

ESCUELA SUPERIOR POLITECNICA DEL LITORAL



CENTRO DE EDUCACION CONTINUA

Diplomado en Auditoría Informática

IV PROMOCION

PROYECTO

TEMA:

Auditoría de Sistemas al Proceso de Cobranzas Individuales en el Departamento de Recaudaciones de la Empresa Salud S.A., Tomando como Marco Referencial las Prácticas de Control Interno COSO ERM y el Marco Teórico COBIT ®

AUTORES:

Ing. Katty Ronquillo Manjarrez

Ing. Verónica García Vásquez

Ing. Andrés Alvarez Valdez

Año 2011

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL



CENTRO DE EDUCACION CONTINUA

DIPLOMADO EN AUDITORIA INFORMATICA

IV PROMOCIÓN

PROYECTO

TEMA

AUDITORIA DE SISTEMAS AL PROCESO DE COBRANZAS INDIVIDUALES EN EL DEPARTAMENTO DE RECAUDACIONES DE LA EMPRESA SALUD S.A., TOMANDO COMO MARCO REFERENCIAL LAS PRACTICAS DE CONTROL INTERNO COSO ERM Y EL MARCO TEORICO COBIT®

AUTORES

ING. KATTY RONQUILLO MANJARREZ

ING. VERONICA GARCIA VASQUEZ

ING. ANDRES ALVAREZ VALDEZ

AÑO

2011

INDICE

CAPITULO 1. INTRODUCCION	1
1.1 Objetivo del Proyecto	1
1.2 Alcance del Proyecto	1
1.3 Metodología, Estándares y Procedimientos.....	2
CAPITULO 2. MARCO GENERAL DE LA EMPRESA	6
2.1 Introducción.....	6
2.2 Información del Departamento de TI.....	6
2.3 Organigrama del Departamento de TI	6
2.4 Roles y Responsabilidades.....	7
2.5 Infraestructura Técnica	7
2.5.1 Software.....	8
2.5.1.1 Descripción General.	8
2.5.1.2 Módulos	8
2.6 Departamentos Usuarios.....	8
2.6.1 Descripción de cargos.....	9
2.7 Hardware.....	10
2.7.1 Servidor de Aplicaciones.....	10
2.7.2 Servidor de Base de Datos.....	10
CAPITULO 3. AUDITORIA DE LA APLICACIÓN	11
3.1 Introducción.....	11
3.2 Alcance de la Auditoría	11
3.3 Planeación de la Auditoría.....	11
3.4 Antecedentes.....	12
CAPITULO 4. RESULTADOS DE LA AUDITORIA.....	15
4.1 Estrategia y Planeación de los Sistemas de Información.....	15
4.2 Operación de los Sistemas de Información.....	16
4.3 Relaciones con Proveedores Externos	16
4.4 Seguridad de la Información.....	17
4.5 Planeación de la Continuidad del Negocio	18
4.6 Implementación y Mantenimiento de los Sistemas de Aplicación	18
4.7 Infraestructura.....	18
4.8 Controles de los Aplicativos.....	19
4.9 Prueba a los Datos.....	19
CAPITULO 5. CONCLUSIONES	21
CAPITULO 6. BIBLIOGRAFIA	22
ANEXOS.....	23

CAPITULO 1. INTRODUCCION

1.1 Objetivo del Proyecto

Realizar una evaluación exhaustiva sobre los controles implementados en el proceso de cobranzas individuales en el Departamento de Recaudaciones de la Empresa Salud S.A., de manera que puedan ser evaluados tomando como marco referencial las prácticas de control interno COSO ERM y el marco teórico **COBIT®**.

1.2 Alcance del Proyecto

1. Evaluación de la Planeación y Estrategia de los Recursos de Información dentro del departamento.
 - Evaluar las estrategias, los planes y los presupuestos de los sistemas de información para que sean consistentes con las estrategias actuales sean consistentes.
 - Evaluar los ambientes de procesamiento de la computadora e información inherente al departamento.
 - Evaluar el nivel del personal calificado.
 - Evaluar capacitaciones apropiadas al personal.
 - Evaluar las funciones y responsabilidades del personal.
2. Evaluar la Operación y disponibilidad de los Sistemas de Información.
 - Evaluar que los sistemas soporten las funciones del departamento mediante un procesamiento eficiente.
 - Evaluar que los sistemas estén disponibles a medida que sean necesarios para el proceso del departamento.
 - Evaluar que los controles implementados aseguren la calidad de la información.
3. Evaluar la Seguridad de los datos y la información procesada en el departamento.
 - Evaluar y asegurar que los datos y la información se encuentren protegidos de modificaciones, divulgación y uso por parte de personas no autorizadas.
 - Verificar que la información esté debidamente soportada y respaldada ya sea en medio físico o magnético.

- Evaluar que las transacciones procesadas cumplen los controles establecidos.
4. Evaluar el Soporte a la Infraestructura tecnológica de Red otorgado al departamento.
 - Evaluar que el soporte al software de la red y las comunicaciones se implemente apropiadamente y funcionen consistentemente con las intenciones de la Gerencia.
 - Evaluar que, todas las modificaciones al software existente de la red y las comunicaciones se implementen oportunamente.
 - Evaluar que se cuenta con una adecuada administración de los recursos de usuarios en red.
 5. Evaluar el control a las aplicaciones.
 - Pruebas de controles de acceso a usuarios autorizados.
 - Pruebas de controles de Ingreso o validación de datos.
 - Pruebas de controles de rechazo de transacciones no autorizadas.
 - Verificación del cumplimiento de normativas y leyes en cálculos.
 - Pruebas en el Procesamiento de la información.
 - Pruebas de controles en salida de datos de reportes/consultas.
 - Generación de información y reportes para entes de control.

1.3 Metodología, Estándares y Procedimientos

Como parte del proceso de elaboración de la tesis Auditoría de Sistemas al proceso de Cobranzas Individuales en el Departamento de Recaudaciones de la empresa Salud S.A., tomando como marco referencial las prácticas de control interno COSO ERM y el marco teórico **COBIT®**, y con el objeto de presentar una descripción, alcance y cronograma de trabajo, hemos procedido a realizar un informe “Resumen ejecutivo” el cual contendrá el siguiente alcance:

- Introducción.
- Metodología de trabajo.
- Principales inhibidores de TI frente al negocio.

1. Introducción

Una de las mayores preocupaciones para la alta dirección de una entidad ya sea esta de servicios o comercial siempre ha sido la de poder comprender en un lenguaje claro y entendible, si la plataforma tecnológica de información (**TI**) que soporta todas las operaciones críticas que el negocio requiere está lo suficientemente completa, segura y sobretodo debidamente controlada.

La administración de TI integra e institucionaliza las buenas prácticas para garantizar que los sistemas en la empresa soportan los objetivos del negocio. De esta manera, el gobierno de TI facilita que la empresa aproveche al máximo su información, maximizando así los beneficios, capitalizando las oportunidades y ganando ventajas competitivas.

Una mala administración de TI, en la mayoría de las ocasiones, es consecuencia de una mala administración de los procesos globales internos de las empresas. Es común, en la práctica, encontrar empresas que no poseen métricas que permitan establecer de una manera cuantitativa y cualitativa, el grado de madurez de los procesos operativos que soportan a las líneas de negocio críticas, ya que al no tener un área de procesos debidamente eficiente que realice la función de enlace o interfaz entre el usuario final y TI, el área de Sistemas debe incurrir en altos costos operativos para poder adaptar el sistema informático al proceso, muchas veces, sin una directriz adecuada. Lo que termina ocurriendo es que TI se convierte en un “Virtual dueño del proceso” adquiriendo toda la responsabilidad del mismo, en consecuencia terminan generando un costo elevado frente al beneficio que se desea obtener por parte de la alta dirección.

Por lo tanto, el trabajo adecuado y conjunto entre las áreas estratégicas de apoyo es fundamental para el buen gobierno de TI, lo que llevara a un nivel óptimo de administración, gestión y entrega de valor hacia el negocio mediante el servicio continuo de soluciones integrales.

Dentro de este ámbito entra el concepto de Auditoría de sistemas de información, el cual tiene como universo de acción todo el proceso de revisión de la entrega de valor de TI hacia el negocio.

Con este antecedente, el objetivo fundamental de nuestra metodología de auditoría de sistemas es la “**Alineación de la Tecnológica de la Información (TI) con el negocio**”, mediante la evaluación exhaustiva de los controles implementados ya sean estos manuales o automáticos en los sistemas de información que soporten los procesos críticos: Ventas Individual, Emisión y entrega individual, Cobranzas individual, Recaudaciones segundas cuotas, motivo de esta tesis.

Para conseguir este objetivo, hemos contemplado 2 frentes dentro del proceso de auditoría de TI:

- Desarrollar e implementar una estrategia de auditoría de TI basada en riesgos para la organización de acuerdo con los estándares, las directrices y mejores prácticas de auditoría de sistemas adquiridas en base al conocimiento y la experiencia.

- Planear relevamientos específicos para validar que los controles en los sistemas informáticos que soportan al negocio están protegidos y controlados.

2. Metodología de trabajo

La metodología de trabajo a aplicada en esta tesis en el proceso de auditoría de sistemas de información se basará en COSO ERM para las áreas de revisión tecnológica y el marco teórico **COBIT®** alineados en sus 4 dominios, las cuales tendrán como base primordial los procesos existentes orientados íntegramente a riesgos por cada proceso crítico dentro del Sistema Integrado de Gestión de Medicina Pre pagada (SIGMEP) que posee la empresa.

Los cuatro dominios en los que nos basaremos para aplicar la auditoría serán:

Planear y Organizar (PO)

Planeación y estrategia

Aquí se releva la estructura organizacional del área de sistemas, el plan estratégico y operativo, la administración de las inversiones de TI, la administración de los proyectos y la administración de la calidad en la entrega de valor de los servicios de TI.

Entrega y Soporte (DS)

Operaciones

Definición de los SLA's (Niveles de servicios) a nivel interno, identificación de la mesa de ayuda al usuario, administración de problemas o incidentes, y administración de procesos operativos.

Relación con proveedores externos

Definición de los SLA's (niveles de servicios) con los proveedores, monitoreo del cumplimiento de los servicios, y razonabilidad de los contratos con los proveedores.

Seguridad de la información

Existencia de políticas y procedimientos de seguridad, Administración de las seguridades lógicas, identificación y autenticación de accesos, protección de accesos indebidos de terceros, clasificación de datos sensitivos, revisión de pistas de auditoría, seguridad en transmisión de datos, seguridad del acceso físico al centro de cómputo, control y prevención de virus, transferencias electrónicas.

Adquirir e Implementar (AI)

Implementación y mantenimiento de aplicaciones

Estándares de desarrollo y mantenimiento de aplicaciones, procedimientos de control de cambios a programas, control de entrada a producción de nuevas versiones, administración de fases y pruebas en paralelo, ambientes de pruebas, y plan piloto, administración del control de calidad.

Infraestructura

Administración desempeño y documentación de la base de datos, red, hardware y software base.

Monitoreo y Evaluación (ME)

Control a las aplicaciones

Aquí se releva con el usuario final mediante pruebas de escritorio, control de acceso a usuarios autorizados, control de ingreso o validación de datos, rechazo de transacciones no autorizadas, niveles de parametrización, pruebas a los controles en salidas de datos.

Dentro de las técnicas a utilizar para la obtención de la información serán las siguientes:

- Pruebas de escritorio.
- Entrevistas.
- Relación 360° en toma de incidentes (TI, Dueño del proceso, usuario final).
- Reuniones de trabajo.

3. Principales inhibidores

INHIBIDOR	IMPACTO	AREAS	ACCION A TOMAR
Apertura por parte de los dueños de los procesos dentro de la empresa	Medio	SISTEMAS RIESGOS	Se procedió a realizar una presentación ejecutiva para el personal de las áreas auditadas con el fin de que conozcan el alcance y el enfoque de la auditoría.
El tiempo requerido por parte de los integrantes del equipo de elaboración de esta tesis para realizar las inspecciones in-situ.	Medio	EQUIPO DE ELABORACION DE TESIS	Se procedió a adquirir herramientas tecnológicas tales como Laptop y pda's que nos permitió el estar conectados en tiempo real y poder gestionar de una manera más óptima las visitas en la empresa, motivo de esta tesis.

CAPITULO 2. MARCO GENERAL DE LA EMPRESA

2.1 Introducción

Es el sistema de salud que cuenta con la empresa más grande de medicina pre pagada del Ecuador, SALUDSA, el proveedor más importante de servicios ambulatorios privados del país, LATINOMEDICAL y el proveedor más importante de servicios odontológicos privados del país ODONTOCARE.

Formada con el objetivo de proveer soluciones integrales y completas al cliente, esta corporación cuenta con la gran experiencia de 18 años de gestión en medicina pre pagada, 10 años de servicios médicos y 2 años de prestación de servicios dentales, además de los 35 años de labores de sus principales socios, en el campo de los seguros.

Visión

Seremos el mejor sistema integral de salud con vocación de servicio y compromiso con el usuario.

Misión

Ocuparnos de la salud de las personas.

2.2 Información del Departamento de TI

La misión del Departamento de TI es soportar de manera tecnológica todos los negocios de la organización.

2.3 Organigrama del Departamento de TI

La Organización del Departamento de TI es de tipo vertical como muestra el organigrama, contando con un Gerencia de TI que rinde cuentas al directorio de accionistas, debajo de esta Gerencia se encuentran las jefaturas a nivel nacional distribuidas por cada área funcional del departamento, como son: Proyectos, Desarrollo, Producción, Infraestructura y Soporte.

2.4 Roles y Responsabilidades

Gerente de Proyectos.- Esta Gerencia se encuentra a cargo de los proyectos de innovación y cambios de tecnologías dentro de la empresa, los proyectos tienen duración de acuerdo a los alcances establecidos, actualmente existen tres Gerencias de proyectos en curso.

Jefe de Gestión de Servicios y Soporte a Nivel Nacional.- Esta Jefatura es la encargada de los servicios de soporte a nivel nacional en temas de Hardware, Software adquirido y Software de aplicaciones en uso.

Jefe de Producción a Nivel Nacional.- Jefatura encargada de la puesta en producción de nuevas aplicaciones, actualizaciones de aplicaciones adquiridas y desarrolladas in-situ, y cambios de estructuras.

Jefe de Infraestructura a Nivel Nacional.- Jefatura que se encarga del mantenimiento, adquisición de servidores, equipos de comunicación, Firewall, UPS, y todo lo referente a infraestructura.

Jefe de Desarrollo de Aplicaciones a Nivel Nacional.- La jefatura de Desarrollo es la encargada de coordinar los trabajos de desarrollo y mantenimiento de las aplicaciones usadas por las diferentes áreas dentro de la empresa.

2.5 Infraestructura Técnica

La Infraestructuras que soporta las aplicaciones son: Servidores de Bases de Datos, Servidores del Sistema de Archivos, Switch 24 y 48 puertos marca CISCO, Impresoras Epson LX-300+, FX-1170, FX-1180, Lexmark Z32, Z35. Esta infraestructura es necesaria para el funcionamiento de las aplicaciones y sistemas de comunicación en general.

2.5.1 Software

2.5.1.1 Descripción General.

La Empresa actualmente utiliza el Sistema de Gestión de Medicina Pre pagada (SIGMEP) de desarrollo propio en sus áreas administrativas tales como: Ventas, Recaudaciones, Tesorería, Servicio al Cliente y Producción, las áreas Contables Financieras usan además el sistemas INTEGRITY que se interconecta con el sistema administrativo SIGMEP, también se evidencia el uso de software adquirido de Microsoft.

2.5.1.2 Módulos

Los módulos de los que consta el SIGMEP son: Catálogo, Producción, Recaudaciones, Liquidaciones, Reportes y Seguridades, cabe señalar que este sistema no es usado en las áreas médicas sino en las áreas administrativas de SALUD.

El Módulo en el que enfocamos la auditoría es el Recaudaciones que consta básicamente de las siguientes opciones: Actualizaciones de Débitos, Anulación de Notas de Crédito, Consulta de Notas de Crédito, Consulta de Notas de Débito, Cuadre de Caja, Cuotas en Mora o por Cobrar, Cuotas pagadas, Devolución de saldo a favor, Generación de Notas de Crédito, Generación de Notas de Débito, Subida Automática de Débitos, Subida Automática de Débitos Reproceso, Gestión de Citas.

2.6 Departamentos Usuarios.

Los usuarios del sistema están distribuidos dentro de la Empresa en diferentes departamentos tales como: Ventas, Prestaciones y Beneficios, Producción, Auditoría Médica, Liquidaciones, Recaudaciones, Planificación, Despacho, Tesorería, Finanzas.

Estos departamentos usan los módulos del sistema SIGMEP de acuerdo a las necesidades de cada área.

Como hemos indicado enfocaremos la auditoría al Área de Recaudaciones, la misma que se encarga dentro de la empresa a la recuperación de cartera, de manera general el gestor de esta área es dueño de dos procesos bien definidos que son, Cobranza Individual y Recaudación Segundas cuotas y más, considerando la relación directa con los procesos de Venta Individual como proveedor de entrada y el proceso de Emisión y Entrega Individual como proceso de salida.

