



ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

INSTITUTO DE CIENCIAS MATEMÁTICAS

PROYECTO DE GRADUACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

**“INGENIERIA EN AUDITORÍA Y CONTROL DE GESTIÓN
ESPECIALIZACIÓN SISTEMAS INFORMÁTICOS”**

TEMA

**“AUDITORÍA INFORMÁTICA A UNA INSTITUCIÓN DEL SECTOR
FINANCIERO AGENCIA GUAYAQUIL, PERÍODO 2008”**

AUTOR

CPA GEOVANNY GONZÁLEZ NARVÁEZ

Guayaquil- Ecuador

AÑO

2009

DEDICATORIA

A Dios

A Anita

A mis padres

A mis hermanos

A mis sobrinos

AGRADECIMIENTO

A Dios por darme salud, a mis padres por darme la oportunidad y el apoyo para poder estudiar, a mis hermanos por ser mi inspiración, a mis sobrinos por enseñarme lo hermosa que es la vida y a Anita por ser mi apoyo día a día.

DECLARACIÓN EXPRESA

La responsabilidad por los hechos y doctrinas expuestas en este Proyecto de Graduación, así como el Patrimonio Intelectual del mismo, corresponde exclusivamente al **ICM (Instituto de Ciencias Matemáticas)** de la Escuela Superior Politécnica del Litoral.

CPA Geovanny González N.

TRIBUNAL DE GRADUACIÓN

Ing. Pablo Álvarez
DELEGADO ICM

Msc. Omar Ruiz Barzola
DIRECTOR DE PROYECTO

Ing. Dalton Noboa
PRIMER VOCAL PRINCIPAL

FIRMA DEL AUTOR DEL PROYECTO DE GRADUACIÓN

**CPA GEOVANNY GONZÁLEZ NARVÁEZ
AUTOR DEL PROYECTO**

CONTENIDO

CAPITULO I

1. PLAN DE PROYECTO	01
1.1. Proyecto (introducción)	01
1.2. Problema	02
1.3. Propósito	03
1.4. Justificación	03
1.5. Objetivos generales	04
1.6. Objetivos específicos	04

CAPÍTULO II

2. MARCO DE REFERENCIA Y ANALISIS	06
2.1. La Institución	06
2.2. Marco de Referencia para la Auditoría Informática a la Institución Financiera Auditada	09
2.3 Metodología	09
2.3.1 Planeación de la Auditoría.	10
2.3.1.1 Origen de la Auditoria	10
2.3.1.2 Marco de Trabajo	11
2.3.1.3 Alcance	11
2.3.1.4 Desarrollo	12
2.3.1.5. Análisis Estadístico	16

CAPÍTULO III

3. DESARROLLO DE LA AUDITORIA INFORMATICA	18
3.1. Identificación de la Operatividad	18
3.1.1. Banca	19
3.1.2. Crédito y Cartera	23
3.1.3. Contabilidad	25
3.1.4. Sistemas	26
3.2. Planificación y Organización	28
3.3. Cumplimiento de Normas	29
3.4. Cumplimiento de Contratos	33
3.5. Cumplimiento de Política	33
3.6. Evaluación del Control Interno a la Institución	34
3.7. Desarrollo del Análisis Estadístico	36

CAPÍTULO IV

RESULTADOS

CAPÍTULO V

CONCLUSIONES RECOMENDACIONES Y CONTRIBUCIONES

BIBLIOGRAFÍA

ANEXOS

ÍNDICE DE TABLAS

Tabla # 1: Determinación de los sistemas por área a ser evaluada	18
Tabla # 2: Procesos y Transacciones de los Sistemas	20
Tabla # 3: Pruebas al Sistema de Crédito y Cartera	24
Tabla # 4: Observaciones encontradas al sistema de Contabilidad	26
Tabla # 5: Evaluación de los Sistemas por área	29
Tabla # 6: Evaluación del Cableado Estructurado	31
Tabla # 7: Inventario de Licencias de Software	32
Tabla # 8: Contratos Elaborados en el Año 2008	33
Tabla # 9: Inventario de Manuales y Política	34
Tabla # 10: Evaluación Control Interno	35
Tabla # 11: Calificaciones para evaluación del Control Interno	35
Tabla # 12: Tablas Cruzadas Tiempo que trabaja en la institución Financiera VS: El sistema que utiliza es fácil de usar	36
Tabla # 13: Tabla Chi – Cuadrado variable Tiempo que trabaja en la institución Financiera VS: El sistema que utiliza es fácil de usar	37
Tabla # 14: Tablas Cruzadas Edad VS. El Se encuentra conforme con el sistema con que se trabaja en su departamento	38
Tabla # 15: Tabla Chi – Cuadrado variable Edad VS. El Se encuentra conforme con el sistema con que se trabaja en su departamento	39
Tabla # 16: Tablas Cruzadas Variable Tiempo que trabaja en la Institución Financiera VS. Cree usted que es necesario implementar un nuevo Sistema Informático (Core Bancario)	40
Tabla # 17: Tabla Chi – Cuadrado variable Tiempo que trabaja en la Institución Financiera VS. Cree usted que es necesario implementar un nuevo Sistema Informático (Core Bancario)	40

INDICE DE FIGURAS

Figura 1. Organigrama institucional de la Institución a Auditar	08
Figura 2. Marco de Trabajo de la COBIT 4.0	11
Figura 3. Diagrama de procesos de Área de Banca	19
Figura 4. Diagrama de Proporción de repuestas afirmativas	21
Figura 5. Diagrama de Pastel de la proporción de respuestas negativas	22
Figura 6. Diagrama de procesos de Área Crédito y Cartera	23
Figura 7. Diagrama de procesos de Área de Contabilidad	25
Figura 8. Diagrama de procesos de Área de Sistemas	26
Figura 9. Diagrama de casos resueltos VS. No resueltos	27
Figura 10. Diagrama de Red de la Institución	30

CAPÍTULO I

1. PLAN DE PROYECTO

1.1. Proyecto (introducción)

La auditoría informática es la revisión y evaluación de los controles implementados en los sistemas y equipos de procesamiento. Incluye el análisis de los mismos en términos de eficacia, eficiencia y seguridad, a fin de lograr el tratamiento más adecuado y seguro de la información.

La auditoría informática, es importante para el buen desempeño de los sistemas de información, ya que asegura que se mejoren los controles necesarios para que los sistemas sean confiables y posean un buen nivel de seguridad.

El alcance de la auditoría define los límites de la misma, por ello debe existir un acuerdo muy preciso entre auditores y clientes sobre las funciones y sistemas a auditar; como así también se debe acordar la evaluación del cumplimiento de las leyes, normativas y/o estándares aplicables a la organización o entidad auditada.

El proceso de auditoría implica que el auditor realice relevamientos, ejecute pruebas, analice datos, reúna evidencias y finalmente evalúe las fortalezas y debilidades de los controles existentes.

Luego como producto final del trabajo realizado, el auditor redacta un informe para la Gerencia y/o Dirección incluyendo sus observaciones y recomendaciones

1.2. Problema

La Ley General de Instituciones del Sistema Financiero, en su Capítulo 2 desde el artículo 84 al 87, señala, que como medida de control las instituciones del sistema financiero están obligadas a someterse a auditorías internas y externas; las auditorías externas deben ser realizadas por la Superintendencia de Bancos y Seguros y por firmas auditoras independientes certificadas por la misma Superintendencia de Bancos como requisito obligatorio.

Dado que la tendencia en el manejo y procesamiento de la información ha pasado de métodos manuales a electrónicos, la auditoría informática más que un apoyo, es una necesidad al momento de realizar auditoría a los sistemas financieros, por la cantidad de procesos e información que se maneja en medios electrónico.

Debido a que el cambio de manejo y almacenamiento de la información ha evolucionado, el riesgo y la tendencia a fraudes se ha incrementado, es por eso que es necesario mantener un control permanente y actualizado de las medidas de seguridad que sean implementadas para los procesos informáticos en las empresas para reducir el grado de impacto de eventos fortuitos que puedan detener la actividad de la empresa.

Por las causas descritas anteriormente, principalmente por disposición de la Superintendencia de Bancos y Seguros, se Auditará la Institución Financiera en el periodo 2008 para establecer la razonabilidad de los Estados Financieros y dado que la información de esta se maneja electrónicamente, se Elaborará la Auditoría Informática a las áreas más sensibles donde se genera y opera la información del giro del negocio.

- Banca
- Crédito y Cartera
- Contabilidad
- Sistemas

1.3. Propósito

El propósito de este proyecto es analizar y evaluar los procesos, sistemas y medios de manejo de la información, Su grado de confidencialidad, disponibilidad y credibilidad de la institución financiera.

1.4. Justificación

La información hoy en día se ha convertido en un activo de gran importancia para una empresa, la misma que se la puede encontrar impresa, escrita en, almacenada electrónicamente o (lo que es mucho peor) abandonada en ciertas oficinas destinadas, supuestamente, a la “reserva” de la misma. Además, la información se muestra en filmes, grabaciones o directamente mediante el lenguaje oral (conversacional) [6]. Y se transmite por diferentes

medios (sean éstos, convencionales -analógicos- o de última generación -digitales-).

Independientemente del carácter que adopte, se recopile o se comparta, la información y los dispositivos y equipamiento asociados, deben ser protegidos adecuada y eficazmente, garantizándose la disponibilidad, integridad y confidencialidad de la misma.

1.5. Objetivos generales

Revisar y Evaluar las políticas, controles, los sistemas que se manejan en las distintas áreas, los procesamientos de la información por áreas antes de ser consolidada y utilizada en conjunto con sus respectivas seguridades; con el fin de poder calificar el grado de eficiencia de los equipos informáticos con los procesos que realiza para establecer y lograr un uso más adecuado de los recursos informáticos sin dejar de lado la seguridad que debe tener la información que pueda servir para una adecuada toma de decisiones por parte de los directivos a cargo de la institución.

1.6. Objetivos específicos

- Establecer los responsables y principales funciones del área de Tecnología de la Información;
- Verificar y determinar la veracidad de la información por área;
- Verificar y evaluar el proceso del manejo de la información por área; y

- Verificar la forma de manejo de la información en todas sus formas.

CAPÍTULO II

2. MARCO DE REFERENCIA Y ANALISIS

2.1. La Institución

La institución es una entidad financiera de desarrollo, autónoma, de derecho privado y finalidad social y pública. Su funcionamiento se basa en la Ley Orgánica, Estatuto, Reglamentos y Regulaciones; y, su política crediticia se orienta de conformidad con los planes y programas de desarrollo económico y social que expida el Gobierno Nacional.

Misión

Brindar productos y servicios financieros competitivos e intervenir como ejecutor de la política de gobierno para apoyar a los sectores productivos y a sus organizaciones, contribuyendo al desarrollo socio – económico del país.

Visión

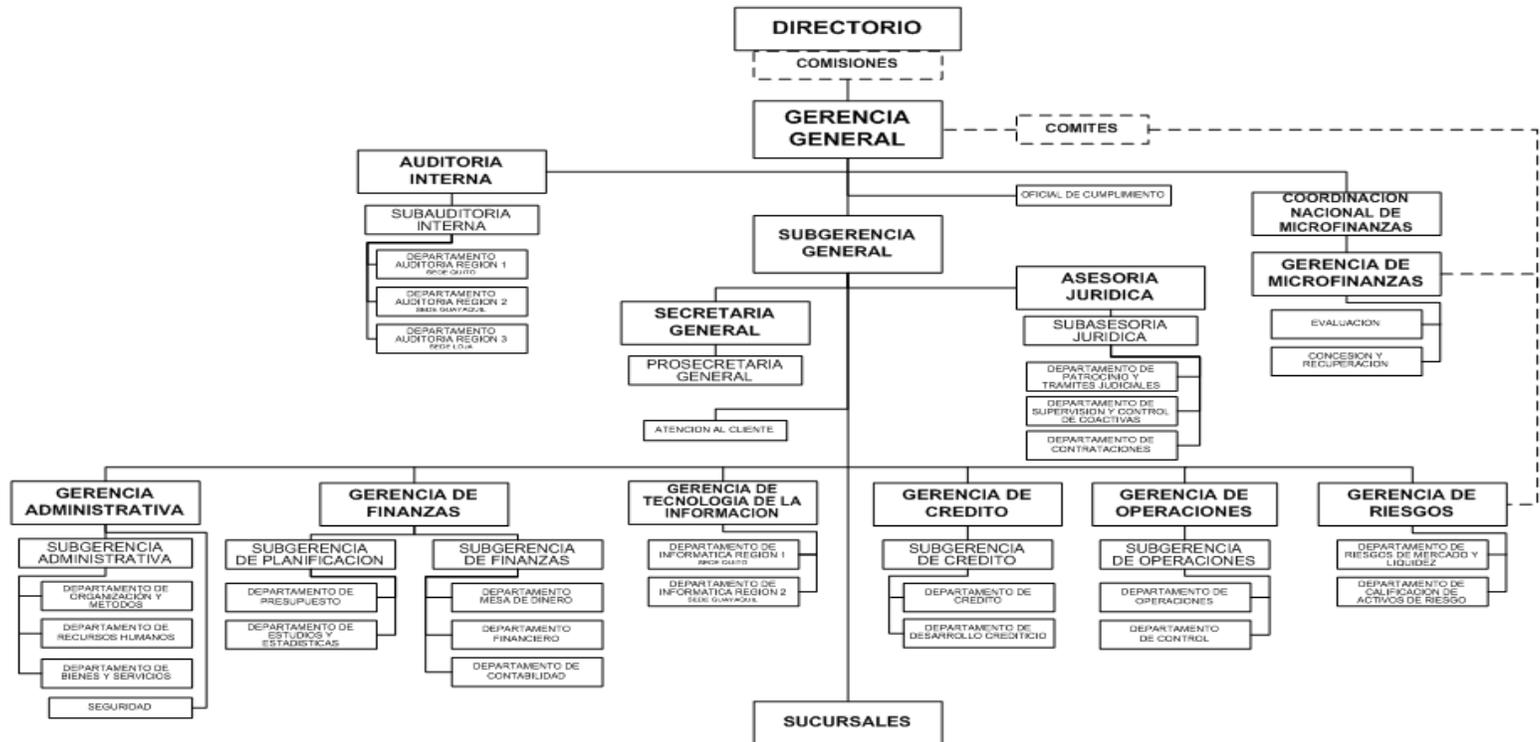
La institución será una institución competitiva, líder en la gestión bancaria para el desarrollo, gracias a su desempeño técnico y transparente, confianza y satisfacción de sus clientes; y a la calidad de sus productos y servicios financieros.

