UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN

CARRERA:
FACULTAD DE SISTEMAS INFORMÁTICOS

TEMA:
AUDITORÍA INFORMÁTICA ORIENTADA A LOS PROCESOS CRÍTICOS DE TARJETA DE DÉBITO GENERADOS EN LA COOPERATIVA DE AHORRO Y CRÉDITO "JUVENTUD ECUATORIANA PROGRESISTA LTDA." APLICANDO EL MARCO DE TRABAJO COBIT.

AUTOR: JORGE EDUARDO CÁRDENAS CHÁVEZ

TUTOR: ING. CRISTÓBAL ALBERTO ÁLVAREZ ABRIL DsD.

2014

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

CERTIFICADO DE RESPONSABILIDAD

Yo, Ing. Cristóbal Álvarez, certifico que el señor Jorge Eduardo Cárdenas Chávez con C.I. No. 1712336138 realizó la presente tesis con el título **"AUDITORÍA INFORMÁTICA ORIENTADA A LOS PROCESOS CRÍTICOS DE TARJETA DE DÉBITO GENERADOS EN LA COOPERATIVA DE AHORRO Y CRÉDITO "JUVENTUD ECUATORIANA PROGRESISTA LTDA." APLICANDO EL MARCO DE TRABAJO COBIT",** que es autor intelectual del mismo, que es original, auténtico y personal.

_____

Ing. Cristóbal Alberto Álvarez Abril DsD

CERTIFICADO DE AUTORÍA

El documento de tesis con título **"AUDITORÍA INFORMÁTICA ORIENTADA A LOS PROCESOS CRÍTICOS DE TARJETA DE DÉBITO GENERADOS EN LA COOPERATIVA DE AHORRO Y CRÉDITO "JUVENTUD ECUATORIANA PROGRESISTA LTDA." APLICANDO EL MARCO DE TRABAJO COBIT"** ha sido desarrollado por Jorge Eduardo Cárdenas Chávez con C.C. No. 1712336138 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de cada uno de los productos de esta tesis sin previa autorización.

_____

Jorge Eduardo Cárdenas Chávez

DEDICATORIA

A mi esposa Blanca, quien ha sido un pilar fundamental en la consecución de todos mis logros, acompañándome con su amor y su perseverancia.

A mi madre Dolores, por su ejemplo profesional y sobre todo por su calidad humana, ha sido mi inspiración en las diferentes etapas de mi vida.

AGRADECIMIENTO

Siento una profunda gratitud hacia mis hermanos Alexandra y Fernando por su apoyo siempre incondicional, han estado conmigo en todos los momentos de mi vida.

Agradezco a todas las personas que conforman la Universidad Tecnológica Israel, estoy seguro que su esfuerzo los llevará siempre por caminos de mucho éxito.

CONTENIDO

Índice de Gráficos.

Índice de Figuras.

Índice de Tablas

RESUMEN

La presente tesis tiene como objetivo principal aplicar una Auditoría Informática a la Cooperativa de Ahorro y Crédito “Juventud Ecuatoriana Progresista Ltda.” en sus procesos de trabajo asociados al desarrollo del producto tarjeta de débito, se ha establecido como marco de trabajo el uso del modelo Cobit.

En el presente trabajo se establece como una necesidad que la Cooperativa aplique una Auditoría Informática pues le permitirá en un inicio establecer los procesos más críticos que administran el producto.

La siguiente fase consta en conocer mediante encuestas al personal, las actividades de trabajo, su frecuencia y su criticidad. Esta información permite al auditor tener una visión general del área.

Se establece la infraestructura tecnológica en hardware y software con que cuenta la Cooperativa a fin de poder establecer las herramientas tecnológicas de apoyo que evaluará la infraestructura, así como también permite al auditor aplicar el marco Cobit en las áreas de aplicación.

Dentro del ejercicio de la Auditoría Informática aplicando el marco de trabajo Cobit, se establecen las vulnerabilidades, los procesos Cobit de evaluación y el nivel de riesgo asociado a cada proceso.

Como resultado de la aplicación de la Auditoría Informática se obtienen evidencias, fruto de los ejercicios de aplicación de las herramientas informáticas, también se presentan los resultados que surgen de la evaluación directa del auditor, utilizando como medios la observación directa, aplicación y uso de las herramientas mediante simulación de usuario o administrador de los recursos.

Todos los resultados son evaluados y clasificados por su nivel de riesgo, lo que permite establecer el nivel de madures de los procesos involucrados en la administración del producto. Finalmente se emite el informe con las recomendaciones y un plan de trabajo propuesto a fin de que las vulnerabilidades sean minimizadas.

CAPÍTULO I

1 TEMA.

AUDITORÍA INFORMÁTICA ORIENTADA A LOS PROCESOS CRÍTICOS DE TARJETA DE DÉBITO GENERADOS EN LA COOPERATIVA DE AHORRO Y CRÉDITO "JUVENTUD ECUATORIANA PROGRESISTA LTDA." APLICANDO EL MARCO DE TRABAJO COBIT.

1.2 PLANTEAMIENTO DEL PROBLEMA.

1.2.1 Definición del problema de investigación.

Dentro de los servicios que ofrece la Cooperativa de Ahorro y Crédito "Juventud Ecuatoriana Progresista Ltda." se encuentra la Tarjeta de Débito, este producto permite a los clientes acceder a la red de cajeros de la Cooperativa así como de otras instituciones financieras ecuatorianas y realizar retiros de dinero con el respectivo débito automático de la cuenta de ahorros del cliente.

Los procesos para el manejo del producto Tarjeta de Débito han estado enfocados en brindar una ágil funcionalidad para el cliente, sin embargo no se han observado a detalle normas de seguridad informática que permitan minimizar los riesgos de posibles errores involuntarios o incluso fraudes que vulneren los sistemas informáticos y ocasionen fallas en la disponibilidad de los servicios, pérdidas de información, compromiso o copia de información importante y sensible.

Los aspectos informáticos que presenten fallas en su funcionamiento o que vean comprometida su información más sensible pueden tener repercusiones graves para la Institución como son: pérdidas financieras por fraudes o errores operativos; pérdida de la confianza de los clientes y afectación en su reputación dentro de la industria financiera.

1.2.2 Delimitación del problema de investigación.

1.2.2.1. Límites teóricos.

La Auditoría Informática es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para

determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas. (Wikipedia)

La Auditoría Informática busca mantener la eficiencia en los sistemas informáticos, verificar que se cumplan las normativas institucionales dentro del uso y manejo de los sistemas informáticos y busca realizar una gestión eficaz de los recursos tecnológicos.

Las amenazas se pueden conceptualizar como un evento que puede afectar de manera directa o indirecta en el funcionamiento de los sistemas informáticos, o la información que contienen los mismos.

Dentro de las instituciones y en particular las financieras existen amenazas que pueden afectar seriamente los sistemas informáticos. Las amenazas pueden ser internas, cuando los usuarios dentro de la institución vulneran la seguridad informática y obtienen algún beneficio o causan daño voluntario o involuntario a la información o a los sistemas tecnológicos, así también las amenazas pueden ser externas y tener las mismas consecuencias ya indicadas.

El riesgo es la posibilidad de que ocurra una amenaza, está presente de forma que se pueda controlar o minimizar.

Existen riesgos inherentes al negocio de intermediación financiera, estos se caracterizan porque pueden ser considerados altos, medios o bajos, dependiendo en gran medida del impacto que puedan tener en caso de ocurrencia.

1.2.2.2. Límites temporales.

El desarrollo del Trabajo de Titulación que se plantea, conlleva un tiempo de ejecución de 4 meses.

El desarrollo del Trabajo de Titulación tendrá su enfoque en la situación actual que presentan los procesos de la Cooperativa de Ahorro y Crédito “Juventud Ecuatoriana Progresista Ltda.” en el año 2013.

1.2.2.3. Limites espaciales.

El desarrollo del Trabajo de Titulación se llevará a cabo en la Cooperativa de Ahorro y Crédito “Juventud Ecuatoriana Progresista Ltda.”, ubicada en la ciudad de Cuenca, provincia del Azuay, Ecuador.

1.3 OBJETIVOS.

1.3.1 Objetivo principal.

Aplicar una Auditoría Informática que evalúe el nivel de cumplimiento de control de los procesos críticos de Tarjeta de Débito, que permita identificar vulnerabilidades y establecer recomendaciones para minimizar riesgos.

1.3.2 Objetivos secundarios.

Establecer el nivel de cumplimiento del marco de trabajo del Modelo COBIT.

Identificar los procesos críticos del área de Tarjeta de Débito y su infraestructura tecnológica.

Evaluar la eficacia y eficiencia de los sistemas de información que evidencien la disponibilidad, confidencialidad e integridad de la información almacenada.

1.4 JUSTIFICACIÓN DE LA INVESTIGACIÓN.

La Auditoría Informática aplicada a la Cooperativa de Ahorro y Crédito “Juventud Ecuatoriana Progresista Ltda.” permitirá que se identifiquen los riesgos existen en los procesos críticos de Tarjeta de Débito, permitiendo así a la alta gerencia, tomar medidas e implementar mejoras que remedien los hallazgos evidenciados durante la ejecución del plan de auditoría.

Como beneficios para la Cooperativa de Ahorro y Crédito “Juventud Ecuatoriana Progresista Ltda.” se establecen que su exposición al riesgo será evaluada una vez finalizada la Auditoría Informática, así como también contará con una metodología que le permitirá mejorar constantemente sus procesos críticos.

La Auditoría Informática planteada, permitirá corregir las posibles deficiencias que se puedan establecer una vez finalizado el ejercicio.

En la actualidad la Auditoría Informática tiene un rol primordial dentro de las instituciones financieras, debido a que entre otros aspectos importantes busca mantener bajo normas de seguridad la información y los datos que la componen, considerados como el activo más importante en las instituciones del sector financiero.

1.5 HIPÓTESIS.

Cuanto mayor es el crecimiento de los procesos de Tarjeta de Débito en la Cooperativa de Ahorro y Crédito “Juventud Ecuatoriana Progresista Ltda.”, tanto mayor es el riesgo de ocurrencia de pérdida financiera originado por una amenaza interna o externa.

1.5.1 Variables del trabajo de graduación.

Crecimiento de los procesos.

Riesgo de ocurrencia.

Pérdida financiera.

Amenaza interna o externa.

1.5.1.1. Definición conceptual.

Crecimiento de los procesos.

Debido al crecimiento de la población económicamente activa que se integra al sistema financiero ecuatoriano, se origina también el crecimiento de los procesos internos dentro de

la Cooperativa con el objetivo de seguir brindando servicios integrales acordes con la realidad nacional.

Riesgo de ocurrencia.

Es la probabilidad de que ocurra un evento, el riesgo es una variable que puede ser medida en el tiempo.

Pérdida financiera.

Es el resultado de operaciones financieras que por su naturaleza afectan al resultado económico de la institución. Afecta negativamente al ingreso o utilidad neta de un ejercicio financiero determinado.

Amenaza interna o externa.

Son factores internos o externos a los que está expuesta la institución financiera, se consideran que pueden ser perjudiciales en la mayoría de casos para la empresa debido a que quienes ejecutan la amenaza buscan intereses particulares que pueden afectar a la institución.

Vulnerabilidad.

En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones. (TECNOLOGÍA)

1.5.2 Operación de las variables.

Variable	Dimensión	Indicador
Crecimiento de los procesos.	Procesos, Tareas.	Aumento, disminución.
Riesgo de ocurrencia.	Eventos.	Probabilidades de ocurrencias.
Pérdida financiera.	Cuentas contables, balances.	Reducción de ingresos, utilidades.
Amenaza interna o externa.	Sabotaje, fraudes, intrusiones.	Tabulación, alta, media, baja.

1.6 MARCO DE REFERENCIA.

1.6.1 Antecedentes teóricos del tema de investigación.

El modelo COBIT ayuda a las empresas a gestionar la información y la tecnología de forma eficiente. Es necesario asegurar el valor de la tecnología, administrar los riesgos que son conocidos como elementos claves del Gobierno Corporativo.

El valor, el riesgo y el control constituyen la esencia del gobierno de TI (Tecnología de Información).

COBIT recomienda que el enfoque se debe mantener alineado las necesidades y requerimientos del negocio utilizando métricas y modelos de madurez para medir sus logros, teniendo en cuenta a los dueños de cada proceso tanto del negocio como de las tecnologías de información.

Para que TI tenga éxito en satisfacer los requerimientos del negocio, la dirección debe implementar un sistema de control interno o un marco de trabajo. El marco de trabajo de control COBIT contribuye a estas necesidades de la siguiente manera:

• Estableciendo un vínculo con los requerimientos del negocio.

• Organizando las actividades de TI en un modelo de procesos generalmente aceptado.

• Identificando los principales recursos de TI a ser utilizados.

• Definiendo los objetivos de control gerenciales a ser considerados (COBIT).

Marco de Trabajo de COBIT.

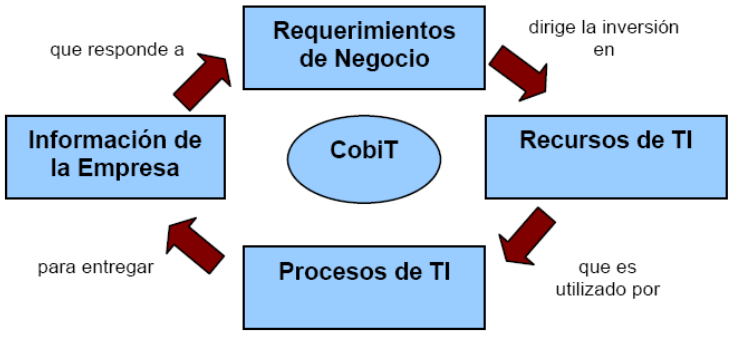
El modelo de COBIT fue creado para ser orientado a negocios y procesos, basado en controles e impulsado por mediciones.

Orientado a Negocios.

El Modelo de COBIT es orientado a negocios ya que se encuentra diseñado para ser una guía para la gerencia, propietarios de los procesos de negocio, los proveedores de servicios, usuarios y auditores de TI. Además es el enfoque de control en TI que se lleva a cabo visualizando la información necesaria para dar soporte a los procesos del negocio. Siendo la Información el resultado de la aplicación combinada de recursos relacionados con la Tecnología de Información, que deben ser administrados por procesos TI.

El Marco de Trabajo de COBIT ofrece herramientas para garantizar la alineación de la administración de TI con los requerimientos del negocio, basados en los principios básicos de COBIT.

Gráfico Principio básico de COBIT.



Estructura del Marco de Referencia COBIT.

El marco de referencia de COBIT consta de objetivos de control de TI de alto nivel y de una estructura general para su clasificación y presentación, que se basan en tres niveles de actividades de TI al considerar la administración de sus recursos, estos son:

Actividades: las actividades y tareas son las acciones requeridas para lograr un resultado medible. Las actividades tienen un ciclo de vida, mientras que las tareas son más discretas.

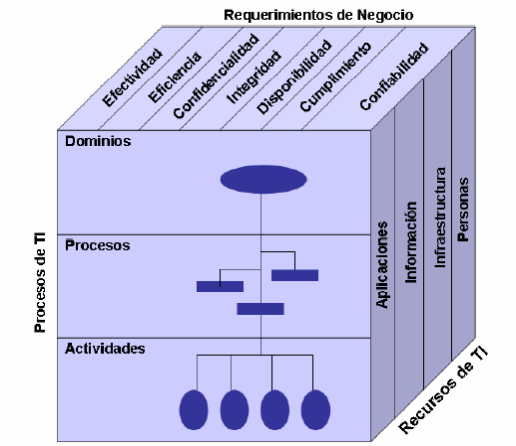
Procesos: son conjuntos de actividades o tareas con delimitación o cortes de control.

Dominios: es la agrupación natural de procesos denominados frecuentemente como dominios que corresponden a la responsabilidad organizacional.

El marco de referencia conceptual puede ser enfocado desde tres puntos estratégicos: criterios de información, recursos de TI y procesos de TI. (COBIT)

Estos tres puntos estratégicos son descritos en el cubo COBIT

Gráfico Cubo de COBIT.



Auditoría Informática aplicada a las Instituciones Bancarias.

Una entidad financiera dispone de diversa información patrimonial y personal de cada uno de sus clientes. Los datos que posee la entidad pueden ser, sus datos personales (nombre, dirección, teléfono), también puede disponer de datos profesionales (actividad a la que se dedica, empresa para la que trabaja), además la posición completa de sus cuentas (saldos), valor tasado de su vivienda en caso de que le haya otorgado un préstamo, nivel de endeudamiento, etc.

La sensibilidad de la información manejada por una entidad financiera es mayor si se tiene en cuenta la totalidad de sus clientes y productos, ya que tienen información más completa y valiosa y por tanto más sensible, que disponer exclusivamente de las cuentas de un único cliente. Los principales riesgos a los que hace frente la gestión de la información son:

Difusión no autorizada, intencionada o no, hacia destinos improcedentes. La confidencialidad es un tema de especial preocupación en cualquier entidad financiera ya que en una entidad bancaria interviene la confianza depositada por el cliente.

Obtención de información errónea, por accidente o por manipulación indebida, y como consecuencia de la normativa a la que está sometida la actividad bancaria perjudicando a los clientes. (Mario Piattini y Emilio del Peso)

La auditoría bancaria busca que se cumplan con las mejores prácticas de seguridad de la información de tal manera que los datos sensibles e importantes para la entidad bancaria estén resguardados.

1.6.2 Marco conceptual.

Sistema Cooperativo Financiero de la Economía Popular y Solidaria. Está compuesto por instituciones no financieras y financieras comprendidas por cooperativas. La Superintendencia de la Economía Popular y Solidaria (SEPS) inició su gestión el 05 de junio 2012 y actualmente se encuentra en transición con la Superintendencia de Bancos y Seguros que estaba encargada del sector financiero cooperativista.

Cooperativa de Ahorro y Crédito. Es una Institución que realiza labores de intermediación financiera, tiene un enfoque solidario, sin un dueño particular, sino que está conformado por

los socios y cada uno tiene derecho a un voto en lo que respecta a las decisiones de la cooperativa.

1.6.3 Marco Jurídico.

El Marco regulatorio para la Cooperativa de Ahorro y Crédito “Juventud Ecuatoriana Progresista Ltda.” se rige por la Ley General de Instituciones del Sistema Financiero.

La entidad de control es la Superintendencia de la Economía Popular y Solidaria.

1.6.4 Citas Bibliográficas.

Según (Echenique, 2006) los tipos de Auditoría Informática, los procedimientos varían de acuerdo a las técnicas y a la filosofía de cada empresa y departamento de auditoría en particular. Sin embargo, existen ciertas técnicas y/o procedimientos que son compatibles en la mayoría de ambientes de informática. Estas técnicas caen en dos categorías: métodos manuales y métodos asistidos por computadora.

Técnicas avanzadas de auditoría con informática.

Cuando en una institución se encuentren operando sistemas avanzados de computación, como el procesamiento en línea, bases de datos y procesamiento distribuido, se podrá evaluar el sistema utilizando técnicas avanzadas de auditoría.

Entre las técnicas recomendadas están:

Pruebas Integrales.

Simulación.

Revisión de acceso.

Operaciones en paralelo.

Evaluación de un sistema con datos de prueba.

Registros extendidos.

Totales aleatorios de ciertos programas.

Selección de determinado tipo de transacciones como auxiliar en el análisis de un archivo histórico.

Resultados de ciertos cálculos.

Todas las técnicas anteriores ayudan al auditor a establecer una metodología para la revisión de los sistemas de aplicación de una institución, empleando como herramientas el mismo equipo de cómputo. (Echenique, 2006)

1.7 METODOLOGÍA.

1.7.1 Métodos generales que se van a utilizar en el proyecto.

El tipo de investigación utilizado para el desarrollo de la Auditoría Informática será:

La investigación de campo, ya que se apoya en la recopilación de información que proviene de encuestas, entrevistas, cuestionarios y observaciones realizadas en el área.

Investigación aplicada, esta permite obtener un nuevo conocimiento técnico con la aplicación inmediata a uno más problemas determinados. Esta investigación es fundamentada en los resultados de la investigación básica.

Métodos.

Método inductivo.- Investigación acerca del manejo de la administración y control de los procesos y documentos en la Institución.

Observación.- Requerimientos de la Institución.

Analítico-Sintético.- Permitirá obtener una mejor solución al problema planteado.

Nivel Clasificatorio.- Permite organizar y ordenar los datos y la información de la Institución clasificándolos en grupos o clases. Ordenar características, similitudes o semejanzas a fin

de establecer una distribución de sus elementos y clasificar dicha información distinguiendo y agrupando.

Técnicas.

Las técnicas que se utilizará para el desarrollo del proyecto son:

Entrevista directa con el Gerente General para la obtención de un criterio general.

Entrevista con los funcionarios de Tarjetas de Débito, Gerente de Tecnología, Jefe de Procesos, Jefe de Bases de Datos, y demás personal de los procesos involucrados, para conocer a nivel de detalle todo el ámbito de trabajo.

Encuestas, a través de esta técnica se obtiene los datos de varias personas que están directamente relacionadas con el proceso de tarjetas de débito y de tecnología de la información, mediante preguntas estructuradas en formularios impresos.

Observación directa que permita evidenciar y documentar los procesos.

CAPÍTULO II

2.1 Marco Teórico.

Teoría Aplicada	Dónde Fue Aplicada	Cómo se aplicó	Qué resolvió
Auditoría. Es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas. (Piattini M. y Del Peso E. (2007). Auditoría Informática)	La auditoría es la base conceptual de la Auditoría Informática, se aplican como principios profesionales del auditor.	Se utilizó como una guía de los principios que se debe seguir en una auditoría.	Establecer el marco fundamental de la auditoría como un entorno de trabajo.
Auditoría Informática. Es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos. (Piattini M. y Del Peso E. (2007). Auditoría Informática)	La Auditoría Informática se aplicó en el estudio y análisis de los procesos, entornos de TI considerados críticos dentro del área de tarjeta de débito.	Se aplicó utilizando los principios básicos de la Auditoría Informática, estableciendo sus etapas y entregando los documentos con las recomendaciones que señalan las mejores prácticas de la industria de medios de pago.	Permitió evidenciar las debilidades en diferentes procesos y entornos de TI.
Base de Datos. Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. (DATOS)	Las bases de datos fueron utilizadas para evidenciar el nivel óptimo de cumplimiento del almacenamiento de información.	Se realizaron revisiones de configuraciones, accesos, almacenamiento y seguridades.	Se pudo verificar que la información sensible es almacenada de forma vulnerable.
COBIT. Marco de referencia de buenas prácticas para el control de TI. Acrónimo en inglés de Objetivos de Control para la Información y	Se aplicó en el desarrollo de la auditoría como un marco de trabajo que apoya de	Se verificaron los principales controles y se determinó el entorno de	Se evidenciaron los niveles de madurez de los procesos

la Tecnología Relacionada, emitido por el IT Governance Institute®. (COBIT)	forma metodológica a la Auditoría Informática.	trabajo que más se ajusta a las necesidades de la auditoría y se aplicó en cada módulo y proceso del área de tarjeta de débito.	de TI y se realizaron las recomendaciones para mejorar el nivel de madurez de la Institución.
Lista de apoyo. Matrices de Investigación. Se utiliza para que el auditor pueda tener claros los puntos a auditar, ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. (GLOSARIO)	Se utilizó en el desarrollo de la auditoría, en la determinación de los procesos a auditar, en redactar los hallazgos, en establecer las recomendaciones.	Se aplicó utilizando una matriz cruzada que permite evidenciar los diferentes ítems que se está trabajando y su relación con otros factores relevantes.	Permite evidenciar los principales controles a revisar. Además de las técnicas a utilizar durante la auditoría, a establecer los hallazgos.
Modelo de Madurez. Modelo utilizado por muchas organizaciones para identificar las mejores prácticas, las cuales son convenientes para ayudarles a evaluar y mejorarla madurez de su proceso de desarrollo de software. (COBIT)	Se aplicó durante los hallazgos de la auditoría para dar un nivel de madurez al cumplimiento que se evidencia en la Institución.	Se utilizó el modelo genérico de madurez que se determina en la versión COBIT 4.1 y se fue colocando una vez que se evidenció el hallazgo.	Los modelos de madurez permiten conocer el nivel de cumplimiento actual que tiene la Institución, su brecha hacia el mejor escenario.
Encuestas. Conjunto de preguntas tipificadas dirigidas a una muestra representativa, para averiguar estados de opinión o diversas cuestiones de hecho. (Española)	Se utilizó en la determinación de la necesidad de realizar una Auditoría Informática. Adicionalmente en el desarrollo de la auditoría se establecieron encuestas enfocadas a obtener el criterio	Se elaboraron encuestas y se aplicaron de forma anónima en el caso de los usuarios funcionales. En el caso de los niveles de responsabilidad se realizaron las encuestas tipo entrevista con	Permitió tener una orientación clara de la forma en que se ejecutan los procesos. Permitió conocer de forma directa la situación actual de los niveles

	del auditado.	presentación de la evidencia o sustento que tiene la afirmación.	críticos de los procesos.