2.6.1 Descripción de cargos



Gerencia Nacional
Quirmaucho Caicedo Jenny Alexandra
Jefatura Regional
Munez Vera Nelson Alfredo
Jefatura Regional
Enfo Illescas Viviana Aydee
Martillo Avala Wendy Teresa
Cargos
Arias Hidalgo Edwar Richard
Cuadros Navarro Luis Stalin

El área de Recaudaciones cuenta con una Gerencia Nacional se encarga de gestionar todo lo referente al servicio al cliente, incluida la cobranza, toma de decisiones, cambios estratégicos y adopción de nuevas políticas siempre que estén alineadas con la estrategia del negocio. Cuenta también con dos jefaturas regionales encargadas de coordinar las tareas dentro del área como Gestión de Cobranza, Gestión de Citas, Autorizaciones Bancarias. Además encontramos cargos como Asistente de Recaudaciones SR, Asistente de Recaudaciones JR y Cobrador, cada uno de ellos encargado de la gestión operativa dentro del área.

2.7 Hardware

Dentro del área de Recaudaciones encontrados 5 computadoras de escritorio marca Lenovo, CORE 2 DUO, 2.4 GHZ, 120 GB en RAM, monitor plano de 17", estos equipos asignados a cada miembro del departamento, y una computadora portátil Toshiba asignada a la jefatura, además el departamento cuenta con un impresora Xerox que es usada para la impresión de facturas y otros documentos.

2.7.1 Servidor de Aplicaciones.

El centro de cómputo cuenta con un sistema de BLADE CENTER con 4 procesadores físicos y 8 lógicos, con un total de 16 GB por cuchilla en RAM, dentro de esta infraestructura está incluido el servidor de aplicaciones, en este se almacenan los objetos de los programas fuentes de las aplicaciones, usadas entre estas, SIGMEP, INTEGRITY, Incidencias HELP DESK, Quejas, CORVU, HIS-ISIS, OPEN-DENTAL.

2.7.2 Servidor de Base de Datos.

El servidor de Base de datos se encuentra en una distribución de BLADE CENTER al igual que el servidor de Aplicaciones, en este servidor se almacenan las bases de datos de las aplicaciones de que cuenta SALUD, este servidor se encuentra dentro del centro de cómputo aquí se almacenan las bases del sistema SIGMEP, INTEGRITY, Incidencias HELP DESK, Quejas, CORVU, HIS-ISIS, OPEN-DENTAL, además se cuenta con un servidor de base de datos alterno en la ciudad de Guayaquil en el que se guarda la información de forma progresiva por medio de un proceso de réplica que se ejecuta cada 10 minutos.

CAPITULO 3. AUDITORIA DE LA APLICACIÓN

3.1 Introducción

De la auditoría realizada al proceso de cobranzas individuales en el Departamento de Recaudaciones de la empresa de medicina pre pagada del Ecuador, Salud S.A., se puede colegir que representan un nivel medio de riesgo tecnológico, ya que pese a que las líneas de negocio se encuentran en fase de automatización, no se tienen identificados los propietarios de la información o dueños de los procesos, no se tiene una medición del nivel de madurez de los procesos y no existe tampoco indicadores de gestión por procesos lo que generaría un riesgo operativo al momento de generar nuevos productos tecnológicos que sustenten la operativa de los sistemas informáticos.

3.2 Alcance de la Auditoría

Dentro del alcance que se propuso al ente auditado (Salud S.A.) se coordinó revisar los siguientes procesos:

Venta Individual
Cobranza Individual
Recaudación Segundas Cuotas y Más
Emisión y Entrega Individual

3.3 Planeación de la Auditoría

Se hace un relevamiento del entorno tecnológico y de recurso humano del área que maneja el Sistema Integrado de Gestión de Medicina Pre pagada (SIGMEP) mediante los formularios de auditoría informática (FAI) que nos permitirá obtener una comprensión pormenorizada.

- Entrevistas con los dueños de los procesos y el respectivo personal operativo para realizar las pruebas de escritorio respectivas.
Ver Anexo A. FAI-001, Anexo B. FAI-002, Anexo C. FAI-003, Anexo D. FAI-004 y Anexo E. FAI-005.
- Elaboración de los flujos y diagramas de procesos.
Ver Anexo F. Diagrama de procesos Salud S.A
- Elaboración de los mapas de riesgos por proceso crítico.
Ver Anexo G. Mapas de Riesgos
- Elaboración del informe ejecutivo que contemplará las observaciones y recomendaciones.

3.4 Antecedentes

- **Emisión y Entrega Individual**

En este proceso se realizará la recepción de los documentos, la notificación a los clientes, la entrega de la carpeta por parte del Ejecutivo de Cuentas de la empresa Salud S.A., las llamadas a través del call center de la empresa Cronix para conocer la satisfacción de los clientes y la revisión de los resultados por parte de la Gerencia de Servicio al Cliente.

Se reciben los documentos para la elaboración del contrato y se revisa que los datos se encuentren completos y correctos. Se revisa la base de Siniestralidad el médico auditor determina si es sujeto a cobertura o no. Si el cliente acepta se ingresa la información del contrato de Gestión de Medicina Pre pagada y se envía la orden para la emisión de tarjeta y factura las cuales serán adjuntadas a la carpeta del cliente.

Se devuelve la cuota inicial al cliente si no existe la aceptación para la firma del contrato.

A través de la empresa Cronix se realiza la llamada post venta para conocer la opinión del cliente. Y la Gerencia de Servicio al Cliente revisa los resultados de las llamadas post venta.

- **Ventas Individual**

En este proceso se prospecta los clientes, se realiza la venta del producto, la auditoría médica así como la recepción y firma de documentos.

Mediante citas telefónicas se realiza las visitas a los prospectos, se realiza la entrega de formularios y se realiza la recopilación de la información para la elaboración de los contratos.

Se identifica los clientes según las enfermedades no cubiertas, así como la presentación de los productos, coberturas y exclusiones, además de la declaración para el chequeo médico por parte del médico auditor de la empresa.

A través de la cita con el médico, se determinará las exclusiones y asegurabilidad del cliente ya el médico emitirá un informe sobre el cual se informa si el cliente es o no sujeto de cobertura.

- **Cobranzas Individual**

El proceso empieza con la generación del reporte de cuotas impagas de clientes individuales, este reporte se emite el primer días hábil del mes, cada ejecutivo de cuenta tiene cartera designada para empezar la gestión de cobranza, la gestión es telefónica, si el cliente es contactado se debe registrar en el control de citas para proceder a realizar la cobranza presencial que consiste en la visita de un cobrador a la dirección que indique el cliente, este también puede solicitar la cita por medio de una llamada telefónica al call center de Salud S.A.

Cada cobrador debe llevar consigo la factura impresa de las cuotas que irá a cobrar, esta factura la puede emitir el ejecutivo de cuentas o el cobrador. Si el cliente no ha podido ser contactado o éste no está interesado en seguir con el contrato de Salud S.A. se deberán anular todas las facturas emitidas antes de anular dicho contrato. Los contratos también se anulan automáticamente si estos tienen más de tres cuotas en MORA.

Por otro lado cada cobrador deberá generar su reporte de visitas y devolver las facturas que no han sido entregadas a los clientes a los al ejecutivo de cuentas para su respectiva anulación, si la gestión es exitosa el cobrador deberá entregar el dinero recaudado al tesorero para que este cancele las facturas cobradas en el sistema, cada día el cobrador genere un reporte de su gestión y cierra la cita gestionada en el sistema que aún permanece abierta y el tesorero genera un reporte de cuadro de caja.

- **Recaudación Segundas Cuotas y Más**

Todo empieza con la intervención del cliente quien decide si el pago de sus cuotas del seguro las hará por medio de “pago directo” en las oficinas de Salud S.A., o con la modalidad de “débito a cuenta” Salud S.A. al momento cuenta con esta modalidad para los Bancos Bolivariano, Guayaquil, Machala, Pichincha, Produbanco, Pacífico, Internacional, Austro solamente, si el cliente cuenta con una cuenta que no pertenezca a estos bancos, el pago deberá ser directo en las oficinas de Salud S.A.

Cuando el ejecutivo de cuenta obtiene la autorización de parte del cliente para el débito a cuenta, éste envía dicha autorización al banco los 15 y 25 de cada mes, la generación de las cuentas por cobrar mensuales de los clientes se realiza los días 27 y 29 de cada mes, posteriormente el ejecutivo genera el “archivo para banco” que no es otra cosa que un archivo plano con características especiales de acuerdo al Banco al que corresponden, este archivo obedece a un trama particular de cada Banco en el que consta el valor adeudado de cada cliente, numero de contrato o contratos, número de cuenta tipo de cuenta código de banco, entre

otros, esta trama llega a cada banco y es procesada, previamente debe existir la autorización del cliente para del débito a cuenta, este archivo plano es enviado a los bancos mediante un dispositivo digital que puede ser un CD.

El Banco procede a subir el archivo existirán cuentas que se debiten y cuentas que no por algún tipo de error en el archivo o en la información contenida en este, este informe de débitos no exitosos es enviado por parte del Banco a Salud S.A., y el ejecutivo de cuenta se encarga de validar la información y el reproceso.

El banco envía dos archivos uno de débitos exitosos y otro de débitos no exitosos, el ejecutivo de cuentas, con el archivo de débitos exitosos ejecuta la subida al sistema de Salud S.A este proceso lo que hace es pasar de MORA a COBRADAS las cuentas por cobrar del mes. El ejecutivo de cuentas toma el archivo de débitos no exitosos y reprocesa, el ejecutivo puede realizar varias acciones después de la revisión de los débitos no exitosos, puede revisar si existe algún error en el archivo, incluso puede solicitar al cliente un nueva cuenta para el débito, para lo cual deberá volver a realizar el proceso de autorización de la cuenta como al principio, aunque el cliente también tiene la opción de solicitar “pago directo”.

Durante todo este proceso, si no ha sido posible el débito durante muchos meses el cliente puede solicitar la anulación del contrato o el sistema anulará el contrato automáticamente.

Las facturas generadas en este proceso son enviadas a los clientes, y las facturas que no han podido ser entregarse archivan en Salud S.A.

CAPITULO 4. RESULTADOS DE LA AUDITORIA

4.1 Estrategia y Planeación de los Sistemas de Información

- La unidad de sistemas todavía no ha implementado un plan estratégico a mediano o a largo plazo, el cual apoye la estrategia general del negocio y los requerimientos de los sistemas de información de la empresa, esto impide que la infraestructura informática actual sea consistente con los objetivos de la Empresa.

Recomendaciones:

La Administración debe definir una estrategia tecnológica a mediano y largo plazo que vaya de acuerdo con las metas y estrategias comerciales de la empresa. Dicha estrategia deberá soportarse en un presupuesto que incluya la inversión y el detalle de los costos operativos para la tecnología de información (hardware, software, personal).

Es necesario que se realice un plan operativo que detalle los proyectos, sus prioridades, recursos y un cronograma de trabajo, lo cual ayudará a asegurar y evaluar que las actividades se realicen para apoyar a los objetivos de la empresa y que los recursos de información se utilicen de manera adecuada.

- La Empresa carece de una clasificación de datos, en el cual se incluya a los dueños y las categorías de seguridad. Esto puede ocasionar que los permisos o reglas de accesos en el sistema aplicativo actual no estén acordes a los perfiles y funciones del personal que accede al mismo.

Recomendaciones:

La Gerencia General deberá establecer un marco de referencia de clasificación general relativo a la ubicación de datos en clases de información, así como la asignación de propiedad. Adicionalmente las reglas de acceso para las clases de datos deberán definirse apropiadamente con procedimientos adecuados y aprobados.

- La Empresa carece de procedimientos que le permitan realizar un entrenamiento cruzado, a fin de contar con personal de respaldo para puestos claves como es el caso del Jefe de Sistemas. Esto es un alto riesgo operativo, debido a la dependencia que se tiene de este personal y que no existe un respaldo técnico que pueda cumplir con las funciones a él encargadas.

Recomendaciones:

La Gerencia de TI deberá establecer procedimientos adecuados a fin de identificar personal clave, el mismo que deberá contar con personal de respaldo, con la finalidad de solucionar posibles ausencias y que afecten el desenvolvimiento normal de los procesos y continuidad del procesamiento de la información.

4.2 Operación de los Sistemas de Información

- Se observó de que los diferentes procesos que se ejecutan en el Departamento de TI de la empresa no se encuentran normados ya que el Manual de Políticas y Procedimientos para los diferentes ambientes de desarrollo y producción, no se encuentran adecuadamente actualizados, se encuentran formatos de procedimientos desactualizados; esto podría ocasionar que no se definan adecuadamente y de manera oportuna los requerimientos operacionales y sus niveles de servicio y que no se detecten problemas que podrían afectar de manera importante el rendimiento del sistema de Recaudaciones y otras áreas de la Empresa.

Recomendaciones:

La Administración de la Empresa y el Jefe de Sistemas deberán establecer responsabilidades y procedimientos para la gestión y operación de las instalaciones de procesamiento de información, los cuales deberán incluir instrucciones operativas y procedimientos apropiados de respuesta a incidentes, así como los niveles de servicio, con el fin de garantizar el correcto funcionamiento de los sistemas de información. Adicionalmente, es responsabilidad de la función de sistemas de información establecer políticas y directrices generales para ésta área, que vayan acorde con el tamaño de la organización y con los planes de la Gerencia.

4.3 Relaciones con Proveedores Externos

- Si bien la Empresa tiene un procedimiento para la adquisición de bienes, el mismo no se encuentra a nivel de detalle en el caso de adquisición de bienes y servicios informáticos, en la que se incluya la emisión de un informe técnico realizado por la jefatura de sistemas, previo a cualquier adquisición. La falta de este procedimiento podría ocasionar que las compras de los recursos tecnológicos que se realicen no cuenten con las especificaciones técnicas necesarias y por lo tanto no se ajusten a los requerimientos de la Empresa.

Recomendaciones:

Se deberá definir políticas y procedimientos de adquisición de bienes y servicios informáticos de forma más detallada en el cual se especifiquen como por ejemplo: requerimiento inicial, número mínimo de proveedores, evaluación, detalles técnicos

entre otros; con el fin de asegurar que las compras que se realicen cumplan con las especificaciones técnicas necesarias de acuerdo con las necesidades de la Empresa.

4.4 Seguridad de la Información

- La Empresa todavía no ha implementado políticas, normas y procedimientos de seguridades adecuados que proporcionen un control eficiente de los recursos de información para el ambiente de procesamiento computacional; es así que no ha definido un propietario de cada activo de información que tome decisiones sobre la clasificación y derechos de acceso; esta situación podría afectar la confidencialidad y confiabilidad de la información, especialmente de la información sensible que se maneja en el área de Recaudaciones.

Recomendaciones:

Implementar una política de seguridad que suministre una orientación general acerca de la asignación de funciones de seguridad y responsabilidades dentro la Empresa. En esta política deberá definirse claramente los procesos de administración de seguridad y los recursos físicos, los propietarios de la información, los perfiles y accesos a la información, entre otros. Esta política deberá ser comunicada a los usuarios y contener al menos lo siguiente:

- La definición de la seguridad de la información, sus objetivos y alcance generales y su importancia;
 - Breve explicación de las políticas, principios, normas y requisitos de cumplimiento en materia de seguridad, que son especialmente importantes para la Empresa, por ejemplo:
 - Prevención y detección de virus y demás software malicioso;
 - Administración personal de claves de usuario
 - Administración de la continuidad del negocio;
 - Consecuencias de las violaciones a la política de seguridad;
 - Definición de las responsabilidades generales y específicas en materia de gestión de la seguridad de la información.
-
- El acceso al ambiente de producción no está adecuadamente restringido, ya que el encargado de la jefatura de sistemas, puede acceder libremente a los archivos de datos, claves de todos los usuarios y a todas las funciones de procesamiento del aplicativo, así como también no existe cambio periódico de la clave en el sistema aplicativo ni en la de acceso a la red.

Recomendaciones:

Es prioritario que el módulo de seguridad sea administrado por personal ajeno a la Jefatura de Sistemas, el cual se encargará de dar los permisos a los usuarios, con el

fin de garantizar una adecuada segregación de funciones en la administración de las seguridades. Además se deberá establecer dentro del sistema aplicativo y la red de comunicaciones, que periódicamente se cambie la clave cada 60 días. Esta clave deberá ser encriptada y administrada por cada usuario. Todos estos procedimientos deberán ser detallados en la política de seguridad de la información de la Empresa.

4.5 Planeación de la Continuidad del Negocio

- La empresa no ha definido un plan de continuidad del procesamiento de la información, situación que ocasiona que no cuente con un instrumento que le permita afrontar adecuadamente eventuales situaciones de emergencia y que asegure un esquema de continuidad del negocio.

Recomendaciones:

Elaborar un plan de contingencia para la tecnología de información que contenga como mínimo un análisis que identifique los principales escenarios de contingencia así como los procedimientos necesarios que permitan solventar efectivamente la continuidad de las operaciones ante cualquier situación de emergencia, para el efecto deberá definir los equipos alternos, respaldos de la información, personal a cargo y la información (teléfonos, e-mails, etc.) que permita contactarlos oportunamente. El plan de contingencias tecnológico deberá ser probado e incorporado como parte del plan de continuidad del negocio en el proceso de administración integral de riesgos.