La institución se caracterizará por la calidad y compromiso de sus recursos humanos, tecnología moderna, estructura orgánica adecuada, administración por procesos; y una base legal que

garantice la óptima gestión técnica y consolide su autonomía para impulsar el desarrollo de los sectores productivos del país.

Figura 1. Organigrama institucional de la Institución a Auditar

ORGANIGRAMA ESTRUCTURAL



Elaborado por: La Institución Financiera

2.2. Marco de Referencia para la Auditoría Informática a la Institución Financiera Auditada

Como medida de control de la Superintendencia de Bancos y Seguros, por medio de la ley para las instituciones del sector financiero, establece que las instituciones financieras deben realizar auditorías como medida de control.

Además para el trabajo a realizar, se utilizará las Normas Internacionales ISO 27002 (Guía de buenas prácticas para la seguridad de la información) y COBIT 4.0, con un enfoque del cumplimiento de la Normativa de Riesgo Operativo para el Sistema Financiero:

2.3. Metodología

La metodología que se aplicó en este trabajo, está basada en las mismas etapas que se realiza en una Auditoría Financiera, las cuales están comprendidas desde un conocimiento completo del negocio hasta la emisión de un informe de las observaciones encontradas con sus respectivas recomendaciones. Para un mejor entendimiento se las detallamos a continuación [5].

Etapas de la Auditoría Informática:

- Planeación de la Auditoría.
- Desarrollo de la Auditoría.
- Emisión del Informe de Auditoría (Observaciones y Recomendaciones).

Adicionalmente como valor agregado al proyecto, se desarrollara un pequeño análisis estadístico para determinar el grado de conformidad que tiene el sistema usado y el nivel de aceptación del nuevo sistema que está por introducirse.

2.3.1. Planeación de la Auditoría.

Mediante la revisión y evaluación de los controles implementados en los sistemas y equipos de procesamiento Incluyendo el análisis de los mismos en términos de eficacia, eficiencia y seguridad, a fin de lograr el tratamiento más adecuado y seguro de la información, el contenido del plan de revisión de sistemas se resume como lo siguiente:

- Origen de la Auditoría
- Marco de Trabajo
- Alcance
- Desarrollo

2.3.1.1. Origen de la Auditoria

La revisión al área de sistemas y de los procesos por donde se encuentra relacionada la información, es un proceso indispensable a la hora de realizar servicios de Auditoría Financiera, esta revisión tiene por objeto ser soporte a la Auditoría Financiera y consultoría al cliente, para guiarlo en medidas de control interno, seguridades, utilización de hardware y software y el control de la calidad sobre la información.

2.3.1.2. Marco de Trabajo

Para la revisión de sistemas de la institución financiera, se adoptará el Marco de trabajo recomendado por COBIT 4.0 [1], el cual se detalla a continuación:

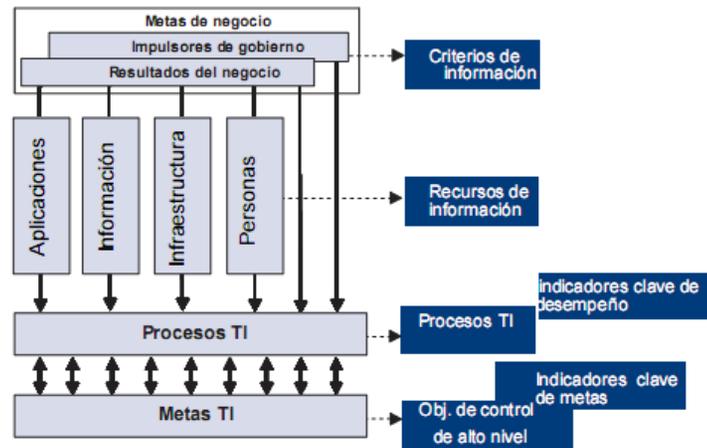


Figura 2. Marco de Trabajo de la COBIT 4.0
Elaborado por: COBIT 4.0

2.3.1.3. Alcance

El alcance de la auditoría estará limitado a la agencia de Guayaquil en las áreas de Banca, Crédito y Cartera, Contabilidad y Sistemas en el periodo comprendido entre Enero primero del 2008 hasta Diciembre 31 del 2008.

Para ello existe un acuerdo muy preciso con la institución Financiera sobre las funciones y sistemas a auditar; como así también se acordó la evaluación del cumplimiento de las leyes, normativas y/o estándares aplicables a la institución.

La revisión de los sistemas informáticos abarcará los siguientes objetivos de control, basados en ISO 27002 y COBIT 4.0., enfocados principalmente en el cumplimiento de la Normativa de Riesgo Operativo para el Sistema Financiero:

- Identificación de la Operatividad
- Planeación y Organización
- Cumplimiento d Normas
- Cumplimiento de Contratos
- Cumplimiento de Políticas
- Evaluación de Control Interno

2.3.1.4. Desarrollo

Identificación de la Operatividad

Se identificarán las áreas donde se genera información desde el punto de vista del giro del negocio.

Se determinarán todas las operaciones y transacciones que realizan cada una de los departamentos que manejan toda clase de información del giro del negocio.

Se identificarán los responsables y/o dueños de la información tanto por cada área como por el área de sistemas de la institución.

Planificación y Organización

Planes Estratégicos de TI

Se analizará los planes estratégicos que tiene la institución a largo y corto plazo ya que la tecnología de la información es parte del plan organizacional y la gerencia es responsable de la implementación y el desarrollo de planes a corto y largo plazo que cumplan la misión y las metas de la organización. En este aspecto, la gerencia debe garantizar que las cuestiones y las oportunidades en materia de tecnología de información se evalúen y se reflejen de manera adecuada en los planes a corto y largo plazo de la organización.

Se evaluará los sistemas existentes en función del grado de automatización del negocio, la funcionalidad, estabilidad, complejidad, los costos y las fortalezas y debilidades, a fin de determinar en qué medida los sistemas existentes dan soporte a los requerimientos de negocio de la organización.

Arquitectura de la Información

La institución debe establecerse un marco general de clasificación con respecto a la ubicación de los datos en clases de información (por ejemplo, categorías de seguridad) así como a la asignación de la propiedad. Las reglas de acceso para las clases deben definirse de manera adecuada, además la gerencia debe definir, implementar y mantener niveles de seguridad

para cada clasificación de datos identificada por encima del nivel "no requiere protección". Estos niveles de seguridad deben representar la cantidad adecuada (mínima) de medidas de seguridad y control.

Cumplimiento de Normas

Básicamente en el cumplimiento de normas, se revisará que la institución cumpla con determinadas normas técnicas tales como:

Cableado Estructurado

Mediante la aplicación de una prueba de cumplimiento, revisaremos si el cableado estructurado cumple con los requisitos mínimos que este requiere.

Licenciamiento

Se controlará el cumplimiento a los arts. 270, 271, 272 de la ley de propiedad intelectual, verificando las licencias de los paquetes de software que posea la institución.

Riesgo Operativo

La Superintendencia de Bancos y Seguros en Octubre del 2005 mediante **Resolución** No. JB-2005-834, imparte una serie de disposiciones para propender a que las instituciones del sistema financiero cuenten con un sistema para la gestión del riesgo operativo que les permita identificar, medir, controlar / mitigar y

monitorear los riesgos derivados de fallas o insuficiencias en los procesos, personas, tecnologías de información y eventos externos incluyendo el riesgo legal [4].

Dada esta resolución, mediante cuestionarios de control, se comprobará el cumplimiento de esta resolución en el ámbito de tecnologías de Información.

- Cumplimiento de Contratos
- Verificación de Contratos
- Se analizarán los contratos constituidos durante el periodo de revisión para verificar su cumplimiento.

Cumplimiento de Políticas

Mediante la revisión de los manuales y políticas establecidas por la institución, se verificará su cumplimiento.

Evaluación del Control Interno

Mediante la aplicación de cuestionarios de control interno evaluaremos el nivel de control que la entidad posee, a continuación mencionamos las áreas de control:

Controles Generales:

- Transmisión de datos
- Acceso a servidores local y remotamente
- Administración del ciclo de vida del software
- Administración de base de datos
- Administración de hardware y redes: cronogramas de mantenimiento, constatación física de equipos suficientes, estado de la red.

Controles de Aplicación:

- Administración de usuarios
- Auditabilidad
- Conexión con bases de datos
- Validación de datos de entrada
- Validación del Procesamiento
- Validación de datos de salida

2.3.1.5. Análisis Estadístico

Dado que la institución está en un proceso de reestructuración y están en procesos de adquirir un nuevo sistema integrado (Core Bancario), como aporte adicional a nuestro trabajo se analizó el nivel de satisfacción en conjunto de la relación que puede tener las características de los usuarios (empleados) con el sistema actual y con el nuevo sistema que está por integrar.

Para esto se procedió a realizar una encuesta y mediante técnicas estadísticas que se las detalla más adelante, se determinará la independencia o dependencia de las variables a analizar.

Para el análisis estadístico se realizó encuestas **(ANEXO 6)** con preguntas de tipo categóricas, para realizar un análisis bivariado de Tablas de Contingencia, con el software estadístico SPSS 11.5. Como referencia para el análisis se determinó lo siguiente:

H0: Las variables son independientes.

Ha: Las variables no son independientes.

Alfa ($\alpha = 0.05$)

Para el análisis se trabajará con el estadístico Chi-cuadrado y como resultado se tendrá que si el valor obtenido de p es mayor a alfa, se acepta la hipótesis H0, caso contrario se rechaza y se acepta Ha.

CAPÍTULO III

3. DESARROLLO DE LA AUDITORÍA INFORMÁTICA

3.1. Identificación de la Operatividad

La institución maneja varios sistemas, que son independientes entre sí y procesa la información de cada área para la cual fue creada, y son los procesos de estos sistemas y la forma de manejar la información de estas áreas las que se van a evaluar para medir el grado de confidencialidad, disponibilidad, integridad y seguridad de la información. Para esto se procedió a efectuar un relevamiento de información con el Gerente del área de sistemas de la institución para que nos proporcione una idea más clara de los sistemas y utilidades que manejan en la institución.

El relevamiento de la información se detalla en el **ANEXO 1**, del cual se pudo consolidar el siguiente cuadro resumen:

Tabla # 1: Determinación de los sistemas por área a ser evaluada

ÁREA	SISTEMA	OBSERVACIONES
Crédito y Cartera	Sistema de Crédito y Cartera COBOL 4.5 – Intranet	Sistema obsoleto. Serias debilidades en procesos que realiza como es el cálculo de interés.
Contabilidad	Sistema de Contabilidad COBOL 4.5	Sistema obsoleto mantiene serias debilidades en sus procesos como es al momento de consolidar la contabilidad por agencia.
Banca	COBOL - ORACLE	Único sistema que se encuentra integrado, serias debilidades en sus procesos como restricciones o alarmas en las transacciones hechas.
Sistemas	Depende si es de Casa Matriz (Quito) o Guayaquil	El departamento no mantiene un control de los sistemas que manejan en las áreas a evaluar.

Elaborado por: Geovanny González Narváez

Para un mejor entendimiento de cada sistema que posee la institución, se procedió a realizar un levantamiento de información en cada una de las áreas inmersas en la evaluación y se obtuvo lo siguiente:

3.1.1. Banca

Del relevamiento de información efectuado al Área de Banca detallado en el **ANEXO 2**, se obtuvo lo siguiente:

El sistema de Banca realiza transacciones básicas como son la de débitos o créditos a las cuentas ya sean estas corrientes o de ahorro, etc.

Los procesos o transacciones que se realizan mediante el sistema de este departamento lo detallamos a continuación en el diagrama de transacciones:

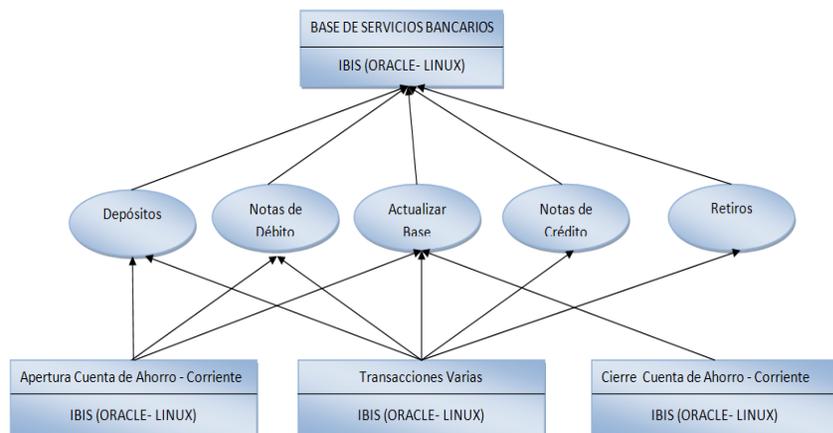


Figura 3. Diagrama de procesos de Área de Banca
Elaborado por: Geovanny González N.

El diagrama presentado muestra las transacciones que se pueden realizar en el sistema de Banca que tiene el nombre de IBIS. Además el departamento tiene a su cargo lo que son depósitos a plazo el mismo que no posee un sistema propio y se lo realiza en hojas de Excel.

Tabla # 2: Procesos y Transacciones de los Sistemas

PROCESO	TRANSACCIÓN	SISTEMA	OBSERVACIÓN
Apertura o Cierre de Cuentas de Ahorro y Corriente	Depósitos Notas de Debito Actualización de BD	IBIS	Existen clientes que no tienen todos los datos completos en la BD.
Transacciones Varias	Depósitos Notas de Debito Actualización de BD Notas de Crédito Retiros	IBIS	El sistema le permite realizar a los cajeros transacciones contra sus propias cuentas.
Cierre Cuentas de Ahorro o Crédito	Actualización de BD	IBIS	Una vez que se ha cerrado la cuenta, el banco aun posee firmas digitalizadas.
Depósitos a Plazo	Ingresos	EXCEL	No se tiene un sistema. Se lo lleva en hojas de Excel.

Elaborado por: Geovanny González Narváez

Del cuestionario aplicado al manejo de información del sistema de Banca (IBIS), se clasificaron las preguntas en 2 grupos.