CAPÍTULO III

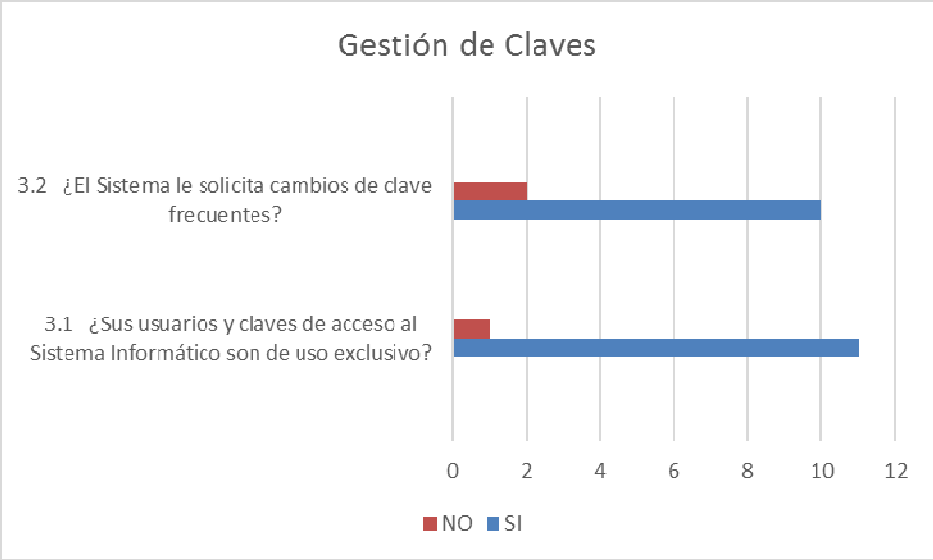
3.1 Encuesta Preliminar a Usuarios del Área de Tarjeta de Débito.

Las encuestas realizadas al personal que labora en el área de tarjeta de débito se han aplicado con el objetivo de establecer un panorama inicial de las principales actividades de trabajo diarias y la forma en que se desarrollan.

El cuestionario utilizado (ver Anexo1) fue realizado con preguntas de opción múltiple, respuestas afirmativas o negativas y respuestas de desarrollo.

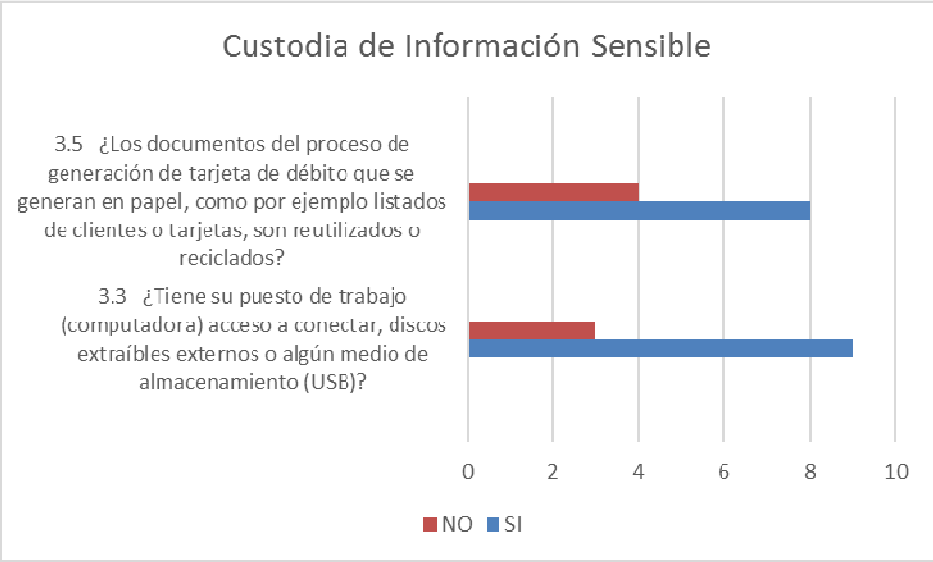
A continuación se presentan los resultados más relevantes obtenidos en la tabulación.

Gráfico Gestión de Claves.



Existen dos usuarios de un total de doce que no tienen conocimiento de la frecuencia del cambio de clave y un usuario que no tiene una clave exclusiva o que la comparte para el ingreso al sistema.

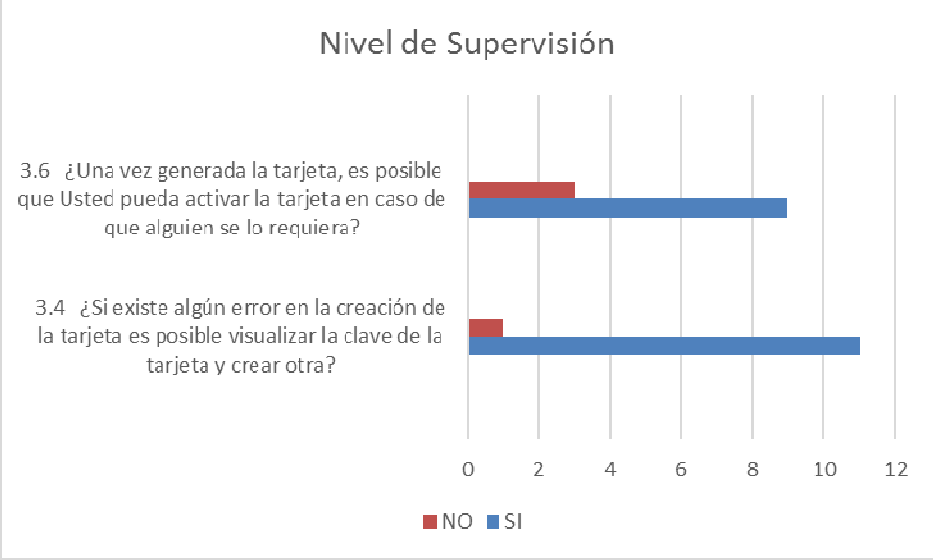
Gráfico Custodia de Información Sensible.



La información sensible generada en papel como reportes o listados no son destruidos.

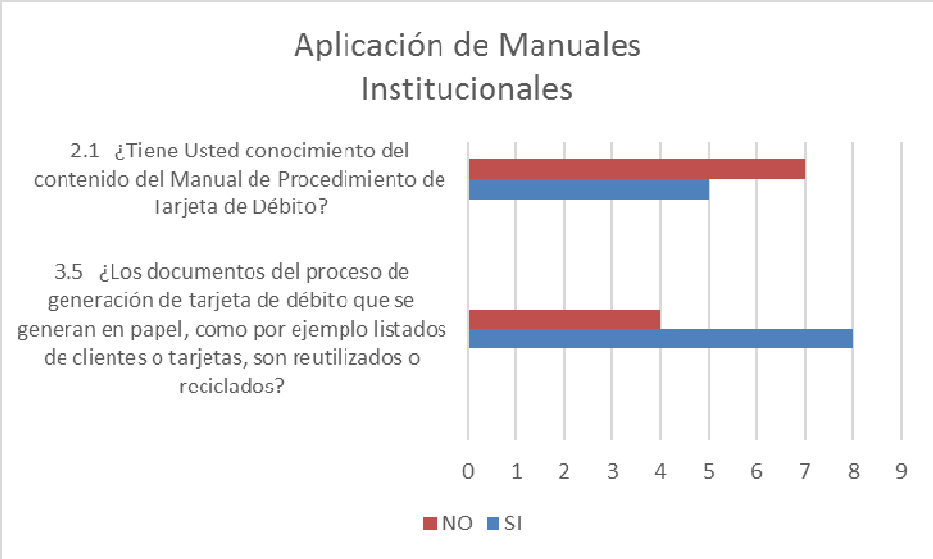
Nueve usuarios tienen la posibilidad de ingresar dispositivos externos a la computadora.

Gráfico Nivel de Supervisión.



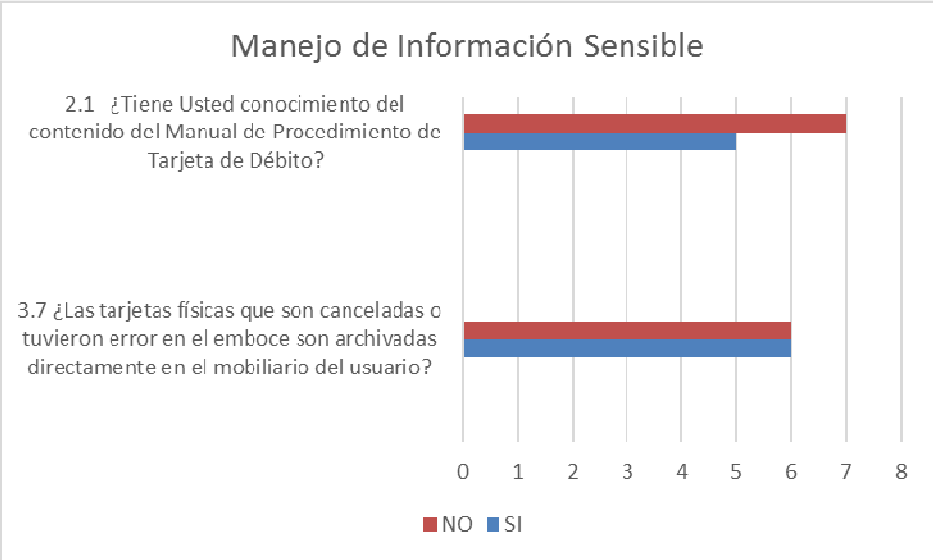
Nueve usuarios pueden activar la tarjeta sin que sea una actividad asignada a su perfil y once usuarios pueden visualizar la clave y volver a imprimir una tarjeta una vez generada la primera tarjeta.

Gráfico Aplicación de Manuales Institucionales.



Siete usuarios de un total de doce indican no conocer los manuales de procedimientos, existe información de listados que no se custodia adecuadamente según se indica en el Manual de Procedimiento de tarjeta de débito.

Gráfico Manejo de Información Sensible.



El 50% de los usuarios no envían la tarjeta a la bóveda para la custodia hasta la destrucción definitiva, como lo indica el Manual de Procedimiento.

El análisis de los resultados obtenidos en las encuestas determina que es importante realizar una Auditoría Informática que permita conocer al detalle el entorno de los procesos y así poder determinar oportunidades de mejora en la seguridad de los procesos críticos del área de tarjeta de débito.

3.2 Determinación del Marco de Trabajo.

COSO.

Es un estándar de control aceptado a nivel mundial.

Es desarrollado por el Committee Of Sponsoring Organitations. Tiene sus inicios en 1992. Es presentado por la Comisión Treadway que está conformada por cinco organizaciones internacionales de profesionales.

Objetivos del Informe COSO.

Establecer una definición común del Control Interno “Marco de Referencia"

Proporcionar el “marco” para que cualquier tipo de organización pueda evaluar sus Sistemas de Control y decidir cómo mejorarlos.

Ayudar a la dirección de las empresas a mejorar el Control de las Actividades de sus organizaciones. (COSO)

Ventajas COSO.

Entre las principales ventajas que se identifican en este modelo son: los usuarios COSO son orientados fuertemente sobre el control interno, gestión de riesgos, fraudes, ética empresarial; así tambien tiene un fuerte enfoque en la publicación de estados financieros confiables.

COSO tiene un fuerte enfoque en toda la organización, incluyendo guias de conrol para TI.

Desventajas COSO.

Como sus desventajas se puede mensionar que varias guias presentan un grado de dificultad que puede derivar en errores al ejecutar las instrucciones. Otra desventaja se presenta en que no se involucra a la alta gerencia en la decisiones de TI.

Enfoque COSO.

El enfoque de COSO se desarrolla para toda la organización. La audiencia a la que está dirigida la norma es para la alta dirección.

ITIL

ITIL es un enfoque ampliamente adoptado para la Gestión de Servicios en el mundo. Proporciona un marco práctico y coherente para identificar, planificar, entregar y mantener servicios de TI para el negocio.

Son cinco las guías básicas para mapear la totalidad del ciclo de vida del Servicio de ITIL, comienza con la identificación de las necesidades y los conductores de los requisitos de TI de los clientes, a través del diseño e implementación del servicio en funcionamiento y, por último, a la fase de seguimiento y mejora del servicio. (ITIL)

Objetivos de ITIL.

Ofrecer un marco común para todas las actividades que se desarrollen en el departamento de TI.

Ventajas ITIL.

Se establecen puntos de acuerdo entre las partes involucradas en los procesos, de esta manera cada área conoce en donde empieza y termina su responsabilidad.

Se desarrolla una administración con un fuerte enfoque al control.

Los resultados finales se enfocan a las necesidades del cliente.

Tiene flexibilidad de adaptación a las necesidades del cliente.

Desventajas ITIL.

El tiempo y esfuerzo de implementación pueden ser extensos debido a la diversidad de controles y enfoques que presenta.

El entendimiento por parte de los implementadores puede resultar complejo, se considera que el entendimiento puede resultar complejo en personal con poca experiencia.

Enfoque ITIL.

Administra el ciclo de vida de un servicio. Su audiencia va desde la dirección, administradores de TI y usuarios.

COBIT.

El modelo COBIT (Control Objetives for Information and Related Technologies) fue desarrollado por ISACA.

ISACA comenzó en 1967, en 1969 el grupo se formalizó, incorporándose bajo el nombre de EDP Auditors Association (Asociación de Auditores de Procesamiento Electrónico de Datos). En 1976 la asociación formó una fundación de educación para llevar a cabo proyectos de investigación de gran escala para expandir los conocimientos y el valor en el campo de

gobierno y control de TI. Conocida como Information Systems Audit and Control Association (Asociación de Auditoría y Control en Sistemas de Información). (COBIT, s.f.)

Objetivos de COBIT.

Busca mantener operaciones eficientes, manteniendo principios de confidencialidad, integridad y disponibilidad de la información, observando el marco regulatorio que se establece para la institución.

Ventajas COBIT.

Busca cubrir las brechas existentes entre riesgos del negocio, necesidades de control y los aspectos técnicos.

Proporciona información que la institución requiere para cumplir sus objetivos trabajando de forma coordinada entre la alta dirección y el departamento de TI.

Ayuda a la alta gerencia a desarrollar un conocimiento de los riesgos de forma fácil y natural.

Desventajas COBIT.

Es un modelo muy profundo que requiere alto grado de estudio en sus componentes o dominios.

El personal que se involucra puede desertar debido al conocimiento tecnológico que se requiere para establecer el criterio que busca COBIT.

Enfoque COBIT.

Tiene un fuerte enfoque para la alta gerencia y el departamento de TI, sus dominios desarrollados son Planear y Organizar, Adquirir e Implementar, Entregar y dar Soporte, Monitorear y Evaluar.

Comparación entre los tres modelos: ITIL, COSO, COBIT.

Inicialmente se ha elaborado una tabla de ponderación del marco de referencia en donde se destacan las principales características de un entorno de trabajado de control y se ha ponderado con un peso de entre cero y uno las principales características cuyos valores

sumados determinan un total y el porcentaje de importancia frente a las demás características.

Tabla de Ponderación de Marco de Referencia.

Características	Objetivos de control	Orientado a Negocios y/o Procesos	Componentes o Dominios	Aplicación Institucional	Costo de Implementación	Facilidad en la interpretación y Aplicación	Total	Porcentaje
Objetivos de Control		1	0.5	1	0.5	1	4	19%
Orientado a Negocios y/o Procesos	1		0.5	1	0.5	0.5	3.5	17%
Componentes o Dominios	0.5	0.5		1	0.5	0.5	3	14%
Aplicación Institucional	1	1	1		0.5	0.5	4	19%
Costos de implementación	0.5	0.5	0.5	1		0.5	3	14%
Facilidad en la Interpretación y Aplicación	0.5	0.5	1	1	0.5		3.5	17%
Total							**21**	**100%**

En la Tabla Matriz de Decisión, se tabularon los datos utilizando los valores obtenidos en la Tabla de Ponderación y se establecieron valores a cada uno de los modelos con el objetivo de realizar una comparación entre sí, obteniendo finalmente un resultado.

La escala utilizada fue de 0 a 5, en donde 0 es el valor más bajo y 5 el valor más alto.

Tabla de Decisión Marco de Referencia.

	Lenguaje	COSO		COBIT		ITIL	
Características	**Porcentaje**	**Valor**	**Total**	**Valor**	**Total**	**Valor**	**Total**
Objetivos de Control	19%	4	0.76	5	0.95	4	0.76
Orientado a Negocios y/o Procesos	17%	4	0.67	5	0.83	4	0.67
Componentes o Dominios	14%	4	0.57	4	0.57	3	0.43
Aplicación Institucional	19%	5	0.95	4	0.76	4	0.76
Costos de implementación	14%	1	0.14	1	0.14	1	0.14
Facilidad en la Interpretación y Aplicación	17%	3	0.50	4	0.67	3	0.50
Valor Total			**3.60**		**3.93**		**3.26**

Los resultados permiten determinar que COBIT con un valor de 3.93 puntos, obtuvo una valoración superior a ITIL y COSO.

COBIT se presenta como un modelo que tiene un fuerte enfoque a establecer objetivos de control integrales. Está orientado fuertemente a las necesidades del negocio y a la participación que tiene el negocio en conjunto con la alta gerencia y TI en la toma de decisiones importantes. Los dominios de control tienen un alto grado de desarrollo y son de fácil interpretación.

Por lo indicado se determina como una opción viable, utilizar el marco de trabajo COBIT, que en su versión 4.1 en español es una herramienta que cumple satisfactoriamente para establecer los controles de Auditoría Informática.

3.3 Determinación Conceptual de Nivel de Riesgo.

El riesgo se ha determinado que es la probabilidad de que una amenaza se presente de forma concreta en un evento dentro de la Cooperativa. Existen riesgos que pueden causar

un mayor impacto en caso de presentarse, los riesgos pueden ser económicos, de reputación u otros.

Para determinar el impacto que tienen los diferentes controles de COBIT aplicados a los procesos Cooperativa, tanto a nivel de usuarios, procesos y tecnología, se ha elaborado una tabla de determinación de riesgo.

3.4 Tabla de Determinación de Riesgo.

Abreviatura	Riesgo	Definición
A	Alto	Es un control que tiene un alto grado de riesgo dentro de la Institución, debe ser revisado.
M	Medio	El control tiene una importancia moderada, sin embargo se recomienda su verificación a fin de evitar que suba de nivel.
B	Bajo	Es un control bajo que tiene poca importancia para la Institución y de la cual no se requiere revisión.

3.5 Definición de Dominios COBIT.

Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Normalmente se ordenan dentro de dominios de responsabilidad de plan, construir, ejecutar y monitorear.

3.5.1 Planear y Organizar (PO).

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas.

3.5.2 Adquirir e Implementar (AI).

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

3.5.3 Entregar y Dar Soporte (DS).

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

3.5.4 Monitorear y Evaluar (ME).

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

3.6 Matriz Dominios Revisión COBIT aplicados a la Cooperativa.

En base a la tabla de Determinación de Riesgo, se han revisado los procesos del área de tarjeta de débito y el entorno de TI que soporta la administración de este producto y se han establecido los controles con calificación A y M que serán revisados en el ejercicio de la auditoría. Los controles calificados con B no serán revisados debido a que se considera de un impacto al riesgo bajo.

Tabla Dominios Revisión COBIT aplicados a la Cooperativa.