4.6 Implementación y Mantenimiento de los Sistemas de Aplicación

- El Departamento de Sistemas no cuenta aún con un procedimiento adecuado para la administración de cambios de software, así como también el control y la distribución de software, lo que podría causar errores en la instalación de versiones del software aplicativo, existen formularios pero se llenan de manera esporádica.

Recomendación:

El Jefe de Sistemas deberá implementar un procedimiento para la administración de cambios de software, cuyo control, monitoreo y seguimiento de aquellos cambios realizados en el sistema aplicativo deberá ser realizado por la unidad de Control de Calidad al no poseer un área de Auditoría Interna.

4.7 Infraestructura

- No existe todavía documentación técnica de los diferentes módulos que se han desarrollado y que forman parte del sistema SIGMEP, ni del diagrama entidad-relación de las diferentes tablas que conforman la base de datos. Esto puede

provocar que ciertos requerimientos solicitados por los usuarios no sean atendidos oportunamente y en caso de ocurrir alguna falla en los sistemas o tablas de información no se pueda restablecer el servicio de manera apropiada.

Recomendación:

El jefe del Departamento de Sistemas deberá elaborar la documentación técnica del sistema aplicativo que tiene la Empresa, la misma que deberá contar con el detalle de cada tabla y el modelo entidad-relación de los diferentes módulos que conforman dicho sistema. Este proceso es una parte fundamental del diseño de sistemas aplicativos y que está inmerso dentro de la metodología de desarrollo e implementación.

4.8 Controles de los Aplicativos

- No se tiene el diagrama entidad relación de las tablas que conforman la base de datos del módulo de Recaudaciones, lo que ocasiona que al producirse un error en el sistema aplicativo, no se cuente con la información técnica, para su corrección.

Recomendación:

El jefe del Departamento de Sistemas deberá elaborar el manual técnico y de usuario del módulo de Recaudaciones a fin de contar con información suficiente en caso de presentarse algún error en la operatividad del aplicativo.

4.9 Prueba a los Datos

- Se observó que el proceso de almacenamiento de toda información bancaria de los clientes la Empresa no realiza ningún tipo de encriptación, siendo estos archivos tipo texto que son almacenados en medios externos magnéticos y ópticos. Esto podría originar un alto riesgo operativo debido a que los datos podrían ser fácilmente manipulados, afectando de manera importante la integridad, confiabilidad y disponibilidad de todos los datos respaldados del sistema SIGMEP.

Recomendación:

El área de Sistemas deberá automatizar la sincronización de datos entre el banco contratante y su sistema de cobro, de manera que cuando exista dinero en la cuenta, el banco pueda obtener en línea el valor real a ser debitado incluyendo pagos atrasados más la mora correspondiente según la ley, esto controlara en parte el riesgo de consistencia de los datos.

La Gerencia General deberá instruir a la Jefatura de Sistemas, la implementación de un método de protección de datos no solo al momento de generar los respaldos de toda la información de la Empresa, sino a los que reposan en el servidor central y prioritariamente la data del Sistema de Información SI. Así como también, controles internos que no permitan acceder a producción a personal de sistemas sin la debida autorización por parte del dueño del proceso.

- Se observó que existen inconsistencias en la generación de las Notas de Protesto de cheques entregados a la Empresa, las notas de protesto se generan como cotizaciones nuevas con motivo NOTIFICACION, las mismas que no se calculan de forma correcta, no se calcula el valor del gasto ni el valor del seguro campesino, es decir, el monto de la nota no es igual al monto protestado, similar problema sucede con los valores de la cuotas y facturas emitidas, lo que evidencia que no existe validación de controles esenciales en los programas de aplicaciones.

Recomendación:

El jefe de sistemas deberá coordinar con el área de desarrollo para que se realicen las correcciones necesarias a los procesos identificados, además se deberán implementar procesos de cuadro intermedios que notifiquen inconsistencias en los procesos de generación de Notas de Protesto.

- Si bien la Empresa estructura del manejo de la información en la Empresa es centralizado; se pudo observar que los procesos de replicación de los Servidores de datos de las sucursales con el Servidor de la Matriz no se encuentran sincronizados, debido a que los mismos son ejecutados de forma manual y sin un orden cronológico. Lo que ocasiona que se origine un desfase de la información existente entre el Servidor Matriz y el de las sucursales, al momento de generar cualquier tipo de reporte de cuadro en el área de Recaudaciones, causando un alto riesgo operativo que afecta de manera importante a la integridad, disponibilidad y confidencialidad de la información.

Recomendación:

La Gerencia General y la Jefatura de Sistemas deberán implementar de forma urgente el afinamiento de los procesos de replicación, y de innovar recursos tecnológicos que ayude de forma óptima y eficaz a que los datos centralizados sean íntegros, confiables y disponibles.

CAPITULO 5. CONCLUSIONES

De la auditoría realizada al proceso de cobranzas individuales en el Departamento de Recaudaciones de la empresa de medicina pre pagada del Ecuador, Salud S.A., se puede colegir que los riesgos asociados al sistema motivo de esta auditoría, representan un nivel medio de riesgo tecnológico, ya que en el aspecto de mantener la información completa se pudo evidenciar la falta de controles en los reportes emitidos por el sistema, en cuanto al aspecto de mantener la información segura se pudo evidenciar que el oficial de seguridad se encuentra dentro del área de tecnología evidenciando una falta de independencia objetiva y de control, y por último, no se tienen identificados los propietarios de la información o dueños de los procesos, no se tiene una medición del nivel de madurez de los procesos y no existe tampoco indicadores de gestión por procesos lo que generaría un riesgo operativo al momento de generar nuevos productos tecnológicos que sustenten la operativa de los sistemas informáticos.

Uno de los pilares fundamentales que debe existir en todo profesional que desempeñe las funciones de auditoría ya sea esta en el campo de la Tecnología de la Información, o en el campo financiero operativo, es la objetividad profesional, ya que esta permite el poder entender desde un punto de vista macro, la dimensión real del problema objeto de la auditoría, y por consiguiente el poder efectuar las recomendaciones respectivas que se adapten de mejor manera a la realidad del entorno en el cual efectuada la auditoría.

Esta introducción es necesaria para indicar que con la realización de esta tesis hemos podido aplicar y sobretodo entender de una manera practica el concepto de "objetividad", ya que por lo general al profesional que desea incursionar en esta rama, le cuesta dejar de lado el punto de vista operativo y sobretodo pensar en función de control más que en la solución final del proceso.

Dentro de la elaboración de esta tesis hemos podido evaluar la eficacia y eficiencia de los controles implementados en el sistema SIGMEP del Departamento de Recaudaciones de la empresa Salud S.A., el relevar los procesos más críticos dentro de este sistema y poder orientarlo a una auditoría basada en riesgos, que es la tendencia en la cual se están enmarcando el nuevo enfoque de auditoría.



Es indispensable la capacitación continua dentro de las diferentes metodologías que existan dentro de la profesión de auditoría de sistemas, de manera que junto con la experiencia adquirida se pueda obtener el criterio profesional necesario para poder desempeñar de una manera óptima y eficaz del rol tan crítico como es el de auditor de sistemas.

CAPITULO 6. BIBLIOGRAFIA

- Cobit 4.0 Marco Referencial
www.isaca.org
- ITIL 3.0 Service Design y Transicion Design
Pdf libros
- CONTROL INTERNO – 2do módulo del diplomado de auditoría de sistemas.
Material proporcionado por el instructor.

ANEXOS

- Anexo A. FAI-001 Clasificación del uso de la computadora
- Anexo B. FAI-002 Relevamiento del ambiente informático
- Anexo C. FAI-003 Relevamiento de los sistemas de aplicación
- Anexo D. FAI-004 Revisión de los sistemas de aplicación
- Anexo E. FAI-005 Comprensión del ambiente de control tecnológico
- Anexo F. Diagrama de procesos Salud S.A
- Anexo G. Mapa de Riesgos

 ESPOL Escuela Superior Politécnica del Litoral		FAI-001	
Clasificación del uso de la computadora		Preparado por:	Katty Ronquillo Verónica García [29/09/10]
EMPRESA: 		Revisado por:	Andrés Alvarez [30/09/10]

INSTRUCCIONES GENERALES

Marque la clasificación apropiada para cada uno de los tres criterios utilizados para determinar el uso de computadoras por la entidad supervisada, y documente las razones para esa clasificación.

CRITERIO DE CLASIFICACIÓN

Extensión del uso		Complejidad		Importancia para el negocio	
Limitado		Simple		Limitada	
Moderado		Moderada	X	Moderada	
Trascendente	X	Compleja		Muy importante	X

RAZONES QUE SUSTENTAN EL CRITERIO DE CLASIFICACION

El uso del sistema Informático de Cartera dentro del area de Recaudaciones de Salud S.A. es de suma importancia, ya que permite obtener datos reales críticos en base a los cuales se generan las transacciones respectivas para obtener el seguimiento exhaustivo del ciclo de vida de la Cobranza.

Además todas las transacciones que la entidad realizan se las hace a través del sistema informático de desarrollo propio.

Ampliación en FAI-003.

CLASIFICACION GENERAL



Indique abajo su clasificación general sobre el uso de computadoras para la entidad y responda de acuerdo a lo indicado para cada clasificación.

Dominante	X
------------------	---

Involucre a un especialista en auditoría informática.

Documente una revisión de alto nivel del ambiente informático. (FAI-002)

Documente una revisión de alto nivel de los sistemas de aplicación. (FAI-003 y 004)

 ESPOL Escuela Superior Politécnica del Litoral	FAI-001		
Clasificación del uso de la computadora	Preparado por:	Katty Ronquillo Verónica García	[29/09/10]
EMPRESA: 	Revisado por:	Andrés Alvarez	[30/09/10]

Documente la estructura del ambiente de control tecnológico. (FAI-005)

Significante	
---------------------	--

Involucra a un especialista en auditoría informática.

Documente una revisión de alto nivel del ambiente informático y detalle los sistemas de aplicación. (FAI-002 y 003)

Documente la estructura del ambiente de control tecnológico. (FAI-005)



Considere la necesidad de evaluar los controles generales del computador.

Menor	
--------------	--

Documente una revisión de alto nivel del ambiente informático y detalle los sistemas de aplicación. (FAI-002)

Usted no tiene que documentar el ambiente informático o la estructura del ambiente de control tecnológico.

Exclusivamente ante situaciones de requerimientos especiales, considere la posibilidad de involucrar a un especialista en auditoría informática.

 ESPOL Escuela Superior Politécnica del Litoral	FAI-002		
Relevamiento del ambiente informático	Preparado por:	Katty Ronquillo Verónica García	[29/09/10]
EMPRESA: 	Revisado por:	Andrés Alvarez	[30/09/10]

I. ASPECTOS GENERALES DEL AREA

PROPÓSITO
Identificar las características principales del departamento de informática de la entidad controlada.

FUNCIONARIOS RESPONSABLES DEL CENTRO DE COMPUTO (Datos referentes a las personas responsables)

Nombre	Cargo	E-mail
Mabel Alban	Jefe De Infraestructura	malban@saludsa.com.ec
Ma. Ángeles Escobar	Gestor De Servidores	mescobar@saludsa.com.ec
José Almeida	Gestor De Comunicaciones Y Centrales Telefónicas	jalmeida@saludsa.com.ec

LOCALIDAD PRINCIPAL (Se describen las características de ubicación y organización del departamento de informática)

Ciudad: Quito Dirección: República del Salvador y Naciones Unidas

Número de personas: **Tres**

Estructura Funcional (Anexar Documentación)
Diagrama de la estructura funcional del departamento de Informática.



Costos operativos constituidos anuales:

Presupuesto de inversión para el presente año:

Sistema de inventario de equipamiento informático: **250,000.00**

Existe No Existe

Medio de almacenamiento:
 Papel Magnético Sistema aplicativo

 ESPOL Escuela Superior Politécnica del Litoral		FAI-002	
Relevamiento del ambiente informático		Preparado por: Katty Ronquillo Verónica García	[29/09/10]
EMPRESA: 		Revisado por: Andrés Alvarez	[30/09/10]

Existen otros centros de cómputo adicionales

Si No

Descripción por cada departamento Informático Adicional:

Se cuenta con un centro de computo principal en la ciudad de Quito, y un sistema de Computo de similares características en Guayaquil.



Localidad	Número de Personas	Actividades que realizan: (desarrollo, mantenimiento, operación y biblioteca, help desk, soporte técnico).	Observaciones
Guayaquil	2	Gestor de Servidores	Francisco Palacios
		Gestor De Infraestructura De Redes Y Comunicación	Pablo Moscoso

2. PLATAFORMA TECNOLÓGICA

PROPÓSITO



Describir los componentes tecnológicos (hardware, software, comunicaciones) que son parte del funcionamiento del departamento de informática.

- Servidor de Bases de Datos.
- Servidor de Aplicaciones.
- Servidor del Sistema de Archivos.
- Swith 24 y 48 puertos marca CISCO.
- Impresoras Epson LX-300+, FX-1170, FX-1180, Lexmark Z32, Z35.

 ESPOL Escuela Superior Politécnica del Litoral		FAI-002	
Relevamiento del ambiente informático		Preparado por:	Katty Ronquillo Verónica García [29/09/10]
EMPRESA: 		Revisado por:	Andrés Álvarez [30/09/10]



2.1 SERVIDORES

Servidor (Función)	Localidad	Marca	Modelo	Tecnología	Número de Procesadores	Memoria RAM (MB)	Disco (MB)	Sistema Operativo	Adquisición o Renta	Contrato de mantenimiento (S/N)	Valor de la inversión
Servidores de Archivos, Bases de Datos, Aplicaciones, Correo Electrónico, Share Point, Servidor de Pruebas, Servidores de Respaldos, y redundancia en General.	Centro de Computo	IBM	BLADE CENTE R H / HS21	BLADE	4 físicos 8 lógicos por cuchilla	16 GB por cuchilla		Windows 2000Server	Adquisición	SI	\$80000



 ESPOL Escuela Superior Politécnica del Litoral		FAI-002	
Relevamiento del ambiente informático		Preparado por:	Katty Ronquillo Verónica García [29/09/10]
EMPRESA: 		Revisado por:	Andrés Alvarez [30/09/10]

2.2 EQUIPOS DE REDES LAN

Canti- dad	Descripción(hub , switch, router, otros)	Mar- ca	Modelo	Protocolo (TCP/IP, IPX/SPX, Netbeui, Appletalk, otros)	Valor de la inversión	Adquisición o alquiler	Contrato de mantenimi- ento (S/N)	Número de Puertos						
								10baseT	100base TX, T4	100base FX	GB Ether- net	AT M	Otros	
2	8 switch	CISCO	CATALYST	TCP/IP	\$30000	Adquisición	NO			SI	SI			

	<h1>ESPOL</h1> <p>Escuela Superior Politécnica del Litoral</p>	FAI-002	
Relevamiento del ambiente informático	Preparado por:	Katy Ronquillo Verónica García	[29/09/10]
EMPRESA: 	Revisado por:	Andrés Alvarez	[30/09/10]

2.3	CABLEADO ESTRUCTURADO <input checked="" type="checkbox"/> Si <input type="checkbox"/> No
	Marca del Sistema: <p style="text-align: center;">UTP CATEGORIA 6</p>
	Número de puntos de voz: <p style="text-align: center;">280</p>
	Número de puntos de datos: <p style="text-align: center;">250</p>
	CABLEADO HORIZONTAL <p style="text-align: center;">SI</p>
	Tipo de cable puntos de voz: <p style="text-align: center;">UTP</p>
	Tipo de cable puntos de datos: <p style="text-align: center;">UTP</p>
	CABLEADO VERTICAL <p style="text-align: center;">SI</p>
	Tipo de backbone de datos: <p style="text-align: center;">FIBRA</p>
	Tipo de cable MDF datos:
	Tipo de cable MDF voz:
	Monto de la inversión: <p style="text-align: center;">\$200.000,00</p>
	Observaciones:



 ESPOL Escuela Superior Politécnica del Litoral		FAI-002	
Relevamiento del ambiente informático		Preparado por:	Katty Ronquillo Verónica García [29/09/10]
EMPRESA: 		Revisado por:	Andrés Alvarez [30/09/10]

2.4 ENLACES WAN

Origen	Destino	Analógico / Digital	Proveedor			Ultima Milla			Ancho de Banda	Protocolo (TCP/IP, SNA, HDLC, SLIP, ATM, Frame Relay, PPP, X25, ISDN, Otros)
			Propio	Empresa	Medio Físico: (satelital, terrestre, radio, Microonda)	Propio	Empresa	Medio Físico		
Digital	Digital	Digital	GLOBAL CROSSING MICROONDA	TERRESTRE, RADIO		GLOBAL CROSSING	FIBRA COBRE	RADIO	5 Mbps	TCP/IP UDP SNA ATM FRAME RELAY MPLS QoS

2.5 PC's POR LOCALIDAD

Número de Pc's disponibles	Localidad	Tipo de procesador / velocidad	Valor de la inversión	Contrato de Mantenimiento (S/N)
228	SALUDSA	CORE 2 DUO 2.4 Ghz	\$ 205.000,40	SI

 ESPOL Escuela Superior Politécnica del Litoral	FAI-002		
	Relevamiento del ambiente informático	Preparado por:	Katty Ronquillo Verónica García
EMPRESA: 	Revisado por:	Andrés Alvarez	[30/09/10]

2.6 CAJEROS AUTOMATICOS (F-CA)

Cantidad	Marca	Modelo	Equipo central al que está enlazado
N/A			

2.7 BASES DE DATOS



Nombre	Proveedor	Versión	Número de licencias	Servidor en que está instalada	Localidad	Valor de la inversión	Contrato de mantenimiento (S/N)
SQL SERVER PROGRESS 9 PROGRESS 10 ORACLE 9I	MICROSOFT	2003	5 PER SEAT	Windows 2003Server	Centro de cómputo	\$10.000,00	SI

Observaciones:

Se está realizando actualmente la migración de la base de datos del manejador de archivos Fox Pro al SQL SERVER 2000.

