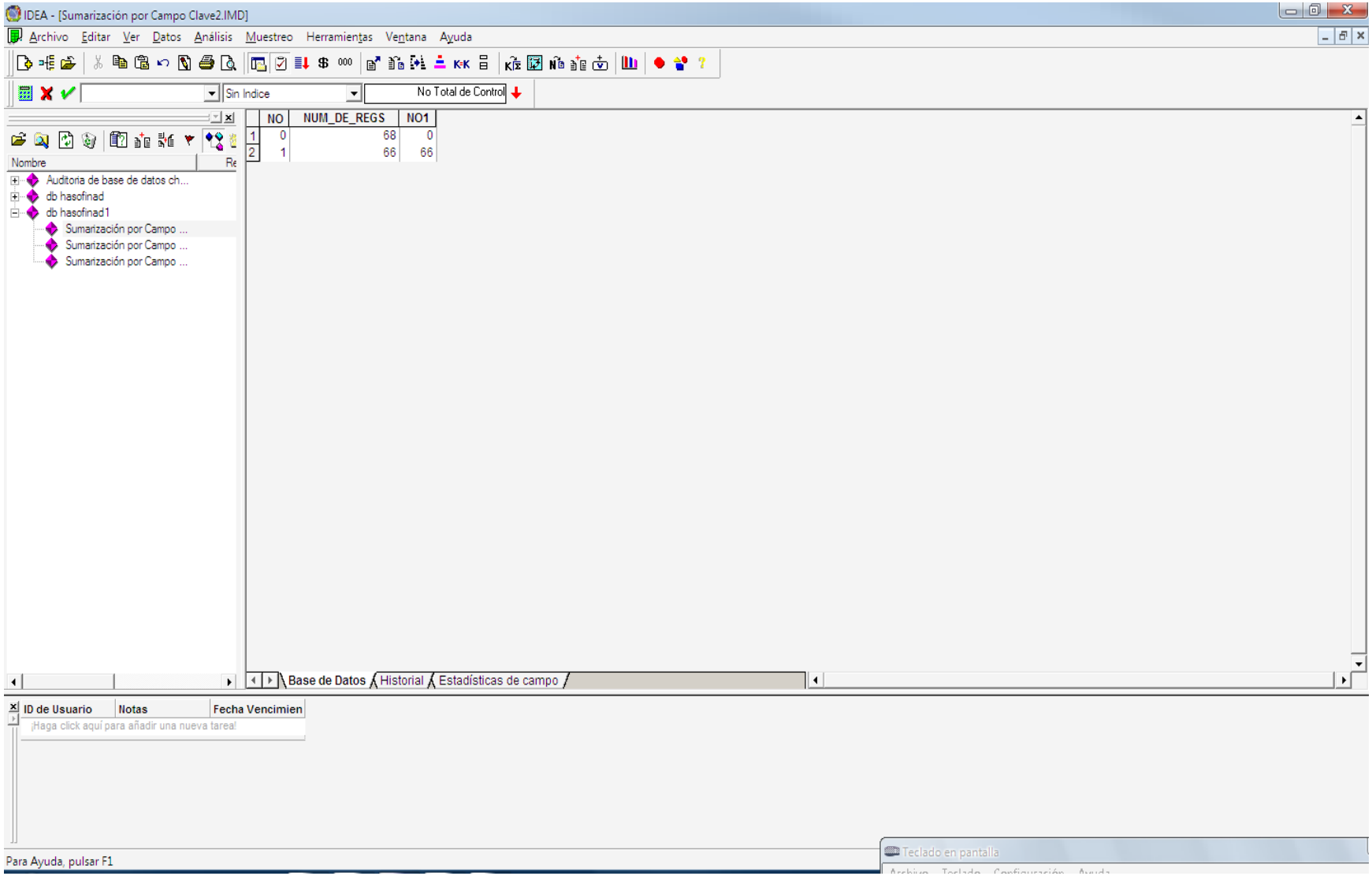
La base de datos está guardada en reportes del propio software, en modo de archivos. El archivo principal es hasofinad1.imd. Capturas de pantallas presentadas a continuación:

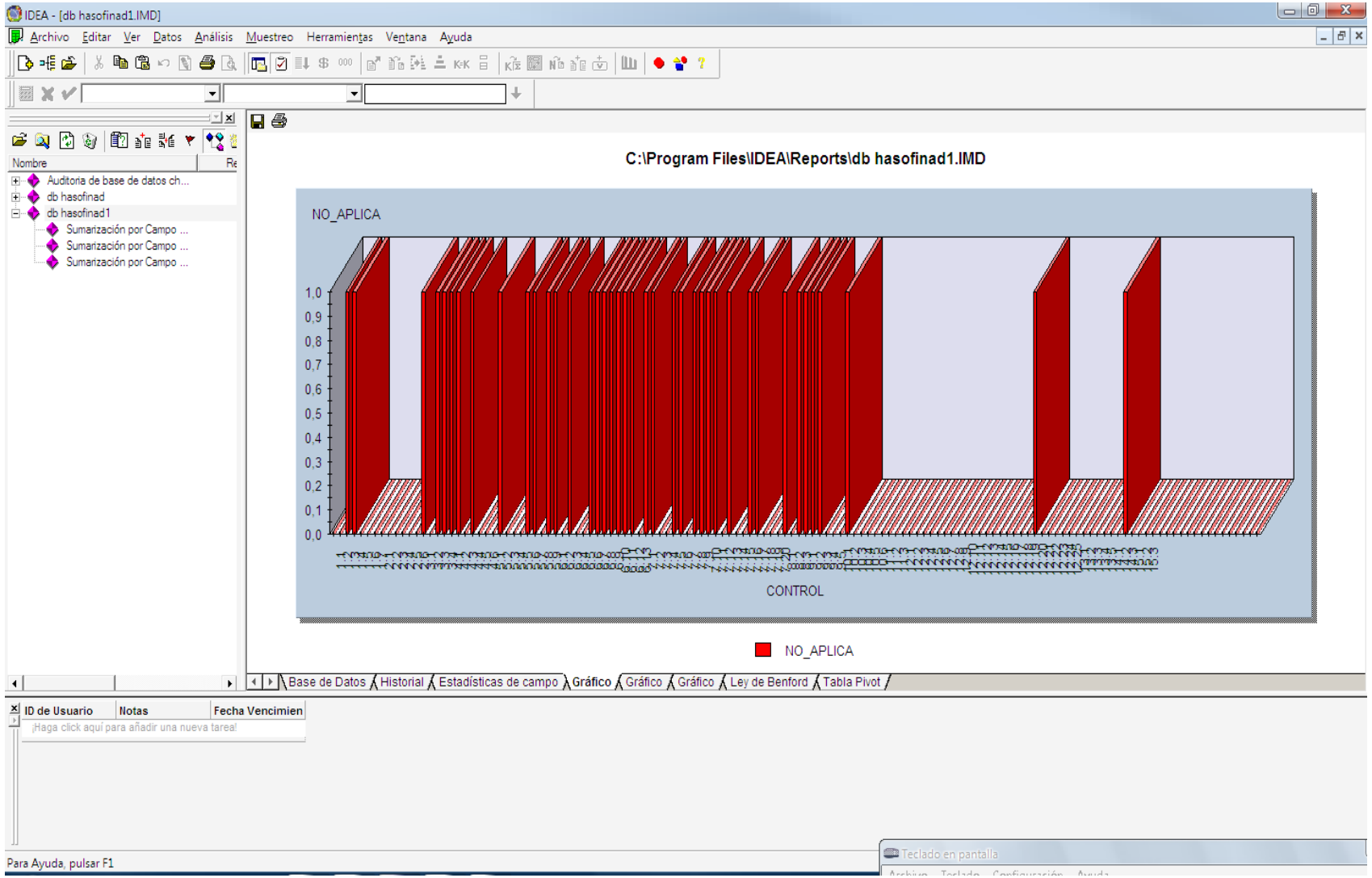



IDEA - [db hasofinad1.IMD]
Archivo Editar Ver Datos Análisis Muestreo Herramientas Ventana Ayuda
Nombre
Auditoria de base de datos ch...
db hasofinad
db hasofinad1
Sumarización por Campo ...
Sumarización por Campo ...
Sumarización por Campo ...
Importar desde ACCESS 20/04/2010 - 12:40
Indexar Base de Datos 20/04/2010 - 12:43
Gráfico 20/04/2010 - 12:54
Gráfico 20/04/2010 - 12:55
Gráfico 20/04/2010 - 12:55
Ley de Benford 20/04/2010 - 13:16
Indexar Base de Datos 20/04/2010 - 13:29
Indexar Base de Datos 20/04/2010 - 13:30
Sumarización de campo indexado 20/04/2010 - 13:30
Indexar Base de Datos 20/04/2010 - 13:31
Sumarización de campo indexado 20/04/2010 - 13:31
Indexar Base de Datos 20/04/2010 - 13:31
Sumarización de campo indexado 20/04/2010 - 13:31
Indexar Base de Datos 20/04/2010 - 13:33
Indexar Base de Datos 20/04/2010 - 13:33
Base de Datos
Historial
Estadísticas de campo
Gráfico
Gráfico
Gráfico
Ley de Benford
Tabla Pivot
ID de Usuario
Notas
Fecha Vencimien
¡Haga click aquí para añadir una nueva tarea!
Para Ayuda, pulsar F1
Teclado en pantalla