Riesgo	Dominio COBIT	Requiere Revisión
A	PO1 Definir un Plan Estratégico de TI	SI
B	PO1.1 Administración del valor de TI	NO
A	PO1.2 Alineación de TI con el negocio	SI
B	PO1.3 Evaluación del desempeño actual	NO
B	PO1.4 Plan estratégico de TI	NO
B	PO1.5 Planes tácticos de TI	NO
B	PO1.6 Administración del portafolio de TI	NO
A	PO2 Definir la arquitectura de información	SI
B	PO2.1 Modelo de arquitectura de información empresarial	NO
B	PO2.2 Diccionario de datos empresarial y reglas de sintaxis de datos	NO
A	PO2.3 Esquema de clasificación de datos	SI
A	PO2.4 Administración de la integridad	SI
M	PO3 Determinar la dirección tecnológica	SI
B	PO3.1 Planeación de la dirección tecnológica	NO
B	PO3.2 Plan de infraestructura tecnológica	NO
B	PO3.3 Monitoreo de tendencias y regulaciones futuras	NO
B	PO3.4 Estándares tecnológicos	NO
B	PO3.5 Consejo de arquitectura	NO
M	PO4 Definir los procesos, organización y relaciones de TI	SI
B	PO4.1 Marco de trabajo del proceso	NO
B	PO4.2 Comité estratégico	NO
B	PO4.3 Comité directivo	NO
B	PO4.4 Ubicación organizacional de la función de TI	NO
B	PO4.5 Estructura organizacional	NO
M	PO4.6 Roles y responsabilidades	SI
B	PO4.7 Responsabilidad de aseguramiento de calidad de TI	NO
B	PO4.8 Responsabilidad sobre el	NO

	riesgo, la seguridad y el cumplimiento	
B	PO4.9 Propiedad de datos y de sistemas	NO
B	PO4.10 Supervisión	NO
M	PO4.11 Segregación de funciones	SI
B	PO4.12 Personal de TI	NO
B	PO4.13 Personal clave de TI	NO
M	PO4.14 Políticas y procedimientos para personal contratado	SI
B	PO4.15 Relaciones	NO
B	PO5 Administrar la inversión en TI	NO
B	PO5.1 Marco de trabajo para la administración financiera	NO
B	PO5.2 Prioridades dentro del presupuesto de TI	NO
B	PO5.3 Proceso presupuestal	NO
B	PO5.4 Administración de costos	NO
B	PO5.5 Administración de beneficios	NO
B	PO6 Comunicar las aspiraciones y la dirección de la gerencia	NO
B	PO6.1 Ambiente de políticas y de control	NO
B	PO6.2 Riesgo corporativo y marco de referencia de control interno de TI	NO
B	PO6.3 Administración de políticas para TI	NO
B	PO6.4 Implantación de políticas de TI	NO
B	PO6.5 Comunicación de los objetivos y la dirección de TI	NO
B	PO7 Administrar los recursos humanos de TI	NO
B	PO7.1 Reclutamiento y retención del personal	NO
B	PO7.2 Competencias del personal	NO
M	PO7.3 Asignación de roles	SI
B	PO7.4 Entrenamiento del personal de TI	NO
B	PO7.5 Dependencia sobre los individuos	NO
B	PO7.6 Procedimientos de Investigación del personal	NO
B	PO7.7 Evaluación del desempeño del empleado	NO
B	PO7.8 Cambios y terminación de trabajo	NO
B	PO8 Administrar calidad	NO
B	PO8.1 Sistema de administración de calidad	NO
B	PO8.2 Estándares y prácticas de calidad	NO

B	PO8.3 Estándares de desarrollo y de adquisición	NO
B	PO8.4 Enfoque en el cliente	NO
B	PO8.5 Mejora continua	NO
B	PO8.6 Medición, monitoreo y revisión de la calidad	NO
A	PO9 Evaluar y administrar los riesgos de TI	SI
A	PO9.1 Alineación de la administración de riesgos de TI y del negocio	SI
M	PO9.2 Establecimiento del contexto del riesgo	SI
A	PO9.3 Identificación de eventos	SI
A	PO9.4 Evaluación de riegos	SI
A	PO9.5 Respuesta a los riesgos	SI
A	PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgos	SI
B	PO10 Administrar proyectos	NO
B	PO10.1 Marco de trabajo para la administración de programas	NO
B	PO10.2 Marco de trabajo para la administración de proyectos	NO
B	PO10.3 Enfoque de administración de proyectos	NO
B	PO10.4 Compromiso de los interesados	NO
B	PO10.5 Estatuto de alcance del proyecto	NO
B	PO10.6 Inicio de las fases del proyecto	NO
B	PO10.7 Plan integrado del proyecto	NO
B	PO10.8 Recursos del proyecto	NO
B	PO10.9 Administración de riesgos del proyecto	NO
B	PO10.10 Plan de calidad del proyecto	NO
B	PO10.11 Control de cabios del proyecto	NO
B	PO10.12 Planeación del proyecto y métodos de aseguramiento	NO
B	PO10.13 Medición del desempeño, reportes y monitoreo del proyecto	NO
B	PO10.14 Cierre del proyecto	NO
A	Al1 Identificar soluciones automatizadas	SI
B	Al1.1 Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio	NO
M	Al1.2 Reporte de análisis de riesgos	SI
B	Al1.3 Estudio de factibilidad y formulación de cursos de acción alternativos	NO

B	AI1.4 Requerimientos, decisión de factibilidad y aprobación	NO
M	AI2 Adquirir y mantener software aplicativo	SI
B	AI2.1 Diseño de alto nivel	NO
B	AI2.2 Diseño detallado	NO
B	AI2.3 Control y adaptabilidad de las aplicaciones	NO
B	AI2.4 Seguridad y disponibilidad de las aplicaciones	NO
B	AI2.5 Configuración e implantación de software aplicativo adquirido	NO
B	AI2.6 Actualizaciones importantes en sistemas existentes	NO
B	AI2.7 Desarrollo de software aplicativo	NO
B	AI2.8 Aseguramiento de la calidad del software	NO
B	AI2.9 Administración de los requerimientos de aplicaciones	NO
B	AI2.10 Mantenimiento de software aplicativo	NO
A	AI3 Adquirir y mantener infraestructura tecnológica	SI
B	AI3.1 Plan de adquisición de infraestructura tecnológica	NO
A	AI3.2 Protección y disponibilidad del recurso de infraestructura	SI
A	AI3.3 Mantenimiento de la infraestructura	SI
M	AI3.4 Ambiente de prueba de factibilidad	SI
M	AI4 Facilitar la operación y el uso	SI
M	AI4.1 Plan para soluciones de operación	SI
B	AI4.2 Transferencia de conocimiento a la gerencia del negocio	NO
B	AI4.3 Transferencia de conocimiento a usuarios finales	NO
B	AI4.4 Transferencia de conocimiento al personal de operaciones y soporte	NO
B	AI5 Adquirir recursos de TI	NO
B	AI5.1 Control de adquisición	NO
B	AI5.2 Administración de contratos con proveedores	NO
B	AI5.3 Selección de proveedores	NO
B	AI5.4 Adquisición de software	NO
B	AI5.5 Adquisición de recursos de desarrollo	NO
B	AI5.6 Adquisición de infraestructura, instalaciones y servicios relacionados	NO

A	Al6 Administrar cambios	SI
M	Al6.1 Estándares y procedimientos para cambios	SI
M	Al6.2 Evaluación de impacto, priorización y autorización	SI
M	Al6.3 Cambios de emergencia	SI
M	Al6.4 Seguimiento y reporte del estatus de cambio	SI
B	Al6.5 Cierre y documentación del cambio	NO
B	Al7 Instalar y acreditar soluciones y cambios	NO
B	Al7.1 Entrenamiento	NO
B	Al7.2 Plan de prueba	NO
B	Al7.3 Plan de implementación	NO
B	Al7.4 Ambiente de prueba	NO
B	Al7.5 Conversión de sistema y datos	NO
B	Al7.6 Prueba de cambios	NO
B	Al7.7 Prueba final de aceptación	NO
B	Al7.8 Transferencia a producción	NO
B	Al7.9 Liberación de software	NO
B	Al7.10 Distribución del sistema	NO
B	Al7.11 Registro y rastreo de cambios	NO
B	Al7.12 Revisión posterior a la implantación	NO
M	DS1 Definir y administrar los niveles de servicio	SI
B	DS1.1 Marco de trabajo de la administración de los niveles de serbio	NO
B	DS1.2 Definición de servicios	NO
B	DS1.3 Acuerdos de niveles de servicio	NO
B	DS1.4 Acuerdos de niveles de operación	NO
M	DS1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio	SI
B	DS1.6 Revisión de los acuerdos de niveles de servicio y de los contratos	NO
B	DS2 Administrar los servicios de terceros	NO
B	DS2.1 Identificación de las relaciones con todos los proveedores	NO
B	DS2.2 Administración de las relaciones con los proveedores	NO
B	DS2.3 Administración de riesgos del proveedor	NO
B	DS2.4 Monitoreo del desempeño del proveedor	NO
M	DS3 Administrar el desempeño y la capacidad	SI
B	DS3.1 Planeación del desempeño y la	NO

	capacidad	
M	DS3.2 Capacidad y desempeño actual	SI
B	DS3.3 Capacidad y desempeño futuro	NO
B	DS3.4 Disponibilidad de recursos de TI	NO
B	DS3.5 Monitoreo y reporte	NO
A	DS4 Garantizar la continuidad de los servicios	SI
B	DS4.1 Marco de trabajo de continuidad	NO
A	DS4.2 Planes de continuidad de TI	SI
A	DS4.3 Recursos críticos de TI	SI
M	DS4.4 Mantenimiento del plan de continuidad de TI	SI
B	DS4.5 Pruebas del plan de continuidad de TI	NO
B	DS4.6 Entrenamiento del plan de continuidad de TI	NO
B	DS4.7 Distribución del plan de continuidad de TI	NO
M	DS4.8 Recuperación y reanudación de los servicios de Ti	SI
M	DS4.9 Almacenamiento de respaldos fuera de las instalaciones	SI
B	DS4.10 Revisión post reanudación	NO
A	DS5 Garantizar la seguridad de los sistemas	SI
A	DS5.1 Administración de la seguridad de TI	SI
A	DS5.2 Plan de seguridad de TI	SI
A	DS5.3 Administración de identidad	SI
M	DS5.4 Administración de cuentas del usuario	SI
B	DS5.5 Pruebas, vigilancia y monitoreo de la seguridad	NO
B	DS5.6 Definición de incidente de seguridad	NO
A	DS5.7 Protección de la tecnología de seguridad	SI
A	DS5.8 Administración de llaves criptográficas	SI
A	DS5.9 Prevención, detección y corrección de software malicioso	SI
A	DS5.10 Seguridad de la red	SI
A	DS5.11 Intercambio de datos sensitivos	SI
B	DS6 Identificar y asignar costos	NO
B	DS6.1 Definición de servicios	NO
B	DS6.2 Contabilización de TI	NO
B	DS6.3 Modelación de costos y cargos	NO
B	DS6.4 Mantenimiento del modelo de costos	NO

B	DS7 Educar y entrenar a los usuarios	NO
B	DS7.1 Identificación de necesidades de entrenamiento y educación	NO
B	DS7.2 Impartición de entrenamiento y educación	NO
B	DS7.3 Evaluación del entrenamiento recibido	NO
B	DS8 Administrar la mesa de servicio y los incidentes	NO
B	DS8.1 Mesa de servicios	NO
B	DS8.2 Registro de consultas de clientes	NO
B	DS8.3 Escalamiento de incidentes	NO
B	DS8.4 Cierre de incidentes	NO
B	DS8.5 Análisis de tendencias	NO
B	DS9 Administrar la configuración	NO
B	DS9.1 Repositorio de configuración y línea base	NO
B	DS9.2 Identificación y mantenimiento de elementos de configuración	NO
B	DS9.3 Revisión de integridad de la configuración	NO
M	DS10 Administración de problemas	SI
B	DS10.1 Identificación y clasificación de problemas	NO
M	DS10.2 Rastreo y resolución de problemas	SI
M	DS10.3 Cierre de problemas	SI
B	DS10.4 Integración de las administración de cambios, configuración y problemas	NO
M	DS11 Administración de la información	SI
M	DS11.1 Requerimientos del negocio para administración de datos	SI
M	DS11.2 Acuerdos de almacenamiento y conservación	SI
M	DS11.3 Sistema de administración de librerías de medios	SI
A	DS11.4 Eliminación	SI
M	DS11.5 Respaldo y restauración	SI
M	DS11.6 Requerimientos de seguridad para la administración de datos	SI
M	DS12 Administración del ambiente físico	SI
B	DS12.1 Selección y diseño de datos	NO
B	DS12.2 Medidas de seguridad física	NO
M	DS12.3 Acceso Físico	SI
B	DS12.4 Protección contra factores ambientales	NO
B	DS12.5 Administración de	NO

	instalaciones físicas	
B	DS13 Administración de operaciones	NO
B	DS13.1 Procedimientos e instrucciones de operaciones	NO
B	DS13.2 Programación de tareas	NO
B	DS13.3 Monitoreo de la infraestructura de TI	NO
B	DS13.4 Documentos sensitivos y dispositivos de salida	NO
B	DS13.5 Mantenimiento preventivo del hardware	NO
M	ME1 Monitorear y evaluar el desempeño de TI	SI
B	ME1.1 Enfoque del monitoreo	NO
M	ME1.2 Definición y recolección de datos de monitoreo	SI
M	ME1.3 Método de monitoreo	SI
M	ME1.4 Evaluación del desempeño	SI
M	ME1.5 Reportes al consejo directivo y a ejecutivos	SI
M	ME1.6 Acciones correctivas	SI
B	ME2 Monitorear y evaluar el control interno	NO
B	ME2.1 Monitorear el marco de trabajo de control interno	NO
M	ME2.2 Revisiones de auditoría	SI
M	ME2.3 Excepciones de control	SI
M	ME2.4 Auto-evaluación de control	SI
B	ME2.5 Aseguramiento del control interno	NO
B	ME2.6 Control interno para terceros	NO
M	ME2.7 Acciones correctivas	SI
M	ME3 Garantizar el cumplimiento regulatorio	SI
M	ME3.1 Identificar las leyes y regulaciones con impacto potencial sobre TI	SI
M	ME3.2 Optimizar la respuesta a requerimientos regulatorios	SI
M	ME3.3 Evaluación del cumplimiento con requerimientos regulatorios	SI
M	ME3.4 Aseguramiento positivo del cumplimiento	SI
	ME3.5 Reportes integrados	NO
M	ME4 Proporcionar gobierno de TI	SI
B	ME4.1 Establecer un marco de trabajo de gobierno para TI	NO
M	ME4.2 Alineamiento estratégico	SI
B	ME4.3 Entrega de valor	NO
B	ME4.4 Administración de recursos	NO

M	ME4.5 Administración de riesgos	SI
M	ME4.6 Medición del desempeño	SI

CAPÍTULO IV

4 APLICACIÓN DE LA AUDITORÍA INFORMÁTICA.

4.1 Información Institucional.

La Cooperativa de Ahorro y Crédito "Juventud Ecuatoriana Progresista" Ltda., es una entidad dedicada a las finanzas sociales, creada mediante acuerdo Ministerial 3310, el 31 de diciembre de 1971 y calificada por la Superintendencia de Bancos y Seguros con Resolución SBS-2003-0596, de agosto 12 de 2003.

En la actualidad cuenta con más de 400 mil socios dueños de la Cooperativa, aproximadamente un 70% de los mismos son mujeres, vinculadas a diferentes actividades micro productivas, tanto de los sectores rurales, como urbano marginales.

Creada en la parroquia de Sayausí, del cantón Cuenca, provincia del Azuay, república del Ecuador, con la iniciativa de 29 jóvenes, ha incursionado en un sostenido apoyo crediticio a los segmentos poblacionales que no tienen acceso al crédito de la banca tradicional, aspecto que ha estimulado la aceptación y confianza de la gente, alcanzando el primer lugar dentro del Ranking de las cooperativas ecuatorianas y actualmente cuenta con 24 agencias en Azuay, Cañar, El Oro, Loja, y Morona Santiago.

Misión.

Brindar productos y servicios financieros de calidad, basados en una cultura organizacional dinámica de excelencia y de sólidos valores para satisfacer las necesidades de la gente.

Visión.

Ser la Cooperativa de Ahorro y Crédito más importante del Ecuador, con Socios satisfechos; por su eficiencia, eficacia y compromiso social.

Valores Corporativos.

Los valores institucionales, son expresados diariamente, con el fin de cumplir los objetivos y lograr el bienestar e igualdad de los Socios, directivos y colaboradores de la Cooperativa JEP.

Compromiso

Puntualidad

Solidaridad

Trabajo en equipo

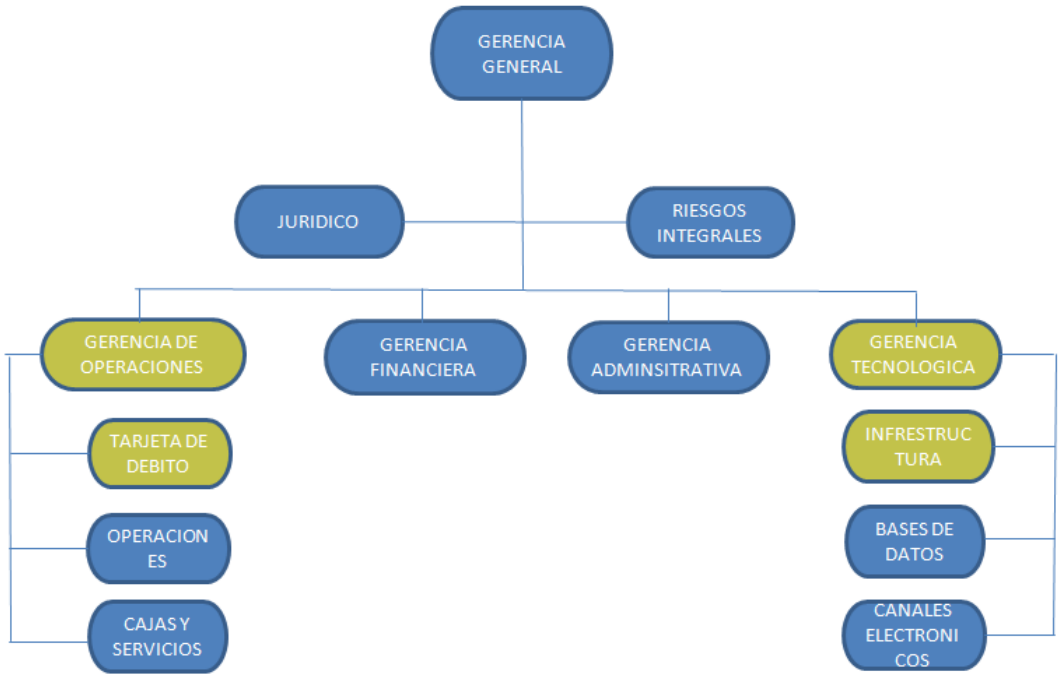
Honestidad

Responsabilidad

Prudencia Financiera

Dinamismo

4.2 Organigrama Departamental.



El departamento de Operaciones cuenta con el área de tarjeta de débito que es la encargada de la administración funcional del producto tarjeta de débito.

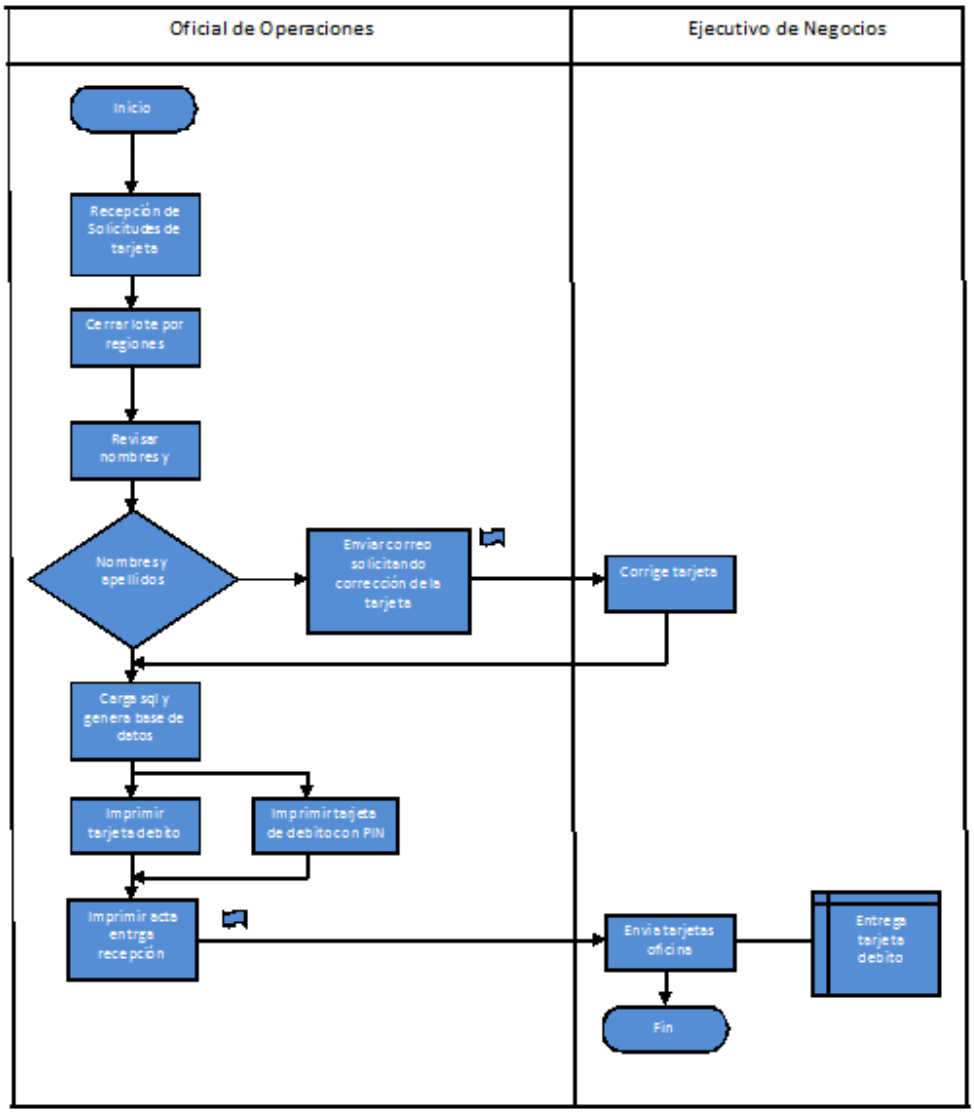
En el departamento de tecnología, el área de infraestructura es la encargada de brindar el soporte de tecnología que requiere el área de tarjeta de débito, configurando usuarios, segmentando la red e instalando los aplicativos necesarios para el funcionamiento del negocio.

Identificación de los Procesos Críticos del Área de Tarjeta de Débito.

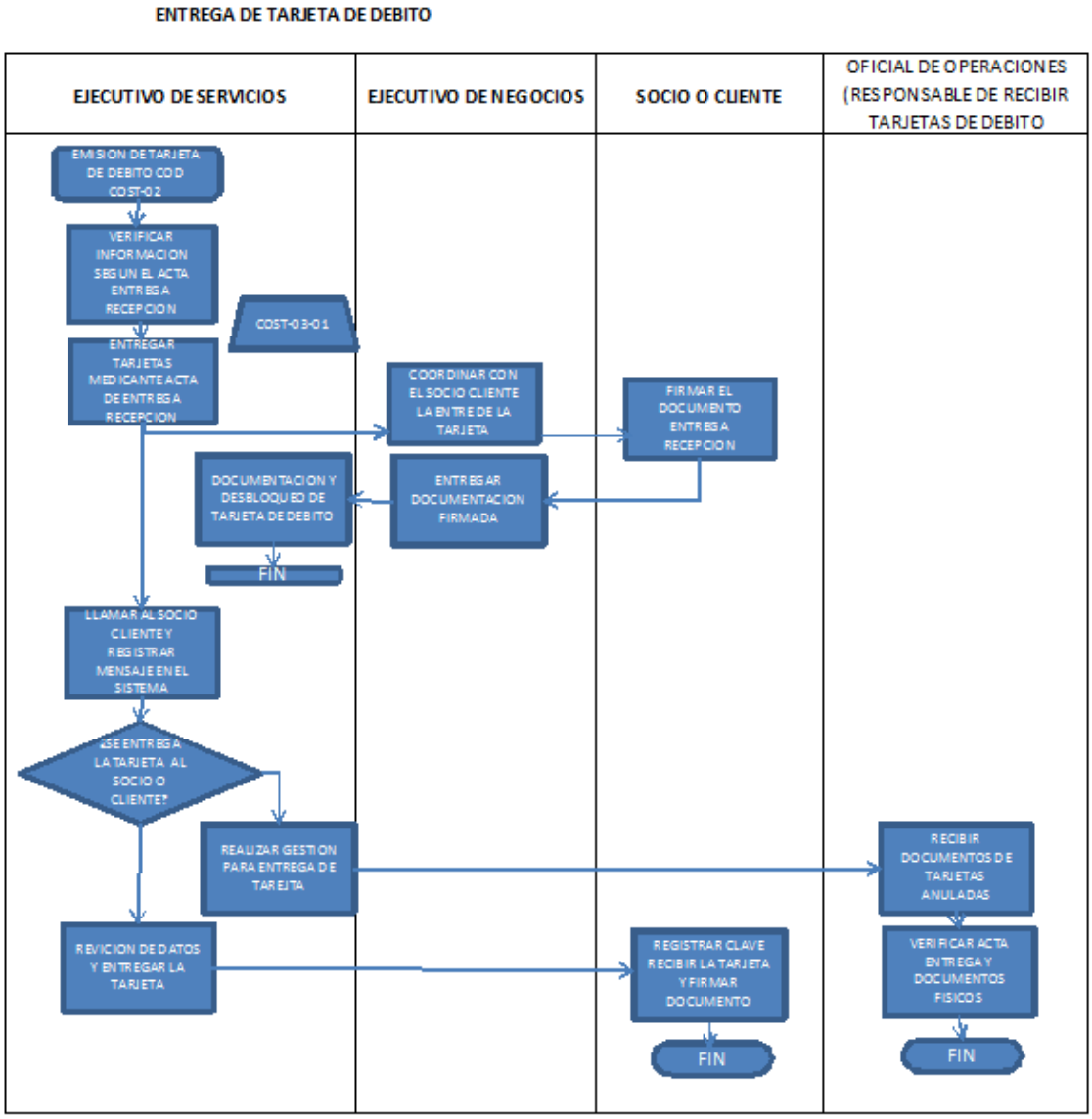
Dentro del área se tiene establecidos los procesos que orientan e identifican la ejecución de las tareas diarias en la administración del producto.

