ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

EVALUACIÓN DE LA GESTIÓN INFORMÁTICA DE LA UNIDAD DE TI DE LA COOPERATIVA DE AHORRO Y CRÉDITO "TEXTIL 14 DE MARZO" USANDO COBIT 4.1.

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

ANASI SUNTASIG KARINA ISABEL
k4ry24@gmail.com

PASPUEL MORALES PAULINA TATIANA
paupaspuel@gmail.com

Director: ING. JAIME FABIÁN NARANJO ANDA
jaime.naranjo@epn.edu.ec

Quito, Junio 2013

DECLARACIÓN

Nosotras, Karina Isabel Anasi Suntasig y Paulina Tatiana Paspuel Morales, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la siguiente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, La Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Karina Isabel Anasi Suntasig

Paulina Tatiana Paspuel Morales

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Karina Isabel Anasi Suntasig y Paulina Tatiana Paspuel Morales, bajo mi supervisión.

Ing. Jaime Naranjo

DIRECTOR DE PROYECTO

AGRADECIMIENTOS

A Dios por cada día de vida que nos da, por cada nueva oportunidad que nos pone en frente, por cada lección aprendida que nos fortalece y ayuda a crecer como persona y profesionalmente.

A mi Papi y a mi Mami que han hecho lo posible por darme una buena educación siendo el apoyo incondicional a lo largo de toda mi vida, por el cariño, protección y amor brindado y sobre todo por los regaños que en su momento fueron necesarios. Gracias infinitas porque sin ustedes no hubiera logrado alcanzar este objetivo.

A los profesores de Ingeniería en Sistemas que han contribuido a mi formación profesional.

A mi compañera de tesis Paulina que durante toda la carrera universitaria a más de ser una compañera en aspectos académicos se ha convertido en una de mis grandes amigas, y con quien hemos conseguido adquirir la tan esperada meta después de todo este tiempo de dedicación y esfuerzo, gracias Pau.

A mis amigas del colegio, con quienes aún conservo una gran amistad y cuyos consejos siempre me han servido de mucho, en especial a Andy y Lu.

Al tutor por ayudarnos con sus conocimientos en la realización de este trabajo, por las correcciones y recomendaciones que nos sirvieron de mucho.

A la Empresa que contribuyó a la finalización de este proyecto con éxito.

KaRi.

DEDICATORIA

Por ser una parte esencial en el logro de esta meta, dedico este proyecto a mi Papá quien me apoya y confía en mí en todo momento, a mi extraordinaria y luchadora Madre a quien admiro mucho por su fortaleza y amor que tiene a su familia, a ustedes les debo prácticamente todo lo que soy. A mi hermano Andrés que con sus palabras oportunas siempre ha sabido aconsejarme. A mi hermana que está a mi lado siempre y de quien siempre cuidaré.

A todos mis primos y primas, que han sido mis primeros amigos. En especial a Jennifer y Evelyn que son como mis hermanas. Con ustedes hemos compartido grandes momentos familiares que siempre llevaré en mi corazón.

A todos mis amigos y amigas de la Poli, que han sido una parte fundamental de mi vida porque son el toque de alegría que hace que cada momento compartido en las aulas y fuera de ellas sea especial. Con quienes durante este tiempo he compartido momentos inolvidables y que con quienes tengo grandes recuerdos que jamás olvidaré. Espero que la amistad aquí formada jamás se acabe.

Los quiero mucho.

KaRi.

AGRADECIMIENTOS

Agradezco a Diosito por haberme dado todo lo que tengo en mi vida, y a Jesús por ser mi compañero y fiel amigo que siempre ha estado guiándome y ayudándome a superar los obstáculos que se me han presentado dándome fuerzas y esperanza.

Agradezco a mis papis, que han estado a mi lado siempre dándome su amor incondicional, su apoyo y sus consejos para que pueda salir delante de la mejor manera y pueda ser la persona que soy; agradezco a mi ñaño que siempre me ayudó en lo que pudo cuando le pedí su ayuda; agradezco a mi ñaña que siempre supo darme su apoyo, por escucharme siempre y por ser mi gran confidente; agradezco a mis enanos Thaís, Mateo y Gabito por llenar mis días de momentos divertidos y tiernos. Los amo a todos.

Agradezco a mi tía Lourdes y a mi prima Andrea por ser personas tan valiosas que han sabido darme tantos momentos memorables; agradezco a mi abuelita por ser una personas tan tierna que supo apoyarme y aconsejarme, y a mi abuelito que aunque no esté conmigo ahora, siempre me consintió y me dio su inmenso cariño mientras estuvo a mi lado.

Gracias a todos mis amigos y a las personas que de una manera u otra llegaron a ser tan importantes en mi vida. Gracias por su apoyo, por su presencia en mi vida, por las huellas que han dejado en mi corazón, por todos los momentos vividos y por los que nos quedan por vivir, y sobre todo por su inmensa amistad y cariño. Son un tesoro que no tiene precio para mí.

Gracias Kari por haber hecho la tesis conmigo, por estar ahí en las buenas y en las malas y por ser una gran amiga.

Gracias a los ingenieros por sus enseñanzas, tanto dentro como fuera de las aulas, gracias por ayudarme a culminar mi carrera universitaria y por darme el ejemplo para ser una excelente profesional en la nueva etapa que está a punto de comenzar.

Paulina Paspuel

DEDICATORIA

“La posibilidad de realizar un sueño es lo que hace que la vida sea interesante”

Paulo Coelho

Por ser una parte muy importante de mi vida, por su apoyo y su cariño le dedico este trabajo a mis padres, hermanos, sobrinos, mis mujeres, mi abuelito y al resto de mi familia.

A Diosito, porque siempre me ha bendecido y ha estado conmigo siempre.

A mis amigos, porque sin ellos la vida en la poli no habría sido tan bella como lo ha sido, y porque yo no habría sido la misma sin ellos: W A,N N, K A, AM C, A R, S T, D M, H M, B C, F S, etc.

A los ingenieros que más que profesores fueron amigos que me dieron su consejo para ser una mejor persona y una buena profesional.

Paulina Paspuel

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN

El presente proyecto de titulación tiene por objetivo realizar la evaluación de la Gestión Informática de la Unidad de TI de la Cooperativa de Ahorro y Crédito “TEXTIL14 DE MARZO” usando COBIT 4.1. Para el desarrollo del mismo se han estructurado cuatro capítulos en los cuales se tratan el análisis situacional de la Organización, planificación y ejecución de la evaluación, análisis de resultados obtenidos y las respectivas conclusiones y recomendaciones.

En el capítulo uno, se caracteriza a la empresa tanto en el aspecto organizacional como en el tecnológico, utilizando la Metodología para la evaluación del desempeño de una unidad informática desarrollada por el Ing. Jaime Naranjo. Adicionalmente se desarrolla una descripción y síntesis del marco de referencia COBIT 4.1, de manera que permita tener una visión general de su enfoque y que sirva de apoyo para la selección de los procesos a evaluarse en base a las necesidades de la Organización.

En el capítulo dos, se planifica la evaluación tomando en cuenta la conformación del grupo evaluador y la herramienta que se utiliza para la medición del nivel de madurez de los procesos seleccionados. Cabe recalcar que para la recolección de información se utilizan las directrices de Auditoria de COBIT de los procesos seleccionados.

En el capítulo tres, se efectúa el análisis de los resultados de los procesos seleccionados en base al nivel de madurez obtenido, y se proponen mejoras para que los procesos analizados alcancen un nivel de madurez futuro que correspondiente a su inmediato superior y con ello mejorar la Gestión de TICs que realiza el departamento de Sistemas.

Finalmente en el capítulo cuatro, se exponen las conclusiones y recomendaciones obtenidas con la realización del presente proyecto.

1. CAPÍTULO 1: ANÁLISIS DE LA SITUACIÓN ACTUAL

1.1. DESCRIPCIÓN DE LA EMPRESA

Nombre: Cooperativa de Ahorro y Crédito “TEXTIL 14 DE MARZO”

Dirección: Matriz – San Rafael (Av. General Enríquez y la Concordia, esquina)

Teléfono: 02 2865-120 / 02 2863-579

Página Web: http://www.14demarzo.fin.ec/cooperativa_de_ahorro_y_credito/

1.1.1. DESCRIPCIÓN HISTÓRICA[1]

En 1986 en San Rafael Valle de los Chillos, nace la Cooperativa de Ahorro y Crédito. TEXTIL 14 DE MARZO, impulsada por los obreros de la fábrica “Indutex”, y constituida como una organización paralela al Comité de Empresa de la fábrica junto con un proceso de capacitación realizado por el Instituto Sindical INESE. Su nombre se debe a la fecha conmemorativa del Día del Trabajador Textil, establecida por decreto profesional debido de un grupo de empresas textiles para mejorar las condiciones laborales de los obreros. [**1**]

Inicialmente para ser miembros de la Cooperativa se debía ser trabajador de la fábrica a la que estaba ligada. En el año 1991, tan sólo se contaba con el Sr. Carlos Díaz, Gerente y Fundador de la Cooperativa, y únicamente se daba servicio a los obreros de las fábricas “Indutex ”, “Textiles Nacionales” y Textiles Durero. Más adelante para mejorar el servicio, se contrataron 2 personas las cuales cubrirían las demandas de sus clientes.

En abril de 1969, se obtuvo la Personería Jurídica con la formación de una directiva provisional en la que participaban los trabajadores más preparados académicamente. De esta manera la Cooperativa inició su funcionamiento en la ciudad de Sangolquí con 62 socios y con un capital de 5000 sucres. Su

[1] Tomado de http://www.14demarzo.fin.ec/cooperativa_de_ahorro_y_credito/ y resumido por las autoras

constitución fue dirigida a la lucha contra la usura que sufrían los trabajadores de "Indutex", estimulación de ahorro y crédito personal y solidario entre los socios.

En 1996, en la Asamblea General, se solicitó que la Cooperativa se declarase como "abierta", siendo aprobada y ratificada dicha solicitud por la decisión unánime de los 110 socios existentes, además de reformar los estatutos vigentes para dejar constancia de los términos acordados.

1.1.2. LINEAMIENTOS

Misión[2]

Atender a nuestros socios con servicios de calidad, eficiencia administrativa e ideas innovadoras. Apoyaremos sus iniciativas a partir de un equipo de trabajo efectivo, una administración responsable y un Cuerpo Directivo comprometido con el crecimiento y solidez de la cooperativa. [**1**]

Visión[2]

Ser una cooperativa de prestigio en el sector financiero, reconocida por su solidez, rentabilidad, cobertura de servicios, que cuenta con personal capacitado y comprometido, procesos eficientes, tecnología y capacidad institucional para responder a la confianza de sus socios. [**1**]

Valores Institucionales[3]

- **Honestidad** a toda prueba en el manejo de los recursos de la cooperativa. El dinero de nuestros depositantes está protegido.
- **Solidaridad** con todos quienes hacen la cooperativa, nuestros socios, clientes y compañeros saben que pueden contar con nuestro apoyo.
- **Integridad** en nuestros actos, ara que los socios y la comunidad sepan que sus recursos están siendo manejados por personas probas e intachables.

[2] Tomado de http://www.14demarzo.fin.ec/cooperativa_de_ahorro_y_credito/
[3] Tomado del Plan Estratégico 2013 de la Coac. "TEXTIL 14 DE MARZO".

- **Compromiso** para que la cooperativa, sus directivos, sus asociados y la comunidad cumplirán con todas las obligaciones contraídas.
- **Transparencia** integral en el manejo y administración de la información de la cooperativa.

Principios [4]

- Adhesión voluntaria.
- Control democrático de los socios.
- Participación económica de los socios.
- Autonomía e independencia.
- Educación, entrenamiento e información.
- Cooperación entre cooperativas.
- Compromiso con la comunidad.

1.1.3. ACTIVIDADES PRINCIPALES[5]

La actividad principal de la Cooperativa de Ahorro y Crédito "TEXTIL 14 de Marzo" se centra en realizar actividades de intermediación financiera y con Responsabilidad Social a sus socios, además de la otorgación de créditos financieros, los cuales se encuentran sujetos a los lineamientos de la Superintendencia de Economía Popular y Solidaria y su reglamento. [**2**]

Cabe recalcar que la Coac. "TEXTIL 14 de Marzo" cuenta con actividades complementarias que permiten proporcionar los servicios financieros que satisfagan las necesidades de sus socios. Entre éstas se pueden mencionar las siguientes:

- Recibir depósitos a la vista y a plazo, bajo cualquier mecanismo o modalidad autorizada.
- Otorgar préstamos a sus socios.
- Efectuar servicios de caja y tesorería.

[4] Tomado del Plan Estratégico 2013 de la Coac. "TEXTIL 14 DE MARZO".
[5] Tomado del Estatuto de la Cooperativa de Ahorro y Crédito TEXTIL 14 DE MARZO LTDA y resumido por las autoras.

- Efectuar cobranzas, pagos y transferencias de fondos, así como emitir giros contra sus propias oficinas o las de las instituciones financieras nacionales o extranjeras.
- Recibir y conservar objetos muebles, valores y documentos en depósito para custodia y arrendar casilleros o cajas de seguridad para depósitos de valores
- Asumir obligaciones por cuenta de terceros a través de aceptaciones, endosos o avales de títulos de crédito así como por el otorgamiento de garantías, fianzas y cartas de crédito internas y externas, cualquier otro documento, de acuerdo con las normas y prácticas y usos nacionales e internacionales.
- Recibir préstamos de instituciones financieras y no financieras del país y del exterior.
- Realizar inversiones preferentemente en este orden en: Sector Financiero Popular y Solidario, Sistema Financiero Nacional y en el mercado secundario de valores y de manera complementaria en el sistema financiero internacional.
- Efectuar inversiones en capital social de cajas centrales.

1.1.4. ORGANIGRAMA FUNCIONAL GENERAL[6]

En el organigrama de la Fig. 1.1, se puede ver que la organización se rige por jerarquías para definir sus niveles de decisión, por lo que tienen una estructura vertical para definir a la Alta gerencia. El nivel de decisión más alto está la Asamblea General de socios; en un nivel inferior se encuentran los Consejos de Administración y Vigilancia, seguidos de los comités y la Gerencia General.

A partir del cuarto nivel se encuentran los diferentes departamentos que se encargan de las operaciones que proporcionan los principales servicios financieros a los socios de la organización. Desde este punto de vista, todos los departamentos se encuentran en el mismo nivel de decisión, lo que indica que

[6] Tomado del Organigrama Funcional de la Coac. “TEXTIL 14 DE MARZO”.

cada uno de ellos tiene la misma importancia dentro de la Organización, sin embargo la ubicación del Departamento de Sistemas no corresponde a un nivel de asesoría para la toma de decisiones. Por tanto, de acuerdo con el organigrama, el nivel en el que se encuentra el departamento de Sistemas no está en concordancia con la finalidad de la unidad o departamento de Sistemas que es dar soporte al resto de departamentos para que satisfagan las necesidades internas de la Organización, las demandas de los socios, así como el cumplimiento de los objetivos de la Organización.