2.8 SOFTWARE DE DESARROLLO Y OTROS PAQUETES ESPECIALES

Nombre	Funcionalidad	Localidad	Valor de la inversión	Contrato de mantenimiento (S/N)
Microsoft Outlook	Correo electrónico	Centro de Cómputo	\$5.000,00	NO
Microsoft Visual Basic 2007	Desarrollo de Aplicaciones	Centro de Cómputo	\$2.000,00	NO

 ESPOL Escuela Superior Politécnica del Litoral		FAI-002	
Relevamiento del ambiente informático		Preparado por:	Katty Ronquillo Verónica García [29/09/10]
EMPRESA: 		Revisado por:	Andrés Alvarez [30/09/10]

Progress 9.0	Desarrollo de Aplicaciones	Centro de Cómputo	\$500,00 C/U	NO
--------------	----------------------------	-------------------	--------------	----

2.9 EQUIPOS PARA GARANTIZAR LA CONTINUIDAD (UPS/MODEMS)

Software/Hardware	Componente	Marca	Modelo o versión	Valor de la Inversión	Localidad
UPS		Tripp-Lite 6 KVA	OMNI SMART	\$ 3.500,00	SALUD S.A.



Observaciones:

3. INVENTARIO DE APLICACIONES

PROPÓSITO

Detallar las aplicaciones que dan soporte a los procesos funcionales de la entidad.

Nombre	Descripción	Número de usuarios	Alcance (Nacional, Regional, Local)	Ambiente tecnológico (sistema operativo, base de datos, interface usuario)	Desarrollo interno o paquete adquirido	Valor de la inversión	Fecha de Implementación	Contrato de mantenimiento
SIGMEP	Sistema Administrativo	100	Nacional	Windows 2003 server	Desarrollo Interno	N/A	2000	No
INTEGRITY	Registro Contables	50	Local	Windows 2003 server	Desarrollo Interno	N/A	2000	No
HIS - ISIS	Sistema Médico	120	Local	Windows 2003 server	Desarrollo Interno	N/A	2000	No

 ESPOL Escuela Superior Politécnica del Litoral		FAI-002	
Relevamiento del ambiente informático		Preparado por:	Katty Ronquillo Verónica García [29/09/10]
EMPRESA: 		Revisado por:	Andrés Alvarez [30/09/10]

OPEN DENTAL	Sistema Médico Dental	50	Local	Windows 2003 server	Desarrollo Interno	N/A	2000	No
-------------	-----------------------	----	-------	---------------------	--------------------	-----	------	----

Observaciones:

4. SEGURIDADES LOGICAS (F-SL)

PROPÓSITO

Detallar las seguridades para el control de acceso por paquetes o utilitarios propios del sistema operativo, Rac-f, entre otros)

Sistema o paquete / ambiente en el que corre	Tipo y longitud mínima y máxima de claves de acceso	Rotación de claves de acceso (automático o manual) y periodicidad	Número de intentos fallidos antes de ingresar al sistema	Número de sesiones simultáneas por usuario	Número de perfiles de usuario	Tiempo permitido de inactividad en el sistema (time out)	Capacidad del sistema o aplicación para generar bitácora de accesos inválidos y de transacciones por usuario	Manejo de claves de acceso históricas
Windows 2003 server	4 – 16	Manual	3	Limitado (1)	200	N/A	SÍ	NO



ESPOL Escuela Superior Politécnica del Litoral	FAI-002		
Relevamiento del ambiente informático	Preparado por:	Katty Ronquillo Verónica García	[29/09/10]
EMPRESA: 	Revisado por:	Andrés Alvarez	[30/09/10]

5. CONTRATO DE SERVICIOS / COMPONENTES TECNOLOGICOS

PROPÓSITO

Describir las contrataciones de tercerización que por concepto de hardware, software o comunicaciones se hubieren realizado en la entidad.

Descripción del servicio / componente Tecnológico	Fecha último contrato	Duración	Costos anuales	Empresa proveedora	Observaciones
Help Desk/Mantenimiento de Equipos Electrónicos	01/10/2010	12 meses	1,200.00	BINARIA	
Enlaces de Comunicación	01/10/2010	12 meses	5,000.00	GLOBAL CROSSING TERRESTRE, RADIO MICROONDA	
Cableado Estructurado	01/10/2010	12 meses	8,000.00	IMSAT	

 ESPOL Escuela Superior Politécnica del Litoral	FAI-003		
Relevamiento de los sistemas de aplicación	Preparado por:	Katty Ronquillo Verónica García	[29/09/10]
EMPRESA: 	Revisado por:	Andrés Alvarez	[29/09/10]

PROPÓSITO

Identificar las características principales de las aplicaciones que soportan las operaciones de la entidad controlada.

Las aplicaciones que deben tomarse en cuenta principalmente son: Recaudaciones, Liquidaciones, Producción, Facturación.

1. ASPECTOS GENERALES

(Identificación de los responsables de la aplicación en la Institución objeto de auditoría y resumen de las principales características funcionales de la aplicación)

Nombre de la aplicación: [SIGMEP]

Descripción: [Sistema Integrado de Gestión de Medicina Pre pagada]

Fecha de puesta en producción: [10/2000]

Número de usuarios: [200]

Procesos que atiende: ingreso de contratos, ingreso de clientes, recaudos, cotización, configuración de planes, facturación, reportes en general.

Responsables de la Aplicación:



Usuario: [Eduardo Izurieta]
 Cargo: [Gerente General]
 E-mail: [eizurieta@saludsa.com.ec]

Técnico: [Isabel Beltrán]
 Cargo: [Jefe De Desarrollo De Aplicaciones]
 E-mail: [ibeltran@saludsa.com.ec]

Observaciones:

2.- PLATAFORMA TECNOLÓGICA

(Describe el entorno tecnológico en el cual opera la aplicación)

 ESPOL Escuela Superior Politécnica del Litoral		FAI-003	
Relevamiento de los sistemas de aplicación		Preparado por:	Katty Ronquillo Verónica García [29/09/10]
EMPRESA: 		Revisado por:	Andrés Alvarez [29/09/10]

Tipo de Procesamiento: Centralizado Distribuido

Sistema Operativo: [Windows 2003 Server]

DBMS: [PROGRESS 9]

Lenguaje: [PROGRESS 9]

Software de Comunicaciones: [No]

Otros: []

Arquitectura: Una capa Dos capas Tres capas

Observaciones: []

3. PRINCIPALES MODULOS

(Se describen los módulos, parte de una aplicación perfectamente identificable, en sus procesos, entradas y salidas y que por sí mismos resuelven un problema funcional)

Nombre del modulo	Descripción
SIGMEP Recaudos Individuales	Actualizaciones de Débitos Anulación de Notas de Crédito Consulta de Notas de Crédito Consulta de Notas de Débito Cuadre de Caja Cuotas en Mora o por Cobrar Cuotas pagadas Devolución de saldo a favor Generación de Notas de Crédito Generación de Notas de Débito Subida Automática de Débitos Subida Automática de Débitos Reproceso Gestión de Citas

Nota: Se debe observar como se relacionan los diferentes módulos del sistema



ESPOL

Escuela Superior Politécnica del Litoral

FAI-003

Relevamiento de los sistemas de aplicación

Preparado por:

Katty Ronquillo
Verónica García

[29/09/10]

EMPRESA:

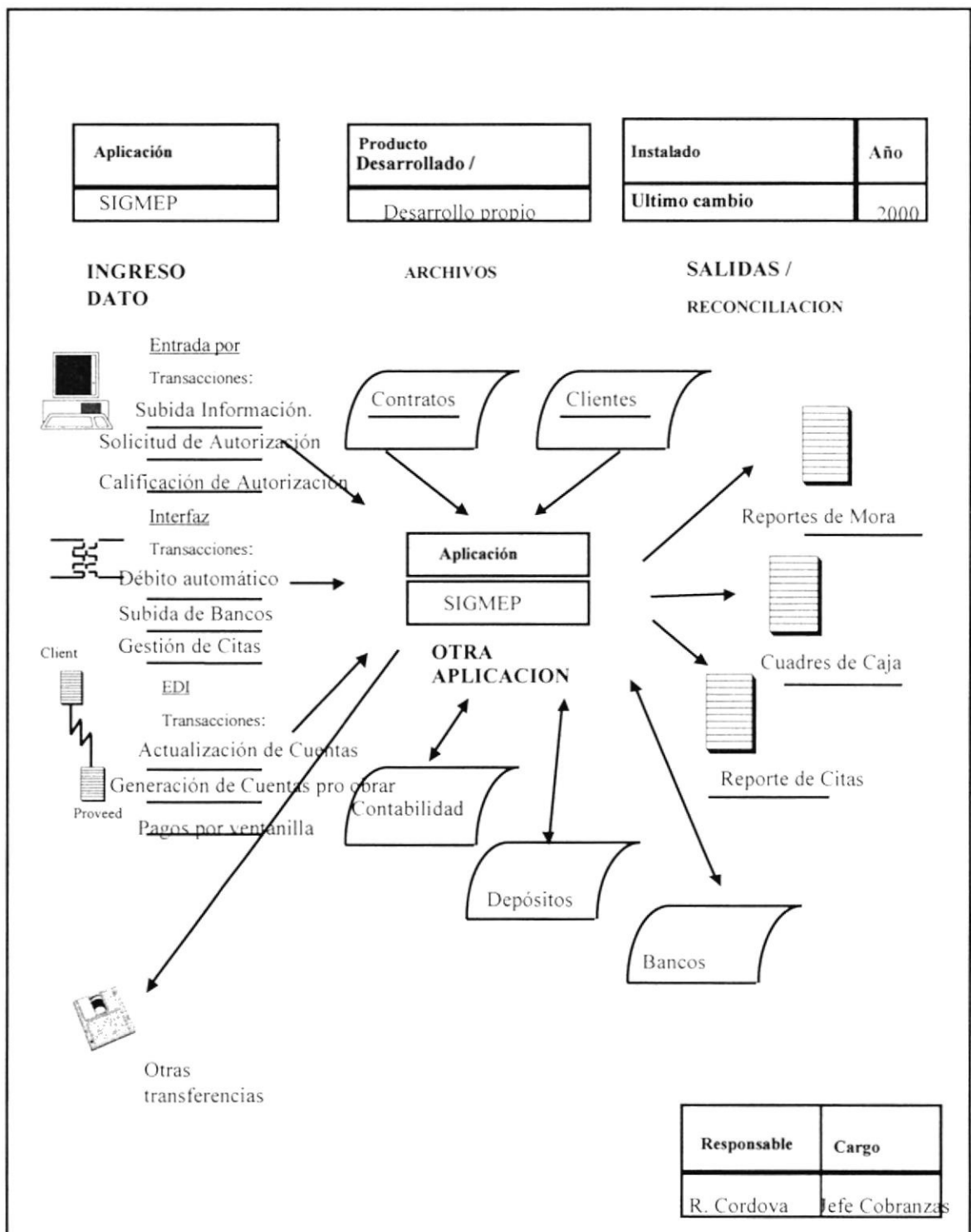




Revisado por:

Andrés Álvarez

[29/09/10]

DIAGRAMA DE FLUJO GRÁFICO DE LOS PROCESOS



 ESPOL Escuela Superior Politécnica del Litoral	FAI-003		
Relevamiento de los sistemas de aplicación	Preparado por:	Katty Ronquillo Verónica García	[29/09/10]
EMPRESA: 	Revisado por:	Andrés Alvarez	[29/09/10]

4. SEGURIDADES

(Información acerca de los mecanismos previstos para impedir el acceso indebido a los datos y sistemas, así como los procedimientos que aseguran la protección de datos y programas)

Controles de Acceso: Si No

Perfiles de Usuarios (roles):

Perfil	Descripción
Jefe De Recaudaciones Y Cobranzas	Usuario con todos los accesos a cada opción definida para el cargo
Asistente de Recaudaciones SR.	Todas las opciones necesarios para la operación diaria
Asistente de Recaudaciones JR.	Todas las opciones necesarias para la operación diaria excepto subida de Autorizaciones Bancarias
Cobrador	Opción solamente para la Gestión de Citas e impresión de Facturas

Pistas de Auditoria: Si No

Descripción:

Existen copias de respaldo de programas y documentación de la aplicación:

Si No

Existen procedimientos para determinar claves de acceso:

Si No



Existen mecanismos de desconexión automática:

Si No

Observaciones: [documentación de aplicaciones no actualizadas, no documentación técnica].

5. DOCUMENTACION

(Información sobre la documentación del sistema la misma que garantiza la continuidad del ciclo de vida de la aplicación)

 ESPOL Escuela Superior Politécnica del Litoral		FAI-003	
Relevamiento de los sistemas de aplicación		Preparado por:	Katty Ronquillo Verónica García [29/09/10]
EMPRESA: 		Revisado por:	Andrés Álvarez [29/09/10]

- Modelo de Procesos: Existe Actualizado Desactualizado
- Modelo de Datos: Existe Actualizado Desactualizado
- Descripción del sistema: Existe Actualizado Desactualizado
- Diseño de diálogos: Existe Actualizado Desactualizado
- Manual de Usuario: Existe Actualizado Desactualizado

6. PRINCIPALES ARCHIVOS / TABLAS DEL SISTEMA



(Se identifica las principales estructuras de datos necesarios para el funcionamiento del sistema)

Nombre	Descripción	Localidad	Volumen/re gistros	%crecimi ento	Clave primaria
N_USUARIOS	Claves de Acceso	Servidor	200		USER
CL04	CONTRATOS	Servidor	1500		CONTRATO NUMERO
CL05	CLIENTES	Servidor	4500		PERSONA NUMERO
CL24	COBRANZAS	Servidor	1500		CONBRANZA NUMERO
CR02	CUOTAS	Servidor	8000		REMESA
CR03 CR04	PAGOS	Servidor	8000		PAGO
CR05 CR08	FACTURAS	Servidor	8000		FACTURA
NC01	NOTAS CREDITO	Servidor	1500		CREDITO NUMERO
ND01	NOTAS DEBITO	Servidor	1500		DEBITO NUMERO

7. REPORTES GERENCIALES PERIODICOS

(Identificación de la información que procesa la aplicación para actividades de toma de decisión, supervisión y control de la empresa)

Nombre	Descripción	Frecuencia	Archivos/Tablas que participan
Reporte de Cartera	Este reporte muestra las cuentas de cobrar vigentes de Salud al inicio de cada	Mensual	CR02 CL04 CR03 CR04

 ESPOL Escuela Superior Politécnica del Litoral		FAI-003	
Relevamiento de los sistemas de aplicación		Preparado por:	Katty Ronquillo Verónica García [29/09/10]
EMPRESA: 		Revisado por:	Andrés Álvarez [29/09/10]

	periodo mensual		
Reporte de Mora	Reporte para identificar Contratos para la Gestión telefónica	Mensual	CR02 CL04
Reporte de Anulación de Contratos por Mora	Contratos que son anulados por Mora	Mensual	CR02 CL04 CR03 CR04
Reporte de Citas	Reporte para la preparación y cierre de la gestión de citas por parte de los cobradores.	Diario	CITAS

8. **RESPALDOS PRINCIPALES ARCHIVOS / TABLAS**



(Información específica acerca de los respaldos principales de archivos/tablas, disponibles en el sistema)

Archivo / tabla	Etiqueta	Periodicidad	Políticas de respaldo	Área Responsable
Salud.bck	Salud.bck	DIARIA	MADRUGADA DIA SIGUIENTE	SISTEMAS

9. **INTERFACES CON OTROS SISTEMAS**

(Identificación del grado de integración de la aplicación respecto a otras disponibles en la entidad)

Sistema relacionado	Batch / Línea	Archivos / Tablas que intervienen	Periodicidad	Descripción
CONTABILIDAD INTEGRITY	LINEA	CR03 CR04 CR05 CR08 NC01		PROCESO DE CONTABILIZACION

 ESPOL Escuela Superior Politécnica del Litoral		FAI-004	
Revisión de los sistemas de aplicación		Preparado por:	Katty Ronquillo Verónica García [29/09/10]
EMPRESA: 		Revisado por:	Andrés Alvarez [29/09/10]

SISTEMA DE APLICACION DE: | SIGMEP COBRANZA INDIVIDUAL |

1. PRINCIPAL FUNCIONALIDAD

PROPÓSITO

Identificar los procedimientos funcionales que han sido automatizados en el sistema, por ejemplo para el sistema de cartera, transferencia automática de cartera vigente a vencida. Para el sistema de contabilidad como y cuando se realizan ajustes.