4.3 Procesos Departamento de Tarjeta de Débito.

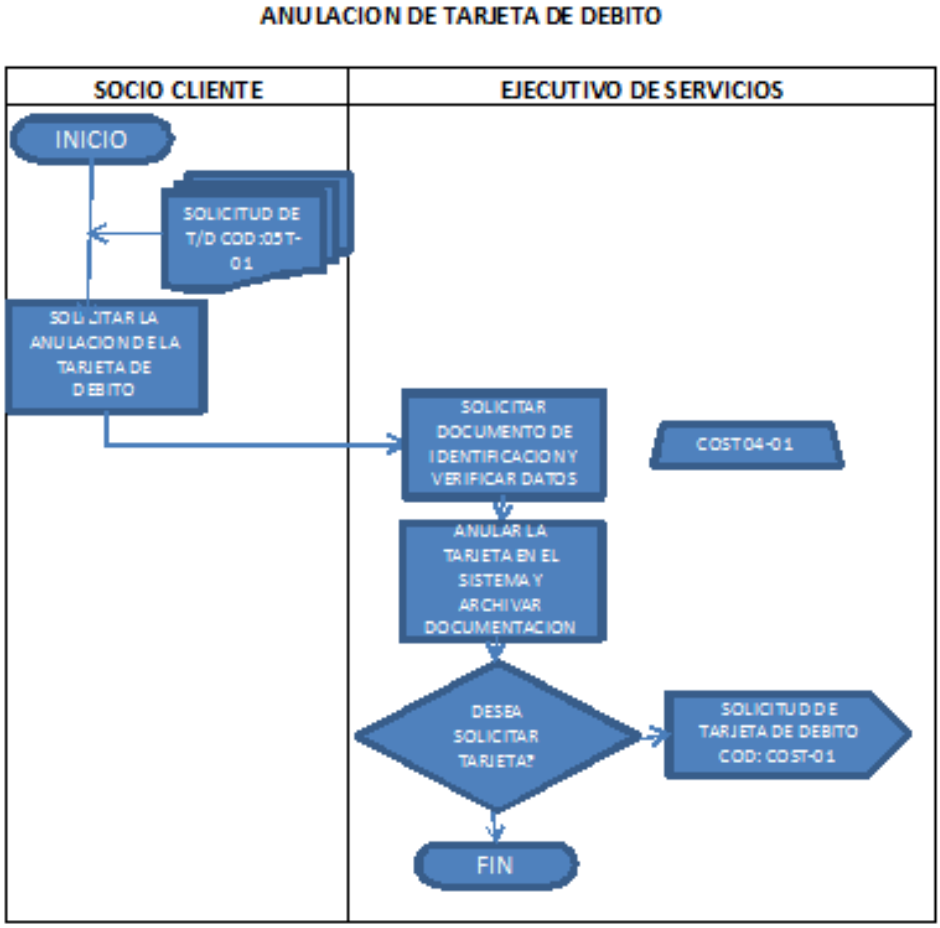
Proceso Emisión de Tarjeta de Débito.



Proceso Entrega de Tarjeta de Débito.



Proceso Anulación de Tarjeta de Débito.



4.4 Análisis de la Infraestructura Física y Tecnológica para Tarjeta de Débito.

La Cooperativa cuenta actualmente con el producto de tarjeta de débito de marca JEP card; cuenta con una infraestructura implementada y en funcionamiento.

4.4.1 Infraestructura de Tecnología de la Información.

La Cooperativa cuenta con un Switch propio el cual fue adquirido a la empresa AlexSoft S.A. para el procesamiento y emisión de tarjetas de débito propias. Las funciones del Switch se detallan a continuación:

Módulo de Seguridad

- Mantenimiento de Usuarios
- Mantenimiento de Roles
- Mantenimiento de Transacciones
- Mantenimiento de Oficinas
- Reinicio de Claves

Módulo de Tarjetas

- Parámetros de Bines
- Parámetros de Productos
- Parámetros de Costos
- Parámetros de Bloqueos
- Solicitud de Tarjetas
- Solicitud de Adicionales
- Suspensión de Tarjetas
- Suspensiones Temporales
- Mantenimiento de Tarjetas
- Renovación de Tarjetas
- Recepción de Tarjetas
- Entrega de Tarjetas
- Entrega Tarjetas con Sobre
- Cambio de Clave
- Activación de Tarjetas
- Activación por Entrega
- Desbloqueo de Tarjetas
- Activación de Tarjetas Canceladas
- Activación de Tarjetas Canceladas por Deuda
- Consulta de Tarjetas
- Consulta de Adicionales

- Reimpresión de Documentos
- Reporte tarjetas Bloqueadas
- Reporte tarjetas Canceladas
- Emisión masiva
- Mantenimiento de Cupos
- Cálculo de costos

Módulo de ATM’s

- Ingreso y mantenimiento de Cajeros Automáticos
- Consulta ATM’s
- Contactos
- Relacionar ATM’s-Contactos
- Relacionar Usuarios a Cajeros
- Start-Stop Cajeros
- Generar archivo de aquerencia
- Contactos
- Relacionar ATM’s-Contactos
- Compilar Imágenes
- Análisis TraficLOG
- Consulta de Transacciones
- Consulta de Journal
- Transacciones sin Confirmación en Cajeros
- Consulta de Switch
- Consulta de Lotes
- Errores en dispensado
- Reporte de Transacciones
- Histórico de Compensación
- Informe Transaccional
- Apertura ATM
- Adicionar dinero ATM
- Cerrar ATM
- Resumen Dispensado
- Emisión de Totales
- Verificación de cuadres

- Retiro Efectivo gavetas
- Totales cierre físico

Módulo de Seguridad

- Generación de Keys
- Activación de Keys
- Consultas de LOGs
- Impresión de Sobres
- Estado de Keys

Administración Parámetros Generales

- Parámetros Extreme
- Ruteo para Cajeros
- Tablas Generales
- Mantenimiento ATM-BIN

4.4.2 Infraestructura de Hardware: Equipos, Características Técnicas.

El Switch de la Cooperativa cuenta con equipos virtualizados sobre un clúster con infraestructura VMWARE, los equipos que conforman el clúster son Blade XH5 de 12 cores con procesador Xeon E7540.

4.4.3 Infraestructura de Software: Versiones, Licencias.

Software Base: Sistemas Operativos, Software de Seguridad.

- Servidor de comunicaciones: Windows Server 2003 Enterprise
- Servidor de Base de Datos: Windows Server 2008 R2
- Servidor Web: Windows Server 2008 R2
- SFTP para el intercambio de información con BANRED
- ON2 para el intercambio de tramas con BANRED
- Firewalls, IDS e IPS instalados en los puntos críticos
- SQL Server 2008 Enterprise
- ATM’s con procesadores Denver y Sierra

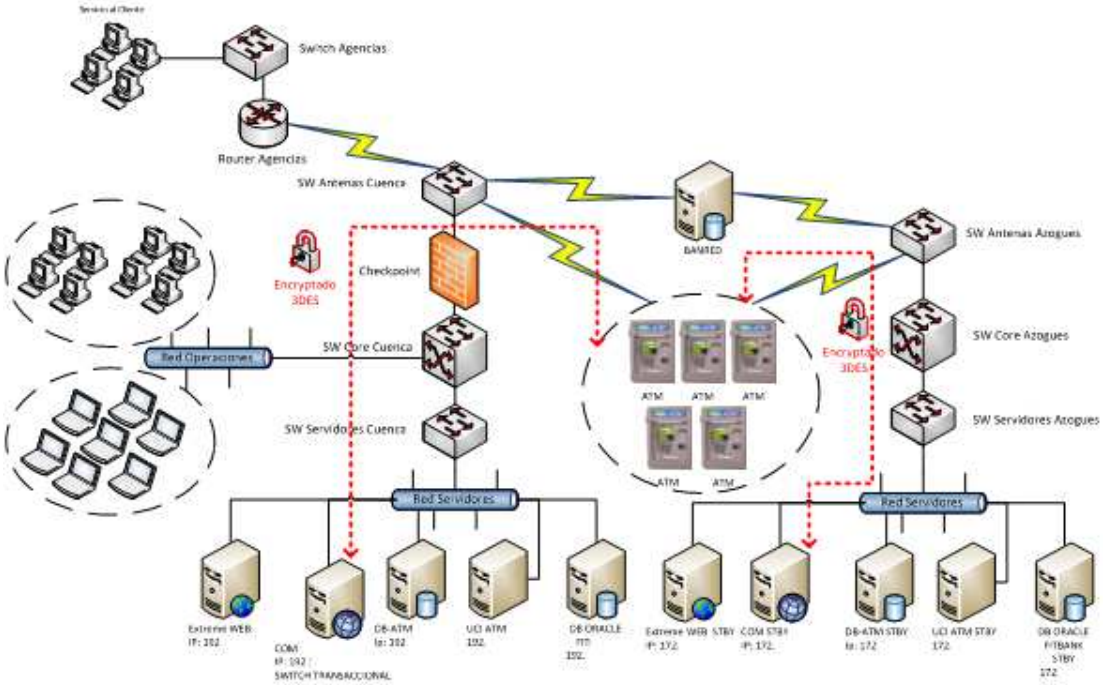
Software de Aplicación: Aplicaciones, Sistemas Transaccionales.

- Aplicativo para manejo de tarjetas de débito EXTREME.
- Aplicativo controlador de ATM's Agilis V3.0.
- Antimalware: SafenSoft con certificación PCI.

4.4.4 Infraestructura de Redes y Comunicaciones: Topologías, Enlaces, Seguridades, Redes Externas.

- Aplicativo con alta disponibilidad y redundancia en el data center principal de Cuenca y el alterno en Azogues.
- Enlaces de comunicación redundantes hacia Banred para la interoperabilidad con tarjetas del sistema financiero nacional.
- Firewall, IPS e IDS checkpoint de última generación para el manejo de seguridad en los canales electrónicos de la Cooperativa.

4.4.5 Topología de la Cooperativa.



Una vez establecido el entorno auditable de tarjeta de débito en base a los procesos que se realizan y a la infraestructura de TI, se determinan en la Matriz de Investigación de campo los controles y las técnicas que se utilizarán en la auditoría.

En la Matriz de Investigación de campo de identifican los dominios que se van a auditar con el objetivo de control determinado por COBIT, adicionalmente se detalla las herramientas de investigación que se utilizarán durante el desarrollo de la auditoría.

4.5 Matriz de Investigación de Campo.

Riesgo	Dominio	Objetivo COBIT	Vulnerabilidad	Herramienta Técnica
A	PO1.2 Alineación de Ti con el negocio	Educar a los ejecutivos sobre las capacidades tecnológicas actuales y sobre el rumbo futuro, sobre las oportunidades que ofrece TI, y sobre qué debe hacer el negocio para capitalizar esas oportunidades. Asegurarse de que el rumbo del negocio al cual está alineado TI está bien entendido. Las estrategias de negocio y de TI deben estar integradas, relacionando de manera clara las metas de la empresa y las metas de TI y reconociendo las oportunidades así como las limitaciones en la capacidad actual, y se deben comunicar de manera amplia. Identificar las áreas en que el negocio (estrategia) depende de forma crítica de TI, y mediar entre los imperativos del negocio y la tecnología, de tal modo que se puedan establecer prioridades concertadas. (COBIT)	La estrategia del negocio no esté alineada con la de TI, por consiguiente no se consigan los objetivos institucionales.	N/A

A	PO2.3 Esquema de clasificación de datos	Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información (esto es, pública, confidencial, secreta) de la empresa. Este esquema incluye detalles acerca de la propiedad de datos, la definición de niveles apropiados de seguridad y de controles de protección y, una breve descripción de los requerimientos de retención y destrucción de datos, además de qué tan críticos y sensibles son. Se usa como base para aplicar controles como el control de acceso, archivo o inscripción. (COBIT)	La información crítica puede divulgarse a personas no autorizadas.	N/A
A	PO2.4 Administración de la integridad	Definir e implementar procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en formato electrónico, tales como bases de datos, almacenes de datos y archivos. (COBIT)	Fallas en la integridad y consistencia de los datos puede originar pérdidas al negocio.	N/A
M	PO4.6 Roles y responsabilidades	Definir y comunicar los roles y las responsabilidades para el personal de TI y los usuarios que delimiten la autoridad entre el personal de TI y los usuarios finales y definan las responsabilidades y rendición de cuentas para alcanzar las necesidades del negocio. (COBIT)	Usuarios y personal de TI que pueden tener roles y privilegios críticos sin haber sido comunicados.	N/A
M	PO4.11 Segregación de funciones	Implementar una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo afecte negativamente un proceso crítico. La gerencia también se asegura de que el personal realice solo las tareas autorizadas, relevantes a sus	Intrusión interna, posible sabotaje de información. Errores involuntarios que afecten los servicios.	Obtención del reporte de usuarios y privilegios módulo del sistema.

		puestos y posiciones respectivas. (COBIT)		
M	PO7.3 Asignación de roles	Definir, monitorear y supervisar los marcos de trabajo para los roles, responsabilidades y compensación del personal, incluyendo el requerimiento de adherirse a las políticas y procedimientos administrativos, así como al código de ética y prácticas profesionales. El nivel de supervisión debe estar de acuerdo con la sensibilidad del puesto y el grado de responsabilidades asignadas. (COBIT)	Intrusión interna, posible sabotaje de información. Errores involuntarios que afecten los servicios.	Obtención de los Logs de Auditoría y revisión de la bitácora de observaciones en el sistema.
A	PO9.1 Alineación de la administración de riesgos de TI y del negocio	Establecer un marco de trabajo de administración de riesgos de TI que esté alineado al marco de trabajo de administración de riesgos de la organización. (COBIT)	El riesgo Operativo o Integral de la Institución puede omitir la valoración de riesgo de TI y no tener un plan de contingencia institucional.	N/A
M	PO9.2 Establecimiento del contexto del riesgo	Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados. Esto incluye la determinación del contexto interno y externo de cada evaluación de riesgos, la meta de la evaluación y los criterios contra los cuales se evalúan los riesgos. (COBIT)	El riesgo Operativo o Integral de la Institución puede omitir la valoración de riesgo de TI y no tener un plan de contingencia institucional.	N/A
A	PO9.3 Identificación de eventos	Identificar eventos (una amenaza importante y realista que explota una vulnerabilidad aplicable y significativa) con un impacto potencial negativo sobre las metas o las operaciones de la empresa, incluyendo aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de	Acceso de intrusos a la red de la Institución. Explotación de vulnerabilidades de puertos.	N/A

		recursos humanos y operativos. Determinar la naturaleza del impacto y mantener esta información. Registrar y mantener los riesgos relevantes en un registro de riesgos. (COBIT)		
A	PO9.4 Evaluación de riegos	Evaluar de forma recurrente la probabilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La probabilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio. (COBIT)	Ocurrencia de un evento de riesgo sin que la Institución esté preparada.	N/A
A	PO9.5 Respuesta a los riesgos	Desarrollar y mantener un proceso de respuesta a los riesgos diseñados para asegurar que los controles efectivos en costo mitigan la exposición en forma continua. El proceso de respuesta a riesgos debe identificar estrategias tales como evitar, reducir, compartir o aceptar riesgos; determinar responsabilidades y considerar los niveles de tolerancia a riesgos. (COBIT)	Ocurrencia de un evento de riesgo sin que la Institución esté preparada.	N/A
A	PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgos	Priorizar y planear las actividades de control a todos los niveles para implementar las respuestas a los riesgos, identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución. Obtener la aprobación para las acciones recomendadas y la aceptación de cualquier riesgo residual, y asegurarse de que las acciones comprometidas están a cargo del dueño (s) de los procesos afectados. Monitorear la ejecución de los planes y reportar cualquier desviación a la alta	Ocurrencia de un evento de riesgo sin que la Institución esté preparada.	N/A

		dirección. (COBIT)		
M	AI1.2 Reporte de análisis de riesgos	Identificar, documentar y analizar los riesgos asociados con los requerimientos del negocio y diseño de soluciones como parte de los procesos organizacionales para el desarrollo de los requerimientos. (COBIT)	Los riesgos de TI pueden tener incidencia negativa en las decisiones del negocio.	N/A
A	AI3.2 Protección y disponibilidad del recurso de infraestructura	Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de administración de cambios de la organización. Incluir una revisión periódica contra las necesidades del negocio, administración de parches y estrategias de actualización, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad. (COBIT)	Cambios no autorizados en el sistema informático con propósitos ajenos a la necesidad institucional.	N/A
A	AI3.3 Mantenimiento de la infraestructura	Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de administración de cambios de la organización. Incluir una revisión periódica contra las necesidades del negocio, administración de parches y estrategias de actualización, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad. (COBIT)	Cambios no autorizados en el sistema informático con propósitos ajenos a la necesidad institucional.	N/A
M	AI3.4 Ambiente de prueba de	Establecer el ambiente de desarrollo y pruebas para soportar la efectividad y eficiencia de las pruebas de factibilidad e	Manipulación de datos o programas productivos por cambios en ambientes de	N/A

	factibilidad	integración de aplicaciones e infraestructura, en las primeras fases del proceso de adquisición y desarrollo. Hay que considerar la funcionalidad, la configuración de hardware y software, pruebas de integración y desempeño, migración entre ambientes, control de la versiones, datos y herramientas de prueba y seguridad. (COBIT)	desarrollo vinculados con los productivos.	
M	Al4.1 Plan para soluciones de operación	Desarrollar un plan para identificar y documentar todos los aspectos técnicos, la capacidad de operación y los niveles de servicio requeridos, de manera que todos los interesados puedan tomar la responsabilidad oportunamente por la producción de procedimientos de administración, de usuarios y operativos, como resultado de la introducción o actualización de sistemas automatizados o de infraestructura. (COBIT)	Cambios no autorizados en el sistema informático con propósitos ajenos a la necesidad institucional.	N/A
M	Al6.1 Estándares y procedimientos para cambios	Establecer procedimientos de administración de cambio formales para manejar de manera estándar todas las solicitudes (incluyendo mantenimiento y parches) para cambios a aplicaciones, procedimientos, procesos, parámetros de sistema y servicio y, las plataformas fundamentales. (COBIT)	Cambios no autorizados en el sistema informático con propósitos ajenos a la necesidad institucional.	N/A
M	Al6.2 Evaluación de impacto, priorización y autorización	Garantizar que todas las solicitudes de cambio se evalúan de una manera estructurada en cuanto a impactos en el sistema operacional y su funcionalidad. Esta evaluación deberá incluir categorización y priorización de los cambios. Previo a la migración hacia producción, los interesados	Cambios no autorizados en el sistema informático con propósitos ajenos a la necesidad institucional.	N/A

		correspondientes autorizan los cambios. (COBIT)		
M	Al6.3 Cambios de emergencia	Establecer un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido. La documentación y pruebas se realizan, posiblemente, después de la implantación del cambio de emergencia. (COBIT)	Cambios no autorizados en el sistema informático con propósitos ajenos a la necesidad institucional.	N/A
M	Al6.4 Seguimiento y reporte del estatus de cambio	Establecer un sistema de seguimiento y reporte para mantener actualizados a los solicitantes del cambio y a los interesados relevantes, acerca del estatus del cambio a las aplicaciones, a los procesos, a los procedimientos, parámetros del sistema y servicio y de las plataformas fundamentales. (COBIT)	Cambios no autorizados en el sistema informático con propósitos ajenos a la necesidad institucional.	N/A
M	DS1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio	Monitorear continuamente los criterios de desempeño especificados para el nivel de servicio. Los reportes sobre el cumplimiento de los niveles de servicio deben emitirse en un formato que sea entendible para los interesados. Las estadísticas de monitoreo son analizadas para identificar tendencias positivas y negativas tanto de servicios individuales como de los servicios en conjunto. (COBIT)	Los recursos pueden dejar de funcionar o volverse demasiado lentos ocasionando pérdidas al negocio.	N/A
M	DS3.2 Capacidad y desempeño	Revisar la capacidad y desempeño actual de los recursos de TI en intervalos regulares para determinar si existe suficiente capacidad y	Los recursos pueden dejar de funcionar o volverse demasiado lentos	N/A

	actual	desempeño para prestar los servicios con base en los niveles de servicio acordados. (COBIT)	ocasionando pérdidas al negocio.	
A	DS4.2 Planes de continuidad de TI	Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo y, capacidad de recuperación de todos los servicios críticos de TI. También deben cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas. (COBIT)	Fallas en la disponibilidad de los recursos tecnológicos debido a que no se levantan las líneas de contingencia.	N/A
A	DS4.3 Recursos críticos de TI	Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación. Evitar la distracción de recuperar los puntos menos críticos y asegurarse de que la respuesta y la recuperación están alineadas con las necesidades prioritarias del negocio, asegurándose también que los costos se mantienen a un nivel aceptable y se cumple con los requerimientos regulatorios y contractuales. Considerar los requerimientos de resistencia, respuesta y recuperación para diferentes niveles de prioridad, por ejemplo, de una a cuatro horas, de cuatro a 24 horas, más de 24 horas y para periodos críticos de operación del negocio. (COBIT)	Fallas en la disponibilidad de los recursos tecnológicos debido a que no se levantan las líneas de contingencia.	N/A

M	DS4.4 Mantenimiento del plan de continuidad de TI	Exhortar a la gerencia de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio. Es esencial que los cambios en los procedimientos y las responsabilidades sean comunicados de forma clara y oportuna. (COBIT)	Fallas en la disponibilidad de los recursos tecnológicos debido a que no se levantan las líneas de contingencia.	N/A
M	DS4.8 Recuperación y reanudación de los servicios de Ti	Planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios. Esto puede representar la activación de sitios de respaldo, el inicio de procesamiento alternativo, la comunicación a clientes y a los interesados, realizar procedimientos de reanudación, etc. Asegurarse de que los responsables del negocio entienden los tiempos de recuperación de TI y las inversiones necesarias en tecnología para soportar las necesidades de recuperación y reanudación del negocio. (COBIT)	Fallas en la disponibilidad de los recursos tecnológicos debido a que no se levantan las líneas de contingencia.	N/A
M	DS4.9 Almacenamiento de respaldos fuera de las instalaciones	Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio. El contenido de los respaldos a almacenar debe determinarse en conjunto entre los responsables de los procesos de negocio y el personal de TI. La administración del sitio de almacenamiento	Pérdida de información sensible por falta de respaldo en la contingencia.	N/A

		externo a las instalaciones, debe apegarse a la política de clasificación de datos y a las prácticas de almacenamiento de datos de la empresa. La gerencia de TI debe asegurar que los acuerdos con sitios externos sean evaluados periódicamente, al menos una vez por año, respecto al contenido, a la protección ambiental y a la seguridad. Asegurarse de la compatibilidad del hardware y del software para poder recuperar los datos archivados y periódicamente probar y renovar los datos archivados. (COBIT)		
A	DS5.1 Administración de la seguridad de TI	Administrar la seguridad de TI al nivel más alto apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio. (COBIT)	Afectación al negocio por falta de inclusión de los riesgos de TI en los planes administrativos.	N/A
A	DS5.2 Plan de seguridad de TI	Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad. Asegurar el plan está implementado en las políticas y procedimientos de seguridad junto con las inversiones apropiadas en los servicios, personal, software y hardware. Comunicar las políticas y procedimientos de seguridad a los interesados y a los usuarios. (COBIT)	Afectación al negocio por falta de inclusión de los riesgos de TI en los planes administrativos.	N/A
A	DS5.3 Administración de identidad	Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, entorno de TI, operación de sistemas,	Usuarios con accesos a los aplicativos con perfiles sensibles con usuarios o claves genéricas.	N/A

		desarrollo y mantenimiento) deben ser identificables de manera única. Permitir que el usuario se identifique a través de mecanismos de autenticación. Confirmar que los permisos de acceso del usuario al sistema y los datos están en línea con las necesidades del negocio definidos y documentados y que los requerimientos de trabajo están adjuntos a las identidades del usuario. Asegurar que los derechos de acceso del usuario se solicitan por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se despliegan técnicas efectivas en coste y procedimientos rentables, y se mantienen actualizados para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso. (COBIT)		
M	DS5.4 Administración de cuentas del usuario	Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por un conjunto de procedimientos de la gerencia de cuentas de usuario. Debe incluirse un procedimiento de aprobación que describa al responsable de los datos o del sistema otorgando los privilegios de acceso. Estos procedimientos deben aplicarse a todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de	Usuarios con privilegios sensibles que pueden ocasionar un compromiso de información o ejecutar procesos críticos no autorizados.	Obtención de los reportes de usuarios del Active Directory: Revisión con el listado del personal que ha salido de la Institución. Revisión de los perfiles y privilegios asignados de acuerdo a la posición que ocupa el empleado en la Institución.

		emergencia. Los derechos y obligaciones relativos al acceso a los sistemas e información de la empresa deben acordarse contractualmente para todos los tipos de usuarios. Realizar revisiones regulares de la gestión de todas las cuentas y los privilegios asociados. (COBIT)		
A	DS5.7 Protección de la tecnología de seguridad	Garantizar que la tecnología relacionada con la seguridad sea resistente al sabotaje y no revele documentación de seguridad innecesaria. (COBIT)	Compromiso o fuga de información sensible.	Escaneo con Nmap de puertos de CheckPoint 256 y 258 para impedir el manejo del Firewall desde el Internet. Verificar que el escaneo no divulgue información de administración del Firewall. El Firewall está administrado por estos puertos.
A	DS5.8 Administración de llaves criptográficas	Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas. (COBIT)	Compromiso o copia de llaves que ponga en riesgo la información transmitida o almacenada en la Institución.	Acceso como usuario administrador al módulo de llaves informáticas. Establecer que las llaves informáticas cumplen el estándar 3DES. Copia de llaves informáticas del módulo origen en un archivo plano.
A	DS5.9 Prevención, detección y	Poner medidas preventivas, detectivas y correctivas (en especial contar con parches de seguridad y control de virus actualizados)	Virus o software malicioso que infecte el entorno institucional y comprometa	Revisión de los Sistemas Operativos con las últimas actualizaciones en parches.

	corrección de software malicioso	en toda la organización para proteger los sistemas de la información y a la tecnología contra malware (virus, gusanos, spyware, correo basura). (COBIT)	información o afecte al servicio.	Revisión de logs de eventos de los antivirus. Revisión al muestreo de las versiones y actualizaciones de las bases de datos de los antivirus en los computadores personales.
A	DS5.10 Seguridad de la red	Garantizar que se utilizan técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes y, detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes. (COBIT)	Puertos abiertos que permiten a intrusos ingresar a la red institucional, copiar, alterar o atacar la información o los servicios de la Institución. Las redes que no están segmentadas pueden compartir archivos de información sensible entre usuarios.	Escaneo de puertos utilizando Nmap. Conexión por Telnet entrante a los puertos abiertos. Verificar conexiones SSH solamente entrantes. Verifica que Telnet saliente utilice mecanismos seguros como encriptación. Verificar que las conexiones web tengan SSL.
A	DS5.11 Intercambio de datos sensitivos	Transacciones de datos sensibles se intercambian solo a través de una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen. (COBIT)	Pérdida o divulgación de información sensible.	Acceso a la red SFTP verificar accesos, contraseñas por defecto, verificar que no existan conexiones FTP.