Se debe tener en cuenta que el organigrama actual está siendo modificado para adecuarse a las recomendaciones de SEPS[7], por lo que se están incluyendo nuevos comités, como el de adquisiciones y de seguridad, y departamentos, como el de Auditoría interna, de riesgos y de planificación de procesos, entre otros, con el fin de segregar las funciones que actualmente están a cargo de los departamentos existentes o que aún no han sido consideradas dentro de la organización.

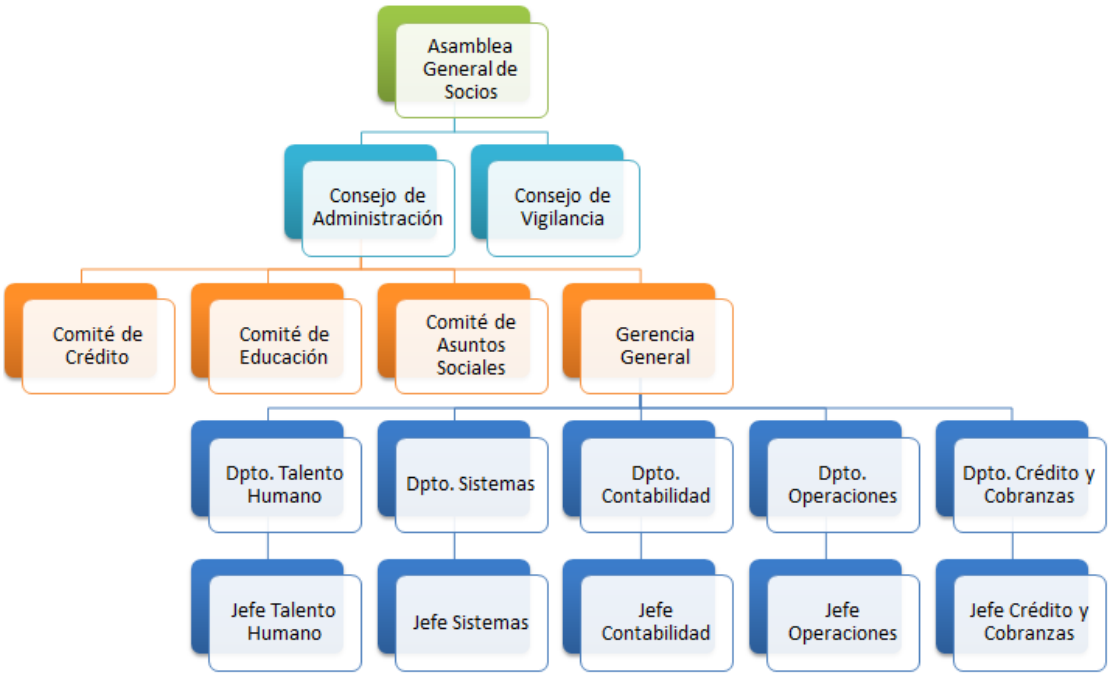

Fig. 1.1 Organigrama Funcional parcial de la Coac. "TEXTIL 14 DE MARZO" [8]

[7] Superintendencia de Economía Popular y Solidaria
[8] Fuente: Tomado del Organigrama Funcional pproporcionado por Coac. "TEXTIL 14 DE MARZO"

1.1.5. DESCRIPCIÓN DEL DEPARTAMENTO DE SISTEMAS [3]

1.1.5.1. Orgánico Funcional del Departamento de Sistemas

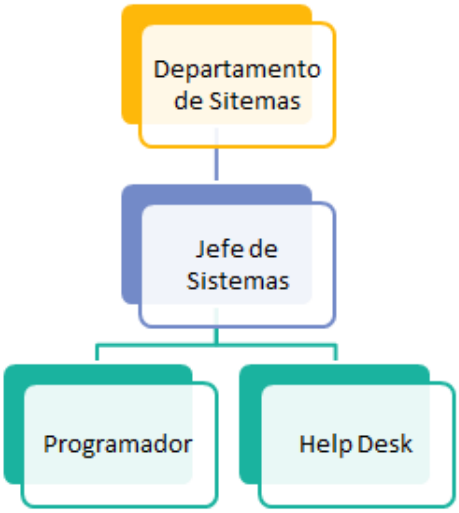

Fig. 1.2 Orgánico Funcional del Departamento de Sistemas [9]

De acuerdo con el organigrama funcional de la empresa de la Fig. 1.2, el Departamento está conformado por el Jefe de Sistemas, el programador y la persona encargada del Help Desk. Cabe mencionar que estas personas son las encargadas de llevar a cabo las actividades relacionadas con la Gestión Informática tanto en la matriz como en todas las sucursales de Coac. “TEXTIL 14 DE MARZO”.

El Departamento de Sistemas es el encargado de tener a punto a todos los recursos y servicios informáticos de la Organización con el fin de garantizar el funcionamiento óptimo, que es indispensable para brindar un correcto servicio a los socios y funcionarios de la Organización. Entre las funciones que desempeña este departamento se pueden mencionar las de analizar, planificar, organizar, dirigir, controlar, implementar y evaluar el Sistema Financiero “Financial Business System” de la Cooperativa, permitiendo la prestación oportuna de los servicios financieros que brinda la cooperativa a sus socios, así como en la prestación oportuna de sus funciones; adicionalmente están en la capacidad de colaborar en

[9] Fuente: Extracto el Organigrama Funcional de Coac. “TEXTIL 14 DE MARZO”

las actividades de desarrollo y administración de los sistemas informáticos, dar soporte y mantenimiento a la infraestructura tecnológica, realizar el procesamiento y garantizar la seguridad de la información; atender los requerimientos de TI que se presentan en el día a día de todos los usuarios de la cooperativa.

1.1.5.2. Actividades del Departamento de Sistemas

Las actividades que desempeña cada miembro del personal del Departamento de Sistemas están definidas en el Manual de Funciones de Cooperativa de Ahorro y Crédito. “TEXTIL 14 DE MARZO”. Sin embargo, estas funciones no son realizadas exclusivamente por cada persona de un determinado cargo debido a la disponibilidad de tiempo, por lo que todos realizan las funciones de otros cargos según sea oportuno y requerido.

Las actividades principales de cada uno de los cargos descritas en el Manual de Funciones de la Coac. “TEXTIL 14 DE MARZO” son las siguientes:

Jefe de sistemas

Es la persona encargada de realizar actividades para dar cumplimiento a las funciones y objetivos de su departamento en conjunto con los demás departamentos de la Organización, para lo cual, en el aspecto administrativo desempeña, las siguientes funciones:

- Participar en la formulación del Plan Estratégico de la Cooperativa.
- Revisión de requerimientos de TI.

En el área de operaciones:

- Revisión del cajero automático con tarjeta de seguridad y el software.
- Cierre de sistema financiero.
- Generación de trasporte de Transacciones SPI[10].
- Verificación de cajas cerradas y afectaciones antes del cierre.
- Verificación que no exista inversiones pendientes antes del cierre.
- Proceso de reclamo de tarjetas de Débito y SPI[10] al banco de Austro.

[10] Sistema de Pagos Interbancarios

- Seguimiento y coordinación, directamente con el personal del Banco de Austro el IESS escalando jerarquías, para dar una resolución satisfactoria a los reclamos de tarjetas de Débito y SPI[11].

En el área de infraestructura tecnológica:

- Revisión de enlaces de comunicación externa, matriz y las diferentes Agencias.
- Revisión del funcionamiento de los servidores.
- Retención de enlaces Cooperativa Banco del Austro.
- Control y administración del Firewall.
- Respaldo base de datos de la cooperativa antes y después del cierre.
- Respaldo base de datos SPI[11].
- Configuración de acceso de conexión del servidor de archivo para los usuarios.
- Monitoreo de la red de comunicación entre todas las oficinas de la cooperativa.
- Supervisión del buen funcionamiento del sistema informático de la cooperativa.
- Administración de la base de datos del sistema financiero de la cooperativa.

En el área de soporte a usuarios:

- Revisión del e-mail institucional.
- Soporte Técnico a usuarios de equipos de computación y software.
- Soporte administrativo a usuarios.
- Coordinación con HelpDesk y área de programación de los requerimientos de TI levantados por los usuarios.

[11] Servicio de Pagos Interbancarios

Programador

Es la persona encargada de participar en desarrollo, implementación, evaluación y mejoramiento de los sistemas computacionales, para lo cual realiza las siguientes actividades:

- Cierre de sistemas financieros para tener listos y actualizados para el próximo día.
- Soporte a técnicos abarca, sistema, comunicaciones, aplicación de escritorio, equipos programas como; Hardware, Software.
- Soporte a usuarios cuando hay erros de los Departamentos.
- Soporte operativo en el manejo d sistema como: Hardware, Software.
- Administra operativamente el Sistema Financial

Helpdesk

Es la persona encargada de atender los requerimientos de TI que se presentan en el día a día de todos los usuarios de la cooperativa, para lo cual realiza las siguientes actividades:

- Brindar el soporte técnico de sistemas y programas (mantenimiento preventivo de Hardware de las diferentes áreas operativas a fin de optimizar el proceso automático de datos y desarrollo de los reportes de gestión.
- Monitoreo y actualizan de antivirus.
- Monitoreo de las redes de comunicación de la Cooperativa LAN- WAN.
- Monitoreo de servidores.
- Cambio de TONERS.
- Administrar y mantiene organizado los archivos de respaldo de información del sistema Financial y mapas de redes LAN.

Para mayor información, consulte el ANEXO E.

1.1.6. SEGURIDAD INFORMÁTICA

1.1.6.1. Física

La Cooperativa cuenta con personal de seguridad privada en su entrada y en el área de Operaciones, es decir, las ventanillas de atención al cliente. Para el ingreso de personal externo al departamento de Sistemas se lleva un registro en una bitácora que maneja el Jefe del departamento, en el que consta el nombre de la persona que ingresa, la fecha y hora junto con su firma de responsabilidad.

El ingreso al área de servidores, es restringido al personal del departamento de Sistemas. Cuenta con condiciones mínimas para su funcionamiento (temperatura, sin filtraciones de agua ni humedad, detector de humo) y el acceso a su configuración es únicamente realizada por el Jefe de Sistemas. En caso de que alguna persona sea autorizada por la alta gerencia para su ingreso a esta área, se tiene una bitácora en la que se registra el nombre, fecha, hora y actividad que va a realizar, además de estar escoltado por una persona perteneciente al departamento.

1.1.6.2. Lógica

Las estaciones de trabajo de la Cooperativa cuentan con contraseñas de acceso y los perfiles de usuario son definidos de acuerdo a las funciones que desempeñen dentro de la Cooperativa.

En cuanto al uso de internet, la mayoría de usuarios solo pueden acceder a aquellos sitios web que estén relacionados con sus actividades laborales, por tanto restringen el acceso a internet para uso personal. No se permite la utilización de puertos USB ni tampoco el almacenamiento de documentación que no corresponda a la Cooperativa en el equipo de escritorio así como en el servidor de archivos.

Los servidores cuentan con contraseñas que son manejadas únicamente por el Jefe de sistemas, por tanto es la única persona que tiene acceso a sus configuraciones.

El departamento de sistemas provee el uso del Sistema Financiero FINANCIAL[12], el mismo que está diseñado para definir perfiles de usuarios y contraseñas cuando sea requerido.

1.1.6.3. Legal

En el caso de alguna contingencia los equipos de la Cooperativa se encuentran asegurados con la empresa AeroSeguros. Este contrato es definido por parte de la Gerencia General, Consejo de Administración y asesoría legal en una asamblea previamente realizada.

1.1.6.4. Datos

El proceso de respaldo de datos en la Cooperativa es realizado por el Sistema Financiero [12] que cierra de sus funciones diariamente. Para ello realiza un respaldo antes del cierre y otro después del cierre, después de que la validez información ha sido aprobada por el Jefe de Contabilidad.

Una vez obtenidos los 2 respaldos se almacenan en el servidor de respaldos, el cual está dotado de un disco duro de un terabyte. Cuando este disco alcanza su capacidad máxima es entregado al Gerente General quien es el encargado de almacenarlo en la caja fuerte de la Cooperativa.

1.1.6.5. Personal

El personal se maneja bajo el Reglamento Interno de Trabajo de la Cooperativa, el cual regirá las funciones laborales y de disciplina de todos los trabajadores acatando las consecuencias que se generen por el incumplimiento de las normas aquí establecidas. La persona encargada de velar por la aplicación del contrato son el Gerente General y el departamento de Talento Humano.

Para la incorporación de un trabajador a la Cooperativa se siguen requisitos previos que los aspirantes deben reunir. La selección de personal se realiza por parte del Departamento de Talento Humano en base a pruebas psicológicas y de conocimientos requeridos según sea el caso. Finalmente se emite un contrato

[12] Sistema Financiero “Financial Bussines System”

escrito basado en el Código del Trabajo, el cual es firmado por parte del Gerente General y el nuevo trabajador.

Una de las condiciones legales del contrato estipula la afiliación patronal al IESS para el trabajador y no se cuentan con otro tipo de seguro. Otros aspectos del contrato son su sueldo, jornada y duración del cargo de trabajo. No se cuenta con un plan de carrera, en su lugar el departamento de Talento Humano garantiza que cada uno de los trabajadores recibirá 4 cursos para su capacitación, de los cuales 2 son de aspectos generales y 2 de aspectos específicos de acuerdo al área en la que estén desempeñando sus funciones.

Adicionalmente, existe un plan de vacaciones anuales y rotativas de acuerdo a un calendario vacacional que el departamento de Talento Humano realiza bajo la revisión y aprobación de Gerencia General. Por otro lado, existen licencias con sueldo en los casos de enfermedad, maternidad, pasantías, congresos, cursos en el exterior y otros previamente autorizados por el Consejo de Administración. En cuanto a los permisos existen los estipulados por el código de trabajo como son permisos con cargo a vacaciones, por enfermedad, entre otros.

1.2. DESCRIPCIÓN DEL MARCO DE REFERENCIA COBIT 4.1 [4]

Actualmente las empresas y organizaciones que están en constante crecimiento cuentan con la utilización de Tecnologías de la Información en la mayoría de sus procesos, con el objetivo de brindar mayor calidad en la entrega de sus servicios, y garantizar la seguridad de la información. Es necesario que la Gerencia sea consciente y tenga el conocimiento de los beneficios adquiridos al invertir en tecnología para el tratamiento y administración de la información y en actividades del negocio ya que de ello dependerá el éxito de la organización.

De acuerdo a las tendencias en el uso de tecnologías de la información que sean de apoyo a la consecución de los objetivos de negocio, ISACA ofrece un marco de trabajo mundialmente aceptado y enfocado en la Gestión de Tecnología de la Información que es COBIT 4.1(Control Objectives for Information and Related Technology). Su propósito es ayudar a las empresas y a sus altos directivos a

establecer un Gobierno de TI mediante la alineación de los objetivos del negocio con los de TI.