IDEA - [db hasofinad1.IMD]
Archivo Editar Ver Datos Análisis Muestreo Herramientas Ventana Ayuda
Sin Indice
No Total de Control
Nombre
Auditoria de base de datos ch...
db hasofinad
db hasofinad1
Sumarización por Campo ...
Sumarización por Campo ...
Sumarización por Campo ...
NO_APLICA SI NO
Base de Datos Historial Estadísticas de campo Gráfico Gráfico Gráfico Ley de Benford
ID de Usuario Notas Fecha Vencimien
¡Haga click aquí para añadir una nueva tarea!
Para Ayuda, pulsar F1
Teclado en pantalla


IDEA - [db hasofinad1.IMD]
Archivo Editar Ver Datos Análisis Muestreo Herramientas Ventana Ayuda
Campos Disponibles
UNIDAD
NO_APLICA
SI
NO
Nombre
Auditoria de base de datos ch...
db hasofinad
db hasofinad1
Sumarización por Campo ...
Sumarización por Campo ...
Sumarización por Campo ...
Estadísticas Numéricas | Valor
Valor Neto | 40
Valor Absoluto | 40
Registros | 134
de Elems. Cero | 94
Valor Positivo | 40
Valor Negativo | 0
de Registros Positivos | 40
de registros Negativos | 0
de Errores de Datos | 0
Valores Correctos | 134
Valor Medio | 0,30
Valor Mínimo | 0
Valor Máximo | 1
Núm de Reg. de Mín. | 1
Núm. de Reg. de Máx. | 3
Desv. Est. Muestral | 0,46
Varianza Muestral | 0,21
Desv. Est. Pob. | 0,46
Varianza Pob. | 0,21
Asimetría Pob. | 0,88
Curtosis Pob. | (1,22)
Base de Datos Historial Estadísticas de campo Gráfico Gráfico Gráfico Ley de Benford Tabla Pivot
ID de Usuario Notas Fecha Vencimien
¡Haga click aquí para añadir una nueva tarea!
Para Ayuda, pulsar F1
Teclado en pantalla


IDEA - [Sumarización por Campo Clave2.IMD]
Archivo Editar Ver Datos Análisis Muestreo Herramientas Ventana Ayuda
Sin Indice
No Total de Control
Nombre
Auditoria de base de datos ch...
db hasofinad
db hasofinad1
Sumarización por Campo ...
Sumarización por Campo ...
Sumarización por Campo ...
NO NUM_DE_REGS NO1
1 0 68 0
2 1 66 66
Base de Datos Historial Estadísticas de campo
ID de Usuario Notas Fecha Vencimien
¡Haga click aquí para añadir una nueva tarea!
Para Ayuda, pulsar F1
Teclado en pantalla


IDEA - [db hasofinad1.IMD]
Archivo Editar Ver Datos Análisis Muestreo Herramientas Ventana Ayuda
Nombre
Auditoria de base de datos ch...
db hasofinad
db hasofinad1
Sumarización por Campo ...
Sumarización por Campo ...
Sumarización por Campo ...
C:\Program Files\IDEA\Reports\db hasofinad1.IMD
NO_APLICA
1,0
0,9
0,8
0,7
0,6
0,5
0,4
0,3
0,2
0,1
0,0
CONTROL
NO_APLICA
Base de Datos
Historial
Estadísticas de campo
Gráfico
Gráfico
Gráfico
Ley de Benford
Tabla Pivot
ID de Usuario
Notas
Fecha Vencimien
¡Haga click aquí para añadir una nueva tarea!
Para Ayuda, pulsar F1
Teclado en pantalla

ANEXO 9

REPORTES DE LA BASE DE DATOS

REPORTE DE BASE DE DATOS (Formato mdi, archivo vinculado).

AN.9.1 ESTADÍSTICAS DE CAMPO: Basadas en los datos ingresados (importados desde IDEA hasta EXCEL)

- **Estadística campo no aplica**

Cliente					**29/04/2010**
Período					**1:38 PM**
Preparado por					
Archivo	db hasofinad.imd				
Campo	NO _ APLICA				
		Estadísticas de Campo			
# de Registros	:		134		
Valor Absoluto	:		40,00	**Valor Neto**	40,00
Valor Medio	:		0,30	**# de Elems. Cero**	94
Valor Positivo	:		40,00	**# de Registros Positivos**	40
Valor Negativo	:		0,00	**# de Registros**	0

				Negativos	
# de Valores Correctos	:		134	**# de Errores de Datos**	0
Valor Mínimo	:		0,00	**Núm. de Reg. Mínimo**	1
Valor Máximo	:		1,00	**Núm. de Reg. Máximo**	3
Desvío Est. Muestral	:		0,46	**Desvío Est. Poblacional**	0,46
Varianza Muestral	:		0,21	**Varianza Poblacional**	0,21
Asimetría Poblacional	:		0,88	**Curtosis Poblacional**	-1,22

- **Estadística campo Si**

Cliente						**29/04/2010**
Período						**2:24 PM**
Preparado por						
Archivo	db hasofinad.imd					
Campo	SI					
		Estadísticas de Campo				
# de	:		134			

Registros						
Valor Absoluto	:		12,00	**Valor Neto**	:	12,00
Valor Medio	:		0,09	**# de Elems. Cero**	:	122
Valor Positivo	:		12,00	**# de Registros Positivos**	:	12
Valor Negativo	:		0,00	**# de Registros Negativos**	:	0
# de Valores Correctos	:		134	**# de Errores de Datos**	:	0
Valor Mínimo	:		0,00	**Núm. de Reg. Mínimo**	:	1
Valor Máximo	:		1,00	**Núm. de Reg. Máximo**	:	10
Desvío Est. Muestral	:		0,29	**Desvío Est. Poblacional**	:	0,29
Varianza Muestral	:		0,08	**Varianza Poblacional**	:	0,08
Asimetría Poblacional	:		2,87	**Curtosis Poblacional**	:	6,27
IDEA						Página1

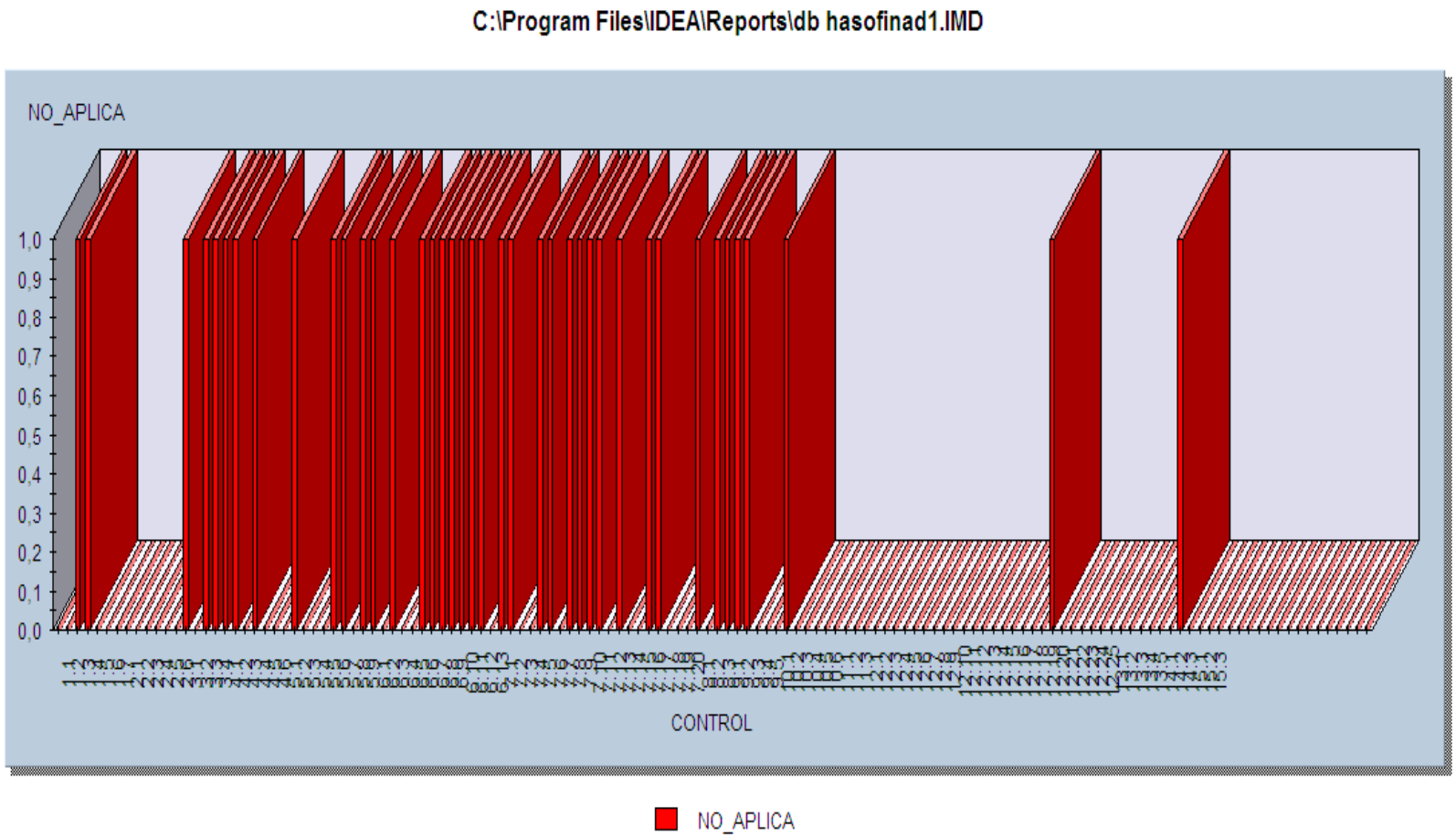
- **Estadística campo No**

Cliente						**29/04/2010**
Período						**1:39 PM**
Preparado por						
Archivo	db hasofinad.imd					
Campo	NO					
		Estadísticas de Campo				
# de Registros	:		134			
Valor Absoluto	:		66,00	**Valor Neto**	:	66,00
Valor Medio	:		0,49	**# de Elems. Cero**	:	68
Valor Positivo	:		66,00	**# de Registros Positivos**	:	66
Valor Negativo	:		0,00	**# de Registros Negativos**	:	0
# de Valores Correctos	:		134	**# de Errores de Datos**	:	0
Valor	:		0,00	**Núm. de**	:	1