EL primer grupo comprende las preguntas donde una respuesta positiva significa un adecuado control o manejo de la información en el sistema como puede ser si el sistema permite que los clientes puedan efectuar transacciones contra sus cuentas en cualquier sucursal u oficina a nivel nacional. Si la respuesta es positiva significa un procedimiento favorable.

El segundo grupo es lo contrario del primero ya que tendrá preguntas donde una respuesta negativa significará un adecuado control o proceso por parte del sistema, por ejemplo, la pregunta puede ser si el sistema permite a los cajeros realizar transacciones o movimientos contra sus propias cuentas.

Vale recalcar que las últimas 7 preguntas que tienen que ver con depósitos a plazo no se las tomaron en cuenta en el análisis de porcentajes. Debido a que no existe un sistema para este proceso.

Del cuestionario aplicado se obtuvo el siguiente resultado.

Grupo 1

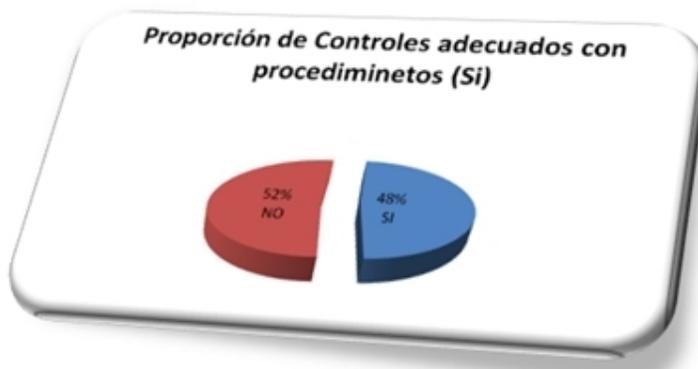


Figura 4. Proporción de repuestas afirmativas
Elaborado por: Geovanny González N.

Del cuestionario aplicado, el mismo que se encuentra en el Anexo 2 se obtuvo que de un total de 35 preguntas donde su respuesta positiva significa un adecuado control proceso por parte del sistema, un 48% que equivale a 17 preguntas del

total de 35 presenta un adecuado control, mientras que el 52 % que representa 18 preguntas de 35, muestra que no mantiene un control adecuado.

Dado que para una institución financiera debe manejar un control muy estricto con su información, se establece que el sistema no presenta serios problemas que puede conllevar a registros erróneos en la BD del departamento.

Grupo 2

Del segundo grupo donde una respuesta negativa significa un proceso o control adecuado, se obtuvo el siguiente resultado.



Figura 5. Diagrama de Pastel de la proporción de respuestas negativas
Elaborado por: Geovanny González N.

Del gráfico podemos observar que se obtuvo un 100% de la evaluación realizada; lo que quiere decir, que la institución financiera está llevando un control en cuanto a restricciones a los usuarios.

3.1.2. Crédito y Cartera

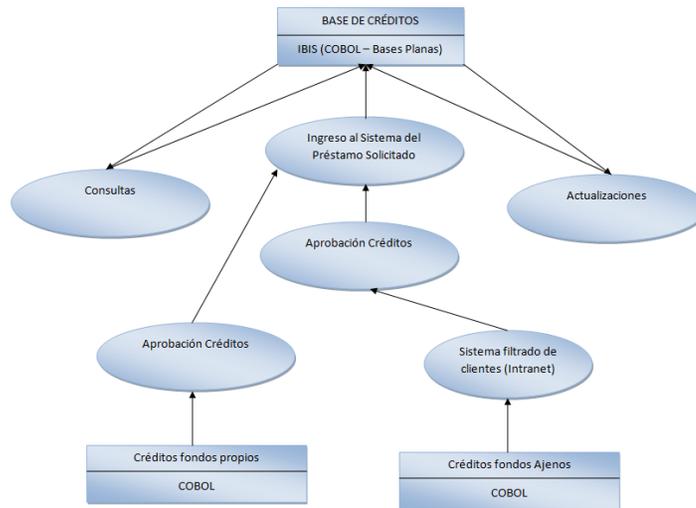


Figura 6. Diagrama de procesos de Área Crédito y Cartera
Elaborado por: Geovanny González N.

Mediante la evaluación ya sea de tipo ocular, pruebas de cumplimiento y mediante el relevamiento de información de los procesos y sistemas que manejan la información en esta área, que se detalla en el **ANEXO 3**; se encontró que este sistema posee muchas deficiencias en todos sus aspectos como es la de confidencialidad, integridad, disponibilidad y seguridad de la información, no se realizó ningún tipo de cuestionario para medir su eficiencia y seguridad; Esto se debe a que el sistema que manejan es un sistema basado en DOS que no realiza más que las transacciones básicas y guarda sus bases en archivos planos a los cuales se pueden acceder desde cualquier terminal y realizar alteraciones a los registros.

Al sistema de Crédito y Cartera. Se le efectuó un análisis y aplicación de pruebas a ciertos terminales del departamento, de lo cual obtuvimos lo siguiente:

Tabla # 3: Pruebas al Sistema de Crédito y Cartera

Prueba	Resultado
Verificación de los privilegios por usuarios	Cada usuario del departamento, tiene acceso a su modulo de trabajo pero pueden ejecutar cualquier módulo del departamento por medio de comandos de DOS.
Calculo de Intereses de los préstamos	El cálculo de intereses se lo realiza de manera manual en una calculadora y es ingresado al sistema para poder imprimir la papeleta de pago.
Módulos y Procesos para ingresar al maestro (Base de Datos) y poder cambiar información	Este proceso esto a cargo de la jefa de área y de su asistente, lo realizan diariamente dado que existe inconsistencias entre la papeleta de pago y lo que el sistema muestra. Además no guardan un registro de los cambios realizados al maestro.
Evaluación del proceso de pago de papeletas.	En este proceso se detecto falta de eficiencia por parte de los empleados del área y parte de la eficiencia se debe al sistema.
Prueba a la información física que posee el departamento	Se le pidió varias expedientes de clientes de los cuales solo se nos proporciono 2 de los 10 pedidos
Respaldo de la Información	El respaldo de esta se lo realiza semanalmente en diskettes o Cd's, los mismos que son guardados en la misma oficina que el servidor.

Elaborado por: Geovanny González Narváez

3.1.3. Contabilidad

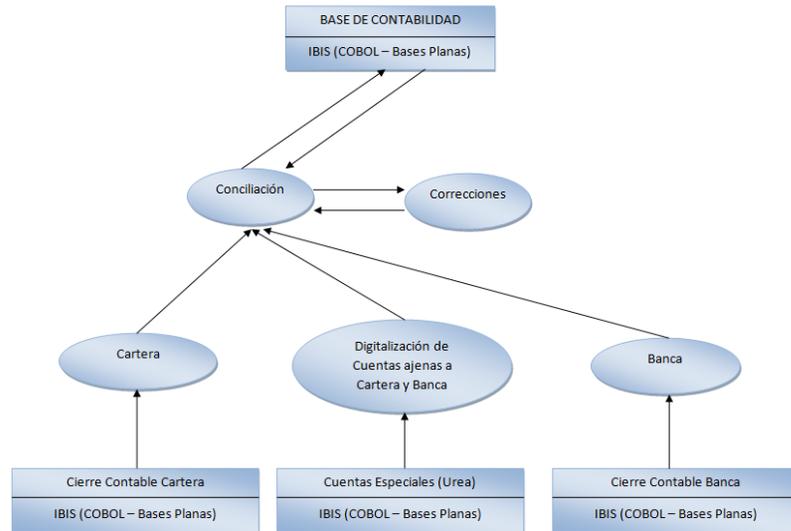


Figura 7. Diagrama de procesos de Área de Contabilidad
Elaborado por: Geovanny González N.

El departamento de Contabilidad al igual que el de Crédito y Cartera, posee un sistema bajo el lenguaje Cobol y presenta similar deficiencias que el de Crédito.

Se presenta a continuación una tabla con lo más relevante encontrado del relevamiento efectuado que se detalla en el **ANEXO 4:**

Tabla # 4: Observaciones encontradas al sistema de Contabilidad

Detalle	Observación
Consolidación de Contabilidad de las Áreas	Al momento de consolidar la información existen inconsistencias y se debe ingresar al maestro y corregir las transacciones.
Registro de Cambios realizado al Archivo Maestro	No se lleva un control de los cambios efectuados al archivo maestro.
Manual de Procedimientos y uso del sistema de Contabilidad.	El manual que posee esta caduco y no guarda los cambios realizados al sistema en su vida de servicio.
Verificación del proceso de consolidación de información	El proceso de consolidación se hace en base a un manual de procedimiento, el mismo que no se encuentra actualizado.
Respaldo de la Información	El respaldo de lo hace semanalmente en Cd's los mismo que son guardados en la misma oficina del servidor.

Elaborado por: Geovanny González Narváez

3.1.4. Sistemas

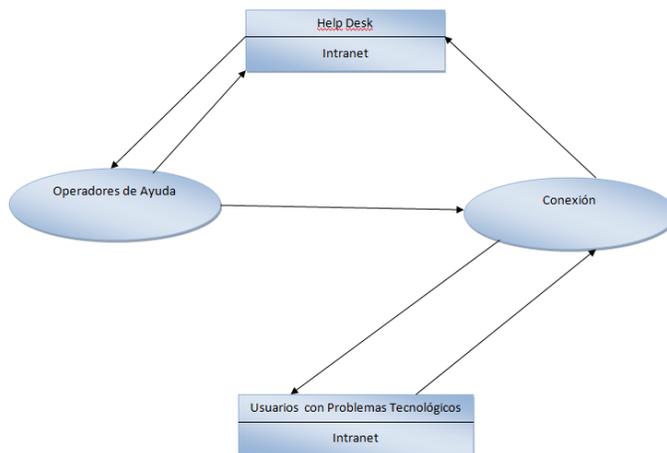


Figura 8. Diagrama de procesos de Área de Sistemas
Elaborado por: Geovanny González N.

Del relevamiento efectuado al área de sistemas, el mismo que lo detallamos en el **ANEXO 5**, se encontró que todos los

procesos se encuentran centralizados en la Ciudad Capital (Quito) y que le Área de Sistemas de Guayaquil, solo maneja lo que es el Help Desk (Soporte Técnico a Usuario) y además sirve de enrutador mediante un router (buscador del camino o ruta) para poder conectar y direccionar a la sucursales y agencias cercanas a la Casa Matriz.

Dado que la Sucursal a evaluar es la de la ciudad de Guayaquil, nos limitaremos a evaluar el procedimiento que realizan en esta, así como sus seguridades y procedimientos.

De la evaluación realizada a lo que tiene que ver con el Help Desk que es el servicio que presta el Área de Sistemas de Guayaquil, se estableció que su operatividad y eficiencia es muy buena ya que mantiene un 75% de requerimientos resueltos del total.

La eficiencia del Help Desk se la estableció por medio de los casos planteados con los casos resueltos y los casos no resueltos, el mismo que lo detallamos a continuación.

Figura 9. Diagrama de casos resueltos VS. No resueltos



Elaborado por: Geovanny González N.

De un total de 1685 casos registrados en el Help Desk hasta el mes de Noviembre se obtuvo un total de 424 casos no resueltos que equivalen a un 25% del total de casos registrados, mientras que el 75% que equivale a un total de 1261 casos, pudieron ser resueltos por el personal de Help Desk. Según las políticas y metas de este servicio, la proporción de casos no resueltos son muy altos ya que su porcentaje de casos no resueltos no debe ser mayor al 10% de los casos registrados.

3.2. Planificación y Organización

De la evaluación efectuada a los sistemas se estableció que la información carece de integridad, disponibilidad, y seguridad por lo caduco que son los sistemas empleados en el Banco, es por esta causa que la Institución procedió a realizar la adquisición de un Core Bancario que integrará todos los procesos y Áreas de la institución a Nivel Nacional.

En la evaluación efectuada se aplicaron procedimientos básicos de auditoría de indagación y entrevistas con los cuales se observó que la institución se encuentra en proceso de reestructuración tecnológica, la misma que se encuentra en áreas de control estratégico, las cuales tienen un responsable de su administración, control y operación de la misma.

Dado el gran cambio tecnológico que se está realizando en la institución, el área de sistemas se encuentra realizando mejoras sustanciales en lo relacionado con definir las políticas, responsables y procedimientos a seguir para cada una de las áreas con respecto a

la tecnología de la información, donde cada responsable de área deberá administrar, gestionar y controlar las políticas y procedimientos para poder mantener una operatividad eficiente de los recursos tecnológicos.

Tabla # 5: Evaluación de los Sistemas por área

ÁREA	SISTEMAS	GRADO DE AUTOMATIZACIÓN	FUNCIONALIDAD	ESTABILIDAD	COMPLEJIDAD	FORTALEZAS	DEBILIDADES
Crédito y Cartera	COBOL-INTRANET	40%	BUENA	BUENA	MEDIA	SIST SOLIDO	SISTEMA CADUCO
Banca	IBIS	70%	BUENA	BUENA	BAJA	-	NO CUMPLE LAS ESPECTATIVAS
Contabilidad	COBOL	40%	BUENA	BUENA	MEDIA	SIST SOLIDO	SISTEMA CADUCO

Elaborado por: Geovanny González Narváez

Con respecto a la arquitectura de la información y su relación con la clasificación de la información con respecto a la ubicación de los datos en clases de información como es la categoría de seguridad que se da en relación a los procesos y áreas donde se genera la misma, se conoció por medio del subgerente del área de sistemas que no existe una clasificación de la seguridad según su prioridad o riesgo por ende no existe procedimientos o políticas a seguir para el trato de la misma.

3.3. Cumplimiento de Normas

El cumplimiento de Normas a Evaluar en la institución se relaciona con la revisión por medios de pruebas de cumplimiento a:

- Cableado Estructurado
- Licenciamiento

Cableado Estructurado

El cableado estructurado que posee la institución es de categoría 5 y es un y está conformado de un sistema de cables, canalizaciones, conectores, etiquetas, espacios y demás dispositivos [2] que están instalados conformando una infraestructura de telecomunicaciones en EL edificio. A continuación mostramos el diagrama de red del edificio en forma general.