Se utilizan estrategias y buenas prácticas que en primer lugar permitirán realizar una evaluación sobre la situación actual de los recursos de la organización incluyendo infraestructura, personas, aplicaciones e información. Posteriormente se determinan qué procesos podrían ser optimizados o implementados para minimizar los riesgos de TI con una adecuada administración y con ello conseguir que la organización pueda alcanzar una mayor competitividad en el mercado.

Finalmente, permite lograr la adquisición de una mejora continua de Gestión de TICs que garantice el cumplimiento de los objetivos del negocio junto con la mejora del rendimiento de los procesos de TI y la elaboración de políticas para un control de TI dentro de la empresa.

1.2.1. CARACTERÍSTICAS

COBIT 4.1 se enfoca en 5 áreas fundamentales:

- Alineación Estratégica: entre los planes del negocio junto a los planes de TI.
- Entrega de valor: se ve reflejado en los beneficios obtenidos a lo largo del ciclo de entrega de los servicios de TI.
- Administración de riesgos: a nivel tecnológico y de información en relación a la empresa.
- Administración de recursos: en cuanto a personas, aplicaciones, infraestructura e información.
- Medición del desempeño: monitoreo de la estrategia para la implementación de los procesos y entrega de servicio tomando en consideración controles para su medición.

Cada una de estas áreas permiten analizar qué procesos de COBIT 4.1 serán utilizados para organizar y administrar los recursos de TI; además cuáles están relacionados con los objetivos del negocio, es decir los procesos que proveen los servicios para la entrega de información que concierne a la organización.

COBIT 4.1 permite la asignación de roles y responsabilidades a personas con perfiles adecuados para:

- La toma de decisiones en las inversiones de TI.
- Brindar los servicios de TI.
- Ser responsables del control y riesgos de TI.

Cabe recalcar que COBIT 4.1 permite proporcionar servicios que den soporte a la estrategia empresarial siendo necesario establecer una arquitectura empresarial para TI que permitan definir metas que serán implementadas con los procesos de TI así como de los recursos de TI, como se observa en la Fig. 1.3.

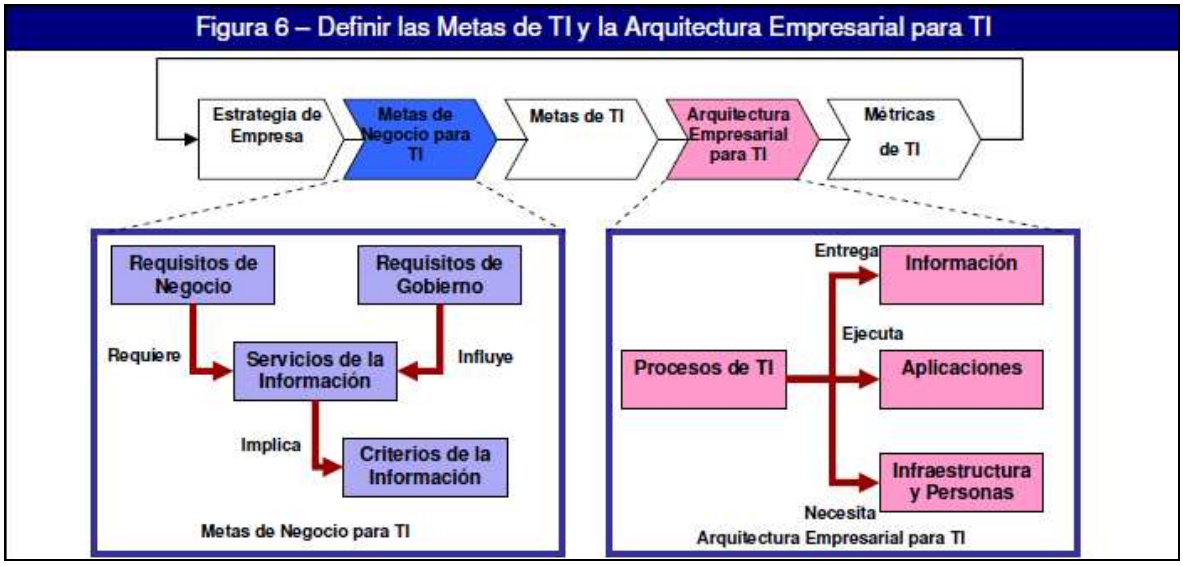

Fig. 1.3 Metas y Negocios de TI[13] [4]

.

1.2.2. ESTRUCTURA DE COBIT 4.1

COBIT 4.1 se encuentra estructurado en 3 elementos fundamentales como se puede ver en la Fig. 1.4:

- Requerimientos del negocio: basados en criterios de información de COBIT 4.1, que permiten el cumplimiento de los objetivos del negocio en función de calidad, seguridad, entre otros.

[13] Fuente: Tomado de COBIT 4.1 versión español, página 11, Figura 6.

- Recursos de TI: basados en la correcta utilización de la información del negocio mediante las aplicaciones usadas por personas y soportado por una adecuada infraestructura tecnológica.
- Procesos de TI: como referencia para la administración de las actividades de TI y sus riesgos mediante la implementación de buenas prácticas y el establecimiento de un lenguaje común para el Gobierno de TI.

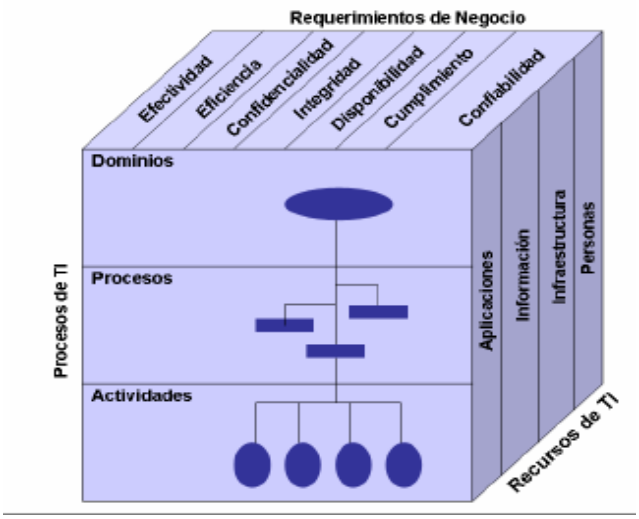

Fig. 1.4 Cubo de COBIT 4.1[14] [4]

1.2.3. DOMINIOS Y PROCESOS

COBIT 4.1 cuenta con 4 dominios y 34 procesos, además de la utilización de criterios que permiten definir el nivel de madurez en el que se encuentran los procesos en cada uno de los dominios.

Para que exista un Gobierno de TI los dominios se encuentran relacionados entre sí, como se observa en la Fig. 1.5.

- Planear y Organizar para tener dirección en la entrega de soluciones y servicios de TI.
- Adquirir e Implementar para proporcionar soluciones para convertirlas en servicios.

[14] Fuente: Tomado de COBIT 4.1 versión español, página 25, Figura 22.

- Entregar y Dar soporte para recibir las soluciones para la posterior utilización de los usuarios finales.
- Monitorear y Evaluar para controlar las soluciones implementadas y asegurar su ciclo de vida.

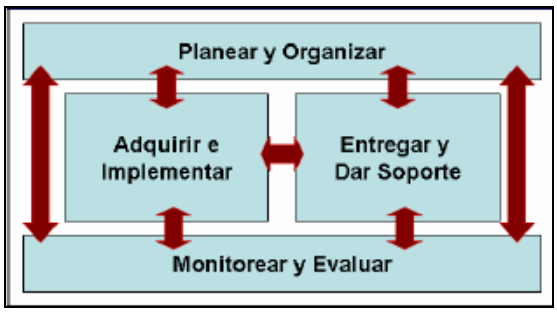

Fig. 1.5 Relación de dominios[15] [4]

Cada uno de los dominios cuenta con procesos que permiten definir responsabilidades y actividades para su cumplimiento, los cuales se detallan a continuación:

1.2.3.1. Planear y Organizar (PO)

Este dominio permite establecer estrategias y tácticas de TI que estén alineadas con los objetivos del negocio, la óptima utilización de los recursos de TI, administración de los riesgos y la gestión de personal adecuado para el manejo de TI.

Sus procesos son los siguientes:

- **PO1 Definir un Plan Estratégico de TI:** para satisfacer los requerimientos del negocio y de TI, dando lineamientos para una estrategia del negocio que permita adquirir beneficios en cuanto a costos y minimizando los riesgos de TI.
- **PO2 Definir la Arquitectura de la Información:** para agilizar la respuesta a los requerimientos del negocio y brindar información disponible,

[15] Fuente: Tomado de COBIT 4.1 versión español, página 12, Figura 12.

confiable, consistente e integra de forma transparente hacia los procesos de negocio.

- **PO3 Determinar la Dirección Tecnológica:** para la utilización de estándares que sean estables para la administración de la tecnología en cuanto a productos, servicios y aplicaciones definidas dentro de un plan de infraestructura tecnológica actual y futura.
- **PO4 Definir los Procesos, Organización y Relaciones de TI:** Que permiten agilizar la respuesta a la estrategia del negocio mientras se da cumplimiento a los requerimientos del gobierno de TI.
- **PO5 Administrar la Inversión en TI:** Contemplar costos, beneficios junto con un presupuesto tecnológico en base a entrevistas con los interesados y a los planes que existan en la empresa para tener un uso efectivo y eficiente de los recursos de TI.
- **PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia:** Proporcionar políticas, procedimientos documentados que sean conocidos, aprobados y apoyados por la Gerencia sobre los servicios de TI. Con ello se logra adquirir un control interno de TI alineado con la administración de la empresa con los riesgos y responsabilidades que eso implique.
- **PO7 Administrar Recursos Humanos de TI:** Establecer políticas para reclutamiento, entrenamiento, evaluación del desempeño del personal de TI, así como su capacitación continua. La asignación de roles y responsabilidades en base a una definición de requerimientos de habilidades para determinados puestos de trabajo.
- **PO8 Administrar la Calidad:** Establecer estándares y prácticas de calidad aceptadas que sean cuantificables y alcanzables, empleando un monitoreo constante para la mejora continua.
- **PO9 Evaluar y Administrar los Riesgos de TI:** Identificar, controlar y mitigar los riesgos de TI que afecten al cumplimento de los procesos y metas del negocio así como de TI, que serán evaluados mediante la implementación de un plan de acción de riesgos cualitativa y cuantitativamente.
- **PO10 Administrar Proyectos:** Coordinar los proyectos asignando responsables y los recursos necesarios para su cumplimiento en fases.

Permitiendo asegurar su calidad con planes de pruebas antes de su implantación, resultados en post-implantación.

1.2.3.2. Adquirir e Implementar (AI)

Este dominio se basa en que las soluciones de TI son identificadas y entregadas para garantizar que sigan contribuyendo al cumplimiento de los objetivos del negocio.

Los procesos de este dominio se describen a continuación:

- **AI1 Identificar soluciones automatizadas:** Realizar un análisis previo a la adquisición de tecnología con base en los requerimientos funcionales del negocio para determinar su factibilidad y rentabilidad.
- **AI2 Adquirir y mantener software aplicativo:** Tener el diseño y configuración de las aplicaciones, es decir que existan procesos adecuados y confiables de desarrollo de software que cumplan con estándares en todo su ciclo de vida.
- **AI3 Adquirir y mantener infraestructura tecnológica:** Para dar soporte tecnológico a las aplicaciones que utiliza la empresa de acuerdo a una arquitectura y estándares tecnológicos aceptados.
- **AI4 Facilitar la operación y el uso:** Mediante documentación como manuales para usuarios de TI. El entrenamiento del uso de las aplicaciones, así como de la infraestructura tecnológica.
- **AI5 Adquirir recursos de TI:** Definir estándares y procedimientos para la selección de proveedores mediante la utilización de contratos de compra y su suministro de hardware, software y servicios incluyendo la selección del personal.
- **AI6 Administrar cambios:** Documentar el registro, evaluación, autorización y revisión de los cambios relacionados a infraestructura y aplicaciones junto con sus soluciones tecnológicas que se presenten.
- **AI7 Instalar y acreditar soluciones y cambios:** Establecer metodologías de prueba que garanticen el funcionamiento de las aplicaciones una vez

que hayan sido instaladas a pesar de que existan problemas en su liberación.

1.2.3.3. Entregar y Dar Soporte (DS)

Este dominio se encarga de la prestación de los servicios, su continuidad y finalmente dar soporte a usuarios finales.

Los procesos de este dominio se describen a continuación:

- **DS1 Definir y administrar los niveles de servicio:** Alinea los niveles de servicios de TI con los requerimientos del negocio emitiendo reportes que garanticen el cumplimiento de los mismos.
- **DS2 Administrar los servicios de terceros:** Cumplir los requerimientos del negocio por parte de terceros que minimicen los riesgos del negocio provistos, mediante el monitoreo continuo de su desempeño.
- **DS3 Administrar el desempeño y la capacidad:** Realizar revisiones continuas junto con la emisión de reportes del desempeño del sistema para dar pronósticos de su funcionamiento.
- **DS4 Garantizar la continuidad del servicio:** Mantener la prestación de los servicios del negocio todo el tiempo, con la implementación de planes de continuidad, contingencias y previas pruebas para reducir el impacto de las interrupciones de los servicios del negocio.
- **DS5 Garantizar la seguridad de los sistemas:** Establecer roles y responsables que mantengan la integridad y protección de la información y activos de TI con políticas de seguridad de acceso.
- **DS6 Identificar y asignar costos:** Capturar, distribuir y reportar costos de TI a los usuarios de los servicios para obtener una mayor rentabilidad con su uso en una relación costo/eficiencia.
- **DS7 Educar y entrenar a los usuarios**: Identificar las necesidades que tienen los usuarios al utilizar las diferentes aplicaciones tecnológicas, documentarlas para un posterior entrenamiento efectivo en cuanto a las TI y a los usuarios.
- **DS8 Administrar la mesa de servicio y los incidentes:** Para la resolución de consultas y problemas por parte de los usuarios de TI. Los

incidentes generados deben ser registrados, reportados, analizados y atendidos.

- **DS9 Administrar la configuración:** Establecer un repositorio con el registro de las configuraciones iniciales y sus actualizaciones que garanticen una mayor disponibilidad, minimizando los problemas de producción.
- **DS10 Administrar los problemas:** Analizar e identificar las causas de los problemas desde su raíz hasta su resolución junto con la propuesta de mejora y además mantener un registro para las posibles acciones correctivas futuras.
- **DS11 Administrar los datos:** Optimizar el uso de la información que garanticen su disponibilidad, recuperación, protección, integridad, respaldo y calidad.
- **DS12 Administrar el ambiente físico:** Definir los requerimientos físicos para instalaciones, factores ambientales, acceso al centro de cómputo y aumentar la protección a los activos de TI.
- **DS13 Administrar las operaciones:** Mantener la integridad de los datos y garantizar que la infraestructura de TI puede resistir y recuperarse de errores y fallas.

1.2.3.4. Monitorear y Evaluar (ME)

Este dominio se enfoca en las revisiones continuas de los procesos de TI y su desempeño, además de la evaluación de su cumplimiento satisfactorio en base a métricas o indicadores de control establecidos.