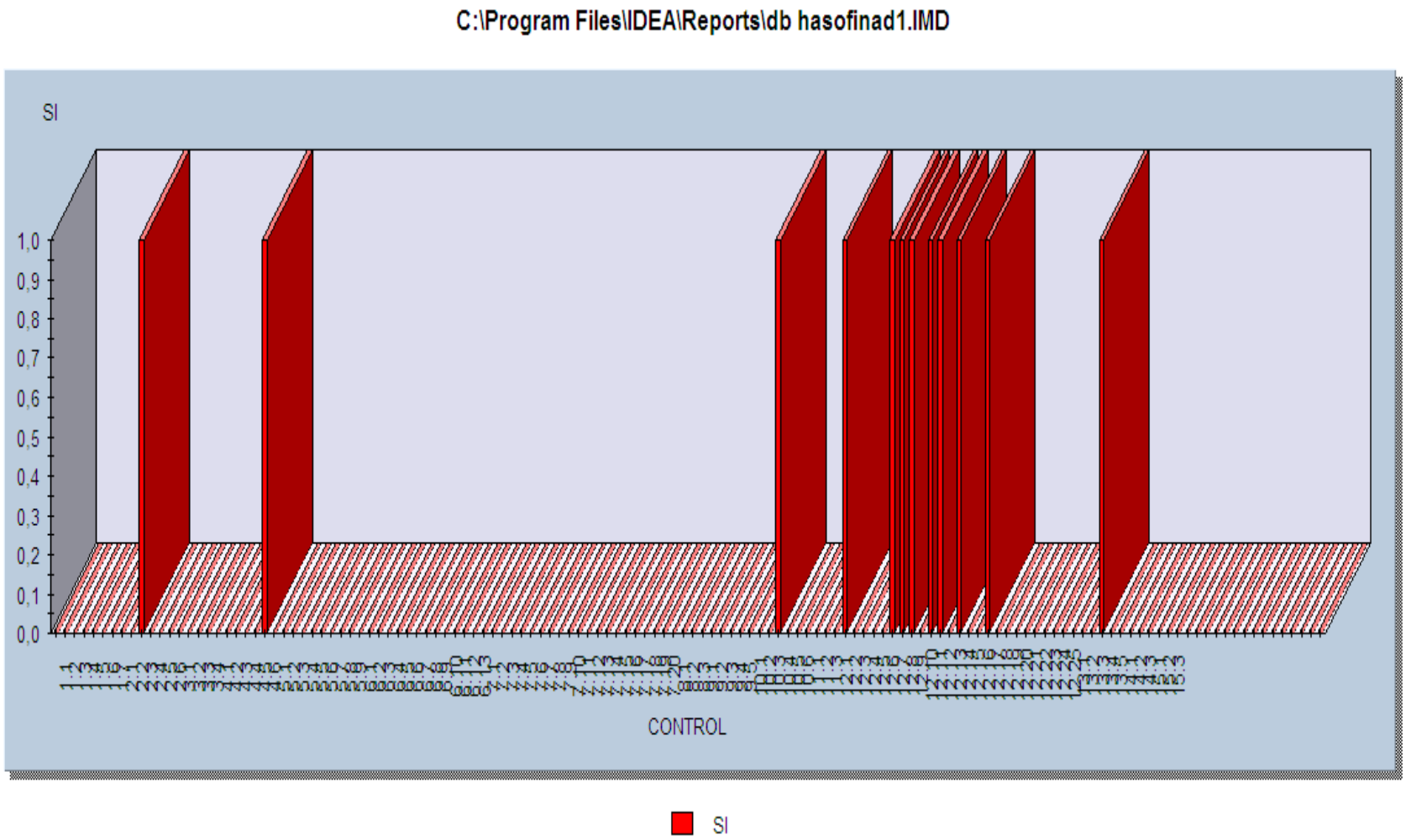
Mínimo				**Reg. Mínimo**		
Valor Máximo	:		1,00	**Núm. de Reg. Máximo**	:	2
Desvío Est. Muestral	:		0,50	**Desvío Est. Poblacional**	:	0,50
Varianza Muestral	:		0,25	**Varianza Poblacional**	:	0,25
Asimetría Poblacional	:		0,03	**Curtosis Poblacional**	:	-2,00
IDEA						Página1

AN.9.3 GRAFICAS POR CAMPOS

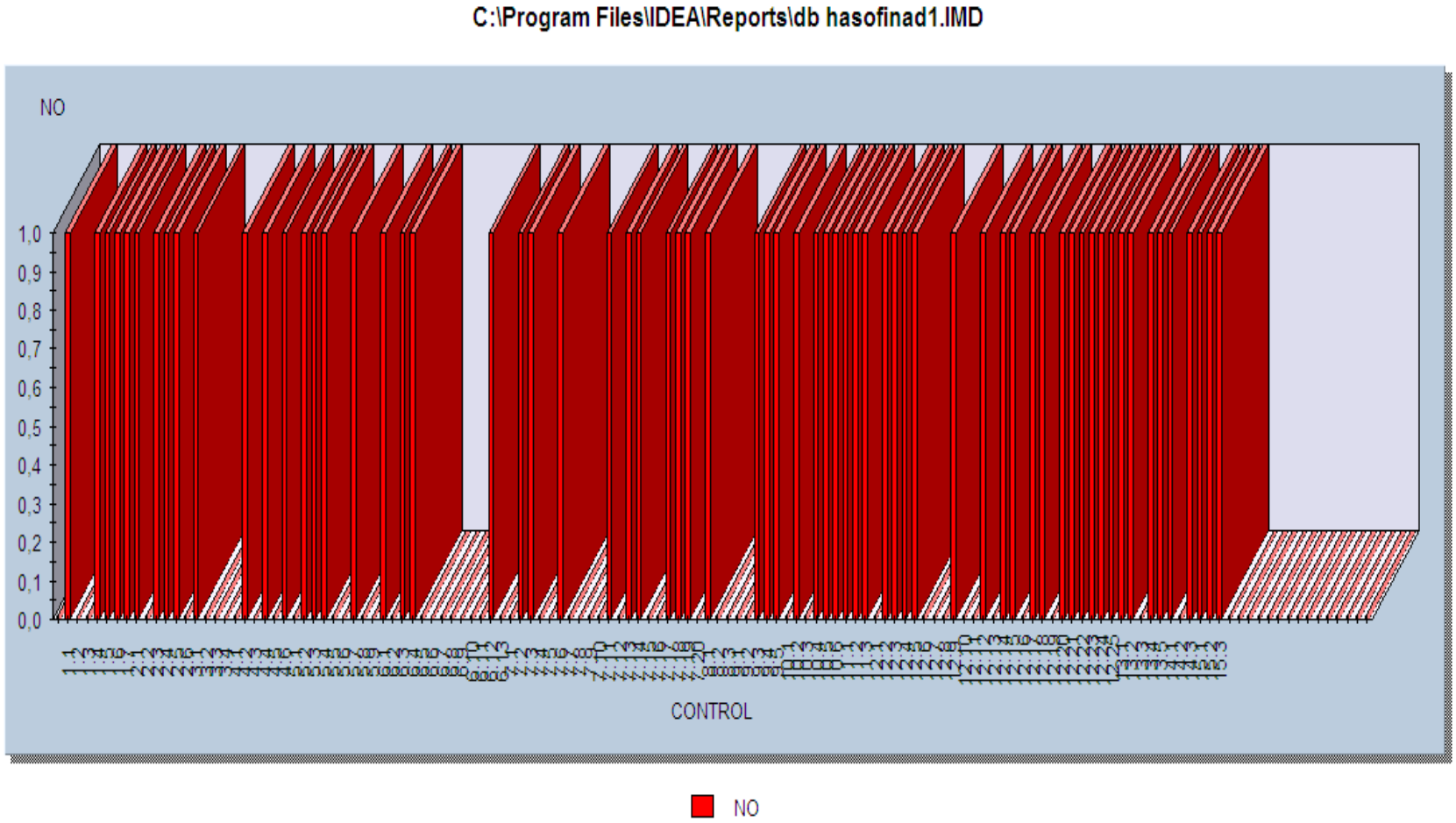
- **No aplica**



- **Si**


C:\Program Files\IDEA\Reports\db hasofinad1.IMD
SI
1,0
0,9
0,8
0,7
0,6
0,5
0,4
0,3
0,2
0,1
0,0
CONTROL
SI

- **No**


C:\Program Files\IDEA\Reports\db hasofinad1.IMD
NO
1,0
0,9
0,8
0,7
0,6
0,5
0,4
0,3
0,2
0,1
0,0
CONTROL
NO

AN.9.4 EXTRACCIÓN POR CAMPOS

(Importado desde IDEA hasta EXCEL, realizado con la herramienta Extracción directa de datos).