Función	Descripción	Archivos / Tablas que intervienen
Autorizaciones de Debito	Registro de Cuentas en los Bancos	CR01 CR02
Cotización	Cotización a contratos IND	CR01 CR02
Archivos para Bancos	Generar archivo de cuentas por debitar a Bancos	CR01 CR02
Subida de Bancos	Subir archivo planos de Bancos	CR01 CR02
Registro de solicitudes de anulación	Registro de solicitudes de anulación.	CL04
Notas de Crédito	Generación de NC	NC01
Notas de Débito	Generación de ND	ND01
Gestión de Citas	Ingreso y baja de citas	Citas

2. PERFIL DE MANTENIMIENTO

PROPÓSITO



Identificar del grado de control existente en la evolución de la aplicación, costos y riesgos relacionados.

INTERNO

Ambientes separados de producción y desarrollo: Si No

Procedimientos de actualización formales: Si No
(Anexar Documentación Mantenimiento de aplicaciones)

Número de personas involucradas: [4]



 ESPOL Escuela Superior Politécnica del Litoral	FAI-004		
Revisión de los sistemas de aplicación	Preparado por:	Katty Ronquillo Verónica García	[29/09/10]
EMPRESA: 	Revisado por:	Andrés Álvarez	[29/09/10]

Observaciones relevantes:

El sistema será migrado próximamente a una interface Windows con bases de datos SQL SERVER 2005; es un sistema totalmente distinto que tiene varias etapas, entre estas una de las principales es la depuración de la Base de Datos Actual, y las interfaces WEB, que reemplazarán totalmente al Sistema SIGMEP.

3. **PRINCIPALES CAUSAS DE FALLA Y PROBLEMAS FUNCIONALES DEL SISTEMA**

Descripción	Tiempo promedio entre fallas (frecuencia):	Tiempo promedio en solucionar el problema:	Formas de solución:	Observaciones
Errores u omisiones de programación en cambios realizados	Eventual	15 días	Pruebas correctas entre base de Pruebas y Producción	Esto provoca retrasos en la ejecución de las tareas de cobranza.
Manejo de datos a través de tablas referenciales indexadas.	Permanente	12 meses	Reingeniería del sistema y rediseño en base de datos.	Esto provoca mucho espacio de almacenamiento, tiempo alto de respuesta.
Puesta de Producción de programas sin control de calidad	Permanente	7 días	Revisión de programas, tarea de cronograma	Desarrollo rápido para soportar las expectativas del negocio.
Bloqueos frecuentes de la Base de Datos	Eventual	inmediato	Matar procesos bloqueados en la Base	Este tipo de errores se da por el no uso de sentencia NO-LOCK en los accesos a la base por parte de los desarrolladores, y por la actualización a la data de forma simultánea.

 ESPOL Escuela Superior Politécnica del Litoral		FAI-004	
Revisión de los sistemas de aplicación		Preparado por: Katty Ronquillo Verónica García	[29/09/10]
EMPRESA: 		Revisado por: Andrés Alvarez	[29/09/10]

PRINCIPALES CAUSAS DE FALLA Y PROBLEMAS TECNICOS DEL SISTEMA

Descripción	Tiempo promedio entre fallas (frecuencia):	Tiempo promedio en solucionar el problema:	Formas de solución:	Observaciones
Limitación en la base de datos por el crecimiento de información	Permanente	18 meses	Migración de la base de datos a SQL Server	Manejo de datos a través de tablas referenciales indexadas en Fox-Pro.
Dependencia de las aplicaciones de variables de entorno de los equipos	permanente	18 meses	Parametrización para la ejecución de los programas	No solamente las aplicaciones Administrativas manejan variables también otras aplicaciones desarrolladas

CONCLUSION PRELIMINAR

Respuestas obtenidas:

1. PRINCIPAL FUNCIONALIDAD IMPLEMENTADA: Satisfactorio.
2. PERFIL DE MANTENIMIENTO: No satisfactorio.
3. PRINCIPALES CAUSAS DE FALLA Y PROBLEMAS FUNCIONALES DEL SISTEMA: No satisfactorio, el tipo de herramienta de desarrollo y almacenamiento y administración de la información no es óptima.

Conclusión Preliminar sobre si este sistema de aplicación Soporta el Procesamiento Confiable de la Información en la entidad objeto de auditoría.

Respalda []

No respalda []



ESPOL

Escuela Superior Politécnica del Litoral

FAI-005

Comprensión del ambiente de control tecnológico

Preparado por:

Katty Ronquillo
Verónica García

[29/09/10]

EMPRESA:



Revisado por:

Andrés Álvarez

[29/09/10]

INSTRUCCIONES GENERALES

Este documento necesita completarse para cada ambiente único de procesamiento de la computadora. Los riesgos identificados se anotan en la sección al final de esta Forma.

A.- VISTA GENERAL DEL AMBIENTE DE PROCESAMIENTO DE LA COMPUTADORA

Identificar el equipo y el sistema operativo de la entidad Unix, Win NT, Win 2000 Server, Novell, AS/400, etc.

Nombre del Ambiente de Procesamiento de la Computadora	INTEL P4, WIN 2003 SERVER, PROGRESS
---	-------------------------------------

Determinar las áreas de controles generales de la computadora relevantes (SI) o (NO)

Áreas de controles generales de la computadora	¿Es esta área de Control general de la computadora relevante en este ambiente de procesamiento de la computadora?	
ESTRATEGIA Y PLANEACION DE LOS RECURSOS DE INFORMACION	SI [X]	NO []
OPERACIONES DE LOS SISTEMAS DE INFORMACION	SI [X]	NO []
RELACIONES CON PROVEEDORES EXTERNOS	SI [X]	NO []
SEGURIDAD DE LA INFORMACIÓN	SI [X]	NO []
PLANEACION DE LA CONTINUIDAD DEL NEGOCIO	SI [X]	NO []
IMPLEMENTACION Y MANTENIMIENTO DE LOS SISTEMAS DE APLICACIÓN	SI [X]	NO []
IMPLEMENTACION Y SOPORTE DE LA BASE DE DATOS	SI [X]	NO []
SOPORTE DE LA RED	SI [X]	NO []
SOPORTE AL SOFTWARE DE LOS SISTEMAS	SI [X]	NO []
SOPORTE AL HARDWARE (EQUIPO)	SI [X]	NO []

Con base en las respuestas de la tabla anterior, cubra únicamente las áreas señaladas como relevantes:

¿Son realizadas algunas de las áreas de controles generales de la computadora por una organización de servicio?	SI []	NO [X]
--	--------	----------



ESPOL

Escuela Superior Politécnica del Litoral

FAI-005

Comprensión del ambiente de control tecnológico

Preparado por:

Katty Ronquillo
Verónica García

[29/09/10]

EMPRESA:



Revisado por:

Andrés Álvarez

[29/09/10]

Organización y personal del ambiente de procesamiento de la computadora

Si está disponible, inserte o adjunte una copia del organigrama de la institución en los papeles de trabajo.

Se adjunta organigrama estructural de la Institución.

Organigrama Adsamed / Tecnología De Negocios



Efectuar una relación de los departamentos relevantes, el número aproximado de personal en cada departamento y los nombres y cargos del personal clave.



ESPOL

Escuela Superior Politécnica del Litoral

FAI-005

Comprensión del ambiente de control tecnológico

Preparado por:

Katty Ronquillo
Verónica García

[29/09/10]

EMPRESA:



Revisado por:

Andrés Álvarez

[29/09/10]

Departamento /Unidad /Área	No. Aprox. de Personal	Nombres y cargos del Personal Clave
Gerencia de Tecnología de Información		Ing. Felipe Dueñas
Desarrollo y Seguridad de la Información		Ing. José Almeida
Producción		Ing. Ma. Mercedes Miño
Redes / Base de Datos		Ing. Francisco Palacios
Soporte a usuarios/ Técnico		Ing. David Carvajal

1. Estrategia y Planeación de Recursos de Información

¿Tiene la entidad un comité directivo de sistemas de información?	SI [] NO [X]
---	-----------------

En el caso de existir, describa brevemente la composición del comité directivo de sistemas de información, así como sus funciones y responsabilidades:

Está conformado por las siguientes personas:

Sus funciones y responsabilidades son:

La periodicidad de reuniones es:

¿Tiene la entidad una estrategia de sistemas de información y/o un plan de sistemas de información a largo plazo?	SI [] NO [X]
---	-----------------

¿Tiene la entidad planes y/o presupuestos de sistemas de información a corto plazo?	SI [X] NO []
---	-----------------

2. Operaciones de los Sistemas de Información


<p>Describa brevemente los procedimientos de operaciones de los sistemas de información de la entidad:</p> <p>Al no existir procesamientos en lote fuera de línea (Batch) no se ha implementado una metodología de control para las operaciones realizadas.</p>



ESPOL

Escuela Superior Politécnica del Litoral

FAI-005

Comprensión del ambiente de control tecnológico	Preparado por:	Katty Ronquillo Verónica García	[29/09/10]
EMPRESA: 	Revisado por:	Andrés Alvarez	[29/09/10]

¿Tiene la entidad un departamento centralizado en el cual se realiza la entrada de datos clave a los sistemas de procesamiento por lote?	SI [<input type="checkbox"/>]	NO [<input checked="" type="checkbox"/>]
--	---------------------------------	--

¿Ha establecido la entidad convenios formales con terceros para el soporte a los usuarios?	SI [<input type="checkbox"/>]	NO [<input checked="" type="checkbox"/>]
--	---------------------------------	--

¿Cómo se programan los trabajos de producción por lotes que se procesan en esta ubicación?
N/A

¿Cómo se imprimen y se distribuyen las copias de los informes de salida para los usuarios?
Se lo realiza de manera manual y es cada vez que exista el requerimiento.

¿Mantiene esta ubicación de procesamiento existencias en blanco de formularios sensitivos?	SI [<input type="checkbox"/>]	NO [<input checked="" type="checkbox"/>]
--	---------------------------------	--

¿Tiene esta ubicación de procesamiento capacidades para firma de cheques automáticos?	SI [<input type="checkbox"/>]	NO [<input checked="" type="checkbox"/>]
---	---------------------------------	--

3. Relaciones con los Proveedores Externos (Tanto proveedores de bienes / servicios externos, así como organizaciones de servicio "Outsourcing")

Haga una relación de los ambientes de procesamiento de la computadora y en cuales existen relaciones con proveedores externos:

Existen contratos para las siguientes compañías y en las siguientes áreas:
<ul style="list-style-type: none"> - [No existe licenciamiento de los equipos] Soporte y Mantenimiento de licencias de Software - [Netcrosssoft / Darwin Pozo] Mantenimiento de Hardware - [No existe] Mantenimiento de Software - [Ing. Pablo Krovina] Servicio de Telecomunicaciones - [BINARIA / Darwin Pozo] Proveedores de equipos de cómputo - [Ing. Pablo Krovina] Mantenimiento de equipos de comunicación - [No existe] Elaboración del Plan de Contingencias (x definir fecha inicio)

¿Quiénes son los responsables del manejo de las relaciones con los proveedores externos? Indique los nombres y cargos de dichos funcionarios, así como sus funciones y responsabilidades.



ESPOL

Escuela Superior Politécnica del Litoral

FAI-005

Comprensión del ambiente de control tecnológico	Preparado por:	Katty Ronquillo Verónica García	[29/09/10]
EMPRESA:	Revisado por:	Andrés Álvarez	[29/09/10]



Contrato	Funcionario Responsable	Función y responsabilidad
PROVEEDORES	Ing. Vicente Chalén	Director General, adquisiciones y contratos

Describa brevemente los procedimientos de la entidad para seleccionar a los proveedores externos y para realizar contratos con ellos. Describa también los procedimientos de la entidad para evaluar la eficacia continua de tales contratos externos.

Se determinan por lo menos dos ofertas para la selección de un proveedor, el Gerente general junto con el Gerente de sistemas definen cual es la mejor opción y recomiendan a dicha compañía, se hace un estudio financiero antes de tomar la decisión y se procede con la aprobación si es del caso.

¿Establecen los contratos de la entidad con los proveedores externos niveles mínimo de cumplimiento de servicio por parte de estos? SI [X] NO []

Describa brevemente los niveles mínimos de servicio y algunos procedimientos de la entidad para monitorear el desempeño de los proveedores contra los mínimos establecidos.

Los niveles mínimos de servicio deberán cumplir con lo estipulado en el contrato, entre estos pueden estar: mantenimientos periódicos, servicio técnico, reposición de tiempo de utilización (dependiendo del servicio brindado), entre otros.

En caso de incumplimiento de alguno de los servicios mencionados en el contrato, se determinan multas, según lo definido en el contrato.

Exclusivamente para organizaciones de servicio (OUTSOURCING)

Describa brevemente los procedimientos de la entidad, si los hay, para evaluar el impacto de ciertas actividades externas sobre sus procesos cotidianos. Considere lo siguiente:

- Si la entidad ha evaluado la suficiencia de las actividades de control en la organización de servicio
- Si la entidad ha evaluado la necesidad de implementar actividades de control para complementar las implementadas por la organización de servicio
- Si la entidad monitorea la eficacia continua de las actividades de control en la organización de servicio y algunas actividades complementarias de control de la entidad.

N/A

4. Seguridad de la Información

Políticas y Procedimientos de Seguridad



ESPOL

Escuela Superior Politécnica del Litoral

FAI-005

Comprensión del ambiente de control tecnológico

Preparado por:

Katty Ronquillo
Verónica García

[29/09/10]

EMPRESA:



Revisado por:

Andrés Álvarez

[29/09/10]

Describa brevemente la naturaleza y alcance de las políticas y procedimientos de seguridad de la información:

Se cubren los siguientes aspectos:

Seguridad Lógica: [*Módulo de Seguridad del Sistema, con base en perfiles de usuario y passwords*]

Seguridad Física: [*Sistema de Accesos, puerta eléctrica para acceso a centro de cómputo.*]

¿Se encuentran por escrito las políticas y procedimientos de seguridad de la información de la entidad?

SI [] NO [X]

¿Tiene la entidad un método o programa para poner en conocimiento del usuario las políticas, procedimientos y prácticas de seguridad

SI [X] NO []

Seguridad Lógica

En la tabla siguiente, relacione los métodos que usa el cliente para restringir el acceso lógico a los sistemas de aplicación y a la información:

Método de Restricción de Acceso (seleccione los utilizados)

Funciones de control de acceso al sistema de administración de red [X]

Software de control de acceso de terceros []

Funciones de control de acceso al sistema operativo [X]

Funciones de control de acceso al sistema de aplicación [X]

¿Están centralizados o descentralizados el soporte y la administración de los métodos de restricción de acceso lógico?

Centralizado [X]

Descentralizado []

Describa el software de administración de la red utilizado por la entidad

El sistema Operativo Windows 2000 Server tiene su propio sistema de administración de red.

Describa el método de control de acceso a las aplicaciones utilizado por la entidad

El sistema de SALUD cuenta con un módulo de seguridades que permite acceder solamente a los usuarios autorizados, a través de un identificador de usuario y una contraseña, la cual es confidencial, todos los usuarios están atados a uno o varios perfiles (dependiendo de sus funciones).

En el sistema de Seguridades, no se ha configurado que las claves sean cambiadas obligatoriamente cada cierto periodo de tiempo por los usuarios.

Relacione las técnicas que usa la entidad para autenticar la identidad de los usuarios que intentan acceder al sistema:



ESPOL

Escuela Superior Politécnica del Litoral

FAI-005

Comprensión del ambiente de control tecnológico

Preparado por:

Katty Ronquillo
Verónica García

[29/09/10]

EMPRESA:



Revisado por:

Andrés Alvarez

[29/09/10]

Describa las técnicas de autenticación

El módulo de Seguridades realiza la autenticación, para lo cual un usuario deberá estar autorizado en la base de datos de usuarios y deberá estar asignado a un perfil específico y tener una contraseña confidencial y personal de cada uno.

El sistema verifica que el usuario ingresado sea un usuario existente en la base de usuarios autorizados y valida que la contraseña coincida con la registrada en el sistema, adicionalmente verifica que el usuario esté activo.

Describa brevemente los procedimientos de la entidad para autorizar el acceso a la información y para asignar los privilegios de acceso a los usuarios:

El director de recursos humanos, debe solicitar a través de un memo al Oficial de Seguridades la creación del usuario y la asignación del perfil correspondiente según las funciones que éste vaya a desempeñar.

El Oficial de Seguridades se encarga de crear el usuario y asignar el perfil requerido. Posteriormente envía un mail de notificación al solicitante.

¿Se ha definido explícitamente la propiedad de la información?

SI [] NO [X]

¿Se ha clasificado la información para efectos de la autorización del acceso?

SI [] NO [X]

¿Quién es el responsable de autorizar el acceso a la información (es decir, de aprobar una solicitud para que se le otorgue a un individuo el acceso a información específica o tipos de información)?

La Gerencia del Área solicitante y el Gerente de TI.

¿Quién es el responsable de asignar los privilegios de acceso a los usuarios (es decir, de fijar los parámetros de software que restringen o permiten ciertos tipos de acceso a cierta información)?

El Oficial de Seguridades el Ing. José Almeida

¿A quién se le permite actualizar el acceso a los datos de producción?