M	DS10.2 Rastreo y resolución de problemas	El sistema de administración de problemas debe mantener pistas de auditoría adecuadas que permitan rastrear, analizar y determinar la causa raíz de todos los problemas reportados considerando: • Todos los elementos de configuración asociados. • Problemas e incidentes sobresalientes. • Errores conocidos y sospechados • Seguimiento de las tendencias de los problemas. (COBIT)	Afectación por errores o problemas recurrentes sin solución definitiva.	Revisión de casos levantados en el sistema Help Desk desde la apertura del caso hasta el cierre de los mismos.
M	DS10.3 Cierre de problemas	Disponer de un procedimiento para cerrar los registros de problemas ya sea después de confirmar la eliminación exitosa del error conocido o después de acordar con el negocio cómo manejar el problema de manera alternativa. (COBIT)	Afectación por errores o problemas recurrentes sin solución definitiva.	Revisión de casos levantados en el sistema Help Desk desde la apertura del caso hasta el cierre de los mismos.
M	DS11.1 Requerimientos del negocio para administración de datos	Verificar que todos los datos que se espera procesar se reciben y procesan completamente, de forma precisa y a tiempo, y que todos los resultados se entregan de acuerdo a los requerimientos del negocio. Las necesidades de reinicio y reproceso están soportados. (COBIT)	Pérdida de información por saturación de los servicios de la Institución.	N/A
M	DS11.2 Acuerdos de almacenamiento y conservación	Definir e implementar procedimientos para el archivo, almacenamiento y retención de los datos, de forma efectiva y eficiente para conseguir los objetivos de negocio, la política de seguridad de la organización y los requerimientos regulatorios. (COBIT)	Pérdida de información sensible por archivos almacenados innecesariamente.	N/A

M	DS11.3 Sistema de administración de librerías de medios	Definir e implementar procedimientos para mantener un inventario de medios almacenados y archivados para asegurar su usabilidad e integridad. (COBIT)	Pérdida de información sensible por archivos almacenados sin inventario.	
M	DS11.4 Eliminación	Definir e implementar procedimientos para asegurar que los requerimientos de negocio para la protección de datos sensitivos y el software se consiguen cuando se eliminan o transfieren los datos y/o el hardware. (COBIT)	Pérdida de información sensible por archivos almacenados sin protección.	Ejecutar comandos SELECT – SQL a las tablas que almacenan la información de tarjetas de débito: Claves Números de tarjetas CVV PVV Fecha de expiración. Track 1 Track 2 Nombres de clientes Cédula de los clientes Número de cuenta
M	DS11.5 Respaldo y restauración	Definir e implementar procedimientos de respaldo y restauración de los sistemas, aplicaciones, datos y documentación en línea con los requerimientos de negocio y el plan de continuidad. (COBIT)	Pérdida de información sensible por archivos almacenados innecesariamente.	N/A
M	DS11.6 Requerimientos de seguridad para la administración de datos	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos para conseguir los objetivos de negocio, las políticas de seguridad de la organización y requerimientos	Pérdida de información por procesos débiles en la transmisión, almacenamiento y custodia de la información.	N/A

		regulatorios. (COBIT)		
M	DS12.2 Medidas de seguridad física	Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio. Las medidas deben incluir, pero no limitarse al esquema del perímetro de seguridad, de las zonas de seguridad, la ubicación de equipo crítico y de las áreas de envío y recepción. En particular, mantenga un perfil bajo respecto a la presencia de operaciones críticas de TI. Deben establecerse las responsabilidades sobre el monitoreo y los procedimientos de reporte y de resolución de incidentes de seguridad física. (COBIT)	Acceso de personas no autorizadas a espacios restringidos.	N/A
M	DS12.3 Acceso Físico	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo las emergencias. El acceso a locales, edificios y áreas debe justificarse, autorizarse, registrarse y monitorearse. Esto aplica para todas las personas que accedan a las instalaciones, incluyendo personal, clientes, proveedores, visitantes o cualquier tercera persona. (COBIT)	Acceso de personas no autorizadas a espacios restringidos.	N/A
M	ME1.2 Definición y recolección de datos de monitoreo	Trabajar con el negocio para definir un conjunto balanceado de objetivos de desempeño y tenerlos aprobados por el negocio y otros interesados relevantes. Definir referencias con las que comparar los objetivos, e identificar datos disponibles a recolectar para medir los objetivos. Se deben	Objetivos de negocio incumplidos por falta de información de alerta oportuna sobre procesos críticos.	N/A

		establecer procesos para recolectar información oportuna y precisa para reportar el avance contra las metas. (COBIT)		
M	ME1.3 Método de monitoreo	Garantizar que el proceso de monitoreo implante un método (Ej. Balanced Scorecard), que brinde una visión sucinta y desde todos los ángulos del desempeño de TI y que se adapte al sistema de monitoreo de la empresa. (COBIT)	Objetivos de negocio incumplidos por falta de información de alerta oportuna sobre procesos críticos.	Revisión de los resultados del Balanced Scorecard y los objetivos planteados para que la tecnología apoye al negocio.
M	ME1.4 Evaluación del desempeño	Comparar de forma periódica el desempeño contra las metas, realizar análisis de la causa raíz e iniciar medidas correctivas para resolver las causas subyacentes. (COBIT)	Objetivos de negocio incumplidos por falta de información de alerta oportuna sobre procesos críticos.	N/A
M	ME1.5 Reportes al consejo directivo y a ejecutivos	Proporcionar reportes administrativos para ser revisados por la alta dirección sobre el avance de la organización hacia metas identificadas, específicamente en términos del desempeño del portafolio empresarial de programas de inversión habilitados por TI, niveles de servicio de programas individuales y la contribución de TI a ese desempeño. Los reportes de estatus deben incluir el grado en el que se han alcanzado los objetivos planeados, los entregables obtenidos, las metas de desempeño alcanzadas y los riesgos mitigados. Durante la revisión, se debe identificar cualquier desviación respecto al desempeño esperado y se deben iniciar y reportar las medidas de administración adecuadas. (COBIT)	Objetivos de negocio incumplidos por falta de información de alerta oportuna sobre procesos críticos.	Ver ME 1.3

M	ME1.6 Acciones correctivas	Identificar e iniciar medidas correctivas basadas en el monitoreo del desempeño, evaluación y reportes. Esto incluye el seguimiento de todo el monitoreo, de los reportes y de las evaluaciones con: • Revisión, negociación y establecimiento de respuestas de administración. • Asignación de responsabilidades por la corrección. • Rastreo de los resultados de las acciones comprometidas. (COBIT)	Procesos críticos sin un adecuad seguimiento y solución que ocasionan pérdidas al negocio.	N/A
M	ME2.2 Revisiones de auditoría	Monitorear y evaluar la eficiencia y efectividad de los controles internos de revisión de la gerencia de TI. (COBIT)	Procesos críticos sin una adecuada revisión que ocasionan pérdidas al negocio.	N/A
M	ME2.3 Excepciones de control	Identificar las excepciones de control, y analizar e identificar sus causas raíz subyacente. Escalar las excepciones de control y reportar a los interesados apropiadamente. Establecer acciones correctivas necesarias. (COBIT)	Procesos críticos sin un adecuad seguimiento y solución que ocasionan pérdidas al negocio.	N/A
M	ME2.4 Auto-evaluación de control	Evaluar la completitud y efectividad de los controles de gerencia sobre los procesos, políticas y contratos de TI por medio de un programa continuo de auto-evaluación. (COBIT)	Procesos críticos sin un adecuad seguimiento y solución que ocasionan pérdidas al negocio.	N/A
M	ME2.7 Acciones correctivas	Identificar, iniciar, rastrear e implementar acciones correctivas derivadas de los controles de evaluación y los informes. (COBIT)	Procesos críticos sin un adecuad seguimiento y solución que ocasionan pérdidas al negocio.	N/A

M	ME3.1 Identificar las leyes y regulaciones con impacto potencial sobre TI	Identificar, sobre una base continua, leyes locales e internacionales, regulaciones, y otros requerimientos externos que se deben de cumplir para incorporar en las políticas, estándares, procedimientos y metodologías de TI de la organización. (COBIT)	Acciones o procesos que ejecute la empresa sin observar los marcos de regulación y que derivan en pérdidas para la Institución.	N/A
M	ME3.2 Optimizar la respuesta a requerimientos externos	Revisar y ajustar las políticas, estándares, procedimientos y metodologías de TI para garantizar que los requisitos legales, regulatorios y contractuales son direccionados y comunicados. (COBIT)	Acciones o procesos que ejecute la empresa sin observar los marcos de regulación y que derivan en pérdidas para la Institución.	N/A
M	ME3.3 Evaluación del cumplimiento con requerimientos externos	Confirmar el cumplimiento de políticas, estándares, procedimientos y metodologías de TI con requerimientos legales y regulatorios. (COBIT)	Acciones o procesos que ejecute la empresa sin observar los marcos de regulación y que derivan en pérdidas para la Institución.	N/A
M	ME3.4 Aseguramiento positivo del cumplimiento	Obtener y reportar garantía de cumplimiento y adhesión a todas las políticas internas derivadas de directivas internas o requerimientos legales externos, regulatorios o contractuales, confirmando que se ha tomado cualquier acción correctiva para resolver cualquier brecha de cumplimiento por el dueño responsable del proceso de forma oportuna. (COBIT)	Acciones o procesos que ejecute la empresa sin observar los marcos de regulación y que derivan en pérdidas para la Institución.	N/A
M	ME4.2 Alineamiento estratégico	Facilitar el entendimiento del consejo directivo y de los ejecutivos sobre temas estratégicos de TI tales como el rol de TI, características	Procesos de TI debilitados por falta de involucramiento	N/A

		propias y capacidades de la tecnología. Garantizar que existe un entendimiento compartido entre el negocio y la función de TI sobre la contribución potencial de TI a la estratégica del negocio. Trabajar con el consejo directivo para definir e implementar organismos de gobierno, tales como un comité estratégico de TI, para brindar una orientación estratégica a la gerencia respecto a TI, garantizando así que tanto la estrategia como los objetivos se distribuyan en cascada hacia las unidades de negocio y hacia las unidades de TI y que se desarrolle certidumbre y confianza entre el negocio y TI. Facilitar la alineación de TI con el negocio en lo referente a estrategia y operaciones, fomentando la co-responsabilidad entre el negocio y TI en la toma de decisiones estratégicas y en la obtención de los beneficios provenientes de las inversiones habilitadas con TI. (COBIT)	institucional.	
M	ME4.5 Administración de riesgos	Trabajar en conjunto con el consejo directivo para definir el nivel de riesgo de TI aceptable por la empresa. Comunicar este nivel de riesgo hacia la organización y acordar el plan de administración de riesgos de TI. Integrar las responsabilidades de administración de riesgos en la organización, asegurando que tanto el negocio como TI evalúen y reporten periódicamente los riesgos asociados con TI y su impacto en el negocio. Garantizar que la gerencia de TI haga seguimiento a la exposición a los riesgos, poniendo especial atención en las fallas y debilidades de control	Procesos de TI debilitados por falta de involucramiento institucional.	N/A

		interno y de supervisión, así como su impacto actual y potencial en el negocio. La posición de riesgo empresarial en TI debería ser transparente para todos los interesados. (COBIT)		
M	ME4.6 Medición del desempeño	Confirmar que los objetivos de TI confirmados se han conseguido o excedido, o que el progreso hacia las metas de TI cumple las expectativas. Donde los objetivos confirmados no se han alcanzado o el progreso no es el esperado, revisar las acciones correctivas de gerencia. Informar a dirección los portafolios relevantes, programas y desempeños de TI, soportados por informes para permitir a la alta dirección revisar el progreso de la empresa hacia las metas identificadas. (COBIT)	Procesos de TI debilitados por falta de involucramiento institucional.	N/A

4.6 Actividades de Auditoría.

En el documento Plan de Auditoría, se establecen los horarios y cronogramas a seguir en el ejercicio de la revisión, este documento ha sido acordado con la alta gerencia y distribuido a todos los involucrados en el proceso de revisión.

4.7 Plan de Auditoría.

Organización:	Cooperativa JEP		
Dirección:	Calle Sucre 10-56 y General Torres	Fechas en sitio:	23 –Sep – 13 al 04 – Oct – 13
Objetivo de la Auditoría:	Aplicar una Auditoría Informática utilizando la metodología COBIT para evaluar y determinar el nivel de cumplimiento de los procesos críticos de Tarjeta de Débito que permitan identificar debilidades y emitir recomendaciones para minimizar riesgos.		
Auditor Líder:	Jorge Cárdenas		
Miembros del equipo:	N/A		
Áreas de revisión:	Software Alexsoft, Servidores, Bases de Datos, Entorno de red cajeros ATM, Procesos y Actividades operativas de Tarjeta de Débito.		
Nomenclatura:	OP: Operaciones TI: Tecnología de información AE: Auditor Externo		

Fecha	Hora	Auditor	Área / Proceso / Función	Contacto
16 Oct 2013	09:00 – 16:00	JC	Reunión de Apertura. OP: Proceso Emisión Tarjeta de Débito TI: Infraestructura de red OP, TI: Módulo de Seguridad	Gerente Sistemas, Gerente Operaciones, Jefe Operativo
17 Oct 2013	09:00 – 16:00		OP: Proceso Emisión Tarjeta de Débito	Jefe Operativo, Asistente Operativo, Jefe

Fecha	Hora	Auditor	Área / Proceso / Función	Contacto
		JC	(Continuación) TI: Arquitectura de red (Continuación) OP, TI: Módulo de Tarjetas	Infraestructura, Asistente Infraestructura
18 Oct. 2013	09:00 – 16:00	JC	OP: Proceso Entrega Tarjeta de Débito TI: Arquitectura de red (Continuación) OP, TI: Módulo de Tarjetas (Continuación)	Jefe Operativo, Asistente Operativo, Jefe Infraestructura, Asistente Infraestructura
21 Oct. 2013	09:00 – 16:00	JC	OP: Proceso Entrega Tarjeta de Débito TI: Gestión de Base de Datos (Continuación) OP, TI: Módulo de Tarjetas (Continuación)	Jefe Operativo, Asistente Operativo, Jefe Infraestructura, Asistente Infraestructura
22 Oct. 2013	09:00 – 16:00	JC	OP: Proceso Anulación Tarjeta de Débito TI: Gestión de Base de Datos (Continuación) OP, TI: Módulo de ATMs	Jefe Operativo, Asistente Operativo, Jefe Infraestructura, Asistente Infraestructura
23 Oct. 2013	09:00 – 16:00	JC	OP: Proceso Anulación Tarjeta de Débito TI: Comunicación de red OP, TI: Módulo de ATMs (Continuación)	Jefe Operativo, Asistente Operativo, Jefe Infraestructura, Asistente Infraestructura
24 Oct. 2013	09:00 – 16:00	JC	TI: Comunicación de red (Continuación) OP, TI: Módulo de ATMs (Continuación)	Jefe Operativo, Asistente Operativo, Jefe Infraestructura, Asistente Infraestructura.
25 Oct. 2013	09:00 – 16:00	JC	OP, TI: Módulo de seguridad	Jefe Operativo, Asistente Operativo, Jefe Infraestructura, Asistente

Fecha	Hora	Auditor	Área / Proceso / Función	Contacto
				Infraestructura.
28 Oct. 2013	09:00 – 16:00	JC	OP, TI: Módulo de Administración de parámetros generales	Jefe Operativo, Asistente Operativo, Jefe Infraestructura, Asistente Infraestructura.
29 Oct 2013	09:00 – 16:00	JC	Reunión Cierre Revisión de hallazgos, correcciones Actividades propias del Auditor	Gerente Sistemas, Gerente Operaciones, Jefe Operativo

Notas: Los auditores se podrían cambiar o adicionar los elementos indicados antes o durante la auditoría, dependiendo de los resultados de la investigación en sitio.

4.8 Hallazgos de Auditoría.

Los hallazgos de la auditoría se detallan en la Matriz de Hallazgos, con su respectiva evidencia.

Se ha establecido los niveles de madurez con los que se valorará a los controles, la tabla de madurez recomienda COBIT como un modelo genérico a seguir.

4.8.1 Herramientas Técnicas Utilizadas y Resultados Obtenidos.

PO4.11 Segregación de funciones.

Figura 1. Reporte de Usuarios y Privilegios.

Empresa	Usuario	Nom_Usuario	Perfil	Nom_Perfil	Estado
3	Aastudio	Alfonso Astudillo O	4	Modulo Autorizaciones	A
3	Aastudio	Alfonso Astudillo O	9	Modulo de Tarjetas	A
3	Aastudio	Alfonso Astudillo O	18	Gestiones de clientes	A
3	Aastudio	Alfonso Astudillo O	30	Atencion al Cliente General	A
3	Aastudio	Alfonso Astudillo O	33	Modificación de estados de Tarjetas	A
3	Aastudio	Alfonso Astudillo O	82	Consulta Autorizaciones de todas las empresas	A
3	Aastudio	Alfonso Astudillo O	108	Ingreso y consulta de tran. fraudes	A
3	acarrion	Angel Carrion	8	Operador Centro de Computo	A
3	Amontiea	Angel A Montiel A	8	Operador Centro de Computo	A
3	Aparragm	Agustín Parraga Mero	30	Atencion al Cliente General	A
3	Apeñaloa	Alexandra Peñaloza Aguilar	18	Gestiones de clientes	A
3	Apeñaloa	Alexandra Peñaloza Aguilar	28	Renovaciones	A
3	Apeñaloa	Alexandra Peñaloza Aguilar	30	Atencion al Cliente General	A
3	Apeñaloa	Alexandra Peñaloza Aguilar	84	Mantenimiento Cartera	A
3	Areyescu	Angela María Reyes Cueva	13	Entrega de Tarjetas	A
3	Areyescu	Angela María Reyes Cueva	18	Gestiones de clientes	A
3	Areyescu	Angela María Reyes Cueva	33	Modificación de estados de Tarjetas	A
3	Areyescu	Angela María Reyes Cueva	40	Modifica Datos Generales	A
3	Areyescu	Angela María Reyes Cueva	89	Tarjetas - transacciones -- Normales	A
3	Areyescu	Angela María Reyes Cueva	98	consulta de saldos pestañas	A

PO7.3 Asignación de roles.

Figura 2. Log de Auditoria.

Detalle Cambio en LOG Usuario: administrador

El usuario : **administrador** *hizo el*
a las 09:26:24:738 *horas, en aplicacion* ADM *x la transaccion* AD31

SELECT convert(varchar(10),LogFecha,111) as Fecha,case ISNUMERIC(LogHora) when 1 then substring(LogHora,1,2)+ ":" + substring(LogHora,3,2) + ":" + substring(LogHora,5,2) + "." + substring(LogHora,7,3) else rtrim(LogHora) + ":000" end as Hora, LogUsuario as Usuario, TE.TEDescripcionAccion as DescripcionAccion, LogAplicacion as Aplicacion, LogTransaccion as Transaccion, LogTerminal as Terminal, LogIDentificadorKey as Identificador, LogTabla as Tabla, LogBase as Base, LogHora ,"0" Severidad FROM LogGeneral LEFT JOIN Parametros.dbo.TiposEventosLog TE ON (LogTipoOperacion = TETipoAccion) WHERE LogFecha >= @FechaInicial AND LogFecha <= @FechaFinal ORDER BY LogFecha, LogHora@FechaInicia:2014/10/28@FechaFinal:2014/10/28

DS5.4 Administración de cuentas del usuario.

Figura 3. Reportes de usuarios del Active Directory.

DS5.7 Protección de la tecnología de seguridad

Figura 4. Ping a la red para obtener la IP.