Sus procesos se detallan a continuación:

- **ME1 Monitorear y Evaluar el Desempeño de TI:** Garantizar que se cumplan el conjunto de direcciones y políticas mediante la definición de indicadores y emisión de reportes sistemáticos para el mejoramiento continuo de los recursos de TI.

- **ME2 Monitorear y Evaluar el Control Interno:** Proporcionar sistema de controles internos integrados con el marco de trabajo de los procesos de TI que den cumplimiento de los objetivos de TI y de sus leyes y reglamentos de TI.
- **ME3 Garantizar el Cumplimiento Regulatorio:** Establecer un proceso de revisión para garantizar el cumplimiento de leyes, regulaciones y sus requerimientos de TI para evitar riesgos de incumplimiento.
- **ME4 Proporcionar Gobierno de TI:** Definir un marco de trabajo que contenga procesos, roles y responsabilidades organizacionales para garantizar que las inversiones de TI están alineadas con las estrategias y objetivos de la empresa que serán presentados a los directivos.

1.3. SELECCIÓN DE LOS DOMINIOS Y PROCESOS DE COBIT PARA LA EJECUCIÓN DE LA EVALUACIÓN.

Para la realización de esta evaluación es fundamental definir y seleccionar los dominios y procesos en los que se va a apoyar la evaluación, tomando en cuenta las características del Departamento de Sistemas de la Cooperativa de Ahorro y Crédito. “TEXTIL 14 DE MARZO”, sus objetivos y metas a mediano plazo.

De acuerdo con la perspectiva tecnológica del Plan Estratégico y Plan Operativo del período 2012-2014 que se muestra en la Tabla 1.1, la finalidad del Departamento de Sistemas es “Mejorar la base tecnológica”[16] y su propósito es “Facilitar la funcionalidad de las operaciones institucionales” [16] [**5**], por lo que indica que los procesos más críticos o relevantes para la evaluación son aquellos que se centren en mejorar los recursos tecnológicos y apoyar al cumplimiento de los objetivos definidos en el Plan Estratégico, y aquellos cuya gestión contribuyan a satisfacer las necesidades de los socios de la cooperativa.

[16] Extracto del Plan Operativo 2012-2014 para el Departamento de Sistemas de la Coac. “TEXTIL 14 DE MARZO”

FORMULACIÓN DEL OBJETIVO			
Atributos del Objetivo de 1er Nivel	**Perspectiva Estratégica**		Tecnología
	Finalidad (*¿Qué se va a hacer?*)		Mejorar la base tecnológica
	Propósito (*Para qué se va a hacer*)		Para facilitar la funcionalidad de las operaciones institucionales
	Iniciativas Estratégicas (*cómo se va a hacer*)	**i)**	Actualizando infraestructura del servidor principal
		ii)	Creando la red de contingencias
		iii)	Ejecutando plan de respaldos
		iv)	Desarrollando órdenes de trabajo generados por el cliente interno
		v)	Actualización y optimización de los recursos tecnológicos
	Coordinador del objetivo		Gerencia General
	Ejecutor del objetivo		Tecnología
	Objetivos Transversales Vinculados		Rentabilidad

Tabla 1.1 Perspectiva Tecnológica del Plan Estratégico 2012-2014[17]

Adicionalmente para la selección de los procesos de COBIT 4.1, es necesario realizar un listado de los procesos más relevantes de la Organización y relacionarlos con los procesos que COBIT 4.1 propone.

Cabe recalcar que la Organización no cuenta con un levantamiento de procesos ni documentación que lo avale, por lo que los procesos en la Tabla 1.2 están basados en las funciones que los departamentos de la Organización desempeñan y en ejemplos de mapas de procesos de otras instituciones financieras. [**6**]

[17] Fuente: tomado del Plan Estratégico 2012-204 de la Coac "TEXTIL 14 DE MARZO"

Mapeo de procesos de la Empresa con los procesos de COBIT 4.1		
MACRO-PROCESOS	PROCESOS	PROCESOS ASOCIADOS A COBIT 4.1
1. Gestión de recursos físicos.	• Identificar y adquirir recursos físicos. • Gestionar condiciones de adquisición de recursos físicos. • Dar soporte a recursos físicos. • Inventariar recursos físicos.	PO9 Evaluar y Administrar los Riesgos de TI. AI1 Identificar soluciones automatizadas AI2 Adquirir y mantener software aplicativo AI3 Adquirir y mantener infraestructura tecnológica AI5 Adquirir recursos de TI DS1 Definir y administrar los niveles de servicio DS3 Administrar el desempeño y la capacidad DS4 Garantizar la continuidad del servicio DS12 Administrar el ambiente físico
2. Gestión de créditos.	• Asignar créditos. • Autorizar créditos. • Cancelar créditos.	DS13 Administrar las operaciones
3. Gestión de talento humano.	• Seleccionar y contratar personal. • Planificar capacitaciones al personal según el cargo. • Elaborar la organización funcional de departamentos.	PO4 Definir los Procesos, Organización y Relaciones de TI PO7 Administrar Recursos Humanos de TI DS7 Educar y entrenar a los usuarios.

	• Elaborar manual de funciones del personal. • Evaluar y monitorear periódicamente el desempeño del personal.	
4. Gestión de operaciones.	• Receptar depósitos. • Efectuar retiros. • Cobrar servicios básicos. • Administrar caja general. • Realizar cuadres de operaciones. • Realizar transacciones financieras.	DS2 Administrar los servicios de terceros DS13 Administrar las operaciones
5. Gestión de contabilidad.	• Realizar cuadres diarios de caja general. • Manejar caja chica. • Controlar transacciones financieras. • Consolidar balances contables de la cooperativa.	DS13 Administrar las operaciones
6. Gestión de planificación estratégica.	• Desarrollar el plan estratégico. • Monitorear y actualizar el plan estratégico. • Definir iniciativas estratégicas para mejorar la atención al cliente y para impulsar la gestión de negocios de la cooperativa. • Identificar riesgos financieros. • Emitir informes de las actas a toda la Organización • Desarrollar planes de Auditoria y control de	PO1 Definir un Plan Estratégico de TI. PO3 Determinar la Dirección Tecnológica. PO4 Definir los Procesos, Organización y Relaciones de TI. PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia PO9 Evaluar y Administrar los Riesgos de TI. DS4 Garantizar la continuidad del servicio.

	gestión. • Realizar análisis de riesgos del negocio. • Comunicar el plan estratégico y operativo a todos los departamentos.	ME2 Monitorear y Evaluar el Control Interno
7. Gestión de tecnología y recursos de TI.	• Dar soporte y mantenimiento a recursos de TI. • Mantener el sistema de información. • Atender requerimientos tecnológicos de los usuarios. • Administrar servicios de TI con terceros. • Realizar informes periódicos sobre recursos de TI para la toma de decisiones. • Monitorear el desempeño de los recursos de TI. • Coordinar actividades de las áreas del Departamento de Sistemas. • Capacitar a los usuarios acerca del uso de recursos de TI para el cumplimiento de sus funciones. • Comunicar sobre fallas de servicios a proveedores externos para su mantenimiento. • Monitorear red de comunicación entre todas	PO1 Definir un Plan Estratégico de TI PO2 Definir la Arquitectura de la Información PO3 Determinar la Dirección Tecnológica PO4 Definir los Procesos, Organización y Relaciones de TI PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia PO9 Evaluar y Administrar los Riesgos de TI AI1 Identificar soluciones automatizadas AI2 Adquirir y mantener software aplicativo AI3 Adquirir y mantener infraestructura tecnológica AI4 Facilitar la operación y el uso AI5 Adquirir recursos de TI DS1 Definir y administrar los niveles de servicio

	las oficinas. • Implementar medidas de seguridad en los sistemas informáticos. • Analizar y reportar problemas de seguridad detectados en el sistema financiero[18]. • Realizar Respaldos de la base de datos antes y después del cierre del sistema financiero[20]. • Realizar respaldos de la base de datos SPI[19]. • Realizar el cierre del sistema financiero[20]. • Realizar y actualizar inventarios de equipos del departamento de Sistemas. • Dar asesoramiento para la adquisición de recursos de TI.	DS2 Administrar los servicios de terceros DS3 Administrar el desempeño y la capacidad DS4 Garantizar la continuidad del servicio DS5 Garantizar la seguridad de los sistemas DS7 Educar y entrenar a los usuarios DS11 Administrar los datos DS12 Administrar el ambiente físico DS10 Administrar los problemas DS13 Administrar las operaciones ME1 Monitorear y Evaluar el Desempeño de TI
8. Gestión de control interno y regulaciones externas	• Identificar las leyes, regulaciones o disposiciones de los organismos de control que afectan a la organización. • Coordinar y aprobar las medidas para garantizar el cumplimiento de leyes, regulaciones o disposiciones identificadas.	ME2 Monitorear y Evaluar el Control Interno ME3 Garantizar el Cumplimiento Regulatorio

[18] Sistema Financiero: Financial Bussines System.
[19] Servicio de Pagos Interbancario
[20] Sistema Financiero: Financial Bussines System.

	• Comunicar las medidas aprobadas a todos los involucrados. • Monitorear el cumplimiento de las medidas aprobadas. • Cumplir con las disposiciones de los Organismos de control	
9. Gestión de marketing	• Realizar la publicidad de la cooperativa para la captación de socios. • Desarrollar análisis de mercado.	DS10 Administrar los problemas
10. Gestión de Información	• Capacitación sobre Custodia y Manejo de la Información Institucional. • Establecer medidas para garantizar la seguridad de la información institucional. • Elaboración de actas, disposiciones, aspiraciones o políticas emitidas por Gerencia General. • Comunicación de actas, disposiciones, aspiraciones o políticas emitidas por Gerencia General.	PO2 Definir la Arquitectura de la Información DS11 Administrar los datos DS12 Administrar el ambiente físico ME3 Garantizar el Cumplimiento Regulatorio

Tabla 1.2. Mapeo de los procesos de COBIT 4.1 con los procesos de la Organización [21]

[21] Realizado por las Autoras

Desde este punto de vista, es necesario conocer cómo el departamento de Sistemas apoya al cumplimiento de los objetivos del negocio y el nivel de participación que existe en la toma de decisiones del negocio, para ello se selecciona el proceso “PO1 Definir un plan estratégico de TI”.

Debido a que la Organización maneja información sensible para los socios es necesario conocer cómo se la administra, además de cómo el sistema financiero “Financial”[22] la utiliza y cómo la presenta a sus usuarios, razón por la cual se han escogido los procesos “PO2 Definir la Arquitectura de la Información” y “DS11 Administrar los datos”.

En cuanto a los aspectos relacionados con la administración de los recursos de TI, es necesario conocer bajo qué procesos, políticas o procedimientos se llevan a cabo, qué personas intervienen, cómo son aprobados y comunicados por la Gerencia y qué relación existe entre los miembros de toda la Organización. Por esta razón se han escogido los procesos “PO3 Determinar la Dirección Tecnológica”, “PO4 Definir los Procesos, Organización y Relaciones de TI” y “PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia para ser evaluados”.

Ya que la Organización cuenta con un Departamento de Sistemas definido es fundamental conocer su estructura organizacional interna, los responsables y sus funciones, la capacitación que tienen, quiénes intervienen en la gestión de los recursos humanos así como las políticas y procedimientos que se utilizan para la evaluación del personal. Adicionalmente, de conocer el proceso de entrenamiento que se da a los usuarios de los recursos TI para que puedan llevar a cabo sus actividades por lo cual los procesos que se son “PO7 Administrar Recursos Humanos de TI”, “AI4 Facilitar la operación y el uso” y “DS7 Educar y entrenar a los usuarios”.

La Organización contempla los riesgos dentro del plan estratégico, para ello es necesario realizar un análisis de cómo el Departamento de Sistemas realiza la identificación, mitigación y administración los riesgos de TI, por lo cual se selecciona el proceso de “PO9 Evaluar y Administrar los Riesgos de TI”.

[22] Sistema Financiero: Financial Bussines System.

De acuerdo a la perspectiva tecnológica del plan estratégico, uno de los objetivos es mejorar las operaciones institucionales. Siendo necesario analizar aquellos procesos relacionados con la identificación de soluciones de TI, la adquisición y mantenimiento tanto de software como de hardware, ya que la tecnología apoya la prestación de los servicios del negocio. Teniendo en cuenta este criterio y la existencia de un manual de Adquisiciones general, es necesario identificar los aspectos relacionados con los de TI, por esta razón seleccionan los procesos "AI1 Identificar soluciones automatizadas", "AI2 Adquirir y mantener software aplicativo", "AI3 Adquirir y mantener infraestructura tecnológica" y "AI5 Adquirir recursos de TI".

En el análisis FODA del plan estratégico, la Organización toma en cuenta los servicios de terceros para dar cumplimiento a sus servicios financieros, por lo cual es de suma importancia conocer la administración de los mismos junto con los contratos escritos y las condiciones bajo las cuales son administrados. Por esta razón se seleccionan los procesos "DS1 Definir y administrar los niveles de servicio" y "DS2 Administrar los servicios de terceros".

Dentro del mapa estratégico se consideran aspectos relacionados con "dar satisfacción al cliente externo" por lo que se necesita conocer cómo la Organización junto con el departamento de Sistemas garantizan la continuidad de los servicios para los socios, cómo se estructuran las operaciones y cómo resuelven los problemas de TI, por ello los procesos seleccionados son "DS13 Administrar las operaciones", "DS10 Administrar los problemas" y "DS4 Garantizar la continuidad del servicio".

Adicionalmente, se considera el aspecto de "Modernizar TI" para lo cual se necesita conocer el estado actual de los recursos de TI y mediante ello establecer soluciones que contribuyan a su mejora en base a tecnologías emergentes y buenas prácticas. Bajo estas razones se seleccionan los procesos "DS3 Administrar el desempeño y la capacidad" y "ME1 Monitorear y Evaluar el Desempeño de TI".

Por otro lado, se consideran los aspectos que necesitan ser mejorados con una mayor prioridad o que previamente ya se han tomado en cuenta en la Gestión de

TICs actual. Entre ellos se encuentran los referentes a la seguridad de sistemas como física que responden a las recomendaciones emitidas por los diferentes Organismos de control. Por tanto los procesos seleccionados son “DS5 Garantizar la seguridad de los sistemas” y “DS12 Administrar el ambiente físico”.

Para la selección de los procesos también se debe tomar en cuenta las leyes y regulaciones vigentes emitidas por los organismos de Control, ya que es gran importancia que la Organización mantenga un correcto cumplimiento regulatorio. De acuerdo a este criterio se han seleccionado los procesos “ME1 Monitorear y Evaluar el Control interno” y “ME3 Garantizar el cumplimiento Regulatorio”.

La razón de que los procesos mostrados en Tabla 1.3 son tomados en cuenta para la evaluación es porque dentro del plan estratégico actual no se consideran necesarios para la consecución de los objetivos del negocio.