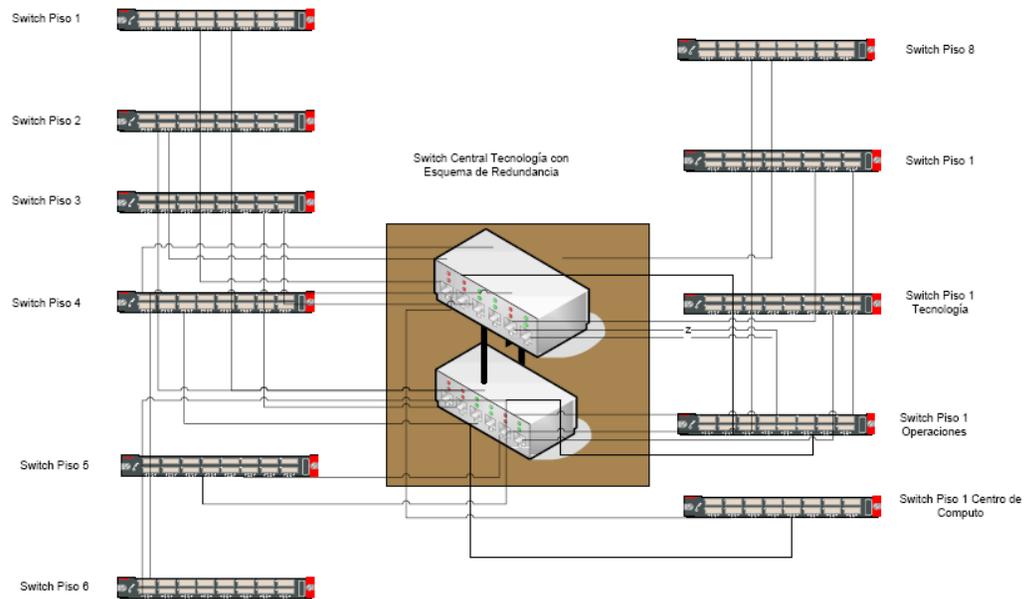


Figura 10. Diagrama de Red de la Institución
Elaborado por: La institución.

Tabla # 6: Evaluación del Cableado Estructurado

ACTIVIDAD	CUMPLIMIENTO	OBSERVACIONES
El cable utilizado cumple las especificaciones de CAT5 y está certificado	SI	
SE posee un esquema gráfico de la estructura de la red del Edificio	SI	
Se encuentra bien identificado cada uno de los cables que se encuentran en el edificio	NO	no poseen los cables identificaciones
el área de servidores cuenta con las especificaciones mínimas como puede ser el control de temperatura y alarmas	NO	no funcionan las alarmas
Los puntos de red se encuentran bien armados	SI	
Se cumple con la especificaciones del largo de cable máximo a ser utilizado	SI	
los swith utilizados con sus cables se encuentran bien clasificados y ordenados	NO	El armario donde se encuentra desordenado y algunos no posee el ambiente adecuado
posee puntos o parte de cableado en malas condiciones	SI	En algunos casos se encontró que se extendido un punto de red uniendo el cable de red con cinta Scotch

Elaborado por: Geovanny González Narváez

Licenciamiento

De la revisión de los paquetes de software y sus respectivas licencias adquiridas detallamos en la siguiente tabla lo encontrado:

Tabla # 7: Inventario de Licencias de Software

TIPO	SOFTWARE	LICECNA	OBSERVACIÓN
BASE DE DATOS	1 ORACLE 10G LICENCIA	OK	-
BASE DE DATOS	1 SYBASE LICENCIA CORPORATIVA	OK	-
BASE DE DATOS	1 SQLSERVER	OK	-
BASE DE DATOS	MYSQL	OK	-
SOFTWARE BASE	WINDOWS XP PROFESSIONAL SP2	OK	-
SOFTWARE DE APLICACIÓN	MICROSOFT OFFICE 2003	OK	-
SOFTWARE BASE	WINDOWS 98 PRO	OK	-
SOFTWARE DE APLICACIÓN	ACL VERSIÓN 8	OK	-
SOFTWARE DE APLICACIÓN	MICROSOFT OFFICE 2007	OK	-
SOFTWARE VERSIONAMIENTO	VISUAL SORCE SAFE	OK	-
ANTISPAM	CA INTEGRATED TRETA MANAGEMENT (ITM)	OK	-
ANTIVIRUS	ETRUST SECURE CONTENT MANAGER	OK	-
SOFTWARE DESARROLLO	POWER BUILDER 10.5	OK	-
BASE DOCUMENTAL	ALCHEMY 7.0	OK	-
SISTEMA OPERATIVO	LINUX RED HAT ENTERPRISE AS V.4	OK	-
SOFTWARE DESARROLLO	POWER BUILDER 9.0	OK	-
SOFTWARE DESARROLLO	POWER BUILDER 9.0	OK	-
BASE DE DATOS	ORACLE9I	OK	-
SOFTWARE DESARROLLO	ORACLE 9I DEVELOPER	OK	-
APLICACIONES SERVER	ORACLE 9I APPLICATION	OK	-
SOFTWARE APLICATIVO	SISTEMA DE CREDITO Y CARTERA	OK	PROPIO
SOFTWARE APLICATIVO	SISTEMA DE CONTABILIDAD	OK	PROPIO

Elaborado por: Geovanny González Narváez

3.4. Cumplimiento de Contratos

En el periodo auditado, solo se realizó un contrato en el ámbito tecnológico que tiene que ver con mantenimiento preventivo y correctivo de equipos de computación.

Tabla # 8: Contratos Elaborados en el Año 2008

TIPO DE CONTRATO	PROVEEDOR	FECHA DE CONTRATO	FECHA DE VIGENCIA	FECHA DE TERMINACIÓN	OBSERVACIONES
Mantenimiento Preventivo de Equipos de Computación	Soluciones Computacionales	14/02/2008	03/03/2008	03/03/2009	El contrato se lo realizó con los procedimientos establecidos por la institución

Elaborado por: Geovanny González Narváez

3.5. Cumplimiento de Política

El cumplimiento de políticas evaluará el grado de de conocimiento y cumplimiento de procedimientos establecidos por manuales y políticas internas de la institución. A continuación mostramos el grado de cumplimiento de las políticas de la institución concerniente a seguridad y procedimientos de manejo de sistemas e información.

Tabla # 9: Inventario de Manuales y Política

ÁREA	MANUAL	APLICACIÓN		OBSERVACIONES
		TOTAL	PARCIAL	
Banca	MANUAL DE PROCEDIMIENTOS DE CIERRE DE MES	X		-
Sistemas	Manual Procedimiento Service Desk 1.0	X		-
Sistemas	SI_Politica de creación de Usuario	X		-
Sistemas	SI-Politica_ecommerce_v01	X		-
Sistemas	SI-Politica_uso_aceptable_TI_v02	X		-
Sistemas	Manual de Instalación y Configuración EVA4100	X		-
Sistemas	PROCESO CONTROL DE CAMBIOS TI Ver 3.0	X		-
Sistemas	Normativa de versionamiento de software	X		-
Sistemas	NORMATIVA ENTREGA PRODUCTOS SOFTWARE	X		-
Contabilidad	MANUAL GENERACIÓN CARTERA 1 EN PC		X	Manual Caduco
Contabilidad	MANUAL CONSOLIDACIÓN CONTABILIDAD	X		Manual Caduco
Sistemas	MANUAL DE PROCEDIMIENTOS A SEGUIR DE LEVANTAMIENTO DEL SISTEMA DE BANCA	X		-
Cartera	RESPALDO DE INFORMACIÓN PARA SISTEMAS EN COBOL		X	Manual Caduco

Elaborado por: Geovanny González Narváez

De la evaluación realizada pudimos observar que el área de contabilidad y Crédito, no desarrollan un adecuado manejo de políticas. Motivo por el cual presentan un alto grado de errores de registros de información en el sistema. Tales como, el procedimiento para consolidar la contabilidad de la agencia que se realiza con la una bitácora desactualizada.

3.6. Evaluación del Control Interno a la Institución

Dado que nuestro proyecto solo cubre la agencia de la ciudad de Guayaquil y en esta no funciona o no posee los servidores donde se almacena la información de la institución. La evaluación de control interno se la realizó en base al cumplimiento de las políticas y

procedimientos establecidos para el área de sistemas de Guayaquil. Dicha evaluación se realizó con pruebas básicas de auditoría de indagación y entrevistas al proceso de Help Desk ya que esta es su actividad principal, al conocimiento de procedimientos básicos por parte de los integrantes del área y de la evaluación de la seguridad física que se posee en el área de servidores que poseen. Vale recalcar que esta área solo funciona de repetidora por medio de un router para que las agencias aledañas se puedan comunicar con Casa Matriz.

De la evaluación se obtuvo lo siguiente:

Tabla # 10: Evaluación Control Interno

EVALUACIÓN	CALIFICACIÓN
DE UN TOTAL DE 1585 CASOS REGISTRADOS EN EL HELP DESK, EL 75% PUEDIERON SER RESUELTOS	MUY BUENA
EL PERSONAL ÁREA SE ENCUENTRA CAPACITADA PARA ACTUAR EN CASOS DE EMERGENCIA COMO UN INCENDIO	MALA
LA INFRAESTRUCTURA DEL ÁREA DE SERVIDORES ES ADECUADA PARA SU USO COMO POR EJEMPLO POSEE PISO ANTI ESTÁTICO	MUY BUENA
EL EQUIPO DE DETECCIÓN DE HUMO SE ENCUENTRA EN FUNCIONAMIENTO	MALA
EXISTE SEGURIDAD AL ÁREA DE SISTEMAS	MALA

Elaborado por: Geovanny González Narváez

Tabla # 11: Calificaciones para evaluación del Control Interno

CALIFICACIÓN	VALOR
MUY MALA	10
MALA	20
BUENA	30
MUY BUENA	40
EXCELENTE	50

Elaborado por: Geovanny González Narváez

En base a la tabla # 11 se llegó a establecer que el área de sistemas de la agencia de Guayaquil posee una calificación de 200 sobre 400 con respecto de su control interno. Esto significa que el control interno del área de sistemas es deficiente aunque su calificación sea de 200 que es el 50%. Esto se debe que por ser una institución financiera, su seguridad y por ende el control interno debe ser

implacable por la cantidad de información delicada que se maneja en sus sistemas.

3.7. Desarrollo del Análisis Estadístico

Del análisis estadístico desarrollado a través de una encuesta y analizado con el programa estadístico SPSS versión 11.5, a los dos únicos departamentos de la institución que poseen el sistema basado en COBOL, el mismo que no se encuentra integrado, se obtuvo lo siguiente:

Tabla # 12: Tablas Cruzadas Tiempo que trabaja en la institución Financiera VS: El sistema que utiliza es fácil de usar.

		TIEMPO_T			Total	
		Menos de 10	Entre 10 y 20	Más de 20		
S I S T	Si	Count	1	3	3	7
		% within TIEMPO_T	33,3%	75,0%	100,0%	70,0%
F	No	Count	2	1	0	3
		% within TIEMPO_T	66,7%	25,0%	,0%	30,0%
Total		Count	3	4	3	10
		% within TIEMPO_T	100,0%	100,0%	100,0%	100,0%

Fuente: SPSS – Datos Procesados variable Tiempo que trabaja en la institución Financiera VS: El sistema que utiliza es fácil de usar.

Tabla # 13: Tabla Chi – Cuadrado variable Tiempo que trabaja en la institución Financiera VS: El sistema que utiliza es fácil de usar.

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	3,254(a)	2	,197
N of Valid Cases	10		

Fuente: SPSS – Datos Procesados variable Tiempo que trabaja en la institución Financiera VS: El sistema que utiliza es fácil de usar.

Mediante la aplicación del análisis de Tablas cruzadas (Tablas de Contingencia) realizado con el software estadístico SPSS versión 11.5, podemos observar que para las personas que se encuentran laborando en la institución menos de 10 años, el sistema no les parece fácil de usar, y según la tendencia que presentan los datos podemos ver que el nivel de satisfacción o facilidad para el uso del sistema, se incrementa con los años de trabajo que posee ya que para el 75% de los encuestados que se encuentran entre las edades de 10 y 20 años de servir a la institución, el sistema le parece fácil de usar y por último el 100% (la totalidad) de los que tienen más de 20 años de antigüedad el sistema es de fácil uso.

Se podría afirmar que existe una dependencia entre la variable “el sistema es fácil de usar” con la variable “años que se encuentra laborando en la institución”.

Para poder afirmar la dependencia de las variables, se procedió a realizar la prueba de hipótesis y se obtuvo que efectivamente las variables son dependientes ya que se obtuvo un valor p mayor al 0.05 de significancia, con el cual podemos afirmar lo analizado y podemos concluir que existe suficiente evidencia estadística para decir que el grado de satisfacción o facilidad de uso del sistema depende de los años de permanencia que tienen los empleados en la institución.

Tabla # 14: Tablas Cruzadas Edad VS. El Se encuentra conforme con el sistema con que se trabaja en su departamento.

		EDAD			Total	
		Menor 30	Entre 30 y 40	Mayor 40		
C C N F C R M	Si	Count	0	2	1	3
		% within EDAD	,0%	50,0%	33,3%	30,0%
No	Count	3	2	2	7	
		% within EDAD	100,0%	50,0%	66,7%	70,0%
Total	Count	3	4	3	10	
		% within EDAD	100,0%	100,0%	100,0%	100,0%

Fuente: SPSS – Datos Procesados variable Edad VS. El Se encuentra conforme con el sistema con que se trabaja en su departamento.

Tabla # 15: Tabla Chi – Cuadrado variable Edad VS. El Se encuentra conforme con el sistema con que se trabaja en su departamento.

Chi-	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	2,063(a)	2	,356
N of Valid Cases	10		

Fuente: SPSS – Datos Procesados variable Edad VS. El Se encuentra conforme con el sistema con que se trabaja en su departamento.

Al igual que en el caso anterior se procedió a realizar el mismo tipo de análisis para encontrar si las variables son dependientes. La conclusión encontrada la detallamos a continuación.

El 100% de los encuestados que tienen menos de 30 años, respondieron que no se encuentran conformes con el sistema actual, entre las personas que se encuentran entre los 30 y 40 años de edad, existe un 50% que se encuentra satisfecho con el sistema y otro 50% que no se encuentra satisfecho con el sistema.

Se puede observar que el comportamiento es similar al análisis anterior y también posee un valor p mayor al 0.05, por lo que podemos concluir que existe también suficiente evidencia estadística para afirmar que la variable satisfacción con el sistema usado es dependiente de la edad que posee el empleado.