Solamente a la Oficial de Seguridades, siempre y cuando exista una autorización escrita (via mail), del gerente de TI

¿Se permite el acceso externo a/desde los sistemas de la computadora (por ejemplo, por vía de marcación telefónica o por redes externas)?

SI [] NO [X]

¿Quién tiene tal acceso?

Propósito de tal acceso y métodos usados para restringir el acceso

N/A



ESPOL

Escuela Superior Politécnica del Litoral

FAI-005

Comprensión del ambiente de control tecnológico	Preparado por:	Katty Ronquillo Verónica García	[29/09/10]
EMPRESA:	Revisado por:	Andrés Alvarez	[29/09/10]



¿Se transmite información a través de redes externas públicas (tales como la Internet, redes de valor agregado)? SI [X] NO []

¿Se permite el acceso de Internet a /desde sus sistemas de la computadora? SI [X] NO []

Describa los métodos usados para proteger los sistemas de la entidad del acceso a/desde redes públicas (por ejemplo, la Internet, redes de valor agregado):

N/A

Describa el software Protector (Firewall) de Internet

Describa cómo se configuran y se usan los protectores (firewalls). Considere lo siguiente:

- ¿Dónde se localizan?
- ¿Cuál es su función (una vía, dos vías, etc.)?
- ¿Qué tecnologías usan?
- ¿Cómo están configurados?
- ¿Cómo se manejan?

¿Tiene la entidad dirección world wide web (w.w.w.)? SI [X] NO []
<http://www.saludsa.com/>

¿Qué tipo de servicios están disponibles en la dirección de la red de la entidad?

Acceso a información sobre la entidad (informativo) [SI]
Capacidad para ordenar y/o pagar por bienes o servicios previstos por la entidad [NO]
Capacidad para comunicarse con clientes seleccionados vía e-mail [SI]

Describa el servidor de Internet y/o el suministrador del servicio de Internet de la entidad:

Proveedor de servicio de Internet de terceros [SI]
Equipo independiente que no se relaciona con el sistema de la entidad [SI]

¿Tienen los usuarios acceso al software generador de reportes? SI [X] NO []
A través de cada módulo.

¿Tienen los usuarios la capacidad de recibir datos (to download) y manipular la información del sistema de aplicación? SI [X] NO []



ESPOL

Escuela Superior Politécnica del Litoral

FAI-005

Comprensión del ambiente de control tecnológico

Preparado por:

Katty Ronquillo
Verónica García

[29/09/10]

EMPRESA:



Revisado por:

Andrés Alvarez

[29/09/10]

En caso afirmativo a la pregunta anterior, describa cómo se usan tales capacidades (qué información puede ser recibida, cómo ésta se puede manipular, cómo se usan los resultados de dichas actividades) y cómo se controlan:

Existen opciones que generan archivos planos que los usuarios autorizados (dentro de su perfil de acceso), pueden manipularlos a través de la herramienta Excel por ejemplo.

¿Tienen los usuarios la capacidad de transmitir datos (to upload) a los sistemas de aplicación, fuera del sistema de aplicación normal de entrada de datos?

SI [] NO [X]

En caso afirmativo a la pregunta anterior, describa cómo se usan tales capacidades (qué información pueden ser transmitida, la fuente de dicha información, efectos sobre otros datos de aplicación) y cómo se controlan:

N/A

Seguridad Física

¿Qué métodos usa la entidad para restringir el acceso físico a esta ubicación de procesamiento?

[SI] Tarjetas de entrada para el Centro de Cómputo.

[NO] Combinaciones de cerraduras de puertas

[SI] Guardias/recepcionistas para controlar a los visitantes

Relacione todos los grupos (internos y externos) cuyo acceso físico está permitido a este ambiente de procesamiento de la computadora. Por cada grupo, indique si se le ha otorgado acceso completo o restringido e indique la naturaleza de las restricciones.

Grupo	Naturaleza de las Restricciones de Acceso Físico, Si las Hay
Desarrollo	<i>Restringido, solo los analistas de desarrollo</i>
Producción (Red, B/D, etc)	<i>Restringido, solo técnicos de red y operadores</i>
Operaciones	<i>Total al personal de Sistemas</i>
Usuarios	<i>Restringido, solo personal autorizado.</i>
Visitantes/Practicantes/Vendedores	<i>Restringido total.</i>
Contratistas externos para el procesamiento de datos	<i>Restringido total.</i>

¿Qué tipo de controles ambientales se tienen establecidos en esta ubicación de procesamiento para prevenir daños al equipo de la computadora?

[SI] Sistema de control de incendios


[SI] Censores de Humo



ESPOL

Escuela Superior Politécnica del Litoral

FAI-005

Comprensión del ambiente de control tecnológico	Preparado por:	Katty Ronquillo Verónica García	[29/09/10]
EMPRESA: 	Revisado por:	Andrés Alvarez	[29/09/10]

<input type="checkbox"/> SI] Censores de fuego
<input type="checkbox"/> NO] Aire acondicionado (incluye sensor de humedad y temperatura)
<input type="checkbox"/> SI] Piso Falso
<input type="checkbox"/> SI] Puerta de Seguridad
<input type="checkbox"/> SI] Cámara de Seguridad
<input type="checkbox"/> SI] Tableros de control eléctrico y UPS's
Otros: cableado de red eléctrica regulada para las tomas de computadoras y extintores en el área.

5. Planeación de la Continuidad del Negocio

¿Tiene la entidad un plan de continuidad del negocio?	SI [] NO [X]
---	-----------------

¿Tiene la entidad algún tipo de arreglo que permita la restauración del procesamiento de la computadora en el caso de una emergencia?	SI [X] NO [] <i>Centro Computo alterno en GYE</i>
---	---

¿Se almacenan copias de respaldo de todos los programas de los sistemas de aplicación y archivos de datos importantes en un lugar fuera de la ubicación?	SI [X] NO []
--	-----------------

Haga una relación de los programas de los sistemas de aplicación y/o archivos de datos por los cuales NO se almacenan copias de respaldo en un lugar fuera de la ubicación.

Respaldos de información

¿El proceso de respaldo implementado por la entidad, permite la recuperación de la información cuando se necesite?

Si, los respaldos son almacenados en cd-writers los mismos que son guardados en una casilla de un Banco en Quito.

¿La información se almacena en cumplimiento con los periodos aplicables de retención definidos por la entidad?

Si, la política señala 5 años como minimo.

¿La información se destruye en cumplimiento de los periodos aplicables de retención y métodos de eliminación definidos por la entidad?

Si, la información es destruida pasado el periodo de 5 años, sujetándose a las políticas definidas al respecto.

¿La información almacenada se categoriza y se les pone etiquetas para ayudar en la identificación del periodo adecuado de retención?

Si, y los respaldos se graban con la fecha en que se realizó el respaldo.


¿Los periodos de retención están definidos de conformidad con las leyes, reglamentos y estrategias corporativas de la entidad?



ESPOL

Escuela Superior Politécnica del Litoral

FAI-005

Comprensión del ambiente de control tecnológico	Preparado por:	Katty Ronquillo Verónica García	[29/09/10]
EMPRESA: 	Revisado por:	Andrés Álvarez	[29/09/10]

Si, 5 años.



Documentar:

- Políticas, procedimientos, normas y guías con respecto a la eliminación, retención, respaldo y registros electrónicos
- Responsabilidades y descripciones laborales de los encargados de la custodia de los respaldos

6. Implementación y Mantenimiento de los Sistemas de Aplicación

<p>Describe la naturaleza de la metodología del desarrollo de sistemas y mantenimiento del cliente:</p>	<p>La metodología es SDLC (en cascada), consta de las siguientes etapas:</p> <ul style="list-style-type: none"> - Análisis del Sistema - Planificación del desarrollo del sistema - Diseño del Sistema - Implementación del Sistema - Mantenimiento del Sistema <p>El modelo de desarrollo SDLC prevé la generación de algunos documentos previos al inicio de la primera etapa:</p> <ul style="list-style-type: none"> - Estándares de documentación - Metodologías, técnicas y teorías de desarrollo del proyecto. - Control de Versiones - Estándares de Programación. <p>En la etapa de diseño del sistema, se deben elaborar:</p> <ul style="list-style-type: none"> - Documento de especificaciones del diseño del sistema - Manual de Usuario del Sistema <p>En la implementación se debe utilizar el Control de Versiones y los Estándares de Programación y se tiene como resultado al Código generado.</p> <p>Las pruebas del sistema incluyen:</p> <ul style="list-style-type: none"> - Pruebas del Usuario - Pruebas de Interfaces - Pruebas de Validación
---	--

¿Utiliza la entidad algunos sistemas de apoyo de decisiones y/o sistemas de información ejecutiva?	SI [] NO [X]
--	-----------------

 ESPOL Escuela Superior Politécnica del Litoral	FAI-005		
Comprensión del ambiente de control tecnológico	Preparado por:	Katty Ronquillo Verónica García	[29/09/10]
EMPRESA: 	Revisado por:	Andrés Álvarez	[29/09/10]

¿De qué fuentes obtiene la entidad los sistemas de aplicación? (desarrollo propio/adquiridos - a quién?)

Nombre del Sistema de Aplicación	Fuente
Ver FAI-003	

¿Tiene la entidad acceso a una copia actual del código fuente para todos los sistemas de aplicación importantes?	SI [X] NO []
--	-----------------

Software Comprado

Describa brevemente los procedimientos de la entidad para adquirir, implementar y mantener el software de aplicación comprado, incluyendo las funciones y responsabilidades de cualesquier individuos o grupos involucrados en este proceso.

Considere los siguientes tipos de procedimientos, según sean aplicables:

- Selección y compra de nuevos sistemas de aplicación
- Adaptación del software comprado
- Pruebas de los nuevos sistemas de aplicación y/o de las nuevas versiones de los sistemas de aplicación existentes, incluyendo cualquier adaptación
- Aprobación de nuevos sistemas de aplicación y/o modificaciones a los sistemas de aplicación existentes, antes de su implementación
- Traslado de los programas nuevos o modificados desde su desarrollo o prueba a las bibliotecas de producción (es decir, implementación de los programas nuevos o modificados)
- Validación de la integridad de la conversión de la información y de la exactitud de los nuevos sistemas de aplicación y/o de las nuevas versiones de los sistemas de aplicación existentes.

N/A

Si la entidad mantiene copias de los programas de producción fuente en bibliotecas, ¿quién actualiza el acceso a dichas bibliotecas? y a quién otorga?

El Gerente de Sistemas es el responsable de controlar el acceso y la actualización de las bibliotecas de producción. Todo esto se controla a través de la autorización en los formularios de Control de Versiones en Share Point.

¿Quién actualiza el acceso a las bibliotecas por el tiempo de ejecución de los programas de producción? y quién tiene acceso a la biblioteca de producción?



N/A. puesto que en producción solo están instalados los ejecutables.

Software Desarrollado Internamente

Describa brevemente los procedimientos de la entidad para desarrollar, implementar y mantener el software de aplicación, incluyendo las funciones y responsabilidades de cualesquier individuos o grupos involucrados en este proceso.

Considere los siguientes tipos de procedimientos, según sean aplicables:

- Pruebas de los nuevos sistemas de aplicación y/o modificaciones a los sistemas de aplicación existentes

	<h1>ESPOL</h1> <p>Escuela Superior Politécnica del Litoral</p>	FAI-005	
Comprensión del ambiente de control tecnológico	Preparado por:	Katty Ronquillo Verónica García	[29/09/10]
EMPRESA: 	Revisado por:	Andrés Álvarez	[29/09/10]

- Aprobación de nuevos sistemas de aplicación y/o modificaciones a los sistemas de aplicación existentes
- Traslado de los programas nuevos o modificados desde su desarrollo o prueba a las bibliotecas de producción (es decir, implementación de los programas nuevos o modificados)
- Validación de la integridad de la conversión de la información y de la exactitud de los nuevos sistemas de aplicación y/o modificaciones a los sistemas de aplicación existentes.

Hay un servidor dedicado para almacenamiento de los programas fuente 10.10.44.4 . Allí se realizan pruebas individuales con el usuario, revisiones de auditoría interna de Sistemas, entre otros.

¿Quién actualiza el acceso a las bibliotecas de los programas de producción fuente? y a quién otorga?
 El Jefe de Producción, es el encargado de realizar la actualización del acceso a las bibliotecas y programas de producción fuentes. Estos accesos son otorgados a los encargados de desarrollo, principalmente están otorgados para Myriam Morejón, quien está encargado del desarrollo y mantenimiento de aplicaciones.

¿Quién actualiza el acceso a las bibliotecas por el tiempo de ejecución de los programas de producción? y quién tiene acceso a la biblioteca de producción?
 N/A

¿Usa la entidad prototipos como parte del desarrollo de nuevos sistemas de aplicación? SI [X] NO []



7. Implementación y Soporte de la Base de Datos

Describa la arquitectura de datos de los sistemas de aplicación soportados por esta ubicación de procesamiento.	<i>Modelo Relacional</i>
---	--------------------------

Relacione el software de administración de la base de datos usado por los sistemas de aplicación soportados por este ambiente de procesamiento de la computadora y los sistemas de aplicación correspondientes.

Software de Administración de la Base de Datos	Sistemas de Aplicación
PROGRESS	Todas las aplicaciones

¿Mantiene la entidad uno o más diccionarios de datos? SI [] NO [X]

 ESPOL Escuela Superior Politécnica del Litoral	FAI-005		
Comprensión del ambiente de control tecnológico	Preparado por:	Katty Ronquillo Verónica García	[29/09/10]
EMPRESA: 	Revisado por:	Andrés Alvarez	[29/09/10]

Describe cómo se usan los diccionarios de datos:

Describe las responsabilidades para la administración de la base de datos de la institución.	<i>Se Administra el espacio físico del disco del Servidor; la administración de accesos y permisos a la BDD, reorganización de tablas, actualización de estadísticas.</i>
--	---

8. Apoyo a la Red



Describe brevemente el uso de redes del cliente, incluyendo las ubicaciones conectadas a la red, los ciclos y actividades de negocios y que están soportados por los sistemas de aplicación en la red, y las interrelaciones dentro de la red. Considere adjuntar un diagrama general de la red, si hay alguno disponible.

No existe diagrama General de Red

Describe el software de Administración de la Red
Windows 2003 Server

¿Quién actualiza el acceso a la configuración de datos del Software del Sistema de Administración de la Red?
Ing. Francisco Palacios

¿Quién es el responsable de modificar la configuración de datos del Software del Sistema de Administración de la Red?
Ing. Francisco Palacios

	<h1>ESPOL</h1> <p>Escuela Superior Politécnica del Litoral</p>	FAI-005	
Comprensión del ambiente de control tecnológico	Preparado por:	Katty Ronquillo Verónica García	[29/09/10]
EMPRESA: 	Revisado por:	Andrés Alvarez	[29/09/10]

9. Apoyo al Software del Sistema

<p>Describa brevemente los procedimientos de la empresa para adquirir, implementar y mantener el software del sistema (es decir, el sistema operativo y otro software que no se relaciona directamente con los sistemas de aplicación), incluyendo las funciones y responsabilidades de cualesquier individuos o grupos involucrados en este proceso. Cubra los siguientes tipos de procedimientos, según sean aplicables:</p> <ul style="list-style-type: none"> - Pruebas del software de sistemas nuevos y/o modificaciones al software existente - Evaluación del impacto del software de sistemas nuevos o modificados en el procesamiento de los sistemas de aplicación - Aprobación de la implementación del software de sistemas nuevos y/o modificaciones al software existente (v. gr., nuevas versiones de dicho software) - Traslado del software de los sistemas nuevos a las bibliotecas de producción (es decir, implementación de los programas nuevos o modificados) - Validación de la integridad y exactitud del procesamiento del software de los sistemas nuevos o modificados. <p><i>Se cuenta con un proveedor externo a quien se piden proformas y se efectúan las compras de acuerdo a la necesidad.</i></p>
--

10. Apoyo al Hardware



Vista General de la Configuración del Hardware

Para el sistema central de la computadora y otras computadoras o servidores importantes soportados por este ambiente de procesamiento de la computadora, proporcione la siguiente información:

Marca y Modelo	Sistema Operativo y Versión	Ubicación	Años Aproximados de Instalación
Ver FAI-002 en P/T			

Plataforma de Trabajo y Aplicaciones

<p><i>¿Cómo se da mantenimiento al equipo de la computadora?</i></p>	<p><i>Contrato de mantenimiento preventivo contratado con la empresa BINARIA.</i></p> <p><i>La ejecución de mantenimientos se los realiza 4 veces por año, los mismos que son coordinados y supervisados por los operadores delegados.</i></p> <p><i>Finalmente los técnicos de BINARIA deben entregar un reporte de resultados con su firma de responsabilidad.</i></p>
--	--

 ESPOL Escuela Superior Politécnica del Litoral	FAI-005		
Comprensión del ambiente de control tecnológico	Preparado por:	Katty Ronquillo Verónica García	[29/09/10]
EMPRESA: 	Revisado por:	Andrés Alvarez	[29/09/10]

B.- HECHOS IMPORTANTES OCURRIDOS EN ESTE AMBIENTE DE PROCESAMIENTO DE LA COMPUTADORA DESDE LA ULTIMA VISITA DE INSPECCION

Si se han identificado hechos importantes o transacciones inusuales que requieran ser ampliados y puedan tener impacto sobre el plan de rotación.