Procesos No Seleccionados	
Dominios	**Procesos**
PLANEAR Y ORGANIZAR (PO)	PO5 Administrar la Inversión en TI PO8 Administrar la Calidad PO10 Administrar Proyectos
ADQUIRIR E IMPLEMENTAR (AI)	AI6 Administrar cambios AI7 Instalar y acreditar soluciones y cambios
ENTREGAR Y DAR SOPORTE (DS)	DS6 Identificar y asignar costos DS8 Administrar la mesa de servicios y los incidentes DS9 Administrar Configuración
MONITOREAR Y EVALUAR (ME)	ME4 Proporcionar Gobierno de TI

Tabla 1.3 Procesos no seleccionados para la evaluación[23]

En base a estos puntos, seleccionamos los procesos que se muestran en la Tabla 1.4.

[23] Realizado por las Autoras.

Procesos Seleccionados de COBIT 4.1	
Dominios	**Procesos**
PLANEAR Y ORGANIZAR (PO)	PO1 Definir un Plan Estratégico de TI PO2 Definir la Arquitectura de la Información PO3 Determinar la Dirección Tecnológica PO4 Definir los Procesos, Organización y Relaciones de TI PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia PO7 Administrar Recursos Humanos de TI PO9 Evaluar y Administrar los Riesgos de TI
ADQUIRIR E IMPLEMENTAR (AI)	AI1 Identificar soluciones automatizadas AI2 Adquirir y mantener software aplicativo AI3 Adquirir y mantener infraestructura tecnológica AI4 Facilitar la operación y el uso AI5 Adquirir recursos de TI
ENTREGAR Y DAR SOPORTE (DS)	DS1 Definir y administrar los niveles de servicio DS2 Administrar los servicios de terceros DS3 Administrar el desempeño y la capacidad DS4 Garantizar la continuidad del servicio DS5 Garantizar la seguridad de los sistemas DS7 Educar y entrenar a los usuarios DS10 Administrar los problemas DS11 Administrar los datos DS12 Administrar el ambiente físico DS13 Administrar las operaciones
MONITOREAR Y EVALUAR (ME)	ME1 Monitorear y Evaluar el Desempeño de TI ME2 Monitorear y Evaluar el Control Interno ME3 Garantizar el Cumplimiento Regulatorio

Tabla 1.4 Procesos seleccionados para la evaluación[24]

[24] Realizado por las Autoras

2. CAPÍTULO 2: EJECUCIÓN DE LA EVALUACIÓN

2.1. CONFORMACIÓN DEL GRUPO EVALUADOR.

Para la ejecución de la evaluación es necesario definir un grupo de trabajo que conozca ampliamente su área de trabajo y su relación con el departamento de Sistemas. De acuerdo con el Manual de Funciones [**3**], la información necesaria puede ser proporcionada por los jefes de los departamentos que se encuentran identificados en la Fig. 1.1, dada su experiencia y conocimiento. Por esta razón se han escogido a los jefes de aquellos departamentos que son considerados más críticos para el cumplimiento de los objetivos de la organización.

El grupo de trabajo, que desde ahora será llamado Grupo Evaluador, está conformado por las personas que se especifican en la Tabla 2.1.

Grupo Evaluador	
Cargo	**Nombre**
Gerente General	Ing. Edwin Carrera
Jefe de Sistemas	Ing. Verónica Suquillo
Jefe de Operaciones	Dr. Sadid Cassanello
Jefe de Contabilidad	Lcda. Mónica Cajiao
Evaluadoras	Karina Anasi, Paulina Paspuel

Tabla 2.1 Integrantes del Grupo Evaluador[25]

De acuerdo al Manual de Funciones, las responsabilidades de los integrantes del Grupo Evaluador que se relacionan con la gestión de TICs son las que se muestran a continuación:

Jefe de Sistemas

Las principales funciones del Jefe de Sistemas son analizar, planificar, organizar, dirigir, controlar, implementar, evaluar el sistema Financiero de la Cooperativa, permitiendo la prestación oportuna de los servicios financieros que brinda la cooperativa a sus clientes. Además se encarga del mantenimiento de la

[25] Realizado por las Autoras.

infraestructura y recursos de TI necesarios para satisfacer las necesidades de los usuarios, y participa en el proceso de adquisición de recursos y servicios de TI.

Para mayor información, consulte el ANEXO E

Gerente General

La principal responsabilidad que ejerce es la de ser el representante legal, judicial y extrajudicial de la Cooperativa. Propone al Consejo de Administración las políticas, reglamentos y procedimientos para el buen funcionamiento de la Cooperativa, además de las propuestas de plan operativo y estratégico junto con su proforma presupuestaria. Está encargado de informar a los Consejos de Administración y Vigilancia acerca de temas administrativos, operativos y financieros de la Organización junto con su gestión. También define y mantiene el control interno para la gestión eficiente y económica de la Cooperativa. Finalmente, se encarga de ejecutar las políticas sobre los precios de bienes y servicios que brinda la Cooperativa.

Jefe de Contabilidad

Entre las actividades que le conciernen al Jefe de Contabilidad destacan la ejecución del control previo de las transacciones financieras de la Organización, supervisión del manejo, registro, control y emisión adecuado de información contable de la matriz, sucursales y agencias de la cooperativa, control del manejo de la tesorería con el fin de que los fondos sean dirigidos y administrados con criterio de liquidez, rentabilidad, dispersión y seguridad, verificación diaria del cuadre de cuentas, y revisión y cuadre diario de los cajeros automáticos.

Jefe de Operaciones

Las responsabilidades que tiene asignadas dentro del Departamento de Operaciones son las siguientes: revisar los saldos en los bancos, Informar oportunamente de las disponibilidades económicas de acuerdo a reportes de estado bancarios y de caja que le permitan a la Gerencia General la toma de decisiones, legalizar diariamente la documentación referente a ingresos y egresos, supervisar que los cajeros den un excelente servicio en la recepción y

entrega de valores cumpliendo con las disposiciones legales, estatutarias, reglamentarias de la Cooperativa, recibe y revisa la conformidad de los reportes diarios del movimiento de caja con sus respectivos respaldos y revisa la tarjeta que llega del Banco del Austro y envía a las Agencias, entre otras funciones.

2.2.PLANIFICACIÓN DE LA EVALUACIÓN.

Para la realización de la evaluación de los procesos seleccionados se utilizan las directrices de auditoría de COBIT [**7**] lo que permitirá realizar una síntesis de la situación actual con respecto a la Gestión de TICs, y la herramienta Process Maturity Assessment Tool[26] proporcionada por ISACA para medir el nivel de madurez de cada uno de los procesos evaluados.

2.1.1. DIRECTRICES DE AUDITORÍA

Para el planteamiento de la evaluación de la Gestión de TICs de la Organización se emplean directrices de Auditoría de COBIT, las cuales permiten evaluar los controles, procesos, actividades y procedimientos existentes que son realizadas por el departamento de Sistemas para dar cumplimiento a los objetivos de la Organización. [**7**]

Proporcionan una guía con la que los evaluadores pueden definir el proceso de planificación y ejecución de la evaluación, tomando en cuenta varios aspectos como el alcance, la recolección de la información concerniente a los procesos a evaluarse, la determinación de los involucrados dentro de la Gestión de TICs, la documentación necesaria para la evaluación, la identificación de los recursos de TI que estén involucrados con el negocio, entre otros.

Cabe recalcar que con la utilización de las directrices de auditoría de COBIT, se consigue: [**7**]

---

[26] http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Implementing-and-Continually-Improving-IT-Governance1.aspx - Process Maturity Assessment Tool

- Determinar que se cumplan los controles apropiados para la gestión de TICs.
- Identificar las debilidades y riegos que ponen en peligro de la gestión de TICs.
- Aconsejar a los directivos y alta Gerencia sobre las medidas correctivas que deberían realizarse para crear o mejorar los controles con respecto a los procesos.
- Determinar si la orientación de los procesos de TI están ligados al cumplimiento de los objetivos del negocio.
- Identificar todos los recursos de TI y los de mayor criticidad para administrarlos adecuadamente.
- Identificar los estándares que se utilizarán para ayudar a la mejora de los procesos empleados en la Gestión de TICs.
- Justificar una evaluación de riesgos operativos como financieros que contribuyan a una Gestión de TICs que sirva de apoyo al cumplimiento de los objetivos del negocio.
- Establecer objetivos de control que ayuden a la gestión de los procesos identificados como relevantes dentro del departamento de Sistemas.

Además las directrices de Auditoría de COBIT, se cuenta con factores críticos de éxito, entre los cuales se define que “El Gobierno de TI se enfoca sobre los objetivos o metas de la organización, sus iniciativas estratégicas, el uso de la tecnología para incrementar el negocio y, sobre la disponibilidad de suficientes recursos y capacidades para soportar las demandas del negocio”[27] [**4**]

Dentro de la evaluación de la gestión de TICs existe un modelo de madurez genérico que permite determinar el nivel actual en el que se encuentra cada uno de los procesos de TICs y puede ser de utilidad como guía para definir el nivel futuro en el que debería estar dicho proceso.

Las escalas utilizadas de este modelo genérico se tomaron del marco de referencia de COBIT 4.1 y son las siguientes:

[27] Tomado de COBIT Directrices de Auditoría, cuarta edición.

NIVEL	DESCRIPCIÓN
0 No existente	Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.
1 Inicial/ Ad Hoc	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 pero Intuitivo	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 y Medible	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.

Tabla 2.2 Modelo genérico de madurez de COBIT 4.1 [28] [4]

2.1.2. RECOLECCIÓN Y SÍNTESIS DE LA INFORMACIÓN

Para obtener la información necesaria para establecer el nivel de madurez de cada proceso seleccionado se utilizan las directrices de auditoría de COBIT, lo que permite realizar tablas de síntesis en las que se ha establecido la situación actual de cada proceso, estas tablas incluyen diferentes entradas tomadas de las directrices de auditoría que son de ayuda para recolectar la información correspondiente a cada uno de los procesos seleccionados y que posteriormente

[28] Fuente: Tomado de COBIT 4.1 versión Español, página 19, Figura 13.

serán analizadas. Se utiliza una escala para valorar qué nivel de cumplimiento tiene una determina sentencia y las observaciones que se han encontrado en la misma.

Al finalizar la recolección de información de los procesos de cada dominio, se realiza una síntesis del estado actual del dominio en cuestión, con el fin de ofrecer una visión general de los procesos analizados dentro de cada dominio.

Cabe mencionar que parte de la información recolectada se encuentra respaldada por la documentación proporcionada por la Organización y cuyo listado se encuentra en el *ANEXO F*.

2.1.3. MEDICIÓN DEL NIVEL DE MADUREZ DE LOS PROCESOS

Se ha seleccionado la herramienta Process Maturity Assessment Tool[29] debido a la experiencia de su utilización por parte de las Autoras en proyectos anteriores, además de que es aplicable para la versión de COBIT 4.1 que ISACA ofrece.

Esta herramienta permite analizar y medir el nivel de madurez de los procesos basándose en el modelo de madurez de COBIT (CMM) definido en COBIT 4.1.

Para realizar el análisis de los procesos la herramienta ofrece la siguiente estructura para cada nivel de madurez en una escala de 0 a 5, No existente (0), Inicial/Ad Hoc(1), Repetible pero Intuitivo(2), Definido(3), Administrado/Medible(4) y Optimizado(5).

- Las declaraciones CMM son divididas en sentencias simples.

- Se necesita que el usuario atribuya un factor de peso (1 a 10) para indicar la importancia de cada una de las sentencias dentro de la organización y su ambiente interno y externo. Esto permite al usuario disminuir la influencia de las sentencias menos importantes o irrelevantes en la

[29] http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Implementing-and-Continually-Improving-IT-Governance1.aspx - Process Maturity Assessment Tool

calificación global de madurez del proceso. Por defecto se encuentra en un peso de 5 para cada sentencia.

- El usuario debe indicar a qué nivel de acuerdo (cumple) con cada sentencia, usando las siguientes escalas:

    - La sentencia no se cumple en absoluto (Nada).
    - La sentencia se cumple a un nivel limitado (Un poco).
    - La sentencia se cumple a un nivel significativo (Algo).
    - La sentencia se cumple completamente (Completamente).

- La multiplicación del peso por el nivel de cumplimiento de cada sentencia calculará la importancia relativa de cada una de estas sentencias.

Cabe tener en cuenta que el nivel de cumplimiento se calcula de acuerdo a la importancia relativa de cada sentencia y el peso otorgado correspondiente, de tal manera que se pueda obtener la descripción de la situación actual del proceso.

Esta estructura se encuentra distribuida en una hoja de cálculo por cada proceso que permite realizar el cálculo del nivel de madurez del proceso analizado. En la Fig. 2.1 se puede ver una vista parcial del proceso PO1 – Definir un plan estratégico –.

Los cálculos de la herramienta se realizan de la siguiente manera:

- Para calcular la importancia relativa se tiene en cuenta el peso que se asigna a cada sentencia de cada nivel de madurez por el valor que se le asigna a la sección “Está de acuerdo” (cumplimiento). Cada una de los grados de esta sección tienen un valor entre 0 y 1 divididos de la siguiente manera:

    - Nada tiene un valor de 0.
    - Poco tiene un valor de 0,33.
    - Algo tiene un valor de 0,66.
    - Completamente tiene un valor de 1.

- En la tabla que ofrece los resultados finales para el cálculo global de nivel madurez del proceso en cuestión, se toma en cuenta la importancia relativa para hallar el valor de aportación. Para el cálculo de la aportación se realiza un promedio de la importancia relativa de las sentencias por cada nivel de madurez divido para el peso total de cada nivel de madurez. Este valor se multiplica por el valor asignado en la columna de cumplimiento. Por defecto la columna de cumplimiento tiene el valor de 1 en los niveles de 1 a 5 ya que esos niveles aportan un valor a su nivel de madurez, mientras que el valor de cumplimiento del nivel no existente es cero ya que no aporta ningún valor para su nivel de madurez.

- Finalmente, el nivel de madurez global se obtiene de realizar la sumatoria de los valores obtenidos en cada nivel de madurez analizado.

Se debe tener en cuenta que para que haya una mejor comprensión de las preguntas del nivel de madurez No existente, se cambiaron las sentencias de negativas a positiva.