Tabla # 16: Tablas Cruzadas Variable Tiempo que trabaja en la Institución Financiera VS. Cree usted que es necesario implementar un nuevo Sistema Informático (Core Bancario)

		TIEMPO_T			Total	
		Menos de 10	Entre 10 y 20	Más de 20		
N U E - S I S	Si	Count	3	4	3	10
		% within TIEMPO_T	100,0%	100,0%	100,0%	100,0%
S	No	Count	0	0	0	0
		% within TIEMPO_T	0.0%	0.0%	0.0%	0.0%
Total		Count	3	4	3	10
		% within TIEMPO_T	100,0%	100,0%	100,0%	100,0%

Fuente: SPSS – Datos Procesados Tiempo que trabaja en la Institución Financiera VS. Cree usted que es necesario implementar un nuevo Sistema Informático (Core Bancario).

Tabla # 17: Tabla Chi – Cuadrado variable Tiempo que trabaja en la Institución Financiera VS. Cree usted que es necesario implementar un nuevo Sistema Informático (Core Bancario)

	Value
Pearson Chi-Square	.(a)
N of Valid Cases	10

Fuente: SPSS – Datos Procesados Tiempo que trabaja en la Institución Financiera VS. Cree usted que es necesario implementar un nuevo Sistema Informático (Core Bancario).

Mediante este análisis podemos observar que para todas las edades, a pesar que se sientan conformes o no con el sistema, creen que es necesario la implementación de un nuevo sistema ya que el actual puede ser eficaz a la hora de hacer sus funciones pero no es eficiente.

CAPÍTULO IV

RESULTADOS

De la Auditoría Informática realizada al área de sistema y a los procesos y áreas que manejan información ya sea electrónica como física de la institución financiera se determino que:

Los sistemas de Contabilidad y Cartera y Crédito se encuentran caducos.

El área de Crédito y Cartera no cuenta con una seguridad adecuada con respecto a su información tanto física como electrónica.

EL proceso de validación de la contabilidad de todo el banco presenta inconsistencia por motivo que el registro de las transacciones se lo realiza manualmente y existe errores humanos en la digitación.

Desde cualquier terminal del área de Crédito y Cartera se puede tener acceso a todos los módulos del sistema incluso a los de modificación del archivo maestro.

El sistema de Banca (IBIS) realiza transacciones básicas por lo que existe la intervención de un empleado aumentando el riesgo de realizar un mal registro.

El departamento de sistemas de Guayaquil no tiene actividades propias de su nivel, se encuentra en proceso de reestructuración y adecuación ya que servirá de respaldo a la información del servidor principal que se encuentra en la Ciudad de Quito cuando se integre el nuevo sistema.

El cableado estructurado del edificio de la ciudad de Guayaquil posee deficiencias y necesita ser reestructurado.

Las áreas de la institución y sus sistemas no se encuentran integrados.

El respaldo de la información se la realiza de una forma inadecuada.

CAPÍTULO V

CONCLUSIONES RECOMENDACIONES Y CONTRIBUCIONES

Debilidades del sistema, observaciones

De la revisión efectuada a las aplicaciones con las que dispone el Banco, a continuación se presentan las conclusiones y recomendaciones por cada área auditada.

Cartera de Crédito

1. El campo “dirección del cliente” en el sistema no posee la longitud adecuada por lo que presenta información incompleta, limitando las visitas a las muestras seleccionadas.
2. La sesión de usuario del servidor siempre permanece activa y es utilizado por ciertas personas del área que no competen el uso de este equipo.
3. Existen varios procedimientos realizados manualmente que podría conllevar a errores humanos, tal es el caso del cálculo del valor a cancelar de los clientes realizado con calculadora, ya que el sistema no refleja el valor neto a cancelar (incluye dividendo, intereses e interés por mora).

4. Las ventanillas de cobro de cartera no manejan ningún tipo de sistema, solo llevan un registro en una hoja de Excel de lo recaudado en el día.

5. La responsable del área manifestó que el sistema de cartera registra valores distintos a lo contabilizado, lo que conlleva que al final del día sean verificados todos los pagos receptados para que sean corregidos del archivo maestro.

6. El respaldo de la información es almacenado en un computador que se encuentra junto al servidor y en cd's archivados en la oficina de la responsable del área por lo que si ocurre algún siniestro en la oficina se perdería la información actualizada.

7. Desde los terminales (computadores), se puede tener acceso a cualquier modulo del sistema incluso a los módulos que solo debería tener acceso la responsable del departamento por medio de comandos de DOS y son estos módulos donde se pueden modificar los registros.

Se recomienda:

1. Aumentar la longitud de caracteres del capo "dirección del cliente" para mantener una información más precisa de los clientes.

2. Establecer y hacer cumplir políticas para tener un mayor control con los servidores donde se especifique mantener la sesión de usuario cerrada.

2 y 4 Elaborar aplicativos del sistema que elaboren procesos automáticamente como el cálculo del valor a pagar, para llevar un adecuado control de los procesos.

5 Designar un equipo de evaluación de sistemas para que mitigue errores potenciales.

6 Designar un lugar apropiado y seguro para los respaldos diarios de todas las áreas.

7 Eliminar ciertos aplicativos o atributos que poseen los usuarios para evitar que se acceda a módulos o áreas críticas que pueden ocasionar que la información deje de ser integra.

Contabilidad

1. El proceso de consolidación de transacciones presenta inconsistencias en las cuentas ingresadas al sistema por causa de errores humanos al momento de registrar las transacciones en los diversos departamentos. Producto de estos errores, contabilidad ingresa al maestro y modifica las cuentas manualmente.

2. Contabilidad no guarda un registro de los cambios hechos al archivo maestro.

3. Existe inconsistencia entre las cuentas de los comprobantes físicos y las cuentas de registro del sistema, producto del manejo erróneo por parte de los digitadores de los departamentos a la hora de contabilizar.

4. El manual de usuario del sistema de contabilidad se encuentra desactualizado desde 1993, el Administrador Financiero elaboró un manual de procedimientos con los cambios que ha tenido en el transcurso del tiempo.

Se recomienda:

1, 2 y 3 Llevar un registro de los cambios efectuados en el archivo maestro e informar a cada departamento los errores cometidos para que procedan a las correcciones, para que de esta manera se reduzcan las inconsistencias causadas y pueda cruzar la información de los comprobantes físicos con el sistema contable.

4. Desarrollar un manual de sistema actualizado para los registros contables y que este sea distribuido para conocimiento de los usuarios.

Sistemas

1. Existen instalaciones de red inadecuadas donde se utilizan cinta para empatar el cable y poder extender el punto de red.

2. Disponen de detectores de humo en el área de servidores que se encuentran fuera de servicio.

3. No existe conocimiento de medidas a ser tomadas por parte del personal de sistemas en caso de siniestros.

Se recomienda:

1. Realizar una revisión de todos los puntos de red por área para eliminar empates o instalaciones inadecuados.

2 y 3 Habilitar el sistema de detección y poner al conocimiento del personal las medidas que deben tomar en caso de siniestros.

Con el presente trabajo la institución financiera logró conocer la situación real en la que se encuentra con respecto a la tecnología de la información y darse cuenta en términos reales la gran importancia que tiene el migrar al nuevo Core Bancario para que de esta manera poder contar con los Balances Consolidados de todas las agencias a nivel nacional y además que aumentar el grado de confiabilidad, integridad, disponibilidad y seguridad de la información que maneja.

BIBLIOGRAFÍA

1. www.monografias.com,
ISO 27002 y COBIT 4.0 visitada 09/12/08,
2. [http://es.wikipedia.org/wiki/Cable de Categoría 5](http://es.wikipedia.org/wiki/Cable_de_Categoría_5),
Cable Estructurado, visitada 12/12/08
3. <http://www.conelectronica.com/articulos/cable27.htm>,
Estructura de Redes, visitada 12/12/08
4. <http://www.superban.gov.ec/>,
Resolución y decretos, visitada 08/12/2008
5. **Manual de Auditoría**; Proporcionada por una firma de Auditoría,
Edición del 2008.
6. **Auditoría Informática**; de José Antonio Echenique García, Editorial
McGraw-Hill. Segunda Edición.

ANEXOS

Anexo 1

Relevamiento de la Información: Conociendo a la Institución y sus sistemas.

Relevamiento: Área de Sistemas

Del relevamiento efectuado al Departamento de Sistemas con el Gerente del área, pudimos conocer lo siguiente:

Las áreas con las que cuenta la institución financiera son Crédito y Cartera, Banca, Contabilidad y Sistemas. Tanto Crédito y Cartera, Banca y Contabilidad, manejan sistemas totalmente independientes por áreas y localidades a excepción de Banca, por lo que las bases de datos se encuentran partidas por áreas y sucursales. Por este motivo se debe realizar consolidaciones periódicas de todas las áreas. Tarea que se la realiza en la Matriz.

Cada sucursal dispone de su programa de cartera y contabilidad independiente. Respecto al sistema de cartera, éste se consolida en la matriz mediante un sistema hecho en Cobol 4.5; entre las falencias del sistema de cartera están el que no calcula los días de mora, interés devengado, entre otros, esto sólo se calcula al momento que lo requieran, por otra parte el sistema contable fue desarrollado por un contador de la institución financiera en Cobol y el departamento de sistemas no tiene ningún control sobre este sistema, únicamente lo usan los diferentes departamentos, por ende no tiene conocimiento de la consolidación de esta información.

Otro sistema que manejan, es el de Banca, el cual está implementado en Oracle, según se nos informó. Este sistema no dispone de controles,

además solo realiza las operaciones básicas y no mantiene un control adecuado de los procesos que realiza diariamente.

También disponen de una intranet en la cual está la información de cartera consolidada y documentación de la Institución Financiera para uso del personal de la institución.

En conclusión se estableció que los sistemas con que cuenta la Institución Financiera, se encuentran obsoletos y con serias deficiencias de seguridades. Por este motivo se está gestionando la adquisición de un Core Bancario que integrará toda la información de la Institución a Nivel Nacional y por áreas.

Anexo 2

Relevamiento de la Información: sistemas y procesos que manejan

Relevamiento: Área Banca

El relevamiento de Información concerniente a los sistemas e información que maneja este departamento, se lo realizó con la responsable del área (Gerente del Departamento de Banca), de donde se obtuvo la siguiente información:

El sistema informático con que cuenta el área Banca, es el único sistema de la institución que no se encuentra partida la base de datos ya que está integrado a nivel Nacional con sede de los servidores en la Ciudad Capital.

Entre las funciones principales que desarrolla este departamento están los depósitos, retiros, notas de créditos, notas de débito, giros y creación o cierre de cuentas de ahorros y corrientes que es donde empieza o nace la información de este departamento por lo que es ingresada los datos personales del cliente como es la de su firma digitalizada que se guardara en una base única. Este tipo de transacciones son las que modifican los registros de las bases de datos de este departamento que al igual que el resto de departamento de encuentran los servidores en la Casa Matriz (Quito)

El sistema de Banca se lo realizó con la finalidad de mantener una información actualizada y disponible a nivel nacional de los saldos que mantienen los clientes en la institución y de esta manera puedan hacer uso de sus fondos en cualquier agencia o sucursal a nivel nacional.

Dado que el sistema maneja información directamente de la base de datos, el mismo debe contener ciertas restricciones o controles que por ejemplo no permitan que un cajero pueda realizar transacciones directamente de su cuenta de ahorro o corriente y para poder establecer el grado de seguridades que posee el sistema, se realizó una evaluación del mismo mediante un cuestionario que se detalla más a continuación.

PREGUNTA	Técnica	SI	NO	OBSERVACIONES
1. ¿Se puede obtener del sistema reportes de depósitos, retiros, notas de debito, notas de crédito, de una sucursal y consolidado?	O	x		Se lo realiza por medio del departamento de sistemas
2. ¿El sistema de ventanillas tiene parametrizado el monto máximo que un cajero de ventanilla puede pagar en cheque o retiro, de acuerdo a los niveles de autorización establecidos por la Gerencia? (incluyendo pagos de depósitos a plazo cancelados)	PS		x	Los cajeros conocen esta información de manera escrita.
3. ¿Las bases de datos de clientes permite identificar las partes vinculadas a la institución?	O		x	
4. ¿Las bases de datos de depósitos a la vista y a plazo, están centralizadas en la matriz?	O	x		
5. ¿El sistema permite que los clientes pueden efectuar transacciones contra sus cuentas en cualquier sucursal u oficina a nivel nacional?	PS	x		
6. ¿Las transacciones que realizan los clientes en sus cuentas se registran en las bases de datos en tiempo real? ó ¿en qué momento se registran?	O	x		Real para eso es la integración del sistema a nivel nacional
7. ¿El sistema impide efectuar retiros o pagos de cheques sobre saldos de	PS		x	

depósitos no efectivizados?				
8. ¿El sistema automáticamente, transfiere a depósitos restringidos aquellos depósitos asignados como prendas o encajes en el área de préstamos?	PS		X	
9. Para los registros electrónicos de firmas de clientes:			X	
a) ¿Existe acceso restringido al directorio que almacena las firmas escaneadas?	PS			
b) ¿El sistema impide que se imprima los archivos (imagen- jpg) de las firmas de los clientes?	PS		X	
10. ¿El sistema impide que los cajeros de ventanilla y funcionarios autorizados para apertura y cierre de cuentas, realicen transacciones contra sus propias cuentas?	PS			X
11. ¿El sistema no permite que un cajero pueda visualizar el estado de cuenta de un cliente o el saldo de la cuenta?	PS			X
12. ¿En transferencias de dinero entre cuentas, se posee la suficiente información para determinar el origen y destino de los fondos, junto con los datos más relevantes?	O		X	
13. Cuando un menor de edad realiza un retiro de sus fondos, el sistema permite verificar la autorización de su representante legal?	PS		X	
14. El sistema permite retirar montos de saldos restringidos.	PS			X
15. ¿El sistema posee alertas para el cajero de ventanilla cuando se ha	PS			X

acumulado dinero por más de \$3.000 en su puesto de trabajo?				
CONTABILIZACION				
16. Por todas las transacciones por depósitos a la vista y a plazo ¿se genera el asiento contable en forma automática? ¿Detalle las transacciones cuyo asiento no se genera automáticamente?	I PC		X	Manual (Hoja de Excel)
17. Si los asientos contables son automatizados ¿en qué momento se generan los asientos contables?	I PC		x	