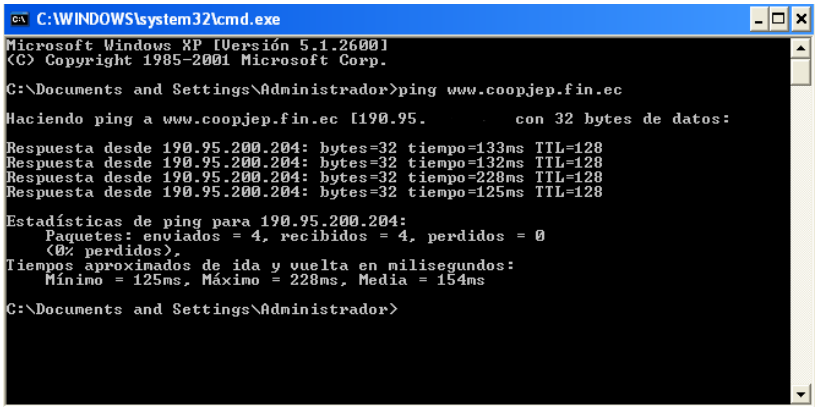
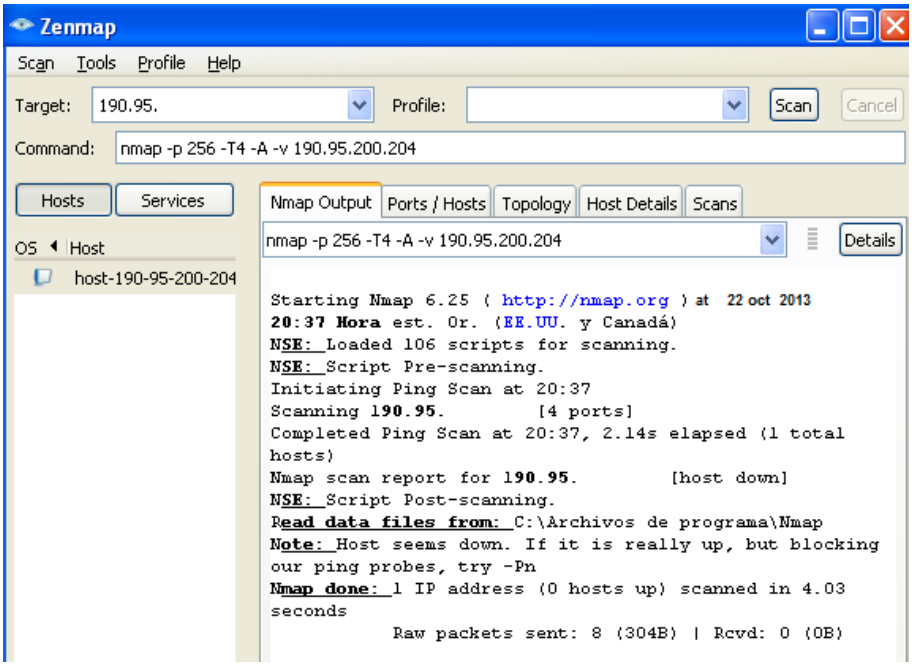


Figura 5. Escaneo a los puertos 256 y 258 utilizando Nmap.



Nota Evidencia: No se encuentran los puertos abiertos.

Figura 6. Verificación de puertos cerrados con Nmap.

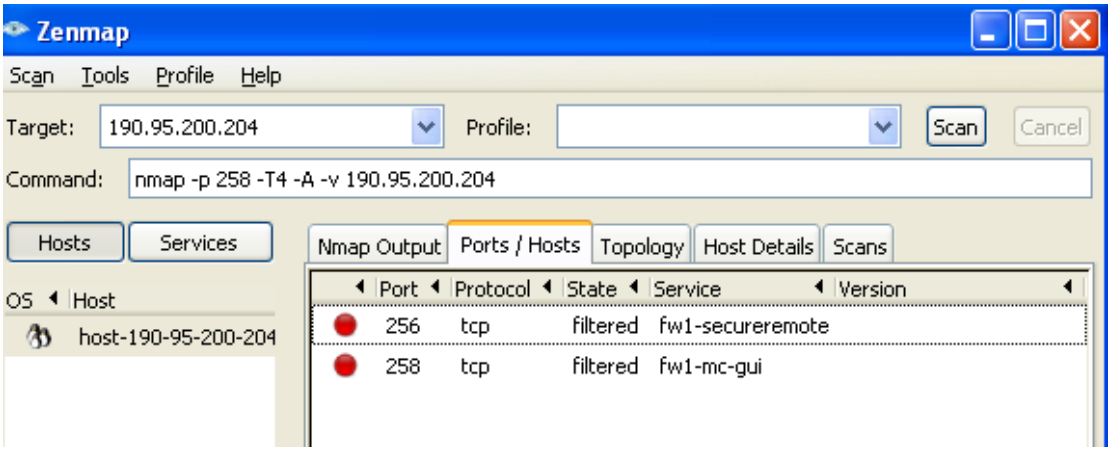
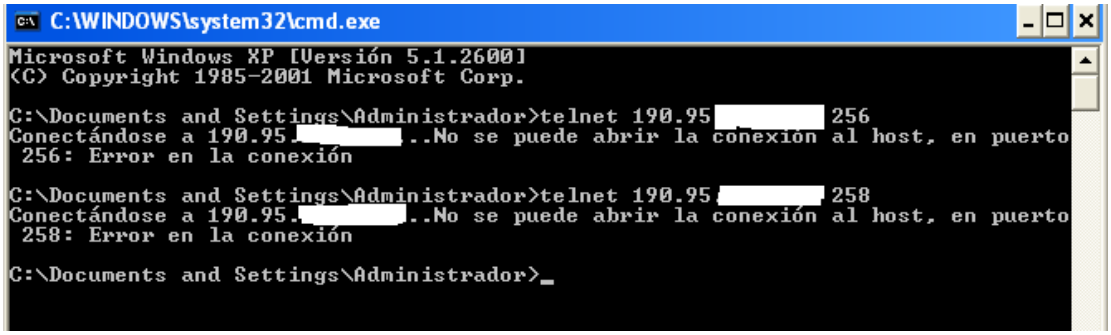
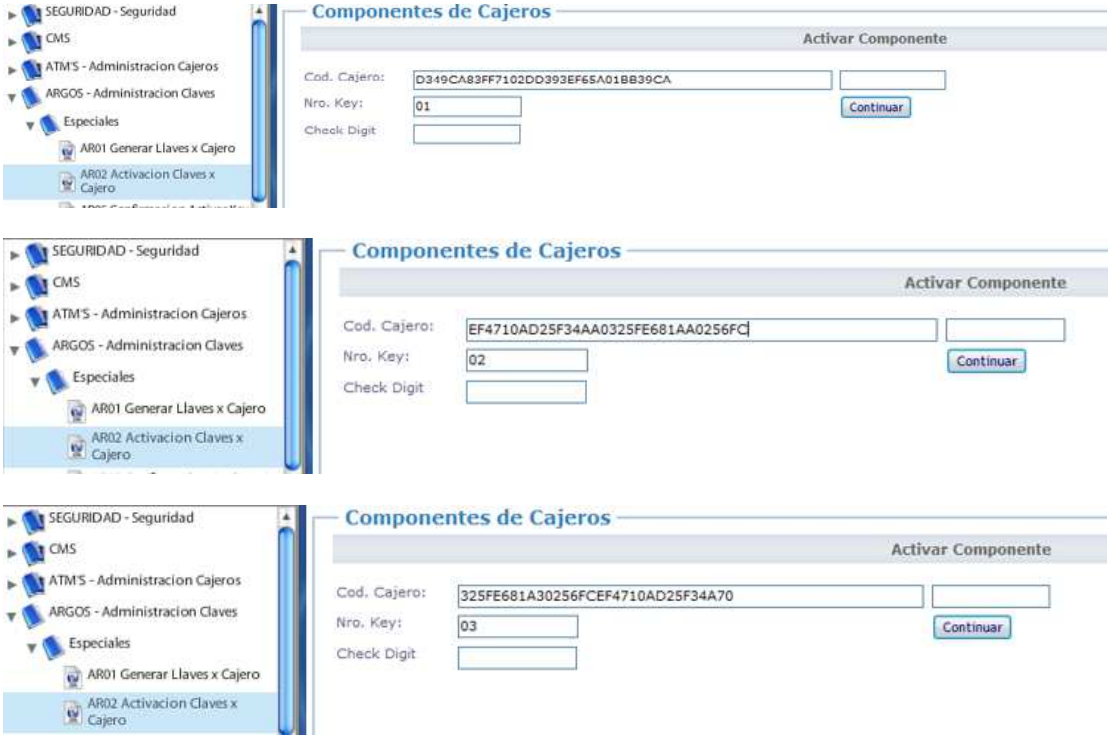


Figura 7. Intento de conexión Telnet a los puertos 256 y 258 no exitosos.



DS5.8 Administración de llaves criptográficas.

Figura 8. Acceso al módulo de llaves informáticas.



Nota Evidencia: Llaves ingresadas por software y editables. Componentes 1, 2 y 3

Figura 9. Consulta Log Llaves Informáticas.

DS5.9 Prevención, detección y corrección de software malicioso.

Figura 10. Revisión de Configuración de Antivirus.

. Revisión de Configuración de Antivirus.

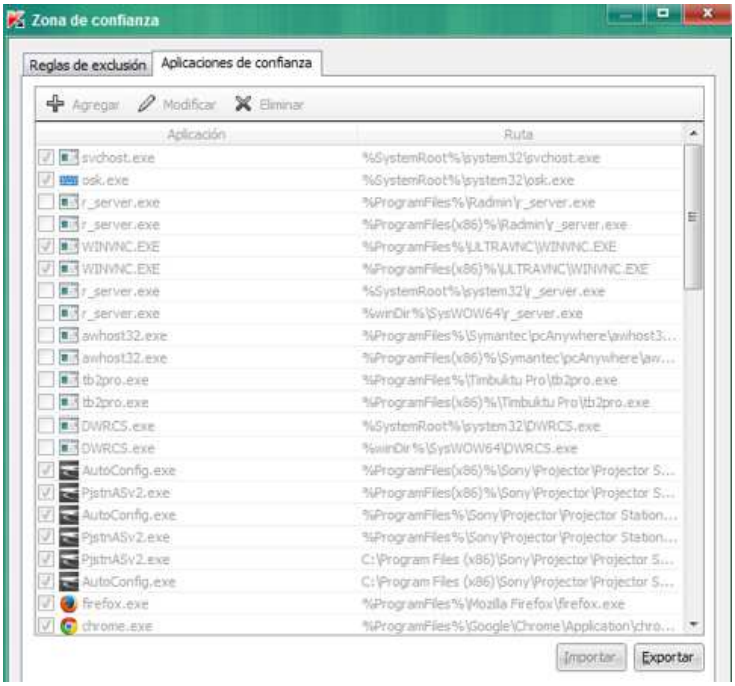


Figura 12. Revisión de Eventos de Antivirus.

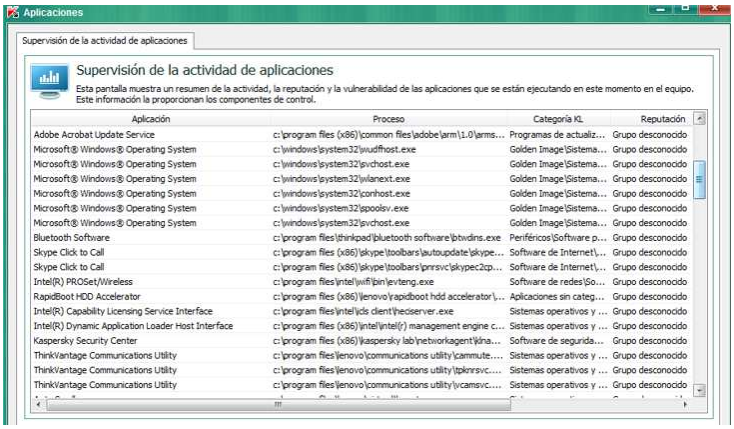


Figura 13. Revisión de Protección de Antivirus.

DS5.10 Seguridad de la red.

Figura 14. Escaneo de puertos utilizando Nmap.

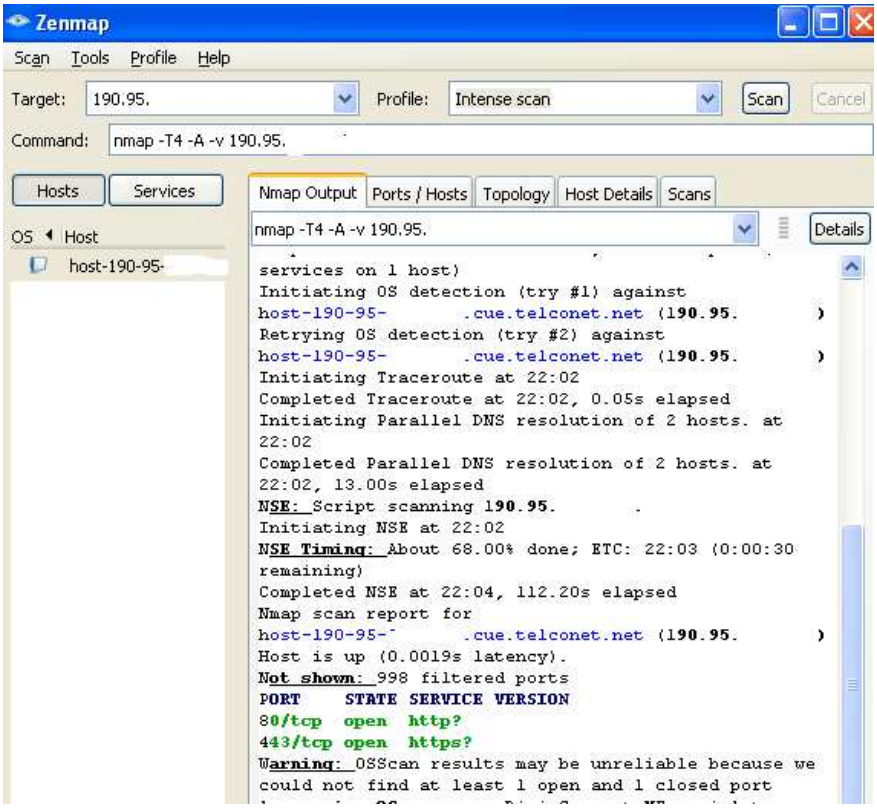
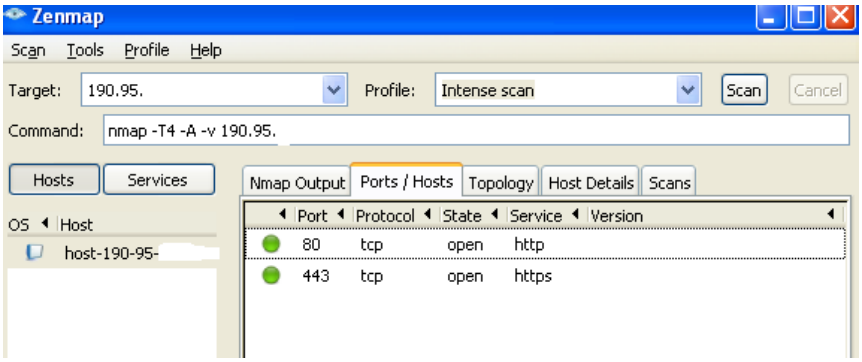
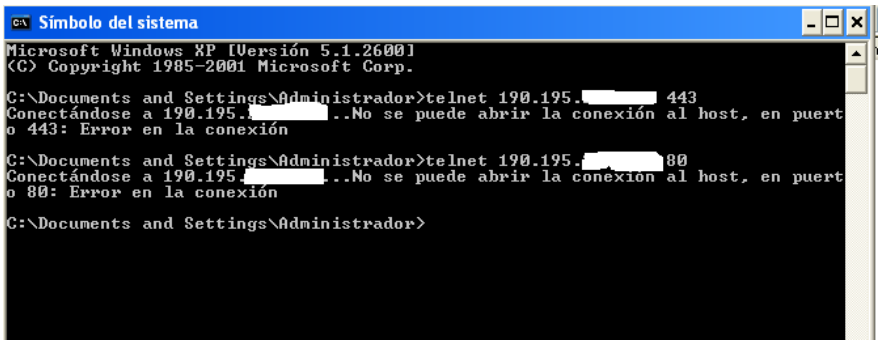


Figura 15. Verificación de abiertos utilizando Nmap.



Nota Evidencia: Se determina que están abiertos los puertos 80 y 443, que son los que generalmente están abiertos.

Figura 16. Intento de conexión Telnet a los puertos 80 y 443 abiertos.

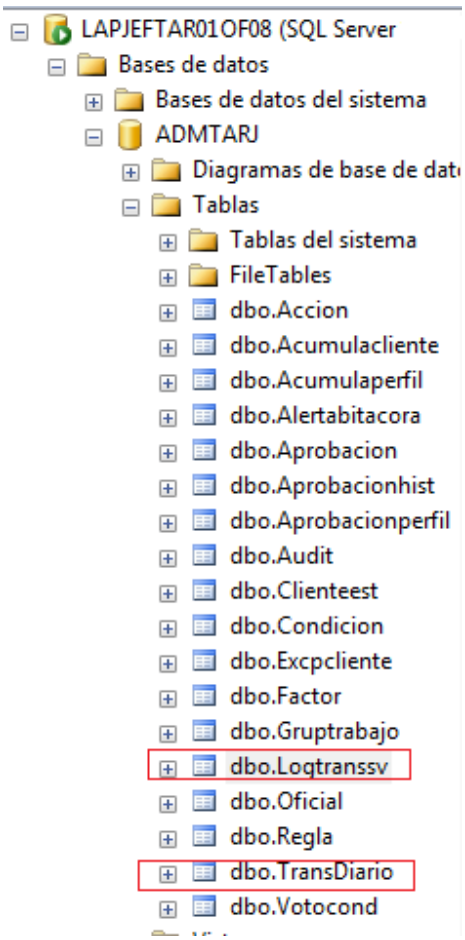


Nota Evidencia: Las conexiones son rechazadas.

Figura 17. Verificación de SSL en la página transaccional. Presenta HTTPS.

DS11.4 Eliminación

Figura 18. Verificación de tablas SQL a revisar.

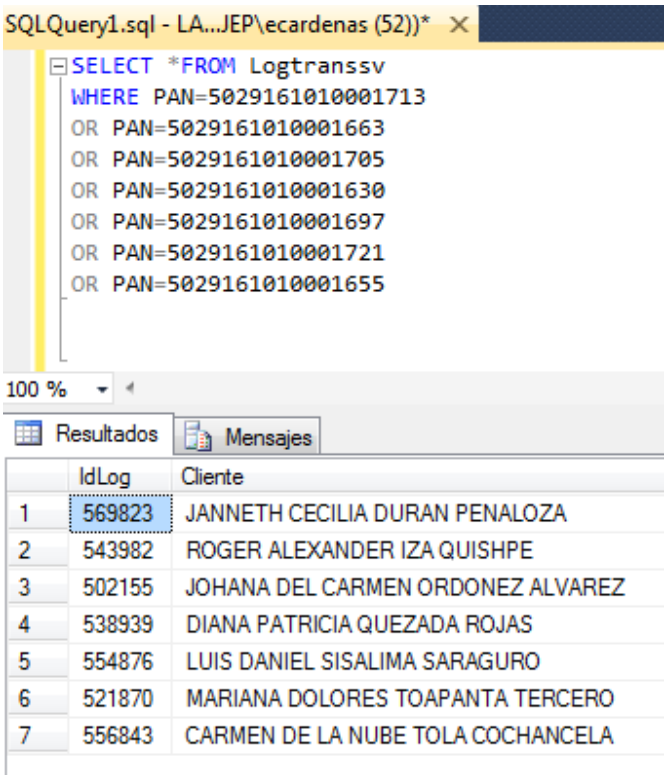


Nota Evidencia: Se ejecutan comandos SELECT – SQL a las tablas que almacenan la información de tarjetas de débito.

Figura 19. Consulta de Clave de Tarjeta.

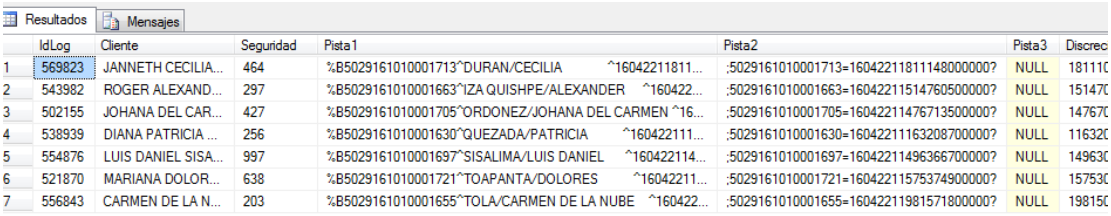
Nota Evidencia: La clave de la tarjeta se puede obtener en claro por pantalla.

Figura 20. Consulta SQL por Tarjeta. Se seleccionan siete tarjetas que realizaron transacciones.



	IdLog	Cliente
1	569823	JANNETH CECILIA DURAN PENALOZA
2	543982	ROGER ALEXANDER IZA QUISHPE
3	502155	JOHANA DEL CARMEN ORDONEZ ALVAREZ
4	538939	DIANA PATRICIA QUEZADA ROJAS
5	554876	LUIS DANIEL SISALIMA SARAGURO
6	521870	MARIANA DOLORES TOAPANTA TERCERO
7	556843	CARMEN DE LA NUBE TOLA COCHANCELA

Figura 21. Almacenamiento información sensible.

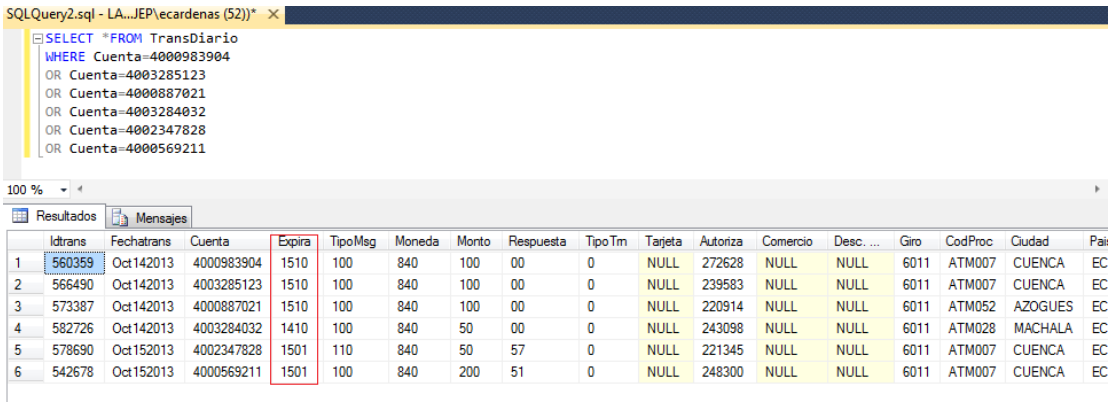


Resultados | Mensajes

	IdLog	Cliente	Seguridad	Pista1	Pista2	Pista3	Discrec
1	569823	JANNETH CECILIA...	464	%B5029161010001713^DURAN/CECILIA ^16042211811...	;5029161010001713=160422118111480000000?	NULL	181110
2	543982	ROGER ALEXAND...	297	%B5029161010001663^IZA QUISHPE/ALEXANDER ^160422...	;5029161010001663=160422115147605000000?	NULL	151470
3	502155	JOHANA DEL CAR...	427	%B5029161010001705^ORDONEZ/JOHANA DEL CARMEN ^16...	;5029161010001705=160422114767135000000?	NULL	147670
4	538939	DIANA PATRICIA ...	256	%B5029161010001630^QUEZADA/PATRICIA ^160422111...	;5029161010001630=160422111632087000000?	NULL	116320
5	554876	LUIS DANIEL SISA...	997	%B5029161010001697^SISALIMA/LUIS DANIEL ^160422114...	;5029161010001697=160422114963667000000?	NULL	149630
6	521870	MARIANA DOLOR...	638	%B5029161010001721^TOAPANTA/DOLORES ^16042211...	;5029161010001721=160422115753749000000?	NULL	157530
7	556843	CARMEN DE LA N...	203	%B5029161010001655^TOLA/CARMEN DE LA NUBE ^160422...	;5029161010001655=160422119815718000000?	NULL	198150

Nota Evidencia: Se verifica que se almacena información sensible del Track1, Track1, Seguridad.

Figura 22. Consulta SQL por Cuenta.