Process	PO1 Definir un Plan Estratégico de TI

Management of the process of *Define a strategic IT plan* that satisfies the business requirement for IT of sustaining or extending the business strategy and governance requirements while being transparent about benefits, costs and risks is: La Dirección de los procesos de Definir el plan estatégico de TI que satisfface los requerimientos del negocio para TI de sustentar o

Assessment Status	Open

LINK Back to Assessment Overview

Nivel de Madur	0	No existente

Nr	Enunciado	Peso	Está de acuerdo.. Nada	Un poco	Algo	Completamente	Relative Importance
1	La planificación estratégica se realiza.	10				x	10,00
2	Existe conciencia de la Gerencia que la planificación estratégica de TI es necesaria para dar soporte a los objetivos del negocio.	10				x	10,00
	Peso Total	20					

Nivel de Madur	1	Inicial/Ad Hoc

Nr	Enunciado	Peso	Está de acuerdo.. Nada	Un poco	Algo	Completamente	Relative Importance
1	La gerencia de TI conoce la necesidad de una planificación estratégica de TI.	10				x	10,00
2	La planificación de TI se realiza según se necesite como respuesta a un requerimiento de negocio específico.	8			x		5,28
3	La planificación estratégica es ocasionalmente discutida en las reuniones de gerencia de TI.	7		x			2,31
4	El alineamiento de los requerimientos del negocio, aplicaciones y tecnología del negocio se llevan a cabo reactivamente en lugar de hacerlo mediante una estrategia de toda la	7			x		4,62
5	La posición de riesgo estratégico se identifica de manera informal sobre una base de proyecto por proyecto.	9			x		5,94
	Peso Total	41					

PO1	Definir un Plan Estratégico de TI		
Nivel	Cumplimiento	Contribución	Valor
0	1,00	0,00	0,00
1	0,69	1,00	0,69
2	0,59	1,00	0,59
3	0,43	1,00	0,43
4	0,55	1,00	0,55
5	0,48	1,00	0,48
	Nivel de Madurez =		2,74

Instructions: A relative Peso between 0 and 10 should be allocated for each Enunciado, and then an 'x' is used to indicate which Enunciado is applicable.

Fig. 2.1 Ejemplo de la hoja de cálculo del Proceso PO1[30]

[30] Realizado por las Autoras

2.3.EJECUCIÓN DE LA EVALUACIÓN

2.3.1. PLANIFICAR Y ORGANIZAR (PO)

2.3.1.1. PO1 DEFINIR UN PLAN ESTRATÉGICO DE TI

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Políticas y procedimientos inherentes al proceso de planificación. • Misión y las metas de la organización • Análisis FODA • Mapa estratégico. • Estrategias tecnológicas.	X			
Roles y responsabilidades del equipo de Dirección • Los propietarios de procesos y la Gerencia llevan a cabo revisiones y aprobaciones formales a los planes de TI.		X		• Los roles y responsabilidades se encuentran definidos en el Manual de Funciones de la Cooperativa. • No se tienen definidos procesos documentados, las actividades de cada departamento sólo se basan en el reglamento general, reglamentos por departamento

				que tienen las políticas establecidas por la Cooperativa y las normativas que impone la SEPS[31].
Objetivos de la Organización a largo y corto plazo • Los planes a corto y largo plazo de tecnología de información son consistentes con los planes a corto y largo plazo de la organización, así como con los requerimientos de ésta.	X			• Para su cumplimiento se basa en los reglamentos internos de cada departamento además del crecimiento de la Cooperativa, satisfacción de los socios, tendencias tecnológicas.
Objetivos de TI a largo y corto plazo • Iniciativas de tecnología de información para soportar la misión y las metas de la organización • Estudios de factibilidad de las iniciativas de tecnología de información. • Evaluación de los riesgos de las iniciativas de tecnología de información. • Inversiones óptimas en tecnologías de información actuales y futuras. • Los proyectos de TI están soportados por la documentación apropiada según lo definido en la metodología de planificación de tecnología de		X		• Las iniciativas de tecnología de información se transmiten a la Gerencia General para ser aprobadas por el Comité Ejecutivo y luego el Consejo de Administración. Las iniciativas son generadas por experiencia del Jefe de Sistemas y por necesidades del negocio. • Se realizan estudios internos de factibilidad basados en la satisfacción de requerimientos (tiempos de respuesta a los usuarios, disponibilidad del servicio, análisis costo-beneficio) del Departamento de Sistemas, pero estos no son documentados ni formalmente aceptados. • Para la inversión en tecnología se tiene en cuenta el análisis costo-beneficios que realiza el departamento

[31] Superintendencia de Economía Popular y Solidaria

información.				de Sistemas y de acuerdo con las necesidades del negocio. • No se tiene una metodología definida. Únicamente se reportan documentos con los resultados de un análisis de costo-beneficio al Gerente y las razones por las que se necesita un determinado recurso. Además, se llevan a cabo reuniones informales para conseguir la aprobación de cada proyecto de TI.
Reportes y minutas de seguimiento de las reuniones del comité de Planificación/Dirección.	X			• Si se tienen actas y libros correspondientes de cada sesión realizada para la toma de decisiones de la organización.

Tabla 2.3 Directrices de auditoría del PO1

2.3.1.2. PO2 DEFINIR LA ARQUITECTURA DE INFORMACIÓN

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Políticas y procedimientos sobre la arquitectura de información. • Estándares internacionales/ Buenas prácticas		X		• No se tienen políticas o procedimientos, se basan en estándares establecidos en la Organización, sólo se rigen por el reglamento general, las políticas establecidas por la Cooperativa y las normativas que

				impone la SEPS[32].
Modelo de la arquitectura de información. • El proceso utilizado para actualizar el modelo de la arquitectura de información toma como base los planes a corto y largo plazo, considera los costos y riesgos asociados y asegura que las aprobaciones formales de la Gerencia sean obtenidas antes de hacer modificaciones al modelo.		X		• Sólo el Jefe de Sistemas puede realizar modificaciones a la base de datos. Para cualquier modificación en la arquitectura de información se consulta con Gerencia General, para la recolección de requerimientos y la toma de decisiones.
• Documentos que soporten el modelo de la arquitectura de información, incluyendo el modelo de datos corporativo		X		• No se tienen documentos sobre la arquitectura de información como el modelo de base de datos, pero para realizar modificaciones a la base de datos existen los respectivos registros en el documento de Paso a Producción y Parametrización.
Diccionario de datos corporativo. • Reglas de sintaxis de datos. • Utiliza algún proceso para mantener			X	• No existe la definición de un diccionario de datos corporativo.

[32] Superintendencia de Economía Popular y Solidaria

actualizado. • Utiliza algún proceso para mantener actualizado.				
Política de propiedad de datos • Clasificación de los datos. • Categorías de seguridad. • Reglas de acceso. • La existencia de un proceso de autorización que requiera que el propietario de los datos autorice todos los accesos a estos datos.		X		• Las seguridades que se aplican a los datos se implementa mediante perfiles de usuarios creados en el sistema Financial. • Las reglas de acceso se implementan dentro del sistema Financial desde el módulo de administración de usuarios. • No se tiene un proceso documentado de autorización que requiera que el propietario de los datos deba autorizar todos los accesos a determinados datos.

Tabla 2.4 Directrices de auditoría del PO2

2.3.1.3. PO3 DETERMINAR LA DIRECCIÓN TECNOLÓGICA

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Políticas y procedimientos relacionados con la planificación y el monitoreo de la infraestructura tecnológica. • Existe un proceso para la creación y la			X	• No se tiene un plan de infraestructura tecnológica independiente, sino que la planificación de la infraestructura se encuentra dentro del plan operativo anual. La evaluación de costos y riesgos se analizan

actualización regular del plan de infraestructura tecnológica para confirmar que los cambios propuestos estén siendo examinados primero para evaluar los costos y riesgos inherentes.				internamente en el departamento de Sistemas y sus resultados son trasmitidos a la Gerencia General para la aprobación y toma de decisiones.
Roles y responsabilidades de la Gerencia de Dirección. • Gerencia apruebe el plan antes de realizar algún cambio	X			
Objetivos y planes a largo y corto plazo de la organización. • Identificar los costos y riesgos asociados, y que dichos cambios reflejen las modificaciones a los planes a largo y corto plazo de tecnología de información.		X		• Se identifican costos y riesgos en la infraestructura de acuerdo a las modificaciones que requiera el negocio y el estudio de factibilidad realizado internamente en el departamento de sistemas. No se tiene documentación formal.
Plan de adquisición de hardware y software de tecnología de información. • Se planean el impacto logístico y ambiental de las adquisiciones tecnológicas. • Suelen satisfacer las necesidades identificadas en el plan de infraestructura tecnológica y si éstos son aprobados		X		• El análisis del impacto de las adquisiciones tecnológicas se realiza de acuerdo a la experiencia del Jefa de Sistemas y no basado en una metodología determinada, sino en estándares propios. • La infraestructura sí satisface las necesidades identificadas, pero éstas se encuentran reflejadas en el plan operativo anual.

apropiadamente				
Plan de infraestructura tecnológica. • El plan de infraestructura tecnológica está siendo comparado contra los planes a largo y corto plazo de tecnología de información			X	• No se tiene un plan de infraestructura ni de tecnologías de la información. Esto se encuentra especificado en el plan operativo anual.
Estándares de tecnología. • La necesidad de evaluar sistemáticamente el plan tecnológico para aspectos de contingencia. • Estándares para los componentes tecnológicos descritos en el plan de Infraestructura tecnológica.			X	• No se tiene un plan tecnológico, excepto el plan operativo anual del departamento de sistemas. • No se tienen estándares para los componentes tecnológicos.

Tabla 2.5 Directrices de auditoría del PO3

2.3.1.4. PO4 DEFINIR LA ORGANIZACIÓN Y RELACIONES DE TI

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Roles y responsabilidades de la Gerencia de Planificación/dirección.		X		• Existe control de cumplimiento de los roles y responsabilidades mediante el formato de desempeño emitido por el departamento de Talento Humano,

• Control del cumplimiento de roles y responsabilidades. • Asignación de un oficial de seguridad para formulación de políticas y procedimientos de control interno y de seguridad.				además del control que lleva a cabo el Jefe del Departamento de Sistemas con respecto a cumplimiento de tareas asignadas y conducta. • No se tiene un oficial de seguridad y tampoco se tienen políticas o procedimientos de seguridad. Se tienen disposiciones gerenciales que hacen referencia al control interno y seguridad.
Organigrama organizacional que muestre la relación entre TI y otras funciones. • Segregación de funciones.		X		• Se tienen definidas las funciones para los roles de Jefe del departamento de Sistemas, programador y Help desk. Sin embargo, en la práctica, las funciones son realizadas por las 3 personas de acuerdo a la disponibilidad de tiempo de cada una.
Políticas y procedimientos relacionados con la organización y las relaciones de TI. • Procesos e indicadores de desempeño para determinación de la efectividad y aceptación de TI. • Procesos de concienciación, comprensión y habilidad para resolución de problemas de administración de información, seguridad y control interno. • Procedimientos aplicables a los contratos de TI, adecuados y consistentes con las políticas		X		• No se tienen procesos documentados para determinación de la efectividad y aceptación de TI. Sin embargo, los indicadores de desempeño son identificados y medidos internamente de acuerdo a la experiencia del Jefe de Sistemas. • No se tienen procesos documentados de concienciación, comprensión y habilidad para resolución de problemas de administración de información, seguridad y control interno. • No se tienen procedimientos documentados para la realización de contratos. Los contratos dependen de cada proveedor y de los términos que se acuerden

de adquisición de la organización. • Procesos para coordinar, comunicar y documentar los intereses dentro y fuera de la estructura organizacional de TI.				entre el cliente y el proveedor. • No se tiene un proceso definido, pero Gerencia emite comunicados y disposiciones para dar a conocer las resoluciones tomadas a nivel tecnológico y organizacional.
Políticas y procedimientos relacionados con el aseguramiento de la calidad. • Identificación y definición de la calidad de roles y responsabilidades. • Programación de recursos, cumplimiento de las pruebas, aprobación del aseguramiento de la calidad antes de que se implementen nuevos sistemas o se produzcan cambios.		X		• No se identifica ni define la calidad de roles y responsabilidades. • No se tienen un procedimiento para evaluar la calidad, sin embargo, internamente el departamento de Sistemas realiza pruebas de funcionamiento y de aceptación antes de la entrega de un equipo o sistema al usuario final antes de que entre a producción.
Políticas y procedimientos utilizados para determinar los requerimientos de asignación de personal de TI		X		• No se tienen políticas o procedimientos en este aspecto, sin embargo, el Jefe de Sistemas puede sugerir la contratación de más personal para cubrir con las necesidades de la organización.

Organigrama organizacional de TI. • Políticas que consideran la necesidad de evaluar y modificar la estructura organizacional para satisfacer objetivos y circunstancias cambiantes.	X			• Se evalúa y se hace modificaciones del organigrama funcional, de acuerdo a los requerimientos del negocio o de disposiciones de la SEPS[33].
Roles y responsabilidades de TI. • Determinación de roles y responsabilidades con respecto a sistemas de información, control interno y seguridad, y procesos claves.		X		• Se tienen definidas las funciones para los roles de Jefe del departamento de Sistemas, programador y Help desk. Pero no se tienen asignadas personas a los procesos claves puesto que no se tienen definidos procesos formales dentro de la Organización.
Descripción de los puestos clave de TI. • Existencia de evaluación y reevaluación de las descripciones de puestos de trabajo de TI.	X			• Se realizan evaluaciones de cada puesto de trabajo descrito en el manual de funciones como mínimo una vez al año y cuando se requiera crear nuevos puestos de trabajo para satisfacer las necesidades del negocio.

Tabla 2.6 Directrices de auditoría del PO4

[33] Superintendencia de Economía Popular y Solidaria

2.3.1.5. PO6 COMUNICAR LAS ASPIRACIONES Y LA DIRECCION DE LA GERENCIA

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Políticas y procedimientos relacionados con el marco referencial de control positivo y el programa de concienciación de la administración, con el marco referencial de seguridad y control interno y con el programa de calidad de servicios de información. • Procedimientos apropiados para asegurar que el personal comprende las políticas y procedimientos implementados. • Programas de conocimiento y conciencia formal para proporcionar comunicación y entrenamiento sobre el ambiente positivo de control de la administración.		X		• No existe procedimientos que aseguren la comprensión de políticas y procedimientos, pero sí se transmiten por medio de comunicados y disposiciones de la Gerencia General.
Reportes de estatus y minutas de las reuniones del comité de planificación. • Documentación de decisiones administrativas sobre sistemas o tecnologías.	X			• Se tienen actas y libros correspondientes de cada sesión realizada para la toma de decisiones de la organización.

Tabla 2.7 Directrices de auditoría del PO6

2.3.1.6. PO7 ADMINISTRAR RECURSOS HUMANOS DE TI

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Políticas y procedimientos relacionadas con la administración de recursos humanos • Se da reforzamiento a la política de no interrumpir los días de descanso. • Si el proceso de retiro del personal de seguridad de la organización es adecuado. • Los procesos de terminación de contrato y cambio de puesto aseguran la protección de los recursos de la organización. • Las políticas y procedimientos de recursos humanos concuerdan con leyes y regulaciones aplicables.		X		• Los días de vacaciones y descanso únicamente se gestiona a través del Reglamento Interno de Trabajo y de acuerdo con el plan anual de vacaciones elaborado por el departamento de Talento Humano • El departamento de Talento Humano toma en consideración las recomendaciones que da la SEPS[34] para talento humano y se toman medidas para cumplir con las leyes y regulaciones aplicables. • En caso de que una persona deje de pertenecer a la organización, el Departamento de Sistemas elimina la cuenta del usuario en cuestión para evitar que pueden ingresar al sistema una vez que haya dejado el puesto de trabajo de forma permanente.