- **EXTRACCIÓN CONTROLES MARCADOS NO**

  Archivo exportado hasta EXCEL

UNIDAD	CONTROL	OBJETIVO	N/A	SI	NO
94	12.12	Adecuada protección contra el acceso o modificación no autorizado durante la transmisión y transporte de información sensible,0.,0.,1.			1
108	13.1	Apropiadas medidas de seguridad física y control de acceso para las instalaciones de acuerdo a las políticas de seguridad, incluyendo dispositivos de información fuera de las instalaciones",0.,0.,1.			1
118	15.3	Auditorías independientes o auto auditorías que garanticen la seguridad operacional y el funcionamiento adecuado de control interno,0.,0.,1.			1
75	10.2	Configuración base, de elementos como punto de verificación, que permita regresar después de las modificaciones",0.,0.,1.			1
10	2.3	Configuración y mantenimiento de los parámetros del software se encuentra debidamente protegida,0.,0.,1.			1
48	7.3	Consideración de necesidades individuales para visualizar, agregar, modificar o eliminar datos para garantizar el control de la seguridad de acceso",0.,0.,1.			1
51	7.6	Control de los usuarios, en forma sistemática, la actividad de sus propias cuentas. Mecanismos de información para supervisar la actividad normal y alertar sobre actividades inusuales",0.,0.,1.			1
87	12.5	Controles suficientes que verifiquen la exactitud, suficiencia y validez de los datos sobre transacciones capturados para su procesamiento",0.,0.,1.			1
4	1.4	Cuantificación y calificación de riesgos por parte de la dirección.,0.,0.,1.			1
113	14.1	Definición de indicadores de desempeño que permitan medir las actividades internas y de terceros. Reportes de desempeño.,0.,0.,1.			1
97	12.15	Definición de periodos de retención y términos de almacenamiento para documentos, datos, programas, reportes y mensajes de entrada y salida",0.,0.,1.			1

14	3.1	Definición de requerimientos operativos y los niveles de servicio futuros,0.,0.,1.			1
6	1.6	Definición de riesgo residual capaz de compensarlo con la contratación de un seguro,0.,0.,1.			1
58	7.13	Dentro de las políticas de la entidad se incluye prácticas de control que permitan verificar la autenticidad de las contrapartes que proporcionan transacciones electrónicas,0.,0.,1.			1
62	13.17	El hardware y software relacionado con seguridad, se encuentra permanentemente protegido para asegurar su integridad y evitar la divulgación de claves secretas",0.,0.,1.			1
12	2.5	,El mantenimiento se efectúa de acuerdo al marco de adquisición y mantenimiento,0.,0.,1.			1
7	1.7	Equilibrar la prevención, la detección, corrección y medidas de control a través de sistemas de control",0.,0.,1.			1
19	4.2	Establecimiento de optimización de los sistemas previendo los recursos requeridos para operar software nuevo o con cambios importantes,0.,0.,1.			1
78	10.5	Establecimiento de procedimientos de administración para la configuración, que aseguren los componentes críticos de los recursos de la organización hayan sido propiamente identificados y mantenidos",0.,0.,1.			1
44	6.12	Establecimiento de sitios de almacenamiento seguros para las copias de la información, documentos y otros recursos que soporten su recuperación y la continuidad del plan de la organización",0.,0.,1.			1
111	13.4	Establecimiento y mantenimiento de suficientes medidas para la protección contra factores ambientales. Equipos o dispositivos especializados para monitorear y controlar el ambiente,0.,0.,1.			1
100	12.18	Estrategia apropiada de respaldo y restauración que asegure una revisión de los requerimientos de la organización, así como el desarrollo, prueba y documentación del plan de recuperación",0.,0.,1.			1
112	13.5	Evaluación de la necesidad de contar con generadores de luz, para conservar el suministro de energía",0.,0.,1.			1
116	14.3	Evaluación de los índices de satisfacción de los usuarios o clientes,0.,0.,1.			1
33	6.1	Existencia de un marco de referencia de continuidad que defina los roles, responsabilidades, las reglas y estructura para documentar el plan y los procedimientos",0.,0.,1.			1
27	5.4	Herramientas apropiadas para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de la configuración, desempeño y disponibilidad de mecanismos de tolerancia de fallas, asignación de recursos y definición de prioridades de tareas",0.,0.,1.			1
8	2.1	Implementación de procedimientos de evaluación de hardware y software para detectar defectos del sistema,0.,0.,1.			1

104	12.22	Implementación de procedimientos y protocolos que aseguren la integridad, confidencialidad y la no negación de mensajes sensitivos cuando se transmiten datos a través de Internet o una red pública",0.,0.,1.			1
80	11.1	Implementación de un sistema de administración de problemas que aseguren el registro, análisis y soluciones de todos los incidentes, problemas o errores. Reportes de problemas significativos",0.,0.,1.			1
103	12.21	Implementación de una política y procedimientos para asegurar que el archivo cumple con los requerimientos legales y de la entidad y se encuentran protegidos y registrados adecuadamente,0.,0.,1.			1
11	2.4	Instalación de software de sistemas de acuerdo con el marco de adquisición y mantenimiento,0.,0.,1.			1
59	7.14	"Las políticas de la entidad, aseguran que se instrumenten controles que proporcionen autenticidad a las transacciones",0.,0.,1.			1
82	11.3	Las prioridades para los procesos emergentes se encuentran documentados y aprobados debidamente por la administración,0.,0.,1.			1
63	7.18	Marco de referencia con adecuadas medidas de control preventivas, detectivas y correctivas para evitar virus computacionales",0.,0.,1.			1
1	1.1	Marco evaluación sistemático de riesgos relacionado al logro de objetivos,0.,0.,1.			1
116	15.1	Monitoreo de las actividades de control interno, a través de la supervisión y comparación en el curso normal de las operaciones",0.,0.,1.			1
71	9.3	Niveles adecuados de atención, a las preguntas de los usuarios que pueden resultar complejas",0.,0.,1.			1
5	1.5	Plan de acción para mitigar los riesgos.,0.,0.,1.			1
35	6.3	Plan escrito que asegure la continuidad de, por lo menos, los servicios básicos",0.,0.,1.			1
25	5.2	Plan para obtener, monitorear y controlar la disponibilidad de los servicios de información",0.,0.,1.			1
21	4.4	Plan pre-establecido para la conversión de datos de un antiguo sistema,0.,0.,1.			1
56	7.11	Plataforma centralizada con instalaciones de comunicaciones rápidas y seguras que manejen los incidentes de seguridad computacional. Establecimiento de responsabilidades de funcionarios para el manejo de incidentes que aseguren una respuesta efectiva,0.,0.,1.			1
81	11.2	Problemas identificados son resueltos de la forma más oportuna y eficiente,0.,0.,1.			1

26	5.3	Procedimiento que asegure el monitoreo del desempeño de los recursos de tecnología información y que las excepciones sean reportadas en forma oportuna y completa,0.,0.,1.			1
106	12.24	Procedimientos apropiados para que aseguren la integridad y autenticidad para transacciones electrónicas sensibles,0.,0.,1.			1
86	12.4	Procedimientos apropiados que aseguren que la entrada de datos es llevada a cabo solo por personal autorizado,0.,0.,1.			1
84	12.2	Procedimientos de manejo de errores, de ser así, estos aseguran que los errores y las irregularidades puedan ser detectados, corregidos y reportados",0.,0.,1.			1
102	12.20	Procedimientos de respaldo incluyen el almacenamiento apropiado para el archivo de los datos y de la documentación relacionada dentro y fuera de las instalaciones,0.,0.,1.			1
91	12.9	Procedimientos establecidos que permitan el manejo y la retención de los datos de salida de los programas de aplicación,0.,0.,1.			1
96	12.14	Procedimientos para el almacenamiento de datos que consideren requerimientos de recuperación, economía y políticas de seguridad",0.,0.,1.			1
99	12.17	Procedimientos para establecer protección a la librería de medios magnéticos,0.,0.,1.			1
30	5.7	Procedimientos para la revisión del hardware que asegure una capacidad justificable económicamente para procesar las cargas de trabajo,0.,0.,1.			1
73	9.5	Procedimientos que aseguren el reporte adecuado de las preguntas de los usuarios y su solución,0.,0.,1.			1
85	12.3	Procedimientos que aseguren que la entidad pueda retener o reproducir los documentos fuente originales durante un tiempo razonable,0.,0.,1.			1
66	8.1	Procedimientos que permitan identificar y documentar las necesidades de entrenamiento de personal que hace uso de los servicios de información,0.,0.,1.			1
72	9.4	Procedimientos que permitan monitorear las preguntas planteadas por los usuarios,0.,0.,1.			1
36	6.4	Procedimientos y guías que minimicen los requerimientos de continuidad con respecto a personal, instalaciones, hardware, software, equipo, formatos materiales de consumo y mobiliario",0.,0.,1.			1
117	15.2	Reporte y conservación de toda la información relacionada con los errores, inconsistencias o excepciones",0.,0.,1.			1
47	7.2	Restricción del acceso lógico y el uso de los recursos a través de un mecanismo de autenticación de los usuarios y de recursos asociados con las reglas de acceso,0.,0.,1.			1

23	4.6	Revisión de los requerimientos del sistema operativo que aseguren las necesidades del usuario,0.,0.,1.			1
77	10.4	Revisión en forma periódica la existencia de software no autorizado en las computadoras de la entidad,0.,0.,1.			1
64	7.19	Se cuenta con sistemas firewall para conexiones a Internet,0.,0.,1.			1
109	13.2	Se mantiene un bajo perfil de las instalaciones relacionadas con TI,0.,0.,1.			1
79	10.6	Software de la organización se encuentra debidamente etiquetado, inventariado y con las respectivas licencias?. Se han realizado pruebas de auditoría al respecto",0.,0.,1.			1
105	12.23	Verificación de la autenticidad e integridad de la información sobre la información electrónica que se origina externamente,0.,0.,1.			1
107	12.25	Verificación periódica de la integridad y lo adecuado de los datos mantenidos en archivos y otros medios magnéticos,0.,0.,1.			1
		TOTAL			**66**