Cambios Importantes

Describa brevemente los cambios importantes, si los hay, en las áreas siguientes:

Cambios en el personal del ambiente de procesamiento de la computadora:

No ha habido cambios significativos desde aproximadamente el año 2000

Modificaciones a las políticas y procedimientos de seguridad de la información (escrita o no escrita):

No.

Modificaciones a la metodología de desarrollo de los sistemas de aplicación:

No.

Modificaciones a las políticas y procedimientos de mantenimiento del software del sistema:

No.

Otros cambios en las políticas y procedimientos del ambiente de procesamiento de la computadora:

No.

Implementación de nuevas versiones de software u otras modificaciones importantes al software de los sistemas o a los sistemas de aplicación:

Cambio a plataforma Windows 200 a Windows 203 Server de los aplicativos.

Describa cambios importantes tales como: adquisiciones, cambios o disposiciones de hardware:

Se han adquirido 150 nuevas PC's para reemplazo de las áreas de Atención al Cliente, Contabilidad Cobranzas, y Producción.

Hay cambios importantes descritos arriba que tengan un impacto sobre el plan de rotación?

No.

C.- PROBLEMAS ENCONTRADOS POR LOS USUARIOS O POR LA GERENCIA DESDE LA ÚLTIMA VISITA DE INSPECCIÓN

Describa los problemas que los usuarios o la gerencia hayan identificado recientemente. Por cada problema identificado, describalo y considere cómo afecta a la conclusión preliminar si este ambiente de procesamiento de la computadora soporta el procesamiento confiable de la información en los ciclos de negocios correspondientes.

Considere los siguientes tipos de problemas:

- Fallas del sistema



ESPOL

Escuela Superior Politécnica del Litoral

FAI-005

Comprensión del ambiente de control tecnológico

Preparado por:

Katty Ronquillo
Verónica García

[29/09/10]

EMPRESA:



Revisado por:

Andrés Álvarez

[29/09/10]

- Errores importantes en los resultados del procesamiento
- Retrasos significativos de procesamiento o pérdida de datos
- Dificultades experimentadas por los usuarios para obtener cambios a los sistemas de aplicación
- Falta de entrenamiento o de soporte a los usuarios
- Dificultades con la implementación de modificaciones al sistema o con las conversiones a nuevos sistemas
- Limitaciones de los sistemas que originan procedimientos manuales adicionales
- Cambios a los sistemas sin la aprobación del usuario
- Otros

Descripción del Problema Identificado

No se han observado problemas relevantes en Sistemas.

Otra Información

Describa cualesquier planes del cliente para mejorar o reemplazar el hardware o software existente:

Entre los principales proyectos de la Gerencia, se tiene planificado implantar:

- *Reemplazar Sistemas Contable Actual.*
- *Reemplazar Sistema Administrativo Actual.*

D.- AUDITORIA

¿Ha realizado auditoria interna trabajo relacionado con este ambiente de procesamiento y/o los sistemas de aplicación?

SI [] NO [X]

Describa el trabajo, considere los siguientes puntos:

- Alcance del trabajo
- Naturaleza del trabajo
- Confiabilidad del trabajo
- Riesgos identificados

No existe

Describa los riesgos identificados para los sistemas de aplicación y cuentas relacionadas

N/A



ESPOL

Escuela Superior Politécnica del Litoral

FAI-005

Comprensión del ambiente de control tecnológico

Preparado por:

Katty Ronquillo
Verónica García

[29/09/10]

EMPRESA:



Revisado por:

Andrés Álvarez

[29/09/10]

¿Han realizado auditores /consultores externos trabajo relacionado con este ambiente de procesamiento y/o los sistemas de aplicación?

SI [] NO [X]

Describe el trabajo, considere los siguientes puntos:

- Alcance del trabajo
- Naturaleza del trabajo
- Confiabilidad del trabajo
- Riesgos identificados

Describe los riesgos identificados para los sistemas de aplicación y cuentas relacionadas

Entre los principales puntos identificados está la elaboración de un Plan de Contingencias y sus respectivas pruebas.

RIESGOS IDENTIFICADOS

Del análisis anterior, ¿se han identificado riesgos?

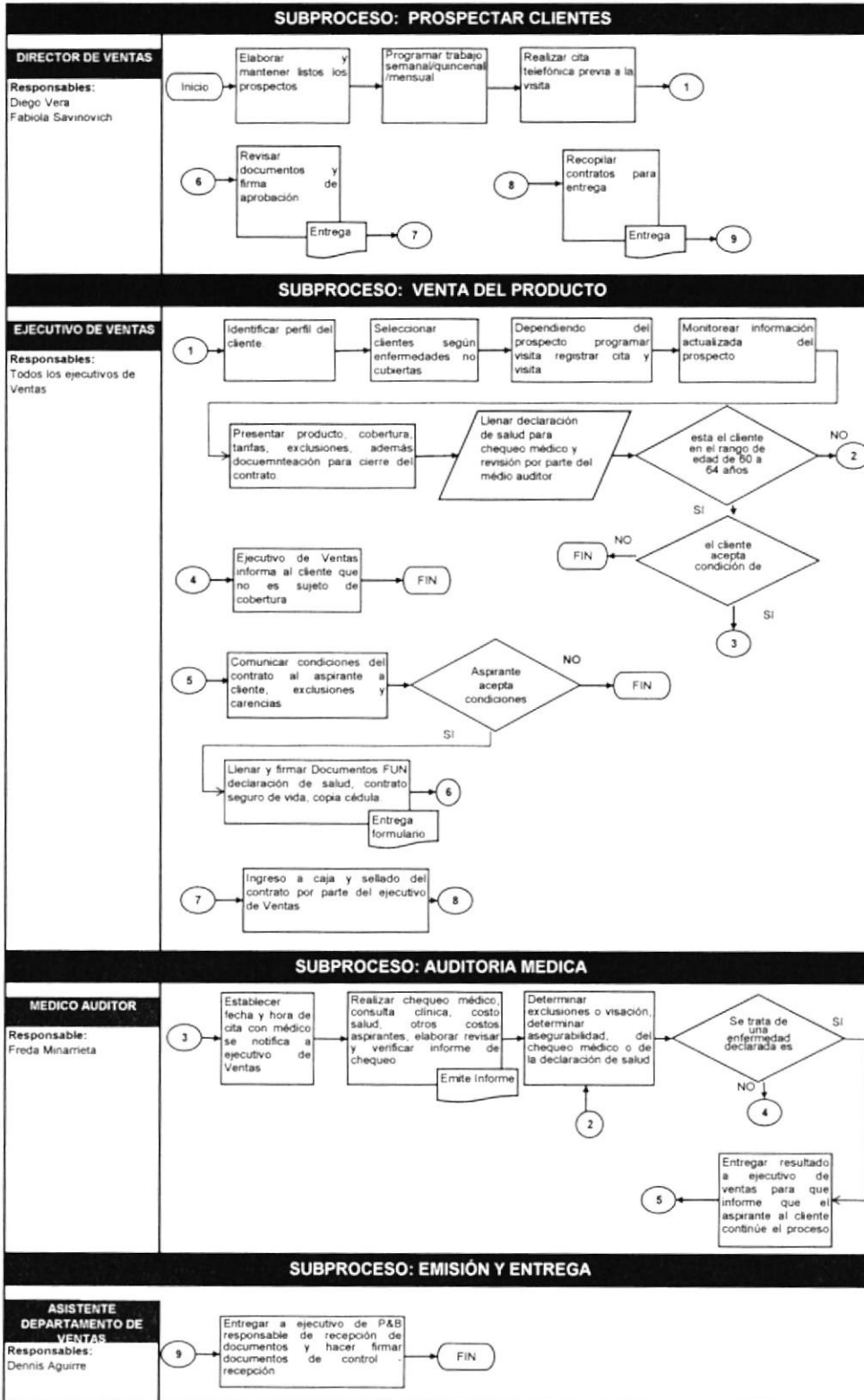
CONCLUSION PRELIMINAR

Revise las respuestas a las preguntas de esta Forma al concluir si este ambiente de procesamiento de la computadora soporta el procesamiento confiable de la información en los ciclos de negocios correspondientes. En particular, considere todas las respuestas "No". Evalúe el impacto, si lo hay, sobre la conclusión y/o considere si hay algunas Observaciones o Recomendaciones Constructivas que deberían comunicarse a la entidad.

Conclusión Preliminar sobre si este Ambiente de Procesamiento de la Computadora Soporta el Procesamiento Confiable de la Información Financiera en la entidad supervisada.

Respalda []

No respalda [X]

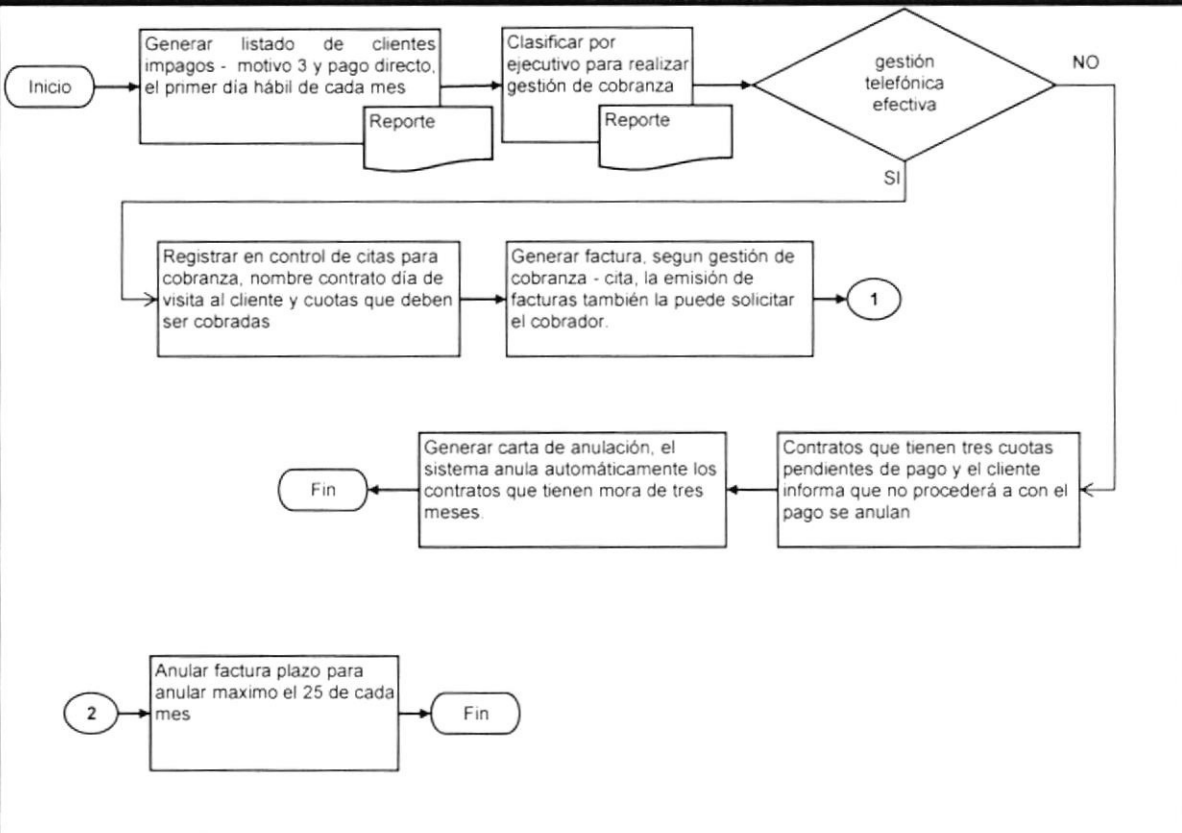




SUBPROCESO: GESTIÓN DE COBRANZA TELEFÓNICA

EJECUTIVO DE CUENTA

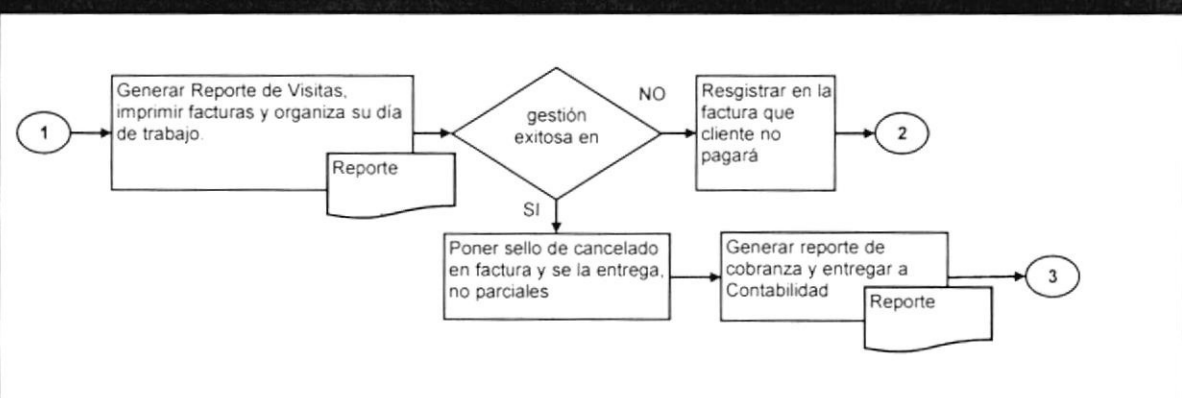
Responsables:
Pamela Bonnard
Diego Vera



SUBPROCESO: GESTION DE COBRANZAS CITAS

COBRADOR

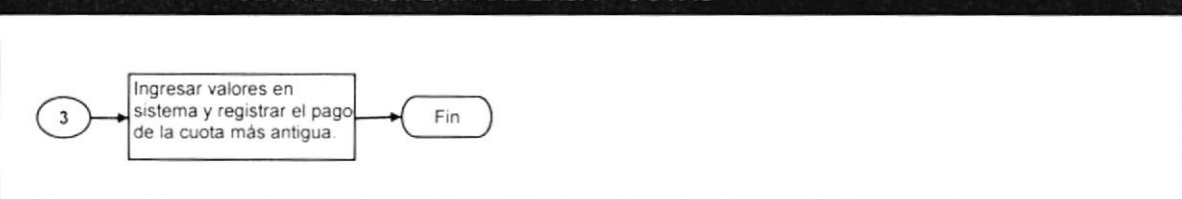
Responsables:
Pamela Bonnard



SUBPROCESO: DAR DE BAJA CUOTAS

ASISTENTE DE TESORERIA

Responsable:
Vicente Chalén

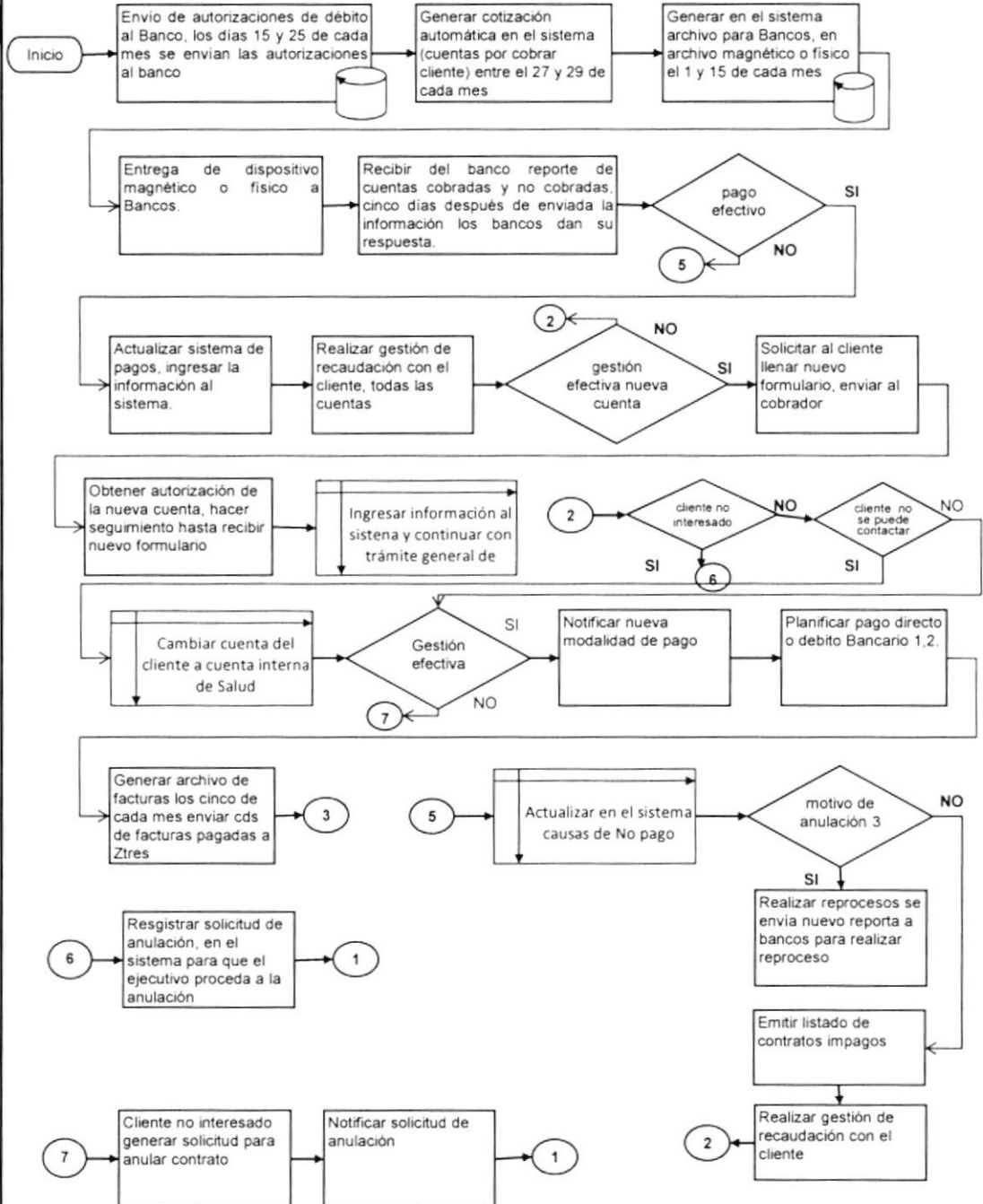




SUBPROCESO: RECEPCIÓN DE DOCUMENTOS

ASISTENTE DE RECAUDACIONES

Responsables:
Martha Franco
Diego Vera





CORPORACIÓN SALUD S.A.
MEDICINA PREPAGADA

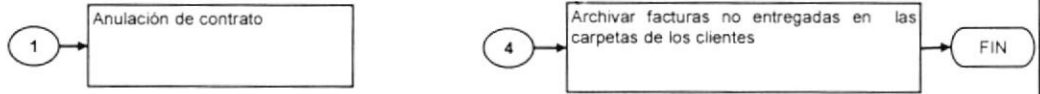
PROCESO: RECAUDACIONES SEGUNDAS CUOTAS Y MÁS