[34] Superintendencia de Economía Popular y Solidaria

Descripciones de puestos, formas de evaluación del desempeño y formas de desarrollo y entrenamiento. • Programas de entrenamiento consistente, con requerimientos mínimos documentados relacionados con educación, conocimiento y la conciencia. • El compromiso de la administración con el entrenamiento y el desarrollo profesional. • Procesos de entrenamiento cruzado y respaldo de personal para las funciones de posiciones críticas. • Evaluaciones tomando como base un conjunto estándar de perfiles de competencia para la posición de forma periódica.		X		• Los programas de entrenamiento son gestionados por Talento Humano y se realizan en coordinación con los otros departamentos para reforzar el conocimiento en ciertos aspectos de sus áreas. • Se cuenta con el compromiso de la administración para el entrenamiento y desarrollo profesional. Esto se hace con la aceptación de cursos específicos y generales cuando sea necesario. • No se tiene respaldo de personal para las funciones de posiciones críticas. • Sí se llevan a cabo evaluaciones periódicas del desempeño del personal.
Expedientes del personal y archivos de puestos de trabajo para posiciones seleccionadas • Criterios para reclutamiento y selección de personal. • Especificaciones de habilidades y conocimientos requeridos.	X			• El procedimiento seguido para reclutamiento y selección de personal es dirigido por Talento Humano y es aceptado y conocido por el resto del personal de la organización.

Tabla 2.8 Directrices de auditoría del PO7

2.3.1.7. PO9 EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Políticas y procedimientos relacionados con la evaluación de riesgos • Marcos referenciales para la evaluación sistemática de riesgos. • Evaluación actualizada regular de riesgos a nivel global y específico de sistemas. • Procedimientos de evaluación de riesgos que toman en cuenta factores internos y externos, y consideran resultados de auditorías, inspecciones e incidentes identificados. • Balance entre las medidas de detección, prevención, corrección y recuperación utilizadas. • Procedimientos formales para comunicar el propósito de la medición de los controles.			X	• No se tienen marcos referenciales para la evaluación del riesgo. Únicamente se cuenta con la experiencia del personal de TI y se realizan de manera interna en el departamento de Sistemas. • No se realiza una evaluación regular de riesgos a nivel de global, sin embargo el análisis de riesgos de TI se realizan en cada proyecto, de manera informal. • No se tienen procedimientos de evaluación de riesgos. Cada evaluación del riesgo se hace de acuerdo a los nuevos requerimientos del negocio que requieran ser implementados. • No se tiene en cuenta un balance entre las medidas de detección, prevención, corrección y recuperación usadas. • No se tienen procedimientos para comunicar el propósito de la medición de controles
Documentos de evaluación de riesgos del negocio. • Incluyen los objetivos de la organización en el		X		• No existe documentación de evaluación de riesgos, pero se maneja internamente dentro del departamento de Sistemas.

proceso de identificación de riesgos.				
Documentos de evaluación de riesgos operativos • Procedimientos para monitoreo y mejoramiento continuo de la evaluación de riesgos y procesos para la creación de controles que mitiguen los riesgos.		X		• No existe documentación de evaluación de riesgos, pero se maneja internamente dentro del departamento de Sistemas.
Detalles de la base sobre la cual se miden los riesgos y la exposición a los riesgos • Incluyen descripción de la metodología de riesgos, identificación de la exposición significativa. • Se usan técnicas de probabilidad, frecuencia y análisis de las amenazas en la identificación de riesgos o cálculos y otros métodos en la medición de riesgos, amenazas y exposiciones.		X		• No existe metodología de riesgos pero sí se realiza la identificación de los mismos a nivel interno del departamento de manera informal, y son comunicados a la Gerencia mediante oficios o reuniones informarles. • No se utilizan técnicas de probabilidad, en su lugar se definen estimaciones con el establecimiento de escenarios y las posibles pérdidas económicas en el establecimiento de los riesgos operativos.
Expedientes de personal para personal seleccionado de evaluación de riesgos			X	• No existe un área que se encargue de la evaluación de riesgos, por lo que el personal que se encarga de dicha tarea es el asignado al departamento de TI.

Políticas de seguros que cubren el riesgo residual • Se toma en cuenta la política organizacional, identificación y medición de riesgos, incertidumbre inherente al enfoque de la evaluación de riesgos, el costo y la efectividad de implementar salvaguardas y controles.			X	• Solo se tienen seguros para riesgos que puedan producir perdidas.
Resultados de las opiniones de expertos o grupos especializados.			X	• Se realiza internamente.
Consulta de las bases de datos de administración de riesgos			X	• No existe una base de datos de administración de riesgos.

Tabla 2.9 Directrices de auditoría del PO9

2.3.1.8. Síntesis global del dominio PO

La Organización en un nivel general está consciente de la importancia de definir procesos documentados para el manejo de tecnologías de información. Sin embargo, estos procesos no han sido definidos formalmente, por lo que son realizados de manera intuitiva y repetitiva. No se cuenta con documentación de las funciones realizadas por el departamento de Sistemas lo que impide una comunicación clara y directa con el resto de la Organización.

Por otro lado, la planificación estratégica de TI se encuentra alineada con la de la Organización lo que permite definir objetivos claros a corto y largo plazo, están sujetos a actualizaciones en base a la aparición de nuevos requerimientos del negocio, regulaciones, aspectos legales y tecnologías emergentes en la industria.

Cabe recalcar que la gestión de Talento Humano de TI establece una organización del departamento de Sistemas anual y sus funciones son sensibles a cambios. Además el Jefe de Sistemas responde al cumplimiento de sus funciones en base a la experiencia, práctica y habilidades adquiridas anteriormente.

Por último, el análisis de riesgos tecnológicos se realiza internamente por el Jefe de sistemas y no cuenta con un proceso documentado, pero sigue una política de comunicación directa a Gerencia General, y se lo realiza de acuerdo a su experiencia y conocimiento adquirido; cabe mencionar que esta responsabilidad no está dentro de sus funciones definidas en el Manual de Funciones de la Organización.

2.3.2. ADQUIRIR E IMPLEMENTAR (AI)

2.3.2.1. AI1 Identificar soluciones automatizadas

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Políticas y procedimientos relacionados con el ciclo de vida de desarrollo de sistemas y con la adquisición de software: • Se ha desarrollado e implementado un enfoque de adquisición central, que describa un conjunto común de procedimientos y estándares para ser seguidos en la adquisición de hardware, software y servicios de tecnología de información. • Existe documentación de los requerimientos de usuarios satisfechos por el sistema existente o a ser satisfechos por el nuevo sistema propuesto o modificado que son revisados y aprobados. • Existe documentación de los requerimientos operativos y funcionales de		X		• El enfoque para la adquisición se encuentra en el manual de Adquisiciones de la Cooperativa, en el que se describen los procedimientos para adquirir cualquier recurso que requiera la empresa. Las autoridades encargadas de aprobar la compra son Gerencia General, Consejo de Administración y su decisión depende del monto del recurso. • Existe una solicitud de requerimientos que los usuarios utilizan para manifestar sus necesidades al departamento del sistema con respecto a hardware y software que utilicen en sus lugares de trabajo. Estas solicitudes son analizadas por el Jefe de Sistemas lo más pronto posible para su cumplimiento. En cuanto se satisfaga el requerimiento el usuario firma un documento de conformidad. • En el manual de adquisiciones se establece que

la solución o soluciones alternativas que incluyen aspectos como el desempeño, seguridad, confiabilidad, compatibilidad. • Las alternativas para la adquisición de los productos de software están claramente definidos y que se puedan adquirir en el mercado, internamente desarrollados, a través de contratos o mejorar el software existente. • Existe un estudio de factibilidad técnica para cada alternativa con el fin de satisfacer los requerimientos establecidos por el usuario. • En cada proyecto de desarrollo, modificación o implementación de sistemas, se lleva a cabo un análisis de los costos y los beneficios. • Se toma en cuenta el modelo de datos de la empresa mientras se identifica y analiza la factibilidad de las soluciones. • Se prepara y documenta un análisis de las amenazas a la seguridad, de las debilidades y los impactos potenciales y las salvaguardas factibles de seguridad y control interno para reducir o eliminar el				deben existir al menos 3 alternativas (proveedores) para la adquisición de soluciones tecnológicas, las cuales entran a un concurso de compra que es analizado por el comité ejecutivo finalmente aprobada por el consejo de administración de acuerdo al monto de la solución tecnológica. • Se realiza un análisis de factibilidad de acuerdo a la experiencia y práctica del Jefe de Sistemas, cuyos resultados son comunicados a Gerencia General, para que sean tomados en cuenta con respecto a la adquisición e implementación de nuevas soluciones. • Si existe un análisis de costo y beneficio para adquisición e implementación de soluciones tecnológicas, sin embargo es un proceso que se realiza internamente en el departamento. • No existe un modelo de datos definido para la identificación de soluciones tecnológicas • Existe un análisis de riesgos que es manejado por el Jefe de Sistemas internamente en el departamento, sin embargo esta función no es responsabilidad asignada a este cargo. • No existen controles ni pistas de auditoria. Sólo se tienen documentos de pasos a producción

riesgo identificado. • Se requieren controles y pistas de auditoría apropiados para ser aplicados en todos los sistemas modificados o nuevos propuestos durante la fase de diseño del proyecto. • Existe un acuerdo con los proveedores de un plan de aceptación para tecnología específica.				cuando se realiza una actualización o cambio en el sistema. • No existe un plan de aceptación para tecnología con los proveedores, únicamente existe una relación contractual con los mismos.
Los contratos seleccionados relacionados con la compra, desarrollo o mantenimiento de software. • Están sujetos a pruebas y revisiones antes de ser aceptados. • En las especificaciones del contrato existen: pruebas de sistema, pruebas de integración, pruebas de hardware y componentes, pruebas de procedimientos, pruebas de carga y estrés, pruebas de afinamiento y desempeño, pruebas de regresión, pruebas de aceptación del usuario, y finalmente, pruebas piloto del sistema total para evitar cualquier falla inesperada del sistema.		X		• Los contratos no están sujetos a pruebas antes de su aceptación pero si a revisiones de Gerencia, Comité Ejecutivo y Consejo de Administración • Dependiendo de la solución tecnológica se pueden incluir pruebas de integración, pruebas de carga, sin embargo esto no es algo estándar para todos los contratos, ya que los términos de los contratos depende de cada proveedor.

Tabla 2.10 Directrices de auditoría del AI1

2.3.2.2. AI2 Adquirir y mantener software aplicativo

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Políticas y procedimientos relacionados con la metodología del ciclo de vida del desarrollo de sistemas. • Existe una metodología del ciclo de vida de desarrollo de sistemas de la organización que se aplica tanto para el desarrollo de nuevos sistemas como para sus modificaciones. • Existen el vínculo con el usuario al crear las especificaciones de diseño y al verificarlas contra los requerimientos del usuario. • Las especificaciones de diseño son aprobadas por Gerencia, los departamentos usuarios afectados. • Se especifican los mecanismos adecuados para la recolección y captura, documentación de requerimientos (seguridad y control internos) para cada proyecto nuevo o modificado.		X		• Sí existe una metodología del ciclo de vida del desarrollo de sistemas compuesto por las fases: recolección de requerimientos, desarrollo, pruebas y aprobación, para la modificación del sistema actual. • El usuario puede interactuar con la especificación de diseño durante todo el ciclo de vida del desarrollo o modificación del sistema. • Las especificaciones son aprobadas por Auditoria Interna, Gerencia General, Jefatura de Sistemas y finalmente por el usuario solicitante. • Se utiliza un formato de solicitud de requerimientos que consta de: origen, área, departamento, prioridad, detalle del requerimiento, persona que lo solicita, comentario, aprobado por, fecha de inicio, fecha de fina y la asignación a un responsable. • No existe un plan de pruebas del software de aplicación, solamente las aprobaciones dentro del ciclo de vida de desarrollo del sistema por parte

• Existe el software de aplicación que es probado de acuerdo con el plan de pruebas del proyecto y los estándares establecidos antes de ser aprobado por el usuario. • Se preparan manuales adecuados de soporte y referencia para usuarios (preferiblemente en formato electrónico) como parte del proceso de desarrollo o modificación de cada sistema.				del usuario y de auditoria interna. • Existen manuales proporcionados por el proveedor del Sistema Financial. En caso de realizar alguna modificación a la funcionalidad del sistema, se realizan manuales de usuario para los cambios que la Jefatura de Sistemas considera convenientes.

Tabla 2.11 Directrices de auditoría del AI2

2.3.2.3. AI3 Adquirir y mantener infraestructura tecnológica

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Políticas y procedimientos relacionados con la adquisición, implementación y mantenimiento de hardware y software. • Existen políticas y procedimientos para el mantenimiento preventivo de hardware para reducir la frecuencia y el impacto de las fallas de desempeño.		X		• Existe un procedimiento de mantenimiento preventivo, y se lo realiza en períodos regulares. • No existe un plan de evaluación para el nuevo hardware y software, pero para soluciones de software existe un ambiente de prueba antes de su paso a producción. • No existe la amenaza de pérdida de datos debido a

• Existe un plan de evaluación formal para el nuevo hardware y software en cuanto al impacto sobre el desempeño global del sistema. • La preparación, instalación y mantenimiento del software del sistema no amenaza la seguridad de los datos y programas almacenados en el sistema.				que se tienen respaldos de la información sensible del negocio, de igual manera los programas se prueban antes de ser puestos en el ambiente de producción.
Documentación sobre vendedores de hardware y software.	X			
Contratos de arrendamiento o acuerdos de arrendamiento con opción de compra de hardware y software	X			

Tabla 2.12 Directrices de auditoría del AI3

2.3.2.4. AI4 Facilitar la operación y el uso

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Los procedimientos de operación y usuarios antes de la implementación, durante las pruebas de aceptación son para asegurarse de que son		X		• No tienen materiales de capacitación para todas las funciones del sistema, únicamente para las que son consideradas como necesarias por parte

completos, exactos y utilizables. • Se crean todas las instrucciones necesarias para el usuario, documentación, procedimientos y materiales de capacitación de manera oportuna para permitir el uso eficiente y eficaz del nuevo sistema. • Se cuenta con documentación informativa y comprensible para el usuario final y los materiales de referencia estén diseñado para todos los niveles de especialización, escrito en un lenguaje sencillo y fácil accesible (por ejemplo, la documentación electrónica). • Se involucrar a grupos de usuarios finales en la creación de la documentación soporte al usuario final, e integrar los procedimientos con los procedimientos de usuario final existentes.				del Jefe de Sistemas. En otros casos este procedimiento se realiza de manera directa al personal. • La documentación generada por el departamento de Sistemas maneja un lenguaje comprensible para los usuarios, y es accesible a los involucrados que lo requieran. • Para la documentación de soporte al usuario únicamente interviene la persona que realice los cambios o actualizaciones del sistema.
Funciones de gestión, procedimientos de seguridad y control, y requisitos de capacitación. • Existe capacitación a los usuarios finales sobre cómo utilizar el sistema de forma eficaz.		X		• El manual de operaciones define como cada usuario debe realizar sus funciones en el módulo correspondiente del sistema. Si existe un cambio al sistema, el Jefe de Sistemas considera necesaria la realización de manuales para la capacitación de los usuarios o una capacitación

• Recopilar información periódica de los usuarios finales, sobre la modificación de la documentación del usuario final, los procedimientos y la capacitación relacionada.				informal. • No existe recopilación periódica de usuarios finales.