PREGUNTA		SI	NO	OBSERVACIONES
APERTURA DE CUENTAS (AHORRO/ CORRIENTE):				
1. Para apertura de cuentas: ¿El cliente posee un número de identificación único en la entidad a través de Cédula o Ruc?	O	X		
2. <u>Controles de validación:</u> los módulos del sistema utilizados para apertura posee, los siguientes controles de validación de datos:	PS			
a) Registro de fechas en un formato específico de acuerdo con lo dispuesto por el Organismo de Control	PS	X		
b) Registro de cifras en un formato específico de acuerdo con lo dispuesto por el organismo de control	PS	X		
c) Que el registro de la identificación del cliente, esté validado para un máximo y un mínimo de caracteres, según el tipo (cédula, RUC, pasaporte)	PS	X		
d) Que el sistema no permita el	PS	X		

PREGUNTA		SI	NO	OBSERVACIONES
a esa cuenta?				
CUENTAS INACTIVAS				
11. ¿El sistema automáticamente determina cuando una cuenta debe pasar a estado inactivo?	PS	X		90 Días
12. ¿Los archivos electrónicos de las imágenes de las firmas de las cuentas inactivas se bloquean para que nadie tenga acceso? (Ej. Se guardan en un directorio con acceso restringido ó se encripta la imagen).	PS		x	
13. ¿El sistema restringe las consultas a los datos de cliente de cuentas inactivas?	PS		X	
CUENTAS DE AHORRO				
14. ¿Cada vez que el cliente solicite una nueva libreta, se debita automáticamente el costo determinado por el Banco? (Art. 6 RDA)	O		X	Manual
15. Cuando se reciben depósitos sin libreta; en el próximo depósito que realice el cliente con la presentación de la libreta, ¿el sistema la actualiza automáticamente?	PS		X	
CUENTAS CORRIENTES				
16. ¿La numeración de las chequeras y los cheques es realizada automáticamente y en forma secuencial por el sistema?	PS	X		
INTERESES				
17. ¿La provisión diaria de intereses causados (devengado) es realizada por el sistema?	O	X		
18. Las tasas de interés que se aplica a los depósitos a plazo y ahorro ¿están			X	

PREGUNTA		SI	NO	OBSERVACIONES
parametrizadas en el sistema?				
19. ¿El sistema dispone de controles para impedir que se apliquen tasas de interés superior a las cubiertas por la AGD?	PS		X	
20. ¿El sistema calcula los intereses se calculan sobre el saldo promedio?	PS	X		
21. ¿El sistema calcula los intereses sobre depósitos de ahorro y a plazo, desde la fecha del depósito en caso de que sea en efectivo y desde la efectivización en caso de depósitos en cheque? (Art. 11 RDA)	PS			No saben

PREGUNTA	Técnica	SI	NO	OBSERVACIONES
Apertura de certificados de depósitos a plazo				
1. ¿Para la apertura de certificados de depósitos a plazo, el sistema asigna una numeración secuencial?	PS		X	No existe sistema
2. ¿El sistema permite cancelar una póliza antes de su fecha de vencimiento?	PS		X	No existe sistema
3. El sistema permite ingresar el plazo en días meses o en años?	PS		X	No existe sistema
Cierre de Depósitos a Plazo				
4. ¿El sistema asigna automáticamente las tasas en depósitos a plazo dependiendo del monto y plazo?	PS		X	No existe sistema
5. ¿El sistema calcula	PS		X	No existe sistema

automáticamente el interés del certificado y la retención en la fuente?				
6. Por los certificados anulados físicamente ¿en el sistema se anula la numeración?	PS O		X	No existe sistema
Provisión de los intereses				
7. El operador puede fijar la tasa de interés a pagar o se encuentra restringido su acceso? Se las selecciona de un DropDowList o es editable?	PS		X	No existe sistema

Anexo 3

Relevamiento de la Información: sistemas y procesos que manejan

Relevamiento: Área Crédito y Cartera

El relevamiento al Área de Crédito y Cartera se lo realizo con la responsable de Área, mediante la cual se conoció lo siguiente:

El departamento de cartera es el encargado de la contabilización de las cancelaciones, abonos, reestructuración y liquidación de los saldos de los diferentes tipos de préstamos que realiza el banco ya sea con fondos propios o con fondos ajenos.

Para el trabajo que realiza este departamento tiene a su disposición los siguientes módulos que se encuentran elaborados en Cobol 4.5:

- Modulo de Cartera
- Modulo de Crédito
- Módulos de actualización o modificación de registros.

Todos los módulos detallados son los que conforman el sistema de cartera y crédito, los mismos que almacenan la información que se realiza diariamente en el Servidor que se encuentra en la oficina de la responsable del área. Todos los empleados de este departamento tienen acceso a todos los módulos menos a los módulos de modificación que son los que pueden hacer alteraciones en los registros y los cuales solo tiene acceso la directora y su Asistente Administrativo aunque desde cualquier terminal de este departamento se puede tener acceso a cualquiera de los módulos por medio de líneas de comando DOS incluso a los módulos de modificación.

El proceso que el cliente pasa para poder realizar un abono es el siguiente:

1. El Cliente llega al departamento de crédito y cartera.
2. Se aloja en al área de espera con un ticket de turno.
3. Se acerca a la ventanilla de abono para que se procedan a realizar el comprobante de pago con el valor a cancelar.
4. Con el comprobante de pago generado se acerca a la ventanilla de caja para proceder a la cancelación.

El mismo proceso de cancelación de un abono pero ahora desde el punto de vista interno del departamento con los sistemas es el siguiente.

1. Las ventanillas de abono y cancelación elaboran el comprobante de pago en el sistema de cartera, el cual se utilizan también para consultar el número de pagare del cliente por medio de su cedula y para ver el valor adeudado e intereses a la fecha respectiva. Vale recalcar que el al momento de utilizar el sistema abono el primer inicio de sesión es para ver los valores e intereses adeudados donde los mismos serán sumados manualmente para posteriormente ingresarlos al mismo sistema abono en una nueva sesión para generar el comprobante de pago el cual se coloca el numero de comprobante manualmente de un listado que tiene cada señorita de ventanilla de abono y cancelación.

Adicionalmente el sistema Regula lo utilizan para realizar el mismo proceso de abono solo que este se lo emplea a fin de mes para no alterar las cuentas que están en corte por lo que se envía a provisiones.

Al momento de realizar el comprobante de pago hay situaciones donde por ejemplo el sistema no emplea la tasa de interés correcta, por lo que se tiene que utilizar adicionalmente el modulo de cartera para poder cambiar las tasas de interés.

2. Una vez el cliente tiene el comprobante se dirige a caja donde se le receptara el dinero y se le entregara una copia de comprobante al cliente, adicional a esta copia la caja entrega la original el comprobante original al departamento de contabilidad y otra copia al departamento de cartera.
3. Un encargado del departamento de carpeta recoge los comprobantes de caja cada cierto tiempo para llevarlos al departamento de cartera para que los asistentes procedan a su contabilización.

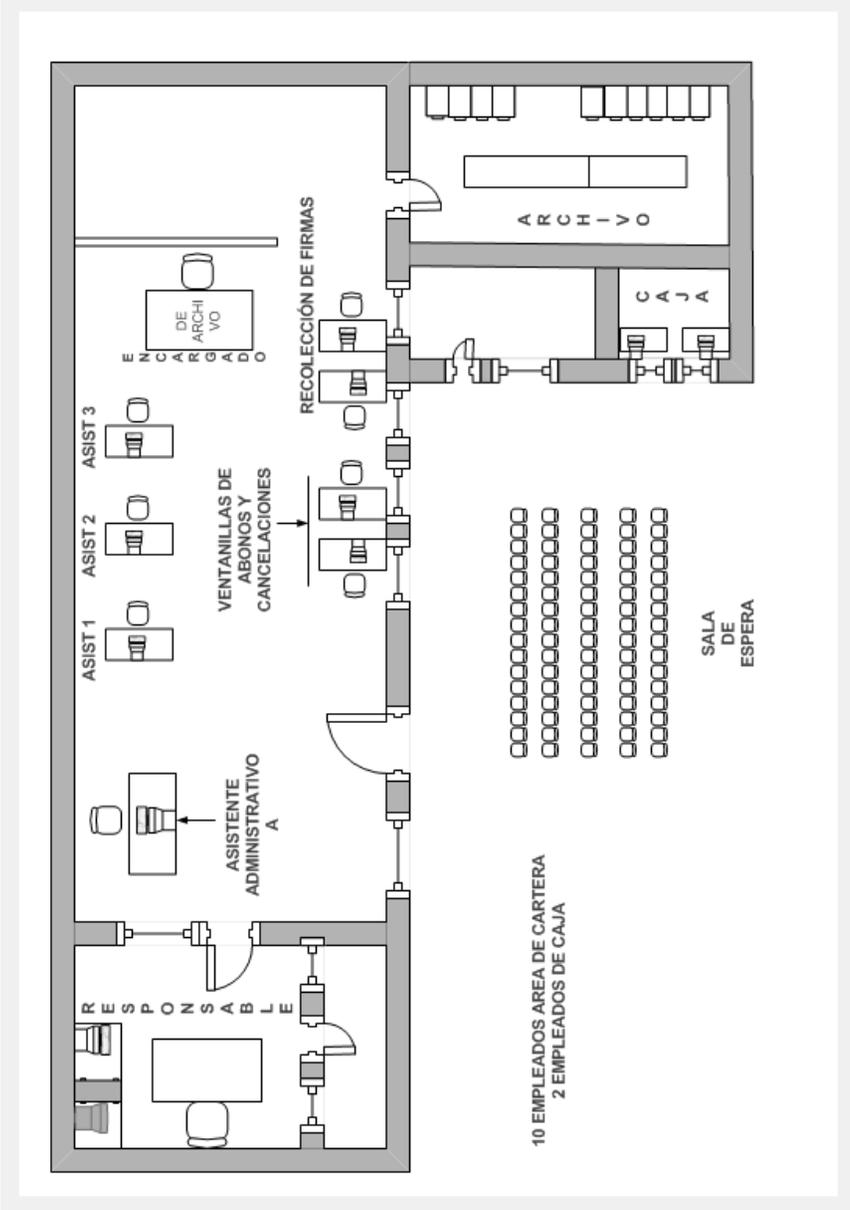
Al fin de día nos informo la responsable de cartera que debe efectuar una revisión de cada comprobante que ingreso en ese día ya que el sistema en ocasiones coloca cantidades erróneas por ejemplo el sistema registra un valor menor a mayor al que el cliente cancelo.

El respaldo de la información la realiza la encargada del área con una copia de los archivos los que son guardados en el mismo disco del servidor, otra copia en un terminal que se encuentra junto al servidor, efectúa una copia en Cd el cual lo tiene en su poder y el departamento de tecnología le solicita backup periódicos y finalmente le reporta a Quito.

Podemos concluir que el sistema de cartera tiene fuertes debilidades de seguridad con respecto a su información ya que carece de integridad y

confidencialidad ya que cualquier empleado del área puede tener acceso a esta.

Se adjunta un diagrama del área para un mejor entendimiento del mismo.



La información tiene distintas formas de almacenamientos y una muy importante sobre todo en el departamento de cartera es los FILE'S de los clientes que recopila la historia crediticia del deudor con sus pagares, tabla de amortización y demás información vital para el crédito concedido. Estas carpetas descansan en el archivo que es un cuarto sin mayor seguridad donde pudimos notar una falta absoluta de organización ya que las carpetas están regadas por todo el cuarto. Y debido a esta forma de llevar los archivos de los clientes, a la presente fecha no se nos entregan la totalidad de las carpetas solicitadas.

Anexo 4

Relevamiento de la Información: sistemas y procesos que manejan

Relevamiento: Área Contabilidad

Del relevamiento realizado con el responsable y Contador General, obtuvimos la siguiente información:

El departamento de contabilidad cuenta con el sistema "IBIS" desde Octubre de 1993, este sistema está elaborado en Cobol con desarrollo en ambiente DOS y ha sufrido diversos cambios hasta la fecha para poderlo adaptar a las exigencias del día.

El "IBIS" cuenta con una interfaz principal donde cada usuario del área de contabilidad ingresa para desarrollar sus actividades diarias por medio de 5 códigos (CONT01, CONT02, CONT03, CONT04, CONT05) los cuales contienen transacciones que van desde la 801 hasta la 865 y se encuentran repartidas entre los 5 códigos.

Las transacciones que están vinculadas a los códigos son las siguientes:

CÓDIGO	TRANSACCIONES
CONT04	844
	850

CÓDIGO	TRANSACCIONES
CONT05	857
	861

CÓDIGO	TRANSACCIONES	
CONT02	810	821
	811	824
	815	825
	819	838
	820	

CÓDIGO	TRANSACCIONES
CONT03	826
	833
	836

CÓDIGO	TRANSACCIONES
CONT01	801
	804
	806

Las transacciones que no se encuentran ligadas a algún código son transacciones que fueron eliminadas o creadas para acontecimientos poco usuales que alteran el registro de contabilidad como fue la conversión de los estados financieros a dólares o la adaptación de los estados financieros a los cambios que sufre el plan único de cuentas de instituciones financiera.

Este sistema es independiente en cada máquina donde cada usuario trabaja con las cuentas asignadas y cada cierto tiempo estas transacciones son integradas al servidor principal.

El sistema IBIS que maneja la parte contable del banco posee un manual desactualizado del uso de este programa. Si no fuera por el contador general de Guayaquil que realiza periódicamente un manual de su autoría, se estaría perdido con el uso de este programa.

Una de las falencias encontrada en este programa es que el encargado de la alimentación del servidor, puede alterar transacciones ya ingresadas y no guarda o lleva un control de los cambios realizados a la base del departamento de contabilidad.

Al momento que realiza la consolidación de las transacciones diarias, nunca cuadra los balances ya que los diferentes usuarios no solo de contabilidad sino también de cartera utilizan mal las cuentas por lo que al momento que se carga al sistema existe un descuadre y el encargado tiene que ingresar al archivo maestro y cambiar las cuentas manualmente y esto produce que el físico de comprobantes con el sistema de cartera nunca será igual al de contabilidad.

Anexo 5

Relevamiento de la Información: Procesos.