- **EXTRACCIÓN CONTROLES MARCADOS SI**

  Archivo exportado hasta EXCEL

UNIDAD	CONTROL	OBJETIVO	N/A	SI	N
22	4.5	Constancia por escrito en la que indique que el producto está completo		1	
90	12.8	Procedimientos de manejo de errores que permitan la identificación de las transacciones erróneas sin que estas sean aun procesadas y sin interrumpir el procesamiento normal		1	
83	12.1	Procedimientos de preparación de datos a ser seguidos por los usuarios a fin de minimizar los errores u omisiones, que aseguren que los errores e irregularidades sean detectados, reportados y corregidos		1	
76	10.3	Procedimientos establecidos aseguran que la existencia y consistencia del registro de la configuración sean revisados en forma periódica		1	
95	12.13	Procedimientos establecidos que impidan la divulgación indebida o desecho de información delicada de la entidad		1	

89	12.7	Procedimientos para el procesamiento de datos que aseguren una adecuada división de funciones y que el trabajo sea verificado en forma rutinaria		1	
88	12.6	Procedimientos para la corrección y reenvío de datos que hayan sido capturados en forma errónea		1	
92	12.10	Procedimientos por escrito para comunicar la distribución de datos de salida		1	
93	12.11	Procedimientos que aseguren la precisión de los reportes de los datos de salida sean revisadas por los usuarios		1	
98	12.16	Procedimientos que aseguren un inventario sistemático del contenido de la librería de medios magnéticos		1	
9	2.2	Programación de mantenimiento rutinario del hardware para reducir los riesgos de falla		1	
110	13.3	Se acompaña a las personas que no forman parte de la empresa, cuando estas entran a las instalaciones		1	
		TOTAL		**12**	

- **EXTRACCIÓN CONTROLES MARCADOS NO APLICA**

Archivo exportado hasta Excel

UNIDAD	CONTROL	OBJETIVO	N/A	S	N
32	5.9	Consideración de contingencia, cargas de trabajo y planes almacenamiento en el aseguramiento de la capacidad requerida	1		
34	6.2	Consistencia del plan de continuidad con el plan de la entidad y toma en consideración el plan a mediano y largo plazo que asegure su consistencia	1		
13	2.6	Control de los cambios del software de acuerdo con los procesos de cambio de la entidad	1		

54	7.9	Controles para asegurar que la identificación y los derechos de acceso de los usuarios estén establecidos y administrados de forma única y centralizada	1		
29	5.6	Controles que aseguren la preparación de pronósticos de carga de trabajo que permitan identificar tendencias y proporcionar la información necesaria para el plan de capacidad	1		
53	7.8	Decisión explícita del dueño de los datos para asegurar que todos los datos se encuentren clasificados en términos de sensitividad de acuerdo con un esquema de clasificación	1		
67	8.2	Definición de grupos, objetivos, entrenadores de las sesiones de entrenamiento de acuerdo a las necesidades establecidas	1		
17	3.4	Desarrollo de materiales de capacitación de los sistemas desarrollados	1		
42	6.10	El plan de continuidad identifica los programas de aplicación, servicio de terceros, sistemas operativos, personal, insumos, archivos críticos así como los tiempos necesarios para la recuperación después de un desastre	1		
2	1.2	Enfoque de evaluación de riesgos considera ámbitos, metodologías, responsabilidades y habilidades requeridas	1		
3	1.3	Enfoque de evaluación enfocado en bienes, amenazas y puntos vulnerables.	1		
18	4.1	Entrenamiento debido a los usuarios y al personal de acuerdo a un plan definido	1		
45	6.13	Establecimiento de procedimientos para evaluar un plan de continuidad y su actualización, después de un desastre ocurrido	1		
49	7.4	Establecimiento de procedimientos que aseguren acciones oportunas relacionadas con los requerimientos de cuentas de usuario. Procedimiento formal que indique el propietario de los datos o del sistema que otorga privilegios de acceso	1		
24	5.1	Identificación y conversión en requerimientos y términos de disponibilidad, el desempeño y la disponibilidad de TI	1		
20	4.3	Implementación de los planes, que se relaciona con la preparación del sitio, adquisición e instalación de equipos, entrenamiento a usuarios, se han preparado revisando y aprobando las partes relevantes	1		
31	5.8	Implementación de mecanismos de tolerancia de fallas, de asignación equitativa de recursos y definición de prioridades, para el uso adecuado de los recursos	1		
52	7.7	La administración de seguridad tiene asegurado la actividad de control para que una inminente violación de seguridad sea notificada inmediatamente al administrador y que las acciones subsecuentes sean consideradas en forma automática	1		

43	6.11	La metodología de continuidad, incluye la identificación de alternativas relativas al centro de cómputo y al hardware de respaldo así como una selección de alternativa final, existencia de contrato formal para este tipo de servicios	1		
46	7.1	La seguridad de tecnología de información es administrada considerando los elementos que aseguren una adecuada seguridad	1		
61	7.16	Las políticas de la entidad, aseguran que la información de transacciones confidenciales es enviada por canales seguros	1		
60	7.15	Las políticas de la entidad, incluyen controles que no permitan que las transacciones pueda ser negadas por ninguna de las partes, por ejemplo a través de firmas digitales y registros de tiempos	1		
114	14.2	Los servicios proporcionados a los usuarios son comparados con los objetivos	1		
41	6.9	Los usuarios cuentan con procedimientos alternativos en caso de emergencias o desastres	1		
39	6.7	Metodología de continuidad para desastres, incluye sesiones de entrenamiento regulares	1		
68	8.3	Personal capacitado y entrenado en los principios de seguridad de sistemas	1		
38	6.6	Plan de continuidad es evaluado en forma regular con base a un plan de acción de acuerdo a los resultados reportados	1		
40	6.8	Plan de continuidad está distribuido solo entre el personal autorizado y cuenta con las seguridades respectivas para evitar su divulgación	1		
16	3.3	Preparación y mantenimiento actualizado los manuales de operaciones	1		
15	3.2	Preparación y mantenimiento actualizado los manuales de procedimientos de los usuarios	1		
37	6.5	Procedimientos de control de cambios que aseguren la actualización del plan de continuidad con requerimientos actuales	1		
74	10.1	Procedimientos que aseguren el registro único de los elementos de la configuración autorizados e identificables en el inventario al momento de la adquisición	1		
101	12.19	Procedimientos que aseguren que los respaldos se realicen de acuerdo con la estrategia de respaldos definida y que su utilidad sea verificada regularmente	1		
70	9.2	Procedimientos que aseguren que todas las preguntas de los usuarios sean registradas por el grupo de ayuda	1		

50	7.5	Proceso de control establecido para revisar y confirmar periódicamente los derechos de accesos	1		
28	5.5	Proceso establecido si incluye la capacidad de pronóstico que permita que los problemas se solucionen antes de que afecten al sistema	1		
65	7.20	Protección consistente a la integridad de todas las tarjetas que son utilizadas para autenticación o almacenamiento de información financiera u otra información sensitiva	1		
57	7.12	Realización en forma periódica una reacreditación de seguridad, para conservar al día el nivel de seguridad	1		
69	9.1	Soporte para usuarios para que interactúen con el personal de manejo de problemas	1		
55	7.10	Todas las actividades de seguridad se encuentran reportadas y revisadas apropiadamente en forma regular para identificar actividades no autorizadas	1		
		TOTAL	**40**		

ANEXO 10

ANTEPROYECTO DE TESIS

Universidad Técnica Particular de Loja

ESCUELA DE CIENCIAS DE LA COMPUTACIÓN

MODALIDAD ABIERTA Y A DISTANCIA

Guía para elaboración de Propuestas de Proyectos de Tesis

Información General del Proyecto

Título del proyecto:	DISEÑO DE UNA GUÍA DE AUDITORÍA PARA EVALUAR EL CONTROL INTERNO INFORMÁTICO	
Duración:	SEIS MESES	
Propuesto por:	Nombre de tesista:	MIREYA ALEXANDRA HERRERA ORTIZ
	Docente Investigador:	ING. DIANA CUENCA
	Línea de Investigación:	AUDITORIA INFORMÁTICA

Propósito / Descripción

Elaborar una herramienta que permita a los auditores informáticos evaluar las debilidades de control interno, que podrían afectar a los diferentes procesos de la tecnología de la información en una organización, considerando los estándares de seguridades y controles como buenas prácticas, así como, basado en una estructura de relaciones y procesos que dirige y controla a la empresa para lograr sus objetivos.

La investigación va a ser llevada a cabo en la empresa HASOFINAD, cuyo ámbito del negocio es el de prestación de servicios de consultoría.

El alcance del trabajo a realizar va a estar orientado a la evaluación del control del ambiente informático, lo cual va a permitir contar con los elementos suficientes que faciliten proceder a la elaboración del "Diseño de la Guía de Auditoría para Evaluar el Control Interno Informático", bajo la estructura de los componentes planteados a continuación:

Componentes:

I. **Consideraciones acerca de la evaluación de control interno en sistemas computarizados de información:** El procesamiento computarizado somete uniformemente todas las transacciones similares a las mismas instrucciones de procesamiento, sin embargo, la posibilidad de errores, como un riesgo de los datos ingresados al computador para procesamiento, pueden tener errores o ser incompletos. La guía contendrá las características diferenciales de los sistemas de control interno informático.