SUBPROCESO: RECEPCIÓN DE DOCUMENTOS

SUBPROCESO: NOTIFICACIÓN AL CLIENTE

EJECUTIVO DE CUENTAS

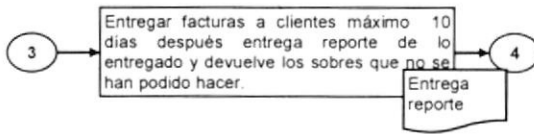
Responsables:
Todos los ejecutivos de Ventas



SUBPROCESO: ENTREGA DE CARPETA

COURIER

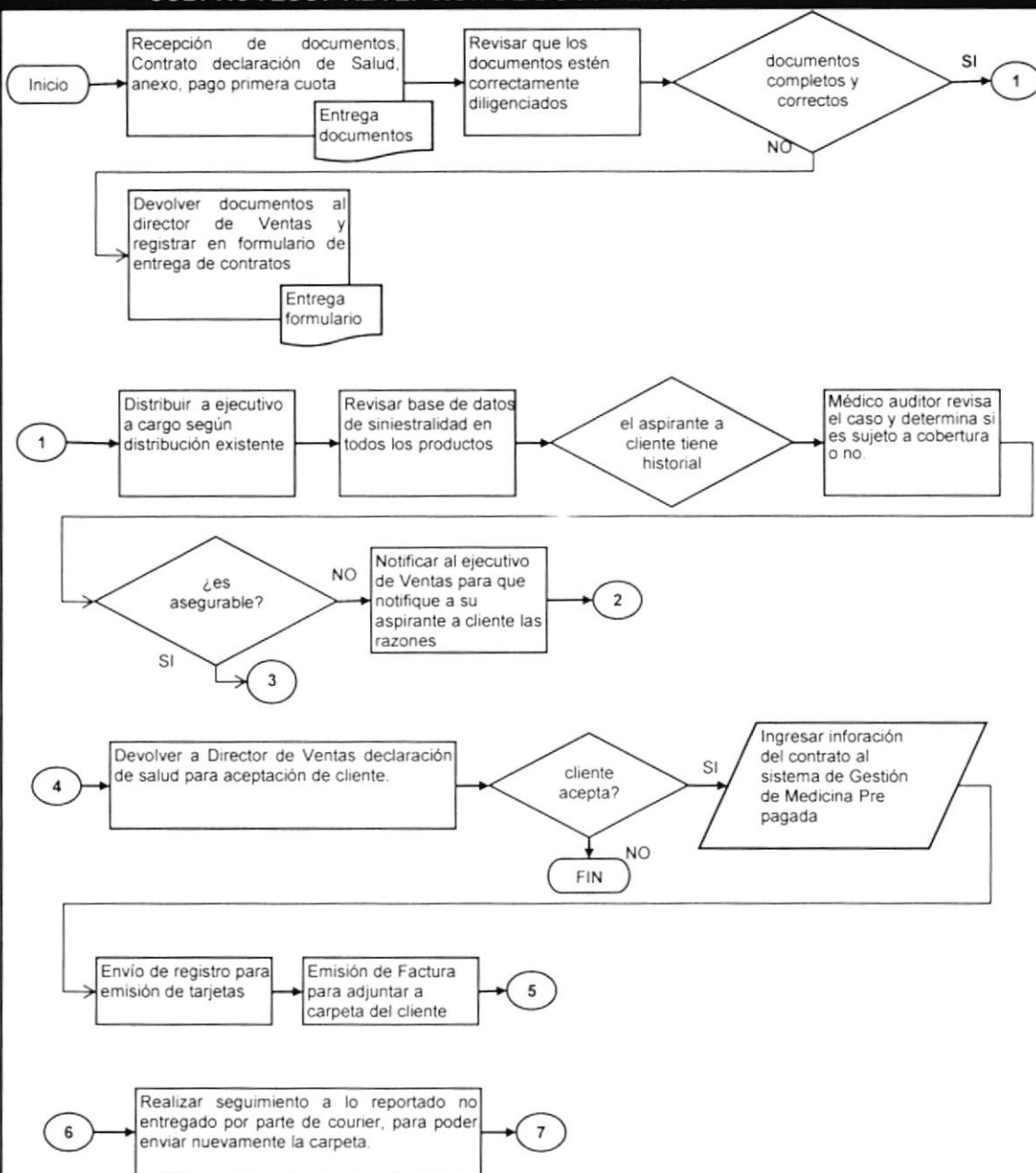
Responsable:
Gladys Rendón



SUBPROCESO: RECEPCIÓN DE DOCUMENTOS

EJECUTIVO DE CUENTA

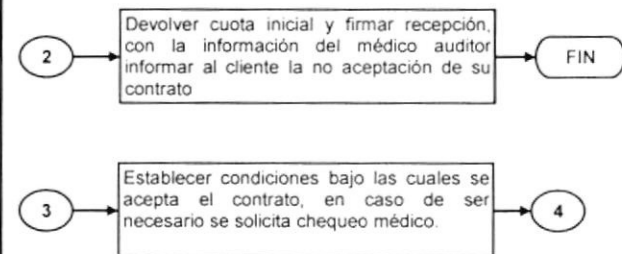
Responsables:
Martha Franco
Diego Vera



SUBPROCESO: NOTIFICACIÓN AL CLIENTE

EJECUTIVO DE VENTAS

Responsables:
Todos los ejecutivos de Ventas





CORPORACIÓN SALUD S.A.
MEDICINA PREPAGADA

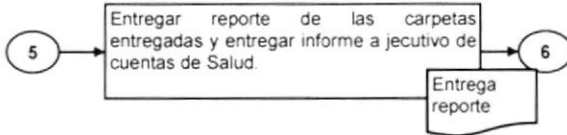
PROCESO: EMISIÓN Y ENTREGA INDIVIDUAL

SUBPROCESO: RECEPCIÓN DE DOCUMENTOS

SUBPROCESO: ENTREGA DE CARPETA

COURIER

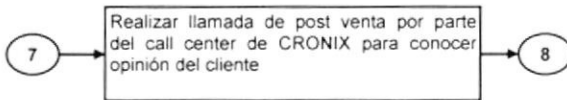
Responsable:
Gladys Rendón



SUBPROCESO: LLAMADA DE POST VENTA

CRONIX

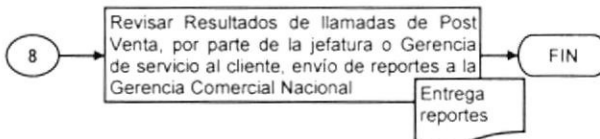
Responsable:
CRONIX



SUBPROCESO: REVISIÓN DE RESULTADOS

GERENCIA DE P&B

Responsable:
Diego Vera



VALORACIÓN Y MAPEO DE RIESGOS

Mapa de Riesgo

NOTA: Llenar solo las celdas que se encuentran sombreadas en color verde, las celdas restantes se encuentran bloqueadas para protección de las formulas que graficarán los riesgos

Vulnerabilidad: Nivel de exposición para que un riesgo se materialice, considerando la estructura de control actual

Escala 1 al 5

Impacto: Posibilidad de que la magnitud del Riesgo afecte el cumplimiento de los objetivos

PROCESO	LIDER PROCESO	RIESGO IDENTIFICADO	CRITICIDAD	VULNERABILIDAD	IMPACTO	VOTO / CARGOS	Calificación Gerente General	Calificación Gerente Financiero	Calificación Gerente de Sistemas	Controles Sugeridos para mitigar riesgos	Costo de aplicar los controles \$ (Alto, Medio, Bajo)	Tratamiento al Riesgo
		LA EMPRESA NO CUENTA CON UN PLAN ESTRATEGICO QUE VAYA DE ACUERDO CON LAS METAS Y ESTRATEGIAS DE LA EMPRESA		5,0	5,0	VOTO IMPACTO	5,0	5,0	5,0	Definir un plan estratégico que vaya de acuerdo con las metas y estrategias de la empresa.	Medio	Mitigar
						VOTO VULNERABILIDAD	5,0	5,0	5,0			
		NO EXISTE UNA CLASIFICACION DE DATOS, QUE INCLUYA A LOS DUEÑOS Y LAS CATEGORIAS DE SEGURIDAD	Medio	4,0	3,0	VOTO IMPACTO	5,0	3,0	3,0	Establecer un marco de referencia de clasificación general a la ubicación de los datos.	Medio	Mitigar
						VOTO VULNERABILIDAD	4,0	4,0	4,0			
		LA EMPRESA NO CUENTA CON PROCEDIMIENTOS QUE PERMITAN REALIZAR UN ENTRENAMIENTO CRUZADO		4,0	4,0	VOTO IMPACTO	5,0	5,0	3,0	Establecer procedimientos adecuados para identificar al personal clave para evitar ausencias.	Medio	Mitigar
						VOTO VULNERABILIDAD	5,0	4,0	4,0			
		NO EXISTE UN MANUAL DE POLITICAS Y PROCEDIMIENTOS PARA LOS AMBIENTES DE DESARROLLO Y PRODUCCION		4,5	4,5	VOTO IMPACTO	4,0	4,0	5,0	Establecer responsabilidades y procedimientos para la gestión y operación de las instalaciones de procesamiento de información.	Medio	Mitigar
						VOTO VULNERABILIDAD	4,0	4,0	5,0			
		LA EMPRESA NO TIENE UN PROCEDIMIENTO DEFINIDO PARA LA ADQUISICION DE BIENES Y SERVICIOS INFORMATICOS		4,0	5,0	VOTO IMPACTO	5,0	5,0	5,0	Definir políticas y procedimientos de adquisición de bienes y servicios informáticos.	Medio	Mitigar
						VOTO VULNERABILIDAD	4,0	4,0	4,0			

VALORACIÓN Y MAPEO DE RIESGOS

Mapa de Riesgo

NOTA: Llenar solo las celdas que se encuentran sombreadas en color verde, las celdas restantes se encuentran bloqueadas para protección de las formulas que graficarán los riesgos

Vulnerabilidad: Nivel de exposición para que un riesgo se materialice, considerando la estructura de control actual

Escala 1 al 5

Impacto: Posibilidad de que la magnitud del Riesgo afecte el cumplimiento de los objetivos

PROCESO	LIDER PROCESO	RIESGO IDENTIFICADO	CRITICIDAD	VULNERABILIDAD	IMPACTO	VOTO / CARGOS	Calificación Gerente General	Calificación Gerente Financiero	Calificación Gerente de Sistemas	Controles Sugeridos para mitigar riesgos	Costo de aplicar los controles \$ (Alto, Medio, Bajo)	Tratamiento al Riesgo
		NO SE HAN IMPLEMENTADO POLITICAS, NORMAS Y PROCEDIMIENTOS DE SEGURIDADES QUE PROPORCIONEN UN CONTROL EFICIENTE A LOS RECURSOS DE INFORMACION		4,0	5,0	VOTO IMPACTO	4,0	5,0	5,0	Implementar una política de seguridad que suministre una orientación acerca de la asignación de dunciones de seguridad y responsabilidades.	Medio	Mitigar
						VOTO VULNERABILIDAD	4,0	4,0	4,0			
		NO HAY UN ADECUADO CONTROL PARA EL ACCESO AL AMBIENTE DE PRODUCCION DE LA EMPRESA		4,0	4,5	VOTO IMPACTO	4,0	4,0	5,0	Se establecerá como política de seguridad que cada cierto tiempo la clave sea cambiada, además deberá ser encriptada.	Medio	Mitigar
						VOTO VULNERABILIDAD	3,0	4,0	4,0			
		LA EMPRESA NO CUENTA CON UN PLAN DE CONTINUIDAD DEL PROCESAMIENTO DE LA INFORMACION		4,0	5,0	VOTO IMPACTO	5,0	5,0	5,0	Elaborar un plan de contingencia para que continuen las operaciones en cualquier situación de emergencia.	Medio	Mitigar
						VOTO VULNERABILIDAD	4,0	4,0	4,0			
		EL DEPARTAMENTO DE SISTEMAS NO CUENTA CON UN PROCEDIMIENTO ADECUADO PARA LA ADMINISTRACION DE CAMBIOS DE SOFTWARE		4,0	4,0	VOTO IMPACTO	3,0	3,0	5,0	Implementar un procedimiento para la administración de cambio de software.	Medio	Mitigar
						VOTO VULNERABILIDAD	3,0	3,0	5,0			
		NO EXISTE DOCUMENTACION TECNICA DE LOS MODULOS DEL SISTEMA SIGMEP		4,5	4,5	VOTO IMPACTO	3,0	4,0	5,0	Elaborar la documentación técnica del sistema aplicativo.	Medio	Mitigar
						VOTO VULNERABILIDAD	3,0	4,0	5,0			
		LA EMPRESA NO CUENTA CON LOS PROGRAMAS FUENTES, DIAGRAMA ENTIDAD RELACION DE LAS TABLAS DE LA BASE DE DATOS DEL		4,5	4,5	VOTO IMPACTO	4,0	4,0	5,0	Elaborar el manual técnico y de usuario del módulo de Recaudaciones.	Medio	Mitigar

VALORACIÓN Y MAPEO DE RIESGOS

Mapa de Riesgo

NOTA: Llenar solo las celdas que se encuentran sombreadas en color verde, las celdas restantes se encuentran bloqueadas para protección de las formulas que graficarán los riesgos

Vulnerabilidad: Nivel de exposición para que un riesgo se materialice, considerando la estructura de control actual

Escala 1 al 5

Impacto: Posibilidad de que la magnitud del Riesgo afecte el cumplimiento de los objetivos

PROCESO	LIDER PROCESO	RIESGO IDENTIFICADO	CRITICIDAD	VULNERABILIDAD	IMPACTO	VOTO / CARGOS	Calificación Gerente General	Calificación Gerente Financiero	Calificación Gerente de Sistemas	Controles Sugeridos para mitigar riesgos	Costo de aplicar los controles \$ (Alto, Medio, Bajo)	Tratamiento al Riesgo
		MODULO DE RECAUDACIONES				VOTO VULNERABILIDAD	4,0	4,0	5,0			
		FALTA DE SEGURIDAD EN EL PROCESO DE ALMACENAMIENTO DE LA INFORMACION BANCARIA DE LOS CLIENTES DE LA EMPRESA	Medio	3,0	4,0	VOTO IMPACTO	4,0	5,0	3,0	Se deberá automatizar la sincronización entre el banco contratante y el sistema de cobro.	Medio	Mitigar
						VOTO VULNERABILIDAD	3,0	3,0	3,0			
		INCONSISTENCIAS EN LA GENERACION DE LAS NOTAS DE PROTESTO DE CHEQUES ENTREGADOS A LA EMPRESA.	Medio	3,5	4,0	VOTO IMPACTO	5,0	5,0	3,0	Coordinar con el área de desarrollo las correcciones a los procesos indicados y monitoreo constante de problemas como éstos.	Medio	Mitigar
						VOTO VULNERABILIDAD	4,0	4,0	3,0			
		LOS PROCESOS DE REPLICACION DE LOS SERVIDORES DE DATOS DE LAS SUCURSALES CON EL SERVIDOR DE LA MATRIZ NO SE ENCUENTRAN SINCRONIZADOS.		3,5	4,5	VOTO IMPACTO	4,0	4,0	5,0	Implementar de manera urgente un afinamiento de los procesos de replicación.	Medio	Mitigar
						VOTO VULNERABILIDAD	3,0	3,0	4,0			