Relevamiento: Área de Sistemas

Del relevamiento realizado al Área de Sistemas, se obtuvo lo siguiente:
En la institución existen dos departamentos de tecnología uno en la matriz que es el departamento principal y uno en Guayaquil en el cual disponen de servicios de helpdesk, comunicaciones e infraestructura; en el resto de sucursales, existen ALRs (primer nivel de atención de helpdesk).

El relevamiento de la información se la efectuó en varias partes con los respectivos responsables.

Bases de datos

Las licencias de bases de datos con las que dispone la institución son:

1 Oracle 10G licencia corporativa
1 Sybase licencia corporativa
1 SQLServer
Mysql

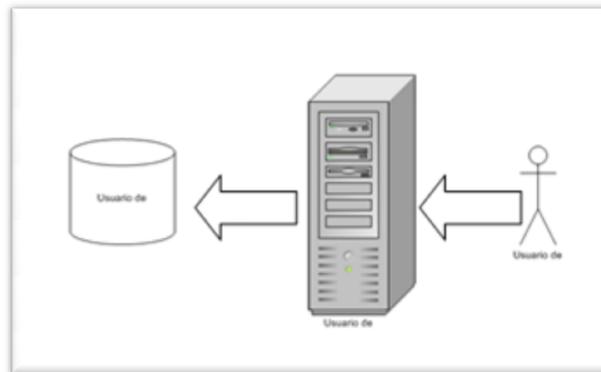
Existe una persona encargada del área de sistemas de las licencias y configuraciones de los programas que posee la institución.

Administración de la base de datos del Sistema IBIS (Banca)

El sistema de Banca es el único que se maneja en forma centralizada el cual está implementado en Cobol con una interfase para pasar la

información a una base de datos Oracle, esta base de datos posee un administrador que implementa algún cambio en el código fuente de la base de datos para arreglos al sistema IBIS del área de Banca.

El sistema se conecta a la base de datos centralizada a través de un usuario de base de datos especial para la aplicación, con la siguiente estructura:



Los usuarios de base de datos tienen permisos restringidos a través de roles especificados en la base de datos, los principales usuarios que ingresan a la base de datos IBIS son:

- Los administradores de base de datos con roles específicos para administración, ellos también tienen la custodia de los usuarios system y el sys los cuales son usuarios con permisos totales sobre el motor y todas las bases de datos, al ser dos personas las responsables deberían restringirse los accesos desde los usuarios system y sys sólo para casos especiales.
- Auditoría interna dispone de un usuario para acceder mediante ACL

- Un usuario de Firmas para extraer la información que se guarde en la base CLI, en donde se guardan las firmas digitalizadas en el sistema VERIFIRM (Sistema de digitalización de firmas) por cada sucursal.
- Diego Jiménez tiene permisos para actualizar un campo en especial de la tabla BNDLREM
- Usuario OPER_SEG, realiza operaciones de desbloqueo de base de datos
- Usuario OPERADOR, para realizar respaldos

La base de datos tiene activado el log de transacciones que se realizan directamente desde la base de datos, sin embargo no es revisado por Auditoría interna o algún responsable de control independiente al área.

Sistema de Digitalización de firmas

El sistema digitalización de firmas es utilizado en cada sucursal en un ambiente Linux. Mediante un proceso batch se toman las imágenes de las firmas de los clientes y se las graba en una base de datos en un ambiente Windows, esta base dispone de un usuario por cada sucursal, los cuales pueden tener dos tipos de roles los cuales son para consultar, ingresar o actualizar la base de firmas.

En la actualidad están haciendo las verificaciones para usar un nuevo sistema llamado DIGITALSOFT

Control de Cambios

Para realizar cambios a los sistemas de la institución, existe un Comité de Control de Cambios y están definidos los procesos, procedimientos y políticas, para proponer, aprobar y poner en producción un cambio a los sistemas o bases de datos. Utilizan el sistema Visual Source Safe (VSS) para restringir el acceso a los fuentes de los sistemas.

El proceso para realizar cambios a los fuentes de los programas es el siguiente:

1. Los clientes (funcionarios operativos) hacen un requerimiento a Organización y Sistemas.
2. Los cambios son analizados por el OyS para analizar cuáles son las fuentes que deben afectar y realizar una planificación del cambio.
3. Se realiza un formulario para solicitar los fuentes necesarios para el cambio y se genera un número RFC el cual identifica cada cambio que se está realizando.
4. Esta solicitud se envía al administrador de herramienta VSS, y pueden liberar los fuentes requeridos para que el personal de desarrollo los pueda copiar a su PC y realizar los cambios requeridos.
5. Al estar terminados los cambios, estos deben ser aprobados por el Comité de Control de Cambios y por el Comité de Calidad, de acuerdo a las políticas en caso de que se requiera cambiar un dato en la base de datos, debe contarse con la presencia de Auditoría Interna.

6. Una vez que han sido aprobados el desarrollador puede depositar los fuentes directamente en el servidor de Producción y da aviso a los administradores del VSS para que vuelvan a bloquear los fuentes utilizados o pasarles los archivos fuentes para que ellos mismos actualicen los archivos del servidor de Producción.

Durante la revisión observamos que existen archivos fuentes liberados que requieren ser bloqueados, sin embargo no han sido bloqueados ya que se ha pasado a otro proyecto y no ha sido informado que se bloqueen como es el caso del sistema de Servicios Bancarios.

Proceso de Respaldos

Este departamento cuenta con 5 personas entre las cuales se encuentra una de reemplazo.

La aplicación que utilizan para realizar los respaldos se llama DataProtector, es utilizada sólo en casa Matriz y los respaldos quedan en un armario dentro del Centro de Cómputo, se está analizando la posibilidad de un sitio alternativo para tener los respaldos, actualmente ya se tiene escogida a una empresa.

Los respaldos se graban en cintas identificadas por códigos de barras.

Los respaldos están programados y se realizan automáticamente mediante una unidad robótica, la cual administra las cintas y da alertas en caso de que hayan ocurrido problemas o si ya no hay espacio en alguna de las cintas. Al poder programar los respaldos, estos pueden ser disecionados a distintos lugares, existiendo una debilidad de control, ya

que ninguna entidad independiente al área revisa hacia donde se direccionan los respaldos.

El sistema dispone de varios usuarios, los cuales tienen distinto tipo de alcance, sólo existe un administrador del programa.

Se está por implementar un acta de pruebas de respaldos, actualmente no hay cómo verificar que se realizan las pruebas respectivas a los respaldos realizados.

Las cintas nuevas son adquiridas y guardadas en el mismo armario donde se guardan las cintas usadas, no existe un control adecuado para el registro de las cintas nuevas que se usan.

Respecto a los nuevos proyectos, se adquirió el nuevo Core Bancario, por lo que se asignara a un equipo del departamento en capacitación sobre el nuevo sistema; otro proyecto es el de Banca en línea, el cual fue postergada su salida a producción para realizar un análisis de Ethical Hacking, el cual ya fue terminado y de acuerdo al informe presentado, se están implementando las recomendaciones observadas.

Seguridad de la Información

Se implementó un área de seguridad e la información, en la cual se encuentran 5 personas, además existe una dirección de seguridad de la información. Todos estos cambios en la estructura organizacional se lo están realizando por el nuevo Core Bancario que se adquirió.

Entre las principales actividades del área están:

- Otorgar permisos de usuarios a los sistemas centralizados tales como IBIS (Sistema de Servicios Bancarios), Microfinanzas y la Intranet Corporativa
- Administrar la configuración del Active Directory para implementación de políticas de seguridad en el acceso a la red del Banco.
- Implementación de políticas de seguridad y su monitoreo.
- Liderar la implementación de lo relacionado a Transparencia de la Información
- Participación de la implementación de Cajeros Automáticos como usuarios de BANRED
- Custodia de las Actas de confidencialidad
- Administración de los certificados digitales de los servicios web
- Seguimiento e implementación de seguridades basados en la norma ISO 27002

El área ha desarrollado un Plan de seguridades y varias políticas de seguridad, las cuales están aprobadas por el Comité de Riesgos, y se han dado a conocer a los usuarios paulatinamente, sin embargo aún faltan por ser aprobadas por el Directorio.

El Plan de continuidad del negocio está aún en etapa de análisis, se tiene planificado que con el nuevo Core , se pueda diseñar un BCP acorde con la nueva tecnología y procesos.

Respecto a las Actas de confidencialidad se tiene implementado un 80% de todo el personal quedando algunos nuevos usuarios por firmar.

Actualmente se encuentran en constante capacitación en cuanto a la implementación de la norma ISO 27002, además se está haciendo un seguimiento a las recomendaciones del informe de Ethical Hacking.

Proceso de creación de usuarios y perfiles a sistemas

Está desarrollada e implementada una política para la creación de usuarios y perfiles de los sistemas centralizados, la cual está publicada en la Intranet corporativa, entre los principales procesos para la creación de usuarios y perfiles de acceso están los siguientes:

1. La Gerencia de Operaciones es la encargada de definir los perfiles y roles que se deben crear en las aplicaciones de IBIS y Microcrédito.
2. En la Intranet está publicado un formulario en archivo de Excel para que cada jefe de área pida que permisos pueda tener su personal a cargo
3. Este formulario es enviado a la Gerencia General luego a Recursos Humanos y luego a Seguridad de Información para su aprobación, en Seguridad de Información.
4. Seguridad Informática chequea que el mail con el formulario tenga el historial y aprobación de los departamentos antes mencionados

Creación de usuarios Sistema IBIS

En un principio el sistema de Banca, no disponía de ningún tipo de control ni de seguridades, en este año, se implementó un módulo de seguridades y se migró a una plataforma más segura y robusta como es Oracle 10G

Actualmente el sistema IBIS posee un módulo de creación de usuarios el cual permite crear roles que contengan permisos para diferentes transacciones, los controles que posee esta aplicación son:

- Caducidad de la contraseña
- Clave encriptada
- Varios roles con diferentes transacciones
- El usuario está relacionado con la máquina

El sistema IBIS dispone de cuatro módulos principales:

- Ventanilla
- Plataforma
- Interno
- Administrativo

Creación de usuarios Sistema Microcrédito

El Sistema de Microcrédito está implementado en la Intranet, lo cual le permite estar centralizado, trabaja en conjunto con el sistema de cartera y crédito, el cual es descentralizado.

El sistema de Microcrédito dispone de los mismos controles del sistema IBIS

Proceso de creación de usuarios y perfiles a la red corporativa

Las políticas de seguridad de la red corporativa está implementada en Active Directory, la cual está administrada por el área de Seguridad Informática, para la creación de usuarios se ha definido que el departamento de Recursos Humanos al ingresar nuevo personal crea un usuario de red con permisos a la Intranet y correo electrónico.

La administración de los usuarios es centralizada y permite tener el control de todos los usuarios a nivel nacional.

Además se efectuó un cuestionario de distintos tipos de seguridades en la institución, el mismo que lo detallamos a continuación:

#	PREGUNTA	SI	NO	N/A	OBSERVACIONES
1	¿Se han adoptado medidas de seguridad en la dirección de informática?	x			Centralizado en casa Matriz
2	¿Existe una persona responsable de la seguridad?	x			Un departamento
3	¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?				
4	¿Existe personal de vigilancia en la institución?	x			
5	¿La vigilancia se contrata:				
	a) Directamente?	x			
	b) Por medio de empresas que venden ese servicio?				
6	¿Existe una clara definición de funciones entre los puestos claves?	x			
7	¿Se investiga a los vigilantes cuando son contratados directamente?			x	
8	¿Se controla el trabajo fuera del horario?		x		
9	¿Se registran las acciones de los operadores para evitar que realicen alguna que pueda dañar el sistema?		x		

10	¿Existe vigilancia en el área de servidores las 24 horas?		x		
11	¿A la entrada del área de servidores existe:				
	a) Vigilante?				
	b) Recepcionista?				
	c) Tarjeta de control de acceso?				
	d) Bitácora de Acceso?	x			
	e) Nadie?				
12	¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?		x		
13	¿Se ha instruido a estas personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización?		x		
14	¿El edificio donde se encuentra la computadora está situado a salvo de:				
	a) Inundación?	x			
	b) Terremotos?	x			
	c) Fuego?	x			
	d) Sabotaje?	x			
15	¿El centro de cómputo da al exterior?		x		
16	¿Tiene el área de servidores una instalación de escaparate y, si es así, pueden ser rotos los vidrios con facilidad?		x		
17	¿Existe control en el acceso a este cuarto?				
	a) Por identificación personal?		x		
	b) Por tarjeta magnética?				
	c) Por claves verbales?				
	d) Otras, especifique cuales en observaciones				
#	PREGUNTA	SI	NO	N/A	OBSERVACIONES
18	¿Son controladas las visitas y demostraciones en el centro de cómputo?. Describa en observaciones como son controladas	x			
19	¿Se registra el acceso al cuarto de personas ajenas a la dirección de informática? Especifique como se realiza dicho registro.		x		
20	¿Se vigilan la moral y el comportamiento del personal de la dirección de informática con el fin de mantener una buena imagen y evitar un posible fraude?	x			
21	¿Existe alarma para				
	a) Detectar fuego /calor o humo) en forma automática?	x			
	b) Avisar en forma manual la presencia del fuego?		x		

	c) Detectar una fuga de agua?		x		
	d) Detectar magnetos?		x		
	e) No existe?				
22	¿Estas alarmas están				
	a) En el área de servidores?	x			
	b) En la cintoteca y/o discoteca?	x			
	c) En el área operativa?	x			
23	¿Existe alarma para detectar condiciones anormales del ambiente?				
	a) En el área de servidores?		x		
	b) En la cintoteca y discoteca?		x		
	c) En el área operativa?		x		
	d) En otros lados? Especifique en observaciones.				
24	¿La alarma es perfectamente audible?			x	
25	¿Esta alarma también está conectada?				
	a) Al puesto de guardias?				
	b) A la estación de bomberos?				
	c) A ningún otro lado?		x		
	d) Otro, especifique en observaciones				
26	Existen extintores de fuego?				
	a) Manuales?	x			
	b) Automáticos?				
	c) No existen?				
27	¿Se ha adiestrado el personal en el manejo de los extintores?		x		
28	¿Los extintores, manuales o automáticos son a base de				
	a) Agua?				
	b) Gas?	x			
	c) Otros?				
29	¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores? Nota: Indique el número de extintores y su estado.		x		4 en buen estado (cargados)
30	Si es que existen extintores automáticos, ¿son activados por los detectores automáticos de fuego?				
31	Si los extintores automáticos son a base de agua, ¿se han tomado medidas para evitar que el agua cause más daño que el fuego?				
32	Si los extintores automáticos son a base de gas, ¿se han tomado medidas para evitar que el gas cause más daño que el fuego?				