II. **Evaluación de los controles generales y de aplicación:** Su importancia radica en el tratamiento de un ambiente de control adecuado, fundamentado en la actitud asumida con respecto al control interno por todos los funcionarios de una organización, así como de la Dirección Superior, y el personal informático. Se definirán los procedimientos de cumplimiento de las normas éticas, de seguridad y de control interno.

III. **Desarrollo de una base de información:** El proceso de una evaluación de control interno comienza con el conocimiento de la estructura global de toda la organización, partes del negocio, sistemas de transacciones, u otros componentes que deban ser evaluados. Una parte importante de este proceso consistirá en obtener una comprensión global del Sistema de Información Computarizado de una organización. En este contexto, los sistemas de control interno serán considerados globalmente, incluyendo los siguientes aspectos: (1) estructura y administración del sistema y (2) hardware, software, y métodos de comunicaciones de datos utilizados.

IV. **Consideraciones de riesgo:** Se considerará las características especiales de los sistemas computarizados y sus riesgos asociados. El análisis específico de la implantación de los controles y la evaluación de su funcionamiento.

V. **Pruebas de Controles:** Se incluirá los procedimientos de evaluación a los procesos informáticos considerando la segregación de tareas en ambientes informáticos, controles de acceso a los programas, así como de los datos de ingreso, procesamiento y salida.

VI. **Aplicación del modelo COBIT:** COBIT fue desarrollado como un estándar para las buenas prácticas de

seguridad y control en tecnología de información, este modelo será utilizado para evaluar los riesgos existentes, a través de los 34 objetivos de control de alto nivel de este modelo y operar a un nivel superior a los estándares de tecnología para la administración de los sistemas de información.

VII. **Seguimiento de recomendaciones:** Las Recomendaciones son acciones correctivas que se presentan en los informes de auditoria o en informes especiales de carácter preventivo, como producto de las deficiencias encontradas en la evaluación del control interno en ambientes informáticos y son dirigidas a las autoridades competentes que tienen la facultad de implementarlas. La tesis presentará como una actividad de retroalimentación el seguimiento de las recomendaciones planteadas a fin de conocer la efectividad de su implementación.

Una vez concluida la Guía de Auditoría, esta será aplicada en la evaluación del ambiente de control interno informático en la empresa, considerando además en lo pertinente, los estándares de ISACA ((Information Systems Audit and Control Association) que contienen principios básicos y procedimientos esenciales de auditoría, que el auditor de Sistemas Informáticos debe tener en cuenta durante el proceso de auditoría, y que son los siguientes:

"Estándar 03 El auditor de SI debe revisar y evaluar si la función de SI está alineada con la misión, visión, valores, objetivos y estrategias de la organización.

04 El auditor de SI debe revisar si la función de SI tiene una declaración clara en cuanto al desempeño esperado por la empresa (eficacia y eficiencia) y evaluar su cumplimiento.

05 El auditor de SI debe revisar y evaluar la eficacia de los recursos de SI y el desempeño de los procesos administrativos.

06 El auditor de SI debe revisar y evaluar el cumplimiento de los requisitos legales, ambientales y de calidad de la información, así como de los requisitos fiduciarios y de seguridad.

07 El auditor de SI debe utilizar un enfoque basado en riesgos para evaluar la función de SI.

08 El auditor de SI debe revisar y evaluar el ambiente de control de la organización.

09 El auditor de SI debe revisar y evaluar los riesgos que pueden afectar de manera adversa el entorno de SI."

Estrategia o Metodología de desarrollo (Opcional)

- **ESTRUCTURAL.-** El Proyecto incluirá el desarrollo de la investigación de los contenidos relacionados con los componentes, utilizando un análisis estructural que defina las relaciones recíprocas de las partes de un todo, concerniente a lo que es un trabajo de evaluación de control interno en tecnología de información.

- **DESCRIPTIVO.-** Permitirá detallar, especificar los hechos originados en la ejecución y control. Permite sacar conclusiones válidas para la investigación.

- **ANALITICO.**- Examinará la ejecución y control y especialmente la incidencia de los mecanismos de control. Permite reconocer la eficiencia eficacia.

Resultados esperados

Presentar un diseño estándar para la realización de una guía de auditoría para evaluar el control interno informático en las organizaciones.

Cronograma

Componente	Tiempo
I. Consideraciones acerca de la evaluación de control interno en sistemas computarizados de información	30 días
II. Evaluación de los controles generales y de aplicación	30 días
III. Desarrollo de una base de información	20 días
IV. Consideraciones de riesgo	30 días
V. Pruebas de controles	30 días
VI. Aplicación del modelo COBIT	30 días
VII. Seguimiento de recomendaciones	10 dias

Bibliografía / Recursos

COBIT, (Control Objetives for Information and related Tecnology. Gobierno, Control y Revisión de la Información y Tecnologías Relacionadas). Marco Referencial.

PIATTINI VELTHUIS, Mario G.; DEL PESO NAVARRO, Emilio. Editorial RA-MA. “Auditoría Informática. Un enfoque práctico”. 1998.

ALVAREZ MARAÑÓN, Gonzalo; PÉREZ GARCÍA, Pedro. Editorial Mc. Graw Hill. “Seguridad Informática para empresas y particulares”. 2004.

GUIAS DE AUDITORIA, Price Waterhouse, 1993

RECURSOS: Internet

ANEXO 11

APROBACIÓN ANTEPROYECTO DE TESIS Y DESIGNACIÓN DIRECTORES DE TESIS

Of. 173 DIIMA-UTPL
Loja, julio 14 de 2009

Ing. Diana Cuenca B., (directora) dccuenca@utpl.edu.ec
Ing. Francisco Álvarez P., (codirector) fjalvarez@utpl.edu.ec
DOCENTES DE LA UNIVERSIDAD
Presente.-

De mi consideración:

Me permito comunicarles que luego de revisar el proyecto de tesis ***"Diseño de una guía de auditoría para evaluar el control interno informático****" presentado por la Sra. Mireya Alexandra Herrera Ortiz, del centro de Quito, designé a ustedes directora y codirector de tesis, respectivamente.*

Cabe indicar que la dirección implica, asesorar, monitorear y dirigir el trabajo de investigación planteado hasta su culminación, tomando en cuenta el plazo establecido en el cronograma de actividades, que rige a partir de la presente fecha.

Además, el (a) estudiante deberá cancelar la cantidad de $125,00 (ciento veinticinco 00/100 dólares) por concepto de inscripción del proyecto de tesis.

Al augurarles el mejor de los éxitos en la dirección y codirección de este importante trabajo de investigación que va en beneficio de la juventud estudiosa de nuestra Alma Mater, hago propicia la oportunidad para expresarles mi consideración y estima.

Atentamente,
DIOS, PATRIA Y CULTURA

Ing. Nelson Piedra Pullaguari
DIRECTOR DE LA ESCUELA DE
CIENCIAS DE LA COMPUTACIÒN

c.c Sra. Alexandra Herrera alexandrah67@hotmail.com

Lidia V.

ANEXO 12

CERTIFICACIÓN HASOFINAD

HASOFINAD Consultoría, Informática y Auditoría

Calle de la Begonias # 91
Urb. La Primavera
QUITO - ECUADOR

Teléfonos: 1700HASOFINAD
093146799

Quito, 26 de febrero del 2010

Srta.
Alexandra Herrera
AUDITORA
Presente

Por medio del presente quiero agradecer a usted el trabajo realizado en la Firma de mi representación, relacionado con la Evaluación del Sistema de Control Informático de HASOFINAD.

Los resultados de la evaluación practicada, así como, sus recomendaciones, serán tomados muy en cuenta en el desarrollo de nuestras actividades, para fortalecer los controles y seguridades determinados con algún grado de riesgo e identificados durante su examen.

Atentamente,

Ing. Marco Herrera Balarezo
PRESIDENTE DE HASOFINAD

BIBLIOGRAFÍA

[1] ISACA. (2009, Julio): "The COBIT Framework". Formato PDF. Disponible para descarga en:
http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/CobiT4_Espanol.pdf

[2] NET.CONSULT. (2009, Julio). "Nuevos conceptos del Control Interno: Informe COSO". Formato HTM. Disponible en:
http://www.netconsul.com/tecnicas/index.php?ver=coso

[3] PIATTINI, Mario G., DEL PESO, Emilio. (Julio, 2009). "AUDITORÍA INFORMÁTICA. UN ENFOQUE PRÁCTICO". Capítulo 2:
Control Interno y Auditoría Informática. Editorial Alfaomega-RAMA.