SQLQuery2.sql - LA...JEP\ecardenas (52))*

```
SELECT *FROM TransDiario
WHERE Cuenta=4000983904
OR Cuenta=4003285123
OR Cuenta=4000887021
OR Cuenta=4003284032
OR Cuenta=4002347828
OR Cuenta=4000569211
```

100 %

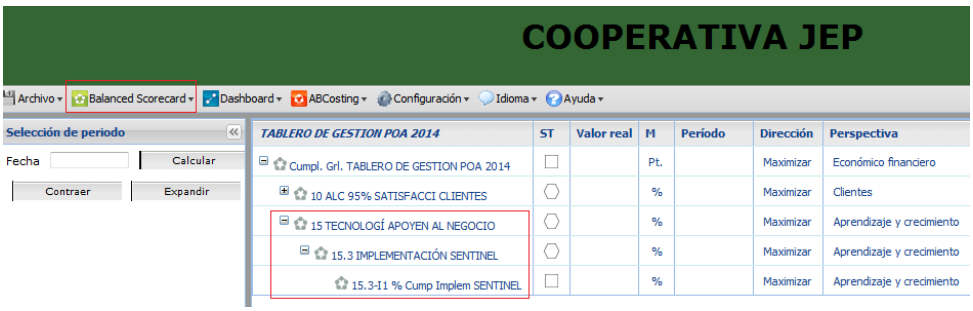
Resultados | Mensajes

	Idtrans	Fechatrans	Cuenta	Expira	TipoMsg	Moneda	Monto	Respuesta	TipoTm	Tarjeta	Autoriza	Comercio	Desc. ...	Giro	CodProc	Ciudad	Pai
1	560359	Oct142013	4000983904	1510	100	840	100	00	0	NULL	272628	NULL	NULL	6011	ATM007	CUENCA	EC
2	566490	Oct142013	4003285123	1510	100	840	100	00	0	NULL	239583	NULL	NULL	6011	ATM007	CUENCA	EC
3	573387	Oct142013	4000887021	1510	100	840	100	00	0	NULL	220914	NULL	NULL	6011	ATM052	AZOGUES	EC
4	582726	Oct142013	4003284032	1410	100	840	50	00	0	NULL	243098	NULL	NULL	6011	ATM028	MACHALA	EC
5	578690	Oct152013	4002347828	1501	110	840	50	57	0	NULL	221345	NULL	NULL	6011	ATM007	CUENCA	EC
6	542678	Oct152013	4000569211	1501	100	840	200	51	0	NULL	248300	NULL	NULL	6011	ATM007	CUENCA	EC

Nota Evidencia: Se seleccionan 6 Cuentas que realizaron retiros de ATM. Se verifica que se almacena la fecha de caducidad.

ME1.3 Método de monitoreo.

Figura 23. Monitoreo Balanced Scorecard en apoyo al negocio.



DS5.11 Intercambio de datos sensitivos.

Figura 24. Acceso a SFTP para verificar operatividad.

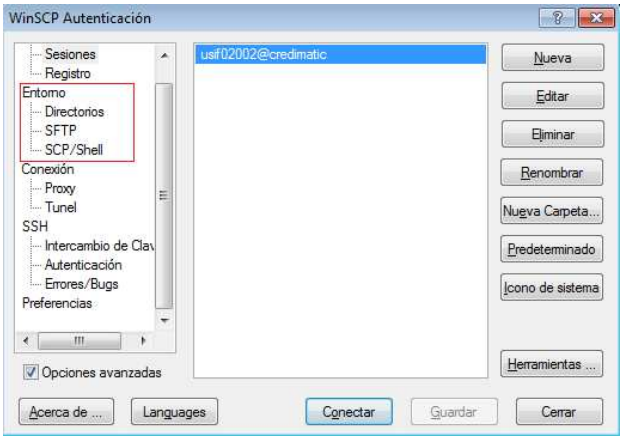
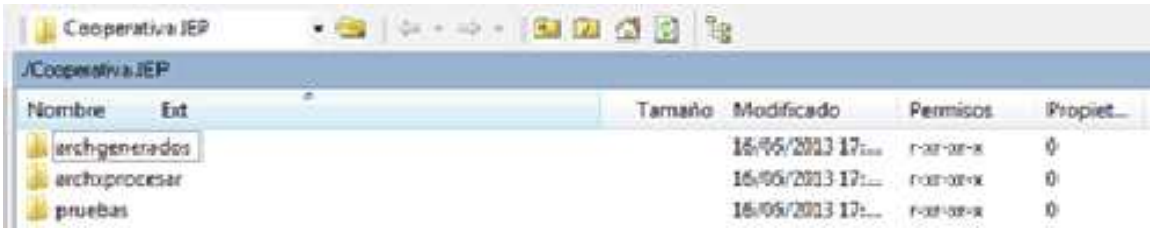


Figura 25. Verificación de carpetas e información de Tarjeta de Débito en SFTP.



DS10.2 Rastreo y resolución de problemas.

Figura 26. Verificación de Administración por Help Desk.

4.9 Modelo Genérico de Madurez.

El Modelo Genérico de Madurez establece los criterios para medir el grado de aplicación de los procesos institucionales a los controles que recomienda COBIT. Los valores de madurez van desde cero hasta cinco de acuerdo a lo que se explica en la siguiente tabla.

Tabla Modelo Genérico de Madurez.

Modelo Genérico del Nivel de Madurez (NM)
0 No Existente- Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.
1 Inicial- Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques *ad hoc* que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.
2 Repetible- Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.
3 Definido- Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.
4 Administrado- Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.
5 Optimizado- Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

4.10 Hallazgos de la Auditoría.

Tabla Hallazgos de la Auditoría.

Dominio	Documentos Requeridos	Hallazgo	N.M
Evidencia PO1.2 Alineación de Ti con el negocio	Plan de capacitaciones. Plan estratégico de negocio. Plan de TI	Se evidencia que la Cooperativa cuenta con un plan de capacitación al usuario, el mismo que se encuentra actualizado al año 2013.	4
Evidencia PO2.3 Esquema de clasificación de datos	Manual general de políticas de gestión de informática y tecnología	Dentro de la Política de Manejo de Información en la Institución, en donde se determina que la información debe ser clasificada en tres niveles, dependiendo de su criticidad, se evidencia que la información no está clasificada como: pública, de uso interno o confidencial en el entorno de tarjeta de débito.	3
Evidencia PO2.4 Administración de la integridad	Proceso de almacenamiento de información electrónica.	Los procesos de almacenamiento seguro se encuentran levantados. Las bases de datos tienen un monitoreo frecuente de su integridad, aunque está a discreción del usuarios realizarlo.	3
Evidencia PO4.6 Roles y responsabilidades	Documento de definición de roles y responsabilidades del personal de TI Plan de capacitación de nuevo personal.	Dentro de los perfiles de cargos del departamento de Recursos Humanos, existen definiciones de perfiles, roles y responsabilidades del personal de TI. Los roles y responsabilidades son transmitidos en el momento de la incorporación y dentro de la etapa de inducción.	4
Evidencia PO4.11 Segregación de funciones	Documento de definición de roles y responsabilidades del personal de TI	Los usuarios tienen asignados perfiles, sin embargo en algunos usuarios los perfiles son demasiado abiertos y no existen segregación de funciones en base a la criticidad de los procesos. Un usuario puede ejecutar varios procesos críticos sin supervisión.	3
Evidencia PO7.3 Asignación de roles	Documento de definición de roles y responsabilidades del personal de TI. Contratos de trabajo.	Se establecen cláusulas de responsabilidad y conductas de ética dentro de los contratos laborales del personal de TI y del departamento de tarjeta de débito.	3

Evidencia PO9.1 Alineación de la administración de riesgos de TI y del negocio	Plan de acción para los riesgos críticos de TI	Existe parcialmente. Se cuenta con un documento de Riesgos Críticos de Administración de TI, sin embargo no se han detallado los procesos críticos del sistema FIT que administran procesan y almacenan información de tarjeta de débito. El documento de Riesgos Críticos de Administración de TI no está en concordancia con los riesgos generales levantados dentro de la Institución.	3
Evidencia PO9.2 Establecimiento del contexto del riesgo	Plan de acción para los riesgos críticos de TI	Ver respuesta anterior.	3
Evidencia PO9.3 Identificación de eventos	Plan de acción para los riesgos críticos de TI	En el documento Riesgos Críticos de Administración de TI identifica de forma general los riesgos asociados a un fallo en los sistemas informáticos, pero no se detallan los impactos asociados a los fallos, así como las consecuencias que pueda tener. Los Logs de IDS,IPS y Firewall son administrados por un oficial de seguridad que hace seguimiento de las alertas.	4
Evidencia PO9.4 Evaluación de riegos	Plan de acción para los riesgos críticos de TI	Se evidencia que no existe evaluación de los riesgos y su probabilidad de impacto utilizando métricas.	1
Evidencia PO9.5 Respuesta a los riesgos	Plan de acción para los riesgos críticos de TI	Existe parcialmente. Se establecen las actividades macro que se deben desarrollar en caso de ocurrencia de un evento, se asignan responsables de la ejecución de los procesos, sin embargo no se especifica la tolerancia al riesgo.	3
Evidencia PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgos	Plan de acción para los riesgos críticos de TI	Se revisa la estabilización de las acciones ejecutadas después de la ocurrencia de un evento mediante un monitoreo del servicio crítico.	5
Evidencia Al1.2 Reporte de análisis de riesgos	Procesos Organizacionales POA Anual	Si existen procesos asociados a los riesgos más críticos de la organización.	5

Evidencia Al3.2 Protección y disponibilidad del recurso de infraestructura	Política – Reglamento de Adquisición y Mantenimiento de la Infraestructura Tecnológica	Dentro del Reglamento de Adquisición de Infraestructura, se tienen contemplados los controles para administrar y auditar los procesos de administración y adquisición de TI, los mismos que son revisados con frecuencia hasta el primer año de funcionamiento.	5
Evidencia Al3.3 Mantenimiento de la infraestructura	Política – Reglamento de Cambios y Desarrollo	Todos los cambios son controlados y administrados por el área de “test”	4
Evidencia Al3.4 Ambiente de prueba de factibilidad	Política – Reglamento de Adquisición y Mantenimiento de la Infraestructura Tecnológica	Todos los cambios realizados a nivel de TI son revisados por un área de “test”, que se encarga de asegurar la existencia de un correcto funcionamiento y aprovechamiento del cambio.	4
Evidencia Al4.1 Plan para soluciones de operación	Reglamento de Operación y Uso de TI	Existen documentos funcionales de aspecto técnico que son proporcionados por los fabricantes, sin embargo no se realiza un análisis de los niveles de servicio que determine oportunamente actuar en la administración de los usuarios.	3
Evidencia Al6.1 Estándares y procedimientos para cambios	Política – Reglamento de Adquisición y Mantenimiento de la Infraestructura Tecnológica	Todos los cambios realizados a nivel de TI son revisados por un área de “test”, que se encarga de asegurar la existencia de un correcto funcionamiento y aprovechamiento del cambio.	4
Evidencia Al6.2 Evaluación de impacto, priorización y autorización	Política – Reglamento de Adquisición y Mantenimiento de la Infraestructura Tecnológica	Si, ver respuesta anterior.	4
Evidencia Al6.3 Cambios de emergencia	Política – Reglamento de Adquisición y Mantenimiento de la Infraestructura Tecnológica	Se encuentran documentados los cambios que se realizan sin pasar por el flujo establecido para revisión, estableciendo los niveles de responsabilidad y autorización.	5
Evidencia Al6.4 Seguimiento y reporte del estatus de cambio	Política – Reglamento de Adquisición y Mantenimiento de la Infraestructura Tecnológica	Todos los cambios realizados a nivel de TI son revisados por un área de “test”, que se encarga de asegurar la existencia de un correcto funcionamiento y aprovechamiento del cambio.	4

Evidencia DS1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio	Política – Reglamento de Soporte de la Infraestructura Tecnológica	Si, los niveles de servicio son monitoreados y se generan reportes para cumplir este propósito, sin embargo en la mayoría de veces no se revisa la información generada por parte del personal responsable. Existen servicios que tienen un valor incremental por encima de lo definido en su creación.	3
Evidencia DS3.2 Capacidad y desempeño actual	Política – Reglamento de Adquisición y Mantenimiento de la Infraestructura Tecnológica	Existen revisiones del desempeño de los recursos de TI, se identifican las posibles debilidades que se puedan presentar como afectación a procesos críticos con el objetivo de mantener los niveles óptimos para la operación.	4
Evidencia DS4.2 Planes de continuidad de TI	Plan de Continuidad y Contingencia de TI	La Institución tiene levantado un plan de continuidad, en donde se establecen los servicios críticos que se deben recuperar en un tiempo determinado. Adicionalmente se tienen establecidos los responsables de ejecutar las tareas de recuperación.	4
Evidencia DS4.3 Recursos críticos de TI	Plan de Continuidad y Contingencia de TI	Si, se establecen los niveles más críticos de la Institución. Los recursos disponibles contingentes son supervisados y generan alerta de fallos.	5
Evidencia DS4.4 Mantenimiento del plan de continuidad de TI	Plan de Continuidad y Contingencia de TI	El plan es revisado con frecuencia semestral para garantizar los cambios que se presenten.	4
Evidencia DS4.8 Recuperación y reanudación de los servicios de Ti	Plan de Continuidad y Contingencia de TI	La Institución tiene levantado un plan de continuidad, en donde se establecen los servicios críticos que se deben recuperar en un tiempo determinado. Adicionalmente se tienen establecidos los responsables de ejecutar las tareas de recuperación. La alta dirección participa del comité de TI, en donde se aprueba el plan de contingencia.	5
Evidencia DS4.9 Almacenamiento de respaldos fuera de las instalaciones	Plan de Continuidad y Contingencia de TI	Si, tanto el sitio alterno, como los datos de respaldo se encuentran en una ciudad diferente al sitio principal.	5

Evidencia DS5.1 Administración de la seguridad de TI	Plan de Continuidad y Contingencia de TI	Los servicios críticos para el funcionamiento del negocio se encuentran detallados en el Plan de Continuidad.	5
Evidencia DS5.2 Plan de seguridad de TI	Política de Seguridad de TI	Si, se encuentran documentadas las políticas de seguridad de TI, se mantienen con control de versiones y de cambios. Las principales políticas son difundidas a los empleados por diferentes medios, siendo los principales el correo electrónico y la Intranet institucional.	5
Evidencia DS5.3 Administración de identidad	Política de Seguridad de TI	Las contraseñas de los usuarios son administradas por el Active Directory, las contraseñas son solicitadas cambio cada tres meses.	5
Evidencia DS5.4 Administración de cuentas del usuario	Política de Seguridad de TI	Los usuarios y claves de empleados nuevos son creados por Talento Humano con petición del área donde labora, con informe de TI. Los procedimientos son generales para visitantes y personal interno. Los usuarios son revisados periódicamente dentro de los planes de auditoría interna.	5
Evidencia DS5.7 Protección de la tecnología de seguridad	Política de Seguridad de TI	La Institución tiene implementados Firewall, IDS, IPS que detienen el tráfico no deseado y los intrusos a la red. No divulgan información sensible, sus puertos se encuentran cerrados.	5
Evidencia DS5.8 Administración de llaves criptográficas	Política de Seguridad de TI	En el módulo FIT de generación de llaves informáticas se puede evidenciar que la generación se la realiza por medio de software, es decir por programación. Con estas llaves se generan tarjetas, PIN o claves de tarjetas, se transmite información para ATMs. La Cooperativa tiene adquirido un módulo “Atalla” adquirida hace un año, pero no se encuentra en producción. Las llaves cumplen con el estándar 3DES.	2

Evidencia DS5.9 Prevención, detección y corrección de software malicioso	Política de Seguridad de TI	Existen instalados y configurados programas antivirus en todos los segmentos de red, los antivirus analizan en tiempo real todo tipo de amenazas. Se evidenció que en varios usuarios el antivirus está desactualizada y no existe reporte de esos eventos. El Firewall impide la descarga de programas desde el Internet.	3
Evidencia DS5.10 Seguridad de la red	Política de Seguridad de TI	Existe una red de equipos configurada con firewalls, pero no está segmentada por departamentos con nivel de criticidad. Los puertos se encuentran cerrados a excepción de los puertos 80 y 443. Las conexiones a estos puertos por medio de Telnet son rechazadas por la red. Las conexiones a los aplicativos web tienen seguridad SSL. Existen contraseñas en bases de datos y servidores que son usadas por defecto, utilizando la contraseña del fabricante.	3
Evidencia DS5.11 Intercambio de datos sensitivos	Política de Seguridad de TI	Dentro de la política de transmisión de datos se ha estipulado que los datos sensitivos debe transmitirse por medios seguros como SFTP, sin embargo se evidencia que información de tarjeta de débito son transmitidos entre los usuarios de forma insegura, como la utilización del correo o la copia a discos externos. Existe un lector de banda magnética que permite leer la banda de las tarjetas generadas, se puede visualizar el track1 y track2 en claro, incluso se puede copiar o editar la información.	2
Evidencia DS10.2 Rastreo y resolución de problemas	Política de Seguridad de TI	Los casos son administrados por el Help Desk, aunque varios de ellos se procesan directo con el usuario debido a la urgencia o criticidad.	4
Evidencia DS10.3 Cierre de problemas	Política de Seguridad de TI	Si existen procedimientos establecidos para cerrar los casos de incidentes que se presenten. Se ejecutan en el Help Desk.	5

Evidencia DS11.1 Requerimientos del negocio para administración de datos	Política de Seguridad de TI	La información que recibe el negocio son procesados de acuerdo a lo requerido. Los niveles de servicio están garantizados por su alta disponibilidad. Están documentados los procedimientos mediante los cuales el negocio puede solicitar información a TI. El procedimiento se cumple satisfactoriamente.	5
Evidencia DS11.2 Acuerdos de almacenamiento y conservación	Política de Seguridad de TI	La información que se almacena, se encuentra en bases de datos con contraseñas y existen administradores encargados de verificar los accesos a la información.	4
Evidencia DS11.3 Sistema de administración de librerías de medios	Política de Seguridad de TI	Están definidos los procedimientos para el manejo de inventario, el mismo que se está cumpliendo de forma satisfactoria.	4
Evidencia DS11.4 Eliminación	Política de Seguridad de TI	Cuando se realizan las transacciones con tarjeta de débito, el sistema informático almacena el track1 y track2 en claro en la base de datos. No se tiene conocimiento sobre la retención de los datos de tarjeta, donde se especifique el periodo y el método de destrucción y/o resguardo. No se tiene un política / procedimiento que soporte el manejo adecuado de la información sensible de tarjetas de débito. No existe una justificación por escrito que esté aprobada por los responsables designados de salvaguardar la seguridad de la información. Los datos sensibles que se están almacenando en bases de datos y medios impresos son: *PIN *PAN * Fecha de expiración La clave de cajero se puede ver en claro por pantalla. No se tiene un esquema definido para encriptar la información de tarjeta. No se utiliza cifrado de disco duro dentro del ambiente	0

		de tarjetas. La información de tarjetas de débito almacenadas en el aplicativo puede ser copiado al disco duro o a un medio extraíble Los usuarios tienen restricción en el uso de dispositivos de almacenamiento externo, sin embargo varios de ellos han obtenido el permiso correspondiente del área de tecnología.	
Evidencia DS11.5 Respaldo y restauración	Política de Seguridad de TI	La Institución tiene levantado un plan de continuidad, en donde se establecen los servicios críticos que se deben recuperar en un tiempo determinado. Adicionalmente se tienen establecidos los responsables de ejecutar las tareas de recuperación. La alta dirección participa del comité de TI, en donde se aprueba el plan de contingencia.	5
Evidencia DS11.6 Requerimientos de seguridad para la administración de datos	Política de Seguridad de TI	En el documento Política de Seguridad la información se clasifica por niveles, sin embargo los usuarios mantiene información que está clasificada como: pública, de uso interno o confidencial. Los documentos que se generan en papel son almacenados en un cancel con protección de llaves, sin embargo la destrucción no se realiza mediante una política que determine tiempos, custodios y metodología de destrucción. Las tarjetas de débito anuladas o canceladas son guardadas en el escritorio de los usuarios por un tiempo indeterminado, muchas veces no se destruye el plástico, guardándose íntegro el plástico. Varios usuarios sin nivel de supervisor o jefe, tiene la posibilidad de duplicar una tarjeta de débito inmediatamente después de que se generó la primera, esto se da cuando existen errores en la primera tarjeta.	3
Evidencia DS12.2 Medidas de seguridad física	Política de Seguridad de TI	El espacio físico del área de tarjeta de débito no tiene delimitados los accesos que sean restringidos o permitidos a los usuarios. Los usuarios de cualquier área ajena pueden ingresar al área de grabación de tarjetas, sin requerir autorización de un jefe o supervisor.	2

Evidencia DS12.3 Acceso Físico	Política de Seguridad de TI	Los usuarios pueden ingresar al centro de grabación o personalización con carteras, celulares, maletas, sin que exista restricción	2
Evidencia ME1.2 Definición y recolección de datos de monitoreo	POA anual.	Si, los objetivos de TI son levantados cada año con relación a la estrategia del negocio. Existen indicadores que se reportan de forma mensual y trimestral, se lo registra por medio del Balanced Scorecard.	4
Evidencia ME1.3 Método de monitoreo	POA anual.	Si, se lo realiza por medio del Balanced Scorecard de forma oportuna.	5
Evidencia ME1.4 Evaluación del desempeño	POA anual.	Si, se lo realiza por medio del Balanced Scorecard de forma oportuna.	5
Evidencia ME1.5 Reportes al consejo directivo y a ejecutivos	POA anual.	Si, se lo realiza por medio del Balanced Scorecard.	5
Evidencia ME1.6 Acciones correctivas	POA anual.	Si, se lo realiza por medio del Balanced Scorecard. Las responsabilidades están establecidas con los dueños de los procesos. El seguimiento se lo realiza por medio del Balanced Scorecard.	5
Evidencia ME2.2 Revisiones de auditoría	Reglamento interno de auditoría.	Existen revisiones periódicas de auditoría para evaluar los controles internos, sin embargo no existe frecuencia o continuidad en las revisiones.	3
Evidencia ME2.3 Excepciones de control	Reglamento interno de auditoría.	Si están identificadas las excepciones. Las excepciones de control son elevadas hasta la dirección correspondiente.	4
Evidencia ME2.4 Auto-evaluación de control	Reglamento interno de auditoría.	No existe un control de autoevaluación, las revisiones se limitan a las auditorías internas o externas.	2
Evidencia ME2.7 Acciones correctivas	Reglamento interno de auditoría.	Si, las acciones correctivas entrar a un proceso de revisión y se realiza el seguimiento hasta el cierre de las novedades.	5

Evidencia ME3.1 Identificar las leyes y regulaciones con impacto potencial sobre TI	Actas comité de TI.	Existe establecido un comité de TI y la alta gerencia en donde se revisan las leyes locales, normativas vigentes, etc. y el impacto que estas tienen sobre TI.	5
Evidencia ME3.2 Optimizar la respuesta a requerimientos externos	Actas comité de TI.	El comité de TI y la alta gerencia son los encargados de realizar la planificación de los cambios y la actualización de las políticas internas.	5
Evidencia ME3.3 Evaluación del cumplimiento con requerimientos externos	Actas comité de TI.	El comité es el encargado de realizar la planificación de los cambios y la actualización de las políticas internas.	5
Evidencia ME3.4 Aseguramiento positivo del cumplimiento	Actas comité de TI.	El comité es el encargado de realizar la planificación de los cambios y la actualización de las políticas internas.	5
Evidencia ME4.2 Alineamiento estratégico	Actas comité de TI.	Se realiza un trabajo en conjunto, todos los cambios estratégicos son aprobados por la alta gerencia y los respectivos consejos. Existe la recomendación de TI sobre las mejores prácticas a implementar. La responsabilidad es compartida entre la alta dirección y TI.	5
Evidencia ME4.5 Administración de riesgos	Actas comité de TI.	Se realiza un trabajo conjunto, todos los cambios estratégicos son aprobados por la alta gerencia y los respectivos consejos.	5
Evidencia ME4.6 Medición del desempeño	Actas comité de TI.	La unidad de TI tiene una estructura propia en independiente, es decir, no está subordinada a otra área y su línea de reporte es a la alta gerencia.	5

4.11 Informe de resultados de la Auditoría Informática.

Informe de Auditoría Informática orientada a los procesos críticos de tarjeta de débito generados en la Cooperativa de Ahorro y Crédito "JEP" aplicando el marco de trabajo COBIT.