33	¿Existe un lapso de tiempo suficiente, antes de que funcionen los extintores automáticos, para que el personal				
	a) Corte la acción de los extintores por tratarse de falsas alarmas?				
	b) Pueda cortar la energía eléctrica?				
	c) Pueda abandonar el local sin peligro de intoxicación?				
	d) Es inmediata su acción?				
34	¿Los interruptores de energía (breakers) están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?	x			
#	PREGUNTA	SI	NO	N/A	OBSERVACIONES
35	¿Saben qué hacer los operadores del área de servidores en caso de que ocurra una emergencia ocasionada por fuego?	x			
36	¿El personal ajeno a operación sabe qué hacer en el caso de una emergencia (incendio)?		x		
37	¿Existe salida de emergencia?		x		
38	¿Esta puerta sólo es posible abrirla:				
	a) Desde el interior?	x			
	b) Desde el exterior?				
	c) Ambos lados				
39	¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen?		x		
40	¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?		x		
41	¿Se han tomado medidas para minimizar la posibilidad de fuego:				
	a) Evitando artículos inflamables en el área de servidores?	x			
	b) Prohibiendo fumar a los operadores en el interior?	x			
	c) Vigilando y manteniendo el Sistema eléctrico?	x			
	d) No se ha previsto?				
42	¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del área de servidores para evitar daños al equipo?	x			
43	¿Se limpia con frecuencia el polvo acumulado debajo del piso falso?		x		

44	¿Se controla el acceso y préstamo en la:				
	a) Discoteca?	x			
	b) Cintoteca?	x			
	c) Programoteca?	x			
45	Explique la forma como se ha clasificado la información vital, esencial, no esencial, etc.				Se la ha clasificado según el sistema ya que no se encuentran integrados los departamentos
46	¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?	x			
47	Explique la forma en que están protegidas físicamente estas copias (bóveda, cajas de seguridad, etc.) que garantice su integridad en caso de incendio, inundación, terremoto, etc.				En bodega fuera del centro de computo
48	¿Se tienen establecidos procedimientos de actualización a estas copias?	X			
50	¿Existe departamento de auditoría interna en la institución?	X			
51	¿Este departamento de auditoría interna conoce todos los aspectos de los sistemas?	X			
52	¿Qué tipos de controles ha propuesto?				
53	¿Se cumplen?				
54	¿Se auditan los sistemas en operación?	X			
55	¿Con que frecuencia?				
	a) Cada seis meses				
	b) Cada año				
	c) Otra (especifique)	X			Cuando lo amerite
56	¿Cuándo se efectúan modificaciones a los programas, a iniciativa de quién es?				
	a) Usuario	X			
	b) Director de informática				
	c) Jefe de análisis y programación				
	d) Programador				
	e) Otras (especifique)				
#	PREGUNTA	SI	NO	N/A	OBSERVACIONES
57	¿La solicitud de modificaciones a los programas se hacen en forma:				

	a) Oral?				
	b) Escrita?	X			
	En caso de ser escrita solicite formatos.				
58	Una vez efectuadas las modificaciones, ¿se presentan las pruebas a los interesados?	X			
59	¿Existe control estricto en las modificaciones?	X			
60	¿Se revisa que tengan la fecha de las modificaciones cuando se hayan efectuado?	X			
62	Se verifica identificación:				
	a) De la terminal				
	b) Del usuario	x			
	C) No se pide identificación				
63	¿Se ha establecido qué información puede ser manipulada y por qué persona?	x			
64	¿Se ha establecido un número máximo de violaciones sucesivas para que el computador cierre esta terminal y se de aviso al responsable de ella?	x			3 violaciones
65	¿Se registra cada violación a los procedimientos con el fin de llevar estadísticas y frenar las tendencias mayores?		X		
66	¿Existen controles y medidas de seguridad sobre las siguientes operaciones?				
	Recepción de documentos	X			
	Información confidencial	X			
	Captación de documentos	X			
	Cómputo electrónico	X			
	Programas	X			
	Discotecas y cintotecas	X			
	Documentos de salida	X			
	Archivos magnéticos	X			
	Operación del equipo de computación	X			
	En cuanto al acceso de personal	X			
	Identificación del personal	X			
	Policía	X			
	Seguros contra robo e incendio	X			
	Cajas de seguridad				
	Otras (especifique)				
67	¿Tienen seguros todos los equipos?		X		

Anexo 6

ENCUESTA AL PERSONAL DEL DEPARTAMENTO DE CARTERA Y CONTABILIDAD
NIVEL DE SATISFACCIÓN

1. Departamento donde labora

Crédito y Cartera

Contabilidad

2. Edad

Menor a 30

Entre 30 y 40

Mayor a 40

3. Máximo nivel de estudio alcanzado

Segundo Nivel

Tercer Nivel

Cuarto Nivel

4. Tiempo que trabaja en la Institución Financiera

Menos de 10 años

de 10 a 20 años

Más de 20 años

5. Se encuentra conforme con el sistema con que se trabaja en su departamento

Si

NO

6. El sistema que utiliza es fácil de usar (amigable)

SI

No

7. Cree usted que es necesario implementar un nuevo Sistema Informático (Core Bancario)

Si

No

8. Usted conocía que se va a implementar un Nuevo Sistema Informático (Core Bancario)

SI

No

9. Ha sido capacitado para el uso del nuevo sistema

Si

No

ENCUESTA AL PERSONAL DEL DEPARTAMENTO DE CARTERA Y CONTABILIDAD
NIVEL DE SATISFACCIÓN

1. Departamento donde labora

Crédito y Cartera

Contabilidad

2. Edad

Menor a 30

Entre 30 y 40

Mayor a 40

3. Máximo nivel de estudio alcanzado

Segundo Nivel

Tercer Nivel

Cuarto Nivel

4. Tiempo que trabaja en la Institución Financiera

Menos de 10 años

de 10 a 20 años

Más de 20 años

5. Se encuentra conforme con el sistema con que se trabaja en su departamento

Si

NO

6. El sistema que utiliza es fácil de usar (amigable)

SI

No

7. Cree usted que es necesario implementar un nuevo Sistema Informático (Core Bancario)

Si

No

8. Usted conocía que se va a implementar un Nuevo Sistema Informático (Core Bancario)

SI

No

9. Ha sido capacitado para el uso del nuevo sistema

Si

No

ENCUESTA AL PERSONAL DEL DEPARTAMENTO DE CARTERA Y CONTABILIDAD
NIVEL DE SATISFACCIÓN

1. Departamento donde labora

Crédito y Cartera

Contabilidad

2. Edad

Menor a 30

Entre 30 y 40

Mayor a 40

3. Máximo nivel de estudio alcanzado

Segundo Nivel

Tercer Nivel

Cuarto Nivel

4. Tiempo que trabaja en la Institución Financiera

Menos de 10 años

de 10 a 20 años

Más de 20 años

5. Se encuentra conforme con el sistema con que se trabaja en su departamento

Si

NO

6. El sistema que utiliza es fácil de usar (amigable)

SI

No

7. Cree usted que es necesario implementar un nuevo Sistema Informático (Core Bancario)

Si

No

8. Usted conocía que se va a implementar un Nuevo Sistema Informático (Core Bancario)

SI

No

9. Ha sido capacitado para el uso del nuevo sistema

Si

No

ENCUESTA AL PERSONAL DEL DEPARTAMENTO DE CARTERA Y CONTABILIDAD
NIVEL DE SATISFACCIÓN

1. Departamento donde labora

Crédito y Cartera

Contabilidad

2. Edad

Menor a 30

Entre 30 y 40

Mayor a 40

3. Máximo nivel de estudio alcanzado

Segundo Nivel

Tercer Nivel

Cuarto Nivel

4. Tiempo que trabaja en la Institución Financiera

Menos de 10 años

de 10 a 20 años

Más de 20 años

5. Se encuentra conforme con el sistema con que se trabaja en su departamento

Si

NO

6. El sistema que utiliza es fácil de usar (amigable)

SI

No

7. Cree usted que es necesario implementar un nuevo Sistema Informático (Core Bancario)

Si

No

8. Usted conocía que se va a implementar un Nuevo Sistema Informático (Core Bancario)

SI

No

9. Ha sido capacitado para el uso del nuevo sistema

Si

No

ENCUESTA AL PERSONAL DEL DEPARTAMENTO DE CARTERA Y CONTABILIDAD
NIVEL DE SATISFACCIÓN

1. Departamento donde labora

Crédito y Cartera

Contabilidad

2. Edad

Menor a 30

Entre 30 y 40

Mayor a 40

3. Máximo nivel de estudio alcanzado

Segundo Nivel

Tercer Nivel

Cuarto Nivel

4. Tiempo que trabaja en la Institución Financiera

Menos de 10 años

de 10 a 20 años

Más de 20 años

5. Se encuentra conforme con el sistema con que se trabaja en su departamento

Si

NO

6. El sistema que utiliza es fácil de usar (amigable)

SI

No

7. Cree usted que es necesario implementar un nuevo Sistema Informático (Core Bancario)

Si

No

8. Usted conocía que se va a implementar un Nuevo Sistema Informático (Core Bancario)

SI

No

9. Ha sido capacitado para el uso del nuevo sistema

Si

No

ENCUESTA AL PERSONAL DEL DEPARTAMENTO DE CARTERA Y CONTABILIDAD
NIVEL DE SATISFACCIÓN

1. Departamento donde labora

Crédito y Cartera

Contabilidad

2. Edad

Menor a 30

Entre 30 y 40

Mayor a 40

3. Máximo nivel de estudio alcanzado

Segundo Nivel

Tercer Nivel

Cuarto Nivel

4. Tiempo que trabaja en la Institución Financiera

Menos de 10 años

de 10 a 20 años

Más de 20 años

5. Se encuentra conforme con el sistema con que se trabaja en su departamento

Si

NO

6. El sistema que utiliza es fácil de usar (amigable)

SI

No

7. Cree usted que es necesario implementar un nuevo Sistema Informático (Core Bancario)

Si

No

8. Usted conocía que se va a implementar un Nuevo Sistema Informático (Core Bancario)

SI

No

9. Ha sido capacitado para el uso del nuevo sistema

Si

No

ENCUESTA AL PERSONAL DEL DEPARTAMENTO DE CARTERA Y CONTABILIDAD
NIVEL DE SATISFACCIÓN

1. Departamento donde labora

Crédito y Cartera

Contabilidad

2. Edad

Menor a 30

Entre 30 y 40

Mayor a 40

3. Máximo nivel de estudio alcanzado

Segundo Nivel

Tercer Nivel

Cuarto Nivel

4. Tiempo que trabaja en la Institución Financiera

Menos de 10 años

de 10 a 20 años

Más de 20 años

5. Se encuentra conforme con el sistema con que se trabaja en su departamento

Si

NO

6. El sistema que utiliza es fácil de usar (amigable)

SI

No

7. Cree usted que es necesario implementar un nuevo Sistema Informático (Core Bancario)

Si

No

8. Usted conocía que se va a implementar un Nuevo Sistema Informático (Core Bancario)

SI

No

9. Ha sido capacitado para el uso del nuevo sistema

Si

No

ENCUESTA AL PERSONAL DEL DEPARTAMENTO DE CARTERA Y CONTABILIDAD
NIVEL DE SATISFACCIÓN

1. Departamento donde labora

Crédito y Cartera

Contabilidad

2. Edad

Menor a 30

Entre 30 y 40

Mayor a 40

3. Máximo nivel de estudio alcanzado

Segundo Nivel

Tercer Nivel

Cuarto Nivel

4. Tiempo que trabaja en la Institución Financiera

Menos de 10 años

de 10 a 20 años

Más de 20 años

5. Se encuentra conforme con el sistema con que se trabaja en su departamento

Si

NO

6. El sistema que utiliza es fácil de usar (amigable)

SI

No

7. Cree usted que es necesario implementar un nuevo Sistema Informático (Core Bancario)

Si

No

8. Usted conocía que se va a implementar un Nuevo Sistema Informático (Core Bancario)

SI

No

9. Ha sido capacitado para el uso del nuevo sistema

Si

No

ENCUESTA AL PERSONAL DEL DEPARTAMENTO DE CARTERA Y CONTABILIDAD
NIVEL DE SATISFACCIÓN

1. Departamento donde labora

Crédito y Cartera

Contabilidad

2. Edad

Menor a 30

Entre 30 y 40

Mayor a 40

3. Máximo nivel de estudio alcanzado

Segundo Nivel

Tercer Nivel

Cuarto Nivel

4. Tiempo que trabaja en la Institución Financiera

Menos de 10 años

de 10 a 20 años

Más de 20 años

5. Se encuentra conforme con el sistema con que se trabaja en su departamento

Si

NO

6. El sistema que utiliza es fácil de usar (amigable)

SI

No

7. Cree usted que es necesario implementar un nuevo Sistema Informático (Core Bancario)

Si

No

8. Usted conocía que se va a implementar un Nuevo Sistema Informático (Core Bancario)

SI

No

9. Ha sido capacitado para el uso del nuevo sistema

Si

No

ENCUESTA AL PERSONAL DEL DEPARTAMENTO DE CARTERA Y CONTABILIDAD
NIVEL DE SATISFACCIÓN

1. Departamento donde labora

Crédito y Cartera

Contabilidad

2. Edad

Menor a 30

Entre 30 y 40

Mayor a 40

3. Máximo nivel de estudio alcanzado

Segundo Nivel

Tercer Nivel

Cuarto Nivel

4. Tiempo que trabaja en la Institución Financiera

Menos de 10 años

de 10 a 20 años

Más de 20 años

5. Se encuentra conforme con el sistema con que se trabaja en su departamento

Si

NO

6. El sistema que utiliza es fácil de usar (amigable)

SI

No

7. Cree usted que es necesario implementar un nuevo Sistema Informático (Core Bancario)

Si

No

8. Usted conocía que se va a implementar un Nuevo Sistema Informático (Core Bancario)

SI

No

9. Ha sido capacitado para el uso del nuevo sistema

Si

No