[4] ISACA. (2009, Julio). "COBIT 4.1- Marcos de Trabajo, Objetivos de Control, Directrices Generales, Modelos de Madurez". Formato PDF. Disponible para descarga en:
http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders1/COBIT6/Obtain_COBIT/Obtain_COBIT.htm

[5] MONOGRAFIAS. Com. (Julio, 2009). "CONTROL INTERNO - INFORME COSO". Marco integrado de control. Formato STHML. Disponible en:
http://www.monografias.com/trabajos12/coso/coso2.shtml#coso

[6] COSO.org. (2009, Julio). "Enterprise Risk Management-Integrated Framework". Formato PDF. Disponible en inglés en :
http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf

[7] CASAS HERNÁNDEZ, Estela. (Agosto, 2009). "IMPORTANCIA DE LA EVALUACIÓN DEL CONTROL INTERNO". Formato PDF. Disponible para descarga en:
http://www.somece.org.mx/simposio06/memorias/autor/files/3_CasasHernandezEstela%20et%20al.pdf

[8] WIKIPEDIA. (2009, Agosto). "Sistemas de Información". Formato HTM. Disponible en:
http://es.wikipedia.org/wiki/Sistema_de_informacion

[9] PC MAGAZINE ENCICLOPEDY. (2009, Agosto). Definición de total batch. Formato HTM. Disponible en:
http://www.pcmag.com/encyclopedia_term/0,2542,t=batch+total&i=38466,00.asp

[10] PC MAGAZINE ENCICLOPEDY. (2009, Agosto). Definición de total hash. Formato HTM. Disponible en:
http://www.pcmag.com/encyclopedia_term/0%2C2542%2Ct%3Dhash+total&i%3D44130%2C00.asp

[11] GOOGLE LIBROS. (2009, Agosto). "Los nuevos conceptos del Control Interno: El Informe COSO". Formato Libro Electrónico. Disponible en:
http://books.google.com.ec/books?id=335uGf3nusoC&pg=PA311&lpg=PA311&dq=control+a+la+modificación+de+sistemas+y+programas&source=bl&ots=ZpFycBdNH6&sig=zkf2-XdA3vTbq8rdUVv1IL0Sc-4&hl=es&ei=8YaESsqvOtmfmAei7NWDAw&sa=X&oi=book_result&ct=result#v=onepage&q=&f=false

[12] ISACA. (2009, Agosto). CURSO CISA 2005. "Capítulo 1. El proceso de Auditoría de SI". Formato PDF. Disponible en:
http://portal.funcionpublica.gob.mx:8080/wb3/work/sites/SFP/resources/LocalContent/34/2/Capitulo_1_CISA_SFP._pdf

[13] ISACA. (2009, Septiembre). COBIT 4.1. "Recursos de TI". Formato PDF. Disponible para descarga en:
http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/CobiT4_Espanol.pdf

[14] COMERCIOMEXICO.COM. (2009, Septiembre). "Qué es el Outsourcing?". Formato HTML. Disponible en:
http://www.comerciomexico.com/notas/outsourcing.html

Concepto de Outsourcing: Outsourcing es el proceso en el cual una firma identifica una porción de su proceso de negocio que podría ser desempeñada más eficientemente y/o más efectivamente por otra corporación, la cual es contratada para desarrollar esa porción de negocio. Esto libera a la primera organización para enfocarse en la parte o función central de su negocio. Es decir, el outsoucing consiste en que una empresa contrata, a una agencia o firma externa especializada, para hacer algo en lo que no se especializa.

[15] JAN'S ILLUSTRATED. COMPUTER LITERACY 101. (2009, Septiembre) FUNDAMENTOS DE COMPUTACIÓN.

"Concepto de programas utilitarios del software de sistema". Formato HTM. Disponible en: http://www.jegsworks.com/lessons-sp/lesson8/lesson8-4.htm.

Concepto de Programas Utilitarios: Ejecutan tareas relacionadas con el mantenimiento de la salud de su computadora - hardware o datos. Algunos se incluyen con el sistema operativo. Estos programas son: Administrador de discos, backup, recuperación de datos, compresión de datos, administrador de archivos.

[16] MITECNOLOGICO. (2009, Septiembre). "Concepto de Recurso Computacional". Formato HTM. Disponible en: http://www.mitecnologico.com/Main/ElRecursoComputacionalSistemasDeInformacion

Concepto de Recurso Computacional: Se entiende como "Recurso Computacional" todo el equipamiento computacional y equipamiento de comunicaciones. En otras palabras, comprende equipamientos como: computador, accesorios del computador, cables de red, equipos de comunicaciones de red y servidores, entre otros. Se asume que tanto la información (contenido) como los recursos accesibles a través de la red son de carácter privado y de propiedad exclusiva de sus dueños, quienes determinan las modalidades de acceso de los mismos.

[17] SIALIER ZAMORA LUIS ALBERTO. (2009, Septiembre). AUDITORÍA DE SISTEMAS. "Revisión de seguridad de sistemas. Concepto de caminos lógicos". Formato HTM. Disponible en: http://www.geocities.com/lsialer/areas3.htm

Caminos lógicos: Las rutas de acceso son caminos lógicos de acceso a información computarizada, estas empiezan generalmente con un terminal y terminan con los datos accesados. A lo largo de este camino existen componentes de hardware y software. Conocer esta ruta es importante porque permite al auditor de sistemas, determinar puntos de seguridad física y lógica, la secuencia típica de estos caminos lógicos es:

1. Terminales: Son usados por el usuario final para identificarse, estos deben tener restricción física de su uso y la identificación de los usuarios o "login" de accesos debe ser controlada con los "passwords" o claves.
2. El software de telecomunicaciones: El software de telecomunicaciones es usado para dar o limitar el acceso a aplicaciones o datos específicos.
3. El software de procesamiento de transacciones: Este software utiliza la identificación del usuario realizada en los terminales (User-Id) y asigna niveles y posibilidades de transacción (añadir, modificar, eliminar, obtener reportes, etc.) en una aplicación determinada basado en archivos o tablas de usuario definidas y solo disponibles al administrador de seguridad.
4. El software de aplicación: El software de aplicación tiene la lógica del procesamiento de los datos definida, esta lógica debe permanecer según las necesidades determinadas por la gerencia, para esto se debe proteger el acceso a los programas que regulan la lógica de estos procesos.
5. El software de administración de base de datos: Por el medio del cual se accesa directamente a la información, este debe tener la definición de los campos de datos y su ejecución debe estar restringido al personal de administración de la base de datos.

[18] WIKIPEDIA. (2009, Septiembre). SISTEMA DE GESTIÓN DE BASE DE DATOS. "Definición d DBSM". Formato HTM. Disponible en: http://es.wikipedia.org/wiki/DBMS

Concepto de sistemas de gestión de base de datos (SGBD); (en inglés: **D**ata**B**ase **M**anagement **S**ystem, abreviado **DBMS**) son un tipo de software muy específico, dedicado a servir de interfaz entre la base de datos, el usuario y las aplicaciones que la utilizan.

[19] WIKIPEDIA. (2009, Septiembre). DICCIONARIO DE DATOS. "Significado de diccionario de datos". Formato HTM. Disponible en:http://es.wikipedia.org/wiki/Diccionario_de_datos

Concepto de diccionario de datos: Un diccionario de datos es un conjunto de metadatos que contiene las características lógicas y puntuales de los datos que se van a utilizar en el sistema que se programa, incluyendo nombre, descripción, alias, contenido y organización. Estos diccionarios se desarrollan durante el análisis de flujo de datos y ayuda a los analistas que participan en la determinación de los requerimientos del sistema, su contenido también se emplea durante el diseño del proyecto. Identifica los procesos donde se emplean los datos y los sitios donde se necesita el acceso inmediato a la información, se desarrolla durante el análisis de flujo de datos y auxilia a los analistas que participan en la determinación de los requerimientos del sistema, su contenido también se emplea durante el diseño.

En un diccionario de datos se encuentra la lista de todos los elementos que forman parte del flujo de datos de todo el sistema. Los elementos más importantes son flujos de datos, almacenes de datos y procesos. El diccionario de datos guarda los detalles y descripción de todos estos elementos.

[20] CARLOSPES.COM. (2009, Septiembre). MINI DICCIONARIO DE DATOS DE CARLOS PES. "Software de red.

Definición". Formato HTM. Disponible en:
http://www.carlospes.com/minidiccionario/software_de_red.php

Definición de software de red: En el software de red se incluyen programas relacionados con la interconexión de equipos informáticos, es decir, programas necesarios para que las redes de computadoras funcionen. Entre otras cosas, los programas de red hacen posible la comunicación entre las computadoras, permiten compartir recursos (software y hardware) y ayudan a controlar la seguridad de dichos recursos.

[21] ISACA. (2009, Septiembre). COBIT 4.1. "MARCO DE TRABAJO COBIT. Controles Generales y de Aplicación". Formato PDF. Disponible para descarga en:
http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/CobiT4_Espanol.pdf

[22] MERCADOTENDENCIAS. (2009, Septiembre). LAS NUEVAS TENDENCIAS DEL CONTROL INTERNO. INFORME COSO. "Actividades de control". Formato HTM. Disponible en:
http://www.mercadotendencias.com/informe-coso-actividades-de-control/

[23] SAP-ABAP. (2009, Septiembre). "BATCH INPUT- Concepto". Formato PHP. Disponible en:
http://sap4.com/wiki/index.php?title=Batch-Input

Definición Bathc Input: Un Batch-Input no es más que un proceso automático de llenado de las pantallas. Cuando alguien nos habla de Bacth-Input se puede estar refiriendo a un fichero plain-text que necesita para que un programa standard (o propio) recoja dicha información, o un programa que simula el proceso de llenado de las pantallas como si el usuario estuviese delante. Así mismo, el juego de datos guarda mucha relación con el Batch-Input, ya que son lo datos que se van a llenar en las pantallas. Un batch input no es más que una forma automática de rellenar una pantalla. Es decir como si una persona picara los datos a mano, con lo que conlleva eso es decir validaciones que haga la pantalla.

[24] WIKIPEDIA. (2009, Septiembre). "LOG (registro). Concepto". Formato HTM. Disponible en:
http://es.wikipedia.org/wiki/Log_(registro)

Concepto de log: Un log es un registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué (who, what, when, where y why, W5) un evento ocurre para un dispositivo en particular o aplicación. La mayoría de los logs son almacenados o desplegados en el formato estándar, el cual es un conjunto de caracteres para dispositivos comunes y aplicaciones. De esta forma cada log generado por un dispositivo en particular puede ser leído y desplegado en otro diferente.
También se le considera cómo aquel mensaje que genera el programador de un sistema operativo, alguna aplicación o algún proceso, en virtud del cual se muestra un evento del sistema.