El presente informe es entregado a la Gerencia General, Gerencia de Tecnología y Gerencia de Operaciones en la reunión de entrega de los resultados del proceso de auditoría.

En el informe se detallan los resultados obtenidos una vez concluida la etapa de revisión de los procesos y entorno de tecnología del área de Tarjeta de Débito dentro de la Cooperativa "Juventud Ecuatoriana Progresista Ltda."

El informe consta de los siguientes puntos:

- Análisis General de los Hallazgos.
- Análisis del Nivel de Madurez Institucional.
- Nivel de Madurez Institucional.
- Recomendaciones de Auditoría.
- Definición de Oportunidades de Mejora.

4.11.1 Análisis General de los Hallazgos.

En el documento Tabla de Hallazgos de la Auditoría que se entrega como un Anexo a este informe, se detallan los controles que se han revisado, los cuestionarios que se aplicaron en el ejercicio de la auditoría, los documentos de respaldo que se solicitaron como soporte de los criterios enunciados por los usuarios participantes del ejercicio de auditoría. Adicional, se incluyen en el documento los hallazgos que se fueron evidenciando en cada dominio que se aplicó al entorno del área de Tarjeta de Débito.

4.11.2 Análisis del Nivel de Madurez Institucional.

Se establecen que los dominios ME con 4,56 y AI con 4,22 puntos obtenidos de un total de 5 puntos en la valoración del cumplimientos de los dominios de control, tienen un modelo de

madurez alto, pues evidencian un fuerte trabajo en la orientación a los controles, el involucramiento de la alta gerencia y la orientación al negocio.

Los procesos dentro de los controles ME y AI se consideran según COBIT como administrados, son procesos que se pueden monitorear y medir el nivel de cumplimiento dentro de la Cooperativa, estos procesos están bajo un enfoque de mejora continua y proporcionan buenas prácticas.

Sin embargo dentro de los controles ME y AI también existen dominios que están por debajo de 4 puntos (ver Matriz de Hallazgos), los cuales son analizados más adelante en la Tabla Definición de Oportunidades de Mejora.

Los dominios PO con 3,25 y DS con 3,66 puntos obtenidos de un total de 5 puntos tienen un esquema de madurez bajo, estos procesos los considera COBIT como definidos, se han estandarizado y documentado, se han dado a conocer pero es el usuario el que administra la ejecución del proceso, por lo que es poco probable su fiel cumplimiento y su detección en caso de que existan desviaciones.

Los dominios PO y DS requieren el mayor esfuerzo en el cumplimiento de las recomendaciones establecidas en la Tabla Definición de Oportunidades de Mejora.

El promedio institucional de madurez de los dominios de control es 3,90 que según

4.11.3 Nivel de Madurez Institucional.

A nivel institucional se obtiene un total de 3,92 puntos de 5 esperados. Se evidencia la existencia de oportunidades de mejora sobre los procesos de tal manera que tengan una orientación a los dominios definidos por COBIT como óptimos.

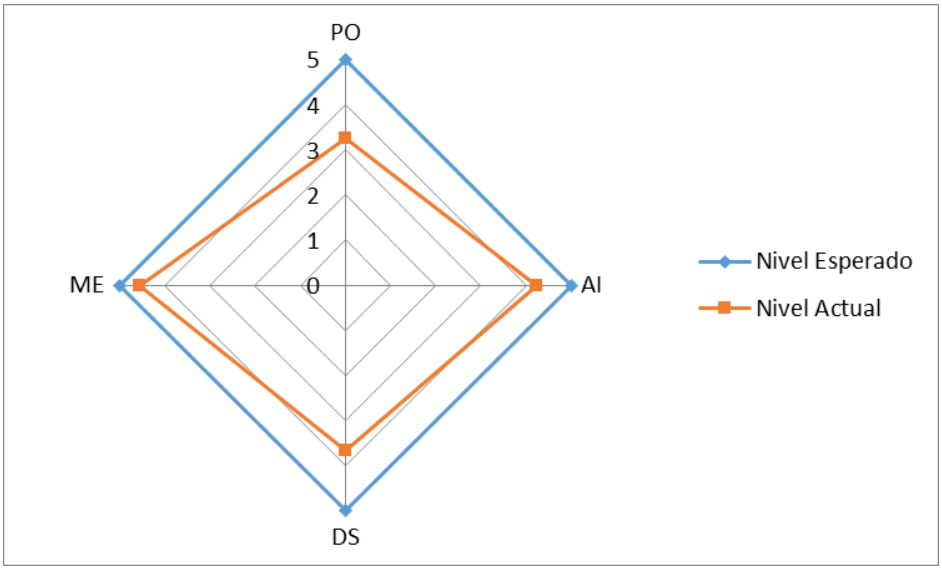
COBIT define a este nivel de madurez como Definido se han estandarizado y documentado, se han dado a conocer pero es el usuario el que administra la ejecución del proceso, por lo que es poco probable su fiel cumplimiento y su detección en caso de que existan desviaciones.

Las oportunidades de mejora se detallan en la Tabla Definición de Oportunidades de Mejora.

Tabla Nivel de Madurez Institucional.

	Madurez	
Dominio	**Esperado**	**Actual**
PO	5	3,25
AI	5	4,22
DS	5	3,66
ME	5	4,56
Promedio Institucional	**5**	**3,92**

Gráfico Nivel de Madurez Institucional.



4.12 Recomendaciones de Auditoría.

Existen controles dentro de la Cooperativa en diferentes dominios (ver Tabla de Hallazgos) que se encuentran con un nivel de madurez entre 4 y 5 puntos, se consideran controles maduros y que brindan seguridad a los procesos que administran.

Se recomienda sobre los controles que tienen entre 4 y 5 puntos mantener una revisión constante a través de auditorías informáticas que permitan evidenciar posibles problemas o deterioro de los controles, a fin de tomar las medidas que sean pertinentes para mantener los niveles ya alcanzados a la fecha.

Sobre los controles que tienen entre 0 y 4 puntos se recomienda aplicar las oportunidades de mejora que se definen en la Tabla de Definición de Oportunidades de Mejora, en donde se han identificado las mejores prácticas recomendadas por COBIT para la administración de los controles de TI y recomendaciones de las mejores prácticas en medios de pago como tarjeta de débito. Las recomendaciones están clasificadas por cada Evidencia de Dominio que originó la revisión, adicionalmente se establecen tiempos de implementación recomendados para ejecutar los cambios y las mejoras a los controles.

4.13 Oportunidades de Mejora.

Tabla de Definición de Oportunidades de Mejora.

Evidencia de Dominio	Recomendación	Tiempo Ejecución (meses)
Evidencia PO2.3 Esquema de clasificación de datos	Implementar un procedimiento que establezca con claridad los dueños de la información, los custodios de la información y un método efectivo de clasificación de la información por cada nivel de criticidad que se ha establecido. El procedimiento debe además contener planes de medición con objetivos cuantificables que permitan medir la efectividad del trabajo, así como también evidenciar y plantear una mejora continua sobre la clasificación y custodia de la información.	4
Evidencia PO2.4 Administración de la integridad	Establecer procedimientos de revisiones periódicas para asegurar que se realicen las tareas de administración de integridad.	2
Evidencia PO4.11 Segregación de funciones	Dentro de la política de asignación de perfiles, se debe añadir la observación que los usuarios no tengan perfiles demasiado abiertos o que puedan tener capacidad de ejecutar tareas sensibles sin segregación de funciones.	4

	Adicionalmente la política debe incluir procedimientos para auditar y revisar los perfiles que se van asignando a un usuario, incluyendo revisiones de perfiles temporales o por reemplazos.	
Evidencia PO7.3 Asignación de roles	Se recomienda realizar una mejora al módulo FIT que permite generar usuarios con perfiles críticos, con el objetivo de que existan alertas y logs de auditoría que sean enviadas de forma automática a un supervisor o jefe, así mismo se deben establecer por escrito las responsabilidades del usuario.	5
Evidencia PO9.1 Alineación de la administración de riesgos de TI y del negocio	Se recomienda modificar el documento de Riesgos Críticos de Administración de TI que incluyan información particular de tarjeta de débito, en los módulos en los que se transmita, almacene o procese dicha información, estableciendo en qué casos se puede guardar información sensible y que niveles de revisión y auditoría aplican. Los riesgos institucionales deben identificar claramente los riesgos y el trato que se debe dar a tarjeta de débito.	3
Evidencia PO9.2 Establecimiento del contexto del riesgo	Ver recomendación anterior.	4
Evidencia PO9.4 Evaluación de riegos	Establecer indicadores y métricas en el Balaced Scorecard sobre el riesgo de ocurrencia y los impactos asociados en los procesos de tarjeta de débito.	4
Evidencia PO9.5 Respuesta a los riesgos	Dentro de los procesos de tarjeta de débito se debe especificar la tolerancia al riesgo, de tal manera que en caso de ocurrencia se minimice la incertidumbre de pérdida financiera o de reputación.	3
Evidencia Al4.1 Plan para soluciones de operación	Elaborar documentos funcionales de la Institución, que tengan un lenguaje claro sobre cómo deben actuar los administradores en caso de ocurrencia de un evento de fallo de cualquier sistema informático.	4

Evidencia DS1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio	Establecer un procedimiento que permita revisar los reportes, alertas y logs que generan los sistemas sobre su rendimiento, de tal manera que se puedan generar alertas tempranas de ocurrencia de un evento.	3
Evidencia DS5.8 Administración de llaves criptográficas	Generar un plan de migración efectivo de las llaves informáticas para que sean generados por un módulo de hardware “Atalla”. Establecer procedimientos seguros sobre la generación, los custodios, el almacenamiento de componentes y criptogramas.	6
Evidencia DS5.9 Prevención, detección y corrección de software malicioso	Configurar el software antivirus para que genere alertas sobre eventos de desconfiguración o desactualización de bases de datos. Las alertas deben ser administradas por un nivel supervisor y generar reportes de seguimiento y eliminación de las novedades.	4
Evidencia DS5.10 Seguridad de la red.	Se recomienda crear un segmento de red exclusivo para equipos de administración y usuarios que procesen, transmiten o almacenen información de tarjeta de débito, el segmento de red debe tener configurados firewalls tanto de entrada como de salida, así también deben establecerse permisos de conexión externa para cada usuario dependiendo de sus funciones. El segmento de red debe ser evaluado periódicamente para evidenciar vulnerabilidades o cambios no autorizados. Generar un procedimiento que regule el uso de contraseñas por defecto en la configuración de equipos de red. Establecer un programa de auditoría frecuente.	6
Evidencia DS5.11 Intercambio de datos sensitivos	Configurar restricciones a nivel de usuario, de tal manera que no se permita la copia de información en medios externos, salvo que exista la debida justificación, en cuyo caso se deberá contar con medios de almacenamiento externo proporcionados por la Institución, los mismos que deben tener un control de inventario, así como también revisiones periódicas sobre su utilización. Los medios de almacenamiento externo deben tener procedimientos seguros de cifrado de información. Eliminar los dispositivos que permitan leer información de la banda magnética, track1 y track2 y establecer por escrito la prohibición de utilizar dispositivos que lean, reproduzcan o graben bandas magnéticas.	4

Evidencia DS11.4 Eliminación	Establecer una política o procedimiento sobre el manejo adecuado de la información sensible de tarjeta de débito, en la misma deben constar las excepciones bajo las cuales se puede almacenar información sensible con sus respectivos niveles de aprobación. Establecer una política institucional que norme el almacenamiento de PIN (clave personal del cliente para transacciones de ATM), el PAN (número de tarjeta) y la fecha de expiración. La política debe contener las bases en las que el negocio requiere justificadamente el almacenamiento de esta información. Las excepciones puede almacenarse en texto claro cuando el negocio lo solicite por excepción, en los casos en que no exista justificación la información deberá almacenarse de forma truncada, de tal manera que no exista la posibilidad de ver el texto en claro directamente. Se deben realizar cambios de programación en el FIT y en las bases de datos que permitan truncar la información del PIN, PAN y Fecha de Caducidad. Los cambios se deben aplicar a todos los módulos y canales en donde se almacene, transmita y guarde la información. Se debe generar un procedimiento institucional que permita cifrar los discos de los servidores y de los computadores personales que almacenen la información de tarjeta de débito.	8
Evidencia DS11.6 Requerimientos de seguridad para la administración de datos	Se recomienda modificar el documento de Riesgos Críticos de Administración de TI que incluyan información particular de tarjeta de débito, en los módulos en los que se transmita, almacene o procese dicha información, estableciendo en qué casos se puede guardar información sensible y que niveles de revisión y auditoría aplican. Se recomienda que existan establecidos tiempos máximos de custodia de la información impresa en papel y se debe establecer un método seguro de destrucción. Las tarjetas de débito anuladas o canceladas deben tener un trato similar a un documento valorado, su custodia debe ser en caja de seguridad y se debe establecer un método seguro de destrucción. Se recomienda realizar una mejora al módulo FIT que permite generar tarjetas duplicadas, con el objetivo de que existan alertas y logs de auditoría que sean enviadas de forma automática a un supervisor o jefe, así mismo se deben establecer por escrito las revisiones y el trato que se deben dar a estas alertas. Es importante implementar cambios en la programación del sistema	10

	FIT en los módulos de tarjeta de débito, a fin de evitar totalmente el almacenamiento del Track1 y Track2 debido a que es información altamente sensible que podría ser utilizada para la duplicación no autorizada de una tarjeta de débito. Los cambios se deben aplicar a todos los módulos y canales en donde se almacene, transmita y guarde la información.	
Evidencia DS12.2 Medidas de seguridad física	Deben establecerse restricciones señalizadas a las áreas críticas de tarjeta de débito y su acceso físico debe ser por un medio de ingreso biométrico. Se deben diseñar bitácoras de ingreso de personal invitado.	4
Evidencia DS12.3 Acceso Físico	Establecer restricciones claras sobre el ingreso de carteras, celulares, maletas al centro de personalización o grabación de tarjeta de débito. El procedimiento debe establecer niveles de responsabilidad y deben crearse reportes de auditoría frecuentes.	2
Evidencia ME2.2 Revisiones de auditoría	Las revisiones de auditoría deben tener un cronograma aprobado por la alta gerencia, en donde se establezcan periodos de revisión, entrega de informes y seguimiento de las actividades relacionadas con la revisión.	3
Evidencia ME2.4 Auto-evaluación de control	Establecer procedimientos que permitan realizar una autoevaluación o auditorías internas en los procesos de tarjeta de débito.	2

4.14 Conclusiones y Recomendaciones.

Conclusiones.

Una vez finalizado en proceso de Auditoría, se ha podido determinar que utilizando el marco teórico COBIT con sus dominios propuestos, así como también observando el enfoque de negocios institucional de la Cooperativa JEP, existen procesos que muestran diferentes tipos de debilidades y riesgos que han sido valorados. Para minimizar las amenazas y los

riesgos se han clasificado en el documento Definiciones de Oportunidad de Mejora que además contiene las recomendaciones que permitirán administrar los riesgos, este documento ha sido entregado a los Directivos de la Cooperativa JEP en la reunión de clausura de acuerdo al Plan de Auditoría.

Se estableció que para una Auditoría Informática es indispensable contar con un como un marco de trabajo que sirva como una guía en el proceso, se determinó que el marco de trabajo del Modelo COBIT desarrollado por ISACA es apropiado para cumplir con estos objetivos, pues busca establecer controles informáticos manteniendo una constante relación con el negocio y sus objetivos, así como también, mantiene un enfoque de procesos.

Durante el análisis de las tareas que se ejecutan, se pudo determinar la criticidad de varios procesos, así como también aspectos de la infraestructura tecnológica que presentaron observaciones, la revisión incluyó observaciones y recomendaciones que permitirán a la Cooperativa mantener el enfoque de negocio, observando la normativa vigente emitida por las entidades de control, en un entorno de trabajo más seguro.

De la revisión de la infraestructura tecnológica, se determinó el nivel de eficacia y eficiencia de los sistemas informáticos que intervienen en los procesos de tarjeta de débito, emitiendo recomendaciones que permitirán que la información almacenada cuente con niveles de seguridad y disponibilidad.

Se estableció que la información de tarjeta de débito constituye uno de los principales activos que mantiene la Cooperativa JEP, estableciéndose recomendaciones para que la administración de la información sensible en todas sus etapas cuente con estándares de seguridad.

Se determina importante mantener un cronograma de auditorías periódico, con revisiones programadas y equipos de trabajo conformados además de responsabilidades establecidas de acuerdo al rol y perfil de cada funcionario.

Recomendaciones.

Se recomienda a la alta gerencia implementar las mejoras recomendadas en el Informe de Auditoría y la Tabla Oportunidades de Mejora de acuerdo a los tiempos establecidos en dicho documento.

Es recomendable se conforme una comisión de alto nivel que realice el seguimiento, coordine y verifique la implantación de las mejoras propuestas.

BIBLIOGRFÍA

Echenique José, Auditoría en Informática, 2006, México, McGraw-Hill

Piattini M. y Del Peso E. (2007). Auditoría Informática, un enfoque práctico. México

COBIT,https://www.isaca.org/Pages/default.aspx?cid=1002083&Appeal=Google&gclid=CP63npqsibsCFSvl7AodlVQAcg

http://www.pergaminovirtual.com.ar/definicion/Base_de_datos.html

http://arm-net.com.ar/es/glosario.html

Lengua Española, Diccionario Real Academia WEB, http://rae.es/

http://www.itil-officialsite.com/

http://www.coso.org/

http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica

DICCIONARIO DE INFORMÁTICA Y TECNOLOGÍA,
http://www.alegsa.com.ar/Dic/vulnerabilidad

ANEXOS

Anexo I

GLOSARIO

Balances. Son los resultados de un ejercicio financiero en un determinado período de tiempo. Reflejan la situación financiera de la institución determinando si el ejercicio tuvo ganancia o pérdida monetaria.

Amenaza. Es un factor interno o externo que puede afectar el normal funcionamiento de una institución.

Riesgo. Es la probabilidad de que una amenaza se realice o se ejecute, por consiguiente se considera que el riesgo en una institución financiera se debe administrar con el objetivo de eliminarlo o minimizarlo.

Proceso financiero. Es un conjunto de actividades y tareas que busca cumplir una determinada tarea.

Evaluar el riesgo. Consiste en determinar mediante normas, indicadores, etc. la criticidad con la que se deben clasificar los riesgos y de esta manera establecer los controles que permitan su mitigación.

Minimizar el riesgo. Se entiende como minimizar, el acto de reducir a la mínima expresión posible ocurrencia de un riesgo.

Auditoría informática. La Auditoría Informática hace referencia a la revisión y evaluación de los diferentes niveles del ámbito de la tecnología, pero además busca determinar la eficacia y eficiencia de los mismos.

Campo de la Auditoría Informática. La Auditoría Informática está presente en los diferentes entornos en los que la tecnología de la información tiene su ámbito de desarrollo.

Seguridad. La seguridad está relacionada con mantener a salvo a las personas o a las cosas. Cuando estos presentan riesgo de sufrir algún tipo de daño, se dice que es una circunstancia insegura.

Seguridad de la Información. Tiene que ver con mantener segura la información de una institución, considerada como un activo muy valioso para el desarrollo del negocio.

Hacker. Es un individuo que vulnera los accesos de sistemas o plataformas a los que no tiene autorización de ingresar, con estas acciones pueden buscar desde notoriedad hasta beneficio económico fruto del fraude.

COBIT. Es un acrónimo para Control Objetives for Information and related Technology (Objetivos de Control para tecnología de la información y relacionada); desarrollada por la Information Systems Audit and Control Association (ISACA) y el IT Governance Institute (ITGI).

COBIT es una metodología aceptada mundialmente para el adecuado control de proyectos de tecnología, los flujos de información y los riesgos que éstas implican. La metodología COBIT se utiliza para planear, implementar, controlar y evaluar el gobierno sobre TI; incorporando objetivos de control, directivas de auditoría, medidas de rendimiento y resultados, factores críticos de éxito y modelos de madurez.

Intrusión. Acceso no autorizado y anónimo a cualquier sistema informático.

Configuración de redes con seguridad. Consiste en conectar varios dispositivos tecnológicos y computadores que permitan a los usuarios trabajar en un mismo entorno, con privilegios y control sobre las actividades que ejecutan. Esta conectividad debe tener niveles de seguridad que permitan resguardar la información y los sistemas.

Configuración de bases de datos con seguridad. Las bases de datos almacenan la información de una institución, siendo muy importante establecer seguridades tanto en la configuración como en la administración

Administración de usuarios. Establecer parámetros en los cuales los usuarios tendrán la posibilidad de desarrollar sus actividades dependiendo de sus roles y responsabilidades que se representan en los perfiles.

Anexo II

Formato de Encuesta Preliminar.

Encuesta Sobre el Manejo de Procesos con Tarjeta de Débito
En la Cooperativa "JEP"

Esta encuesta busca conocer con detalle la forma en la que se realizan los procesos de Tarjeta de Débito dentro de la Cooperativa JEP.

Tiempo aproximado 5 minutos. Por favor conteste con la mayor sinceridad posible.

Cargo Actual: _____ Tiempo de Trabajo en la JEP: _____

Preguntas:

1 Describa brevemente cuatro actividades principales que Usted realice a diario:

a) _____
b) _____
c) _____
d) _____

2 Marque la respuesta que más se acerque a su criterio:

2.1 ¿Tiene Usted conocimiento del contenido la Política de Seguridad de la Información con relación a Tarjeta de Débito?:

SI _____ NO _____

2.2 El proceso de generación (crear) de tarjetas de débito en la empresa es:

a) Irrelevante
b) Poco Importante
c) Importante
d) Muy Importante

2.3 ¿Cómo clasificaría Usted la información del proceso de creación de tarjetas de débito?:

a) Uso Público
b) Uso Interno
c) Confidencial

2.4 ¿Con qué frecuencia en el último año ha recibido la visita de un Departamento de Control (Auditoría, Procesos, etc.)?.

a) Ninguna
b) Una o dos veces
c) Tres a Cinco
d) Más de ocho.

3 Escoja la opción que corresponda a su respuesta.

3.1 ¿Sus usuarios y claves de acceso al Sistema Informático son de uso exclusivo?

SI: _____ NO: _____

3.2 ¿El Sistema le solicita cambios de clave frecuentes?

SI: _____ NO: _____

3.3 ¿Tiene su puesto de trabajo (computadora) acceso a conectar, discos extraíbles externos o algún medio de almacenamiento (USB)?

SI: _____ NO: _____

3.4 ¿Si existe algún error en la creación de la tarjeta es posible visualizar la clave de la tarjeta y crear otra?

¿Sabe usted si la clave de la tarjeta Es posible visualizar la clave de la tarjeta una vez que se generó la misma?

SI: _____ NO: _____

3.5 ¿Puede su usuario activar la tarjeta en el Sistema Informático?

SI: _____ NO: _____

3.6 ¿Puede su usuario generar nuevamente una tarjeta después de que está ya se generó?

SI: _____ NO: _____

Si, su respuesta anterior fue SI, por favor responda brevemente. En qué casos una tarjeta puede volverse a grabar:

_____

_____

3.7 ¿Las transacciones realizadas (débitos bancarios) por el Socio pueden ser reversadas en el Sistema Informático?

SI: _____ NO: _____

3.8 ¿Las transacciones que realiza un socio pueden ser visualizados por su usuario?

SI: _____ NO: _____

4 Por favor responda las siguientes preguntas con una breve explicación:

4.1 Describa brevemente su ambiente laboral, la relación con sus compañeros y jefes.

_____

_____

_____

4.2 Consideraría un cambio de trabajo a otra Institución con el mismo cargo y sueldo que el que tiene actualmente, explique su respuesta.

_____

_____

¡Muchas gracias por su participación!.