[25] ISACA. (2009, Septiembre). COBIT 4.1. "Adquirir y mantener infraestructura tecnológica. Objetivos de control." Formato PDF.
Disponible para descarga en:

http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/CobiT4_Espanol.pdf

[26] WEB DEL PROFESOR. (2009, Septiembre). "Pasos en un estudio de simulación. Corridas piloto." Formato PDF.

Disponible en:

http://docs.google.com/gview?a=v&q=cache:th-K7sf7IVEJ:webdelprofesor.ula.ve/ingenieria/hhoeger/simulacion/PARTE3.pdf+corridas+piloto&hl=es&gl=ec&sig=AFQjCNFimg95CqyP4kBuP5OCa4o8aeAoYQ

Corridas piloto: Estas corridas se hacen para validar el modelo verificado y lo veremos con más detalle mas adelante. Las corridas piloto pueden ser usadas para determinar la sensibilidad del modelo a pequeños cambios en los parámetros de entrada. Cambios importantes implican que una mejor estimación de estos parámetros debe ser obtenida.

[27] BITSIGNALS. (2009, Septiembre). "Ecoder. Editor de código on-line. Descripción." Formato HTM. Disponible en:

http://bitsignals.com/2009/05/31/ecoder-editor-de-codigo-online/

Descripción de un editor de código on-line: Aplicaciones Web que permiten editar código de casi cualquier lenguaje Web o de programación sin la necesidad de instalar alguna herramienta en la PC, enfocada hacia aquellos programadores que no tienen a la mano o no disponen de un IDE o editor de código, ya sea por no estar trabajando en sus propios equipos o bien por alguna razón relacionada.

[28] BLOG PEDRO DEL CASTILLO. (2009, Octubre). "Notas sobre conceptos básicos de aplicaciones Mainframe y Servidores centrales. Concepto de monitor teleproceso.". Formato PDF. Disponible en:
http://www.pdelcastillo.com/files/0108mfr.pdf
Concepto monitor teleproceso: Un monitor TP (teleproceso) ha sido concebido para gestionar procesos y coordinar

programas garantizando la integridad, la coherencia y la seguridad de las aplicaciones. Permite a los clientes o servicios arrancar aplicaciones mediante diferentes técnicas. Ofrece servicios que permiten gestionar el tráfico transaccional entre los clientes, las aplicaciones y los otros recursos, como pueden ser las bases de datos. Tiene funciones de administración, comunicación y repartición de la carga de trabajo, permitiendo así trasladar dinámicamente una parte sobre otro monitor presente en la red.

[29] SIGT.net. (2009, Octubre). "Seguridad en mainframe. Introducción al RACF". Formato XHTML. Disponible en:

http://sigt.net/archivo/seguridad-en-mainframe-introduccion-al-racf.xhtml

[30] CA. (Octubre, 2009). "Seguridad para mainframe. CA ACF2". Formato ASPX. Disponible en:

http://www.ca.com/ar/products/product.aspx?id=111

[31] WIKIPEDIA. (Octubre, 2009). "Software de administración de bases de datos". Formato HTM. Disponible en:

http://es.wikipedia.org/wiki/Software_de_administración_de_bases_de_datos

[32] INSTITUTO DE ESTUDIOS DOCUMENTALES SOBRE CIENCIA Y TECNOLOGÍA. (Octubre, 2009). "Archivos para definir una base de datos. Definición de Archivo Maestro". Formato HTM. Disponible en:
http://www.cindoc.csic.es/isis/01-3-2.htm

Archivo maestro: El archivo maestro contiene todos los registros de una determinada base de datos, cada uno de las cuales consiste en un conjunto de campos de longitud variable. Cada registro se identifica con un número único, asignado automáticamente al ser creado; este número se denomina: Número del archivo maestro o MFN (iniciales de Master File Number).

[33] ADMINISTRACIÓN DE SISTEMAS DE CÓMPUTO. (Octubre, 2009). "Control del procesamiento de la información. Controles de procesamiento de entrada". Formato HTM. Disponible en:

http://sistemas.itlp.edu.mx/tutoriales/admoncomp/tema42.htm

[34] ADMINISTRACIÓN DE SISTEMAS DE CÓMPUTO. (Octubre, 2009). "Control del procesamiento de la información. Controles de procesamiento de salida". Formato HTM. Disponible en:

http://sistemas.itlp.edu.mx/tutoriales/admoncomp/tema42.htm

[35] EL RINCÓN DEL VAGO. (Octubre, 2009). "Procesamiento de transacciones. Gestión del bloqueo." Formato HTML.

Disponible en: http://html.rincondelvago.com/procesamiento-de-transacciones.html

Gestión del Bloqueo: Si existe un conjunto de transacciones de manera que cada transacción esta esperando a que a otra transacción del conjunto diremos que se encuentra en estado de bloqueo.
Para evitar esta situación existe un protocolo de prevención de bloqueo para garantizar que el sistema nunca entrara en un estado de bloqueo.
Prevención de bloqueos: Existen varios esquemas para que se pueden utilizar para la prevención de bloqueos. El más sencillo es el que requiere que cada transacción bloquee todos sus daros antes de empezar a ejecutarse. Otro método es la de imponer un orden parcial de los datos y exigir que una transacción pueda bloquear un dato. Otro método es la expropiación donde se puede asignar una hora de entrada única a cada transacción.
Detección y recuperación de bloqueo: Si un esquema no utiliza algún protocolo que garantice la libertad de bloqueo, debe emplearse un esquema de detección y recuperación. Cada cierto tiempo se examina el estado del sistema para ver si existe algún bloqueo.

[36] OLEA ORG. (Octubre, 2009). "NORMAS, TÉCNICAS Y PROCEDIMIENTOS DE AUDITORÍA EN INFORMÁTICA. Concepto de datos de prueba". Formato HTML. Disponible en:

http://olea.org/~yuri/propuesta-implantacion-auditoria-informatica-organo-legislativo/ch03s03.html

Datos de prueba: Se emplea para verificar que los procedimientos de control incluidos los programas de una aplicación funcionen correctamente. Los datos de prueba consisten en la preparación de una serie de transacciones que contienen tanto datos correctos como datos erróneos predeterminados.

[37] MONOGRAFÍAS.COM. (Octubre, 2009). "CONTROL INTERNO. Pruebas de Cumplimiento". Formato HTML. Disponible en:

http://www.monografias.com/trabajos16/control-interno/control-interno.shtml#PRUEBAS

[38] MIRA NAVARRO, Juan Carlos. (Octubre, 2009). "APUNTES DE AUDITORÍA. Estudio y evaluación del Control Interno. Pruebas de cumplimiento." Formato HTM. Disponible en:

http://www.eumed.net/libros/2006a/jcmn/1e.htm

[39] UNIZAR.ES. (Noviembre, 2009). "MÉTODOS GENERALIZADOS DE ANÁLISIS DE RIESGOS. Análisis what´s if". Formato HTM. Disponible en:

http://www.unizar.es/guiar/1/Accident/An_riesgo/Met_gen.htm

Análisis what´s if: Consiste en el planteamiento de las posibles desviaciones en el diseño, construcción, modificaciones y operación de una determinada instalación industrial, utilizando la pregunta que da origen al nombre del procedimiento: "¿Qué pasaría si...?". Requiere un conocimiento básico del sistema y cierta disposición mental para combinar o sintetizar las desviaciones posibles, por lo que normalmente es necesaria la presencia de personal con amplia experiencia para poder llevarlo a cabo. El resultado es un listado de posibles escenarios o sucesos incidentales, sus consecuencias y las posibles soluciones para la reducción o eliminación del riesgo.

[40] ISACA. (Diciembre, 2009). "COBIT 4.1. Marco Referencial COBIT. Misión de COBIT". Formato PDF. Disponible para descarga en:

http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981

[41] REY, PATRICIO.E. (Diciembre, 2009). "COBIT. LA AUDITORÍA POR PRINCIPIOS DE CONTROL. Antecedentes". Formato PDF. Biblioteca personal.

[42] SOBRINOS SÁNCHEZ, ROBERTO. (Diciembre, 2009). "PLANIFICACIÓN Y GESTIÓN DE SISTEMAS DE INFORMACIÓN. The COBIT Framework. Desarrollo y componentes del COBIT". Fomato PDF. Bibioteca personal.

[43] ISACA. (2009, Julio). "COBIT 4.1- Resumen Ejecutivo". Formato PDF. Disponible para descarga en:

http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders1/COBIT6/Obtain_COBIT/Obtain_COBIT.htm

[44] ISACA. (2009, Julio). "COBIT 4.1- Marco Referencial". Formato PDF. Disponible para descarga en:

http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders1/COBIT6/Obtain_COBIT/Obtain_COBIT.htm

[45] ISACA. (2009, Julio). "COBIT 4.1- Objetivos de control". Formato PDF. Disponible para descarga en:

http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders1/COBIT6/Obtain_COBIT/Obtain_COBIT.htm

[46] CUENCA, Diana. (Enero, 2010). GUÍA AUDITORÍA INFORMÁTICA. "Auditoría de aplicaciones". Biblioteca particular.

[47] CUENCA, Diana. (Enero, 2010). GUÍA AUDITORÍA INFORMÁTICA. "Auditoría de aplicaciones". Biblioteca particular.