Tabla 2.13 Directrices de auditoría del AI4

2.3.2.5. AI5 Adquirir recursos de TI

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Las políticas de TI y los procedimientos de contratación se alinean con las políticas, procedimientos de adquisiciones de la organización. • Participación de la experiencia en TI en un contrato legal que responda a riesgos relacionados con la adquisición. • Existe soporte de software de proveedores y medidas de seguridad.		X		• Los términos de los contratos legales los establece el proveedor, los revisa el Gerente, Comité Ejecutivo y Consejo de Administración dependiendo del monto de la adquisición tecnológica. • Se tiene un soporte de software de proveedores únicamente para software contratado.
Documentación en la recepción de todos los equipos y adquisiciones de software, un inventario	X			

de activos, y evaluación de la calidad antes de hacer la compra. • Se tiene confirmación de que la tecnología adquirida se entrega según las necesidades propuestas con pruebas estándar de los recursos de software/hardware en ambientes adecuados con datos representativos.				
Políticas de gestión de contratos de proveedores y procedimientos de acuerdo con los términos y condiciones legales. • Existen requisitos de licencias y arrendamientos y existe responsabilidades del proveedor y del cliente. • Existen las normas de seguridad, requisitos de control de gestión de documentos y control de calidad de proveedores requeridos.		X		• Existen software aplicativo sin licenciar aunque se requiere la necesidad de la compra de licencias por la SEPS[35]. • En el contrato se encuentran establecidos las responsabilidades tanto del cliente como del proveedor de un determinado recurso de TI. • Únicamente existen normas de seguridad de los proveedores para software contratado.

Tabla 2.14 Directrices de auditoría del AI5

[35] Superintendencia de Economía Popular y Solidaria

2.3.2.6. Síntesis global del dominio AI

La Organización está consciente de la necesidad de adquirir e implementar soluciones tecnológicas que apoyen al cumplimiento de los objetivos del negocio, por esta razón existe un manual de adquisiciones que se enfoca en aspectos globales del negocio. Sin embargo, cabe mencionar que no existe un proceso específico de adquisición de recursos y soluciones de TI.

La responsabilidad de identificar y mantener soluciones automatizadas está a cargo del Jefe de Sistemas, mientras que la adquisición depende de la Alta Gerencia. En el proceso de adquisición, el Departamento de Sistemas se encarga de proporcionar una terna de proveedores basado en un análisis de costo-beneficio y de riesgos tecnológicos que es analizado por el Comité Ejecutivo y finalmente aprobado por la Alta Gerencia.

En cuanto al mantenimiento de recursos de TI, se lo realiza de manera preventiva y correctiva en periodos regulares, sin un proceso documentado. Se realiza sin la utilización de una metodología pero se lleva a cabo de acuerdo a las habilidades, práctica y experiencia del personal del Departamento de Sistemas.

Por otro lado, existe la documentación de manuales de operación proporcionados por el proveedor del Sistema Financial mientras que la producción de la documentación para manuales de operación, material de entrenamiento y documentación de usuarios para las modificaciones al sistema, no está estandarizada y sólo existe en casos considerados como necesarios por el Jefe de Sistemas. Cabe mencionar que la producción de documentación no está contemplada dentro de un plan sino que se realiza de acuerdo a requerimientos del negocio y usuarios.

2.3.3. ENTREGAR Y DAR SOPORTE (DS)

2.3.3.1. DS1 Definir y administrar los niveles de servicio

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Políticas y procedimientos generales para la organización asociadas a las relaciones proveedor/usuario. • La participación en el proceso por parte del usuario se requiere para la creación y modificación de acuerdos. • Existe la definición de las responsabilidades de proveedores y usuarios.		X		• Los usuarios no forman parte de la creación ni de la modificación de los acuerdos. Este proceso es definido por los proveedores de los servicios y revisado por asesoría legal, mientras que para la aceptación interviene la Alta Gerencia. • En los acuerdos existen cláusulas que asignan las responsabilidades de los proveedores así como las que los usuarios deben cumplir durante la adquisición del servicio.
Políticas y procedimientos de la función de servicios de información. • Acuerdos de nivel de servicio como definición, costo, nivel mínimo, nivel de soporte, disponibilidad, confiabilidad, plan de continuidad, requerimientos de seguridad, pagos, mejoras del servicio.		X		• Los acuerdos de nivel de servicio cuentan con aspectos legales como asignación de responsabilidades del proveedor del servicio, personas que van a utilizar el servicio, especificaciones del servicio, condiciones de actualizaciones o modificaciones del servicio, costos del servicio, fecha de inicio y

• Contenido de emisión de reportes operativos, tiempos y distribución. • Métodos de seguimiento de desempeño, revisión/renovación, Actividades de acción correctiva y revisión. • Los usuarios apropiados están conscientes, tienen conocimiento y comprensión con los procesos y procedimientos del acuerdo de nivel de servicio. • Se da seguimiento al desempeño histórico comparándolo con el compromiso de mejora al servicio determinado.				terminación, sanciones por incumplimiento del servicio pero no cuentan con especificaciones tecnológicas del servicio. • Los reportes existen para la aceptación y firma del SLA, mientras que existen documentación de desempeño en casos en que las herramientas propias del servicio los proveen y en informes de actividades del departamento de Sistemas, o en casos de Alta Gerencia los solicite al departamento de Sistemas. • Dentro del SLA se determinan cláusulas para la renovación de los acuerdos o cualquier otra modificación en base a condiciones legales. • Los usuarios tienen conocimiento de los SLA en cuanto al costo y definición del servicio, mas no del procedimiento completo del mismo. • No existe la comparación del desempeño histórico de los servicios por lo tanto no existe una mejora continua del mismo. Únicamente se presentan cambios en los servicios basados en la aparición de nuevos requerimientos.
Documentación de la función de servicios de		X		• En cuanto a la administración de reportes existe para los servicios cuyas herramientas

información • Existe la administración de reportes de desempeño de nivel de servicio sobre todos los problemas encontrados • Programas de mejora del servicio • Acciones a seguir ante la ocurrencia de un bajo desempeño • Acuerdos de niveles de servicio con usuarios internos y externos y proveedores de servicio				propias proporcionan los reportes. • No existen programas de mejoras del servicio, únicamente cambian con la aparición de nuevos requerimientos del negocio. • Si ocurre un bajo desempeño en los servicios son notificados a Gerencia, se analizan las causas del bajo desempeño y el Jefe de Sistemas propone soluciones a Gerencia para que finalmente sean aceptadas. • Los acuerdos de niveles de servicio existen únicamente con los proveedores; mientras que acuerdos con usuarios internos y externos están definidos en sus contratos laborales.

Tabla 2.15 Directrices de auditoría del DS1

2.3.3.2. DS2 Administrar los Servicios de Terceros

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Políticas y procedimientos generales para la organización asociadas con los servicios adquiridos y en particular, con proveedores • Existen políticas y procedimientos de TI			X	• No existen políticas ni procedimientos específicos de TI para la negociación de los contratos. Este procedimiento es realizado por las políticas de la Gerencia, Consejos de

consistentes con las políticas de la organización para la negociación apropiada de los contratos. • Estas políticas y procedimientos especifican la necesidad de contratos, su contenido, y sus administradores. • Los contratos especifican que son hechos para la continuidad de los servicios. • El contenido de los contratos constan aspectos como: seguridad lógica y física, mantenimiento de la calidad por parte de los proveedores, planeación de contingencias y outsourcing, procesos de disolución, proceso de solución de problemas, duración del contrato, requerimientos de seguridad, garantías de confidencialidad, sanciones por bajo desempeño, servicios proporcionados, aprobación formal administrativa y legal. • Existen subcontratos. • Existe independencia entre el proveedor y la organización.				Administración, Vigilancia y Asesoría Legal. • Las políticas y procedimientos en la especificación de contratos que se utilizan son las establecidas en el reglamento general de la empresa, junto con las clausulas mencionadas anteriormente. • Dentro de los contratos únicamente se especifica la descripción del servicio más no especificaciones sobre su continuidad. • El Contenido de los contratos no especifica a detalle los aspectos sobre seguridad lógica y física, garantías, sanciones por bajo desempeño sino que se indica de forma general, al igual que en lo relacionado con los términos de disolución del contrato por el servicio contratado. • Únicamente existen contratos para los servicios de proveedores con terceros, no subcontrataciones. • La relación de dependencia entre la organización y el proveedor se enfoca en la prestación de servicio de manera óptima.
Políticas y procedimientos de la función de servicios de información.		X		• El proceso de selección de proveedores de servicios de terceros de TI son realizados por el Jefe de Sistemas, basado en proformas, en

• Existen procedimientos de selección de proveedores. • El monitoreo continuo de liberación y entrega de servicios por parte de terceros es llevado a cabo por la administración. • Existen los reportes de evaluación para terceros con el fin de evaluar sus capacidades para entregar el servicio requerido.				aspectos de tecnologías emergentes, y en un histórico de proveedores. Sin embargo, es un proceso que no se encuentra documentado. • No se tiene un proceso de monitoreo continuo; en su lugar existen revisiones del desempeño de los servicios por parte del personal de sistemas y de forma reactiva en caso de surgimiento de problemas. • Los reportes de evaluación de los servicios de terceros se generan por las herramientas propias del servicio, y los informes de actividades. No existen más reportes por parte del proveedor o del departamento de Sistemas.
Una lista de todas las relaciones actuales con terceras partes y de los contratos asociados con cada una. • Solo existen negociaciones con los proveedores que constan en la lista.	X			• En el departamento de Sistemas existe un registro de los proveedores actuales con los que se realizan cualquier tipo de negociación en cuanto a servicios.
El reporte del nivel de servicio relacionado con las relaciones y servicios proporcionados por terceras partes.			X	• El único reporte del nivel de servicio con los servicios de terceras partes son los contratos firmados por Gerencia General. También los informes de actividades que son realizados trimestralmente y se enfocan en algunos

				aspectos de los servicios de terceros.
Las minutas de las reuniones en las que se discuten la revisión de los contratos, la evaluación del desempeño y la administración de las relaciones con los proveedores.	X			• Existe un registro de las minutas de las reuniones en las que participan los Consejos de Administración, Vigilancia, Comité Ejecutivo y Gerencia General, que son útiles para revisiones o auditorías por parte de la SEPS[36].

Tabla 2.16 Directrices de auditoría del DS2

2.3.3.3. DS3 Administrar el Desempeño y la Capacidad

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Políticas y procedimientos globales para la organización. • Como la existencia de disponibilidad, monitoreo y reporte del desempeño,		X		• El monitoreo del desempeño de los recursos de TI se realiza periódicamente por parte del departamento de Sistemas para poder prevenir posibles problemas en este aspecto.

[36] Superintendencia de Economía Popular y Solidaria

pronóstico de la carga de trabajo, administración de la capacidad y programación de actividades				En lo que se refiere a infraestructura y aplicaciones el monitoreo es mediante las herramientas propias del sistema operativo sobre el cual funcionan, por lo tanto los indicadores de desempeño dependen de la herramienta.
Representaciones del producto por parte del proveedor con respecto a las normas de capacidad y desempeño. • Existen estadísticas sobre reportes de desempeño, capacidad y disponibilidad son precisas, incluyendo una comparación entre las explicaciones de las variaciones de desempeño históricas y las pronosticadas.			X	• Las estadísticas por parte de los proveedores son generadas por las herramientas propias del sistema operativo.
Una lista de todos los productos actuales del proveedor en lo referente a hardware, software, comunicaciones y periféricos. • Reportes de desempeño en cuanto a oportunidades de mejora o solución de debilidades.		X		• Los reportes generados son para detectar las debilidades de los sistemas y sirven para dar soluciones y mejorar su desempeño.
Reportes de monitoreo de redes de comunicación.	X			• La Jefe de Sistemas se encarga de realizar el monitoreo continuo y proponer las

• Existe un monitoreo continuo del desempeño de todo el equipo y de la capacidad, y si la falta de un desempeño adecuado es considerada por la administración.				consideraciones necesarias para la mejora continua.
Minutas de las reuniones en las que se discuten la planeación de la capacidad, las expectativas de desempeño y la "afinación" del desempeño. • Los usuarios y los grupos de desempeño operativo revisan proactivamente la capacidad, el desempeño, y si se llevan a cabo modificaciones a la programación de actividades relacionadas con la carga de trabajo.		X		• El personal del departamento de Sistemas se encarga de la revisión del desempeño operativo, mientras que el Jefe de Sistemas se encarga de aprobar y ejecutar las acciones pertinentes para sus adecuaciones.
Documentos de disponibilidad, capacidad, carga de trabajo y planeación de recursos. • Existe un plan de disponibilidad, está actualizado y refleja los requerimientos del usuario.			X	• No existe un plan de disponibilidad de los recursos de TI, únicamente los inventarios de los mismos.
Presupuesto de TI anual incluyendo las suposiciones relacionadas con la capacidad y el desempeño.		X		• Dentro del plan operativo anual se encuentra asignado el presupuesto general para lo relacionado con la Tecnología, sin entrar en detalle a la capacidad y desempeño.

Reportes relacionados con el desempeño operativo dentro de la función de servicios de información, incluyendo el reporte y la historia de la solución de problemas.		X		• Existen reportes sobre el desempeño operativo, en cuanto a servicios de información e historial de solución de problemas solo existe su registro dentro del departamento de Sistemas y que es administrado por el Jefe de Sistemas.

Tabla 2.17 Directrices de auditoría del DS3

2.3.3.4. DS4 Garantizar la continuidad del Servicio

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Políticas y procedimientos para la Organización relacionados con los procesos de planificación de recuperación/continuidad. • Una lista de los recursos de sistemas que requieren alternativas (hardware, periféricos, software, centro de cómputo de respaldo		X		• No existen políticas ni procedimientos documentados de TI para garantizar la continuidad de los servicios, actualmente se están desarrollando. Además, se encuentran en el proceso de implementación del plan de contingencias a nivel del departamento y del

para recuperación de SO, aplicaciones, archivos de datos, manuales de operación y documentos de programas, sistemas y usuarios). • Escenarios de desastres varios y respuesta a cada uno, en detalle para llevar a cabo una ejecución paso a paso. Su entrenamiento, concienciación y conocimiento de las funciones individuales y de equipo en el plan de continuidad. • Procedimientos de emergencia para garantizar la seguridad de todos los miembros del personal afectado. • Requerimientos de la agencia reguladora con respecto a la planificación de continuidad.				negocio, que se realizan por pedido de la SEPS [37] y son llevados a cabo por los departamentos y auditoria interna de la Organización. • Existe un listado o inventario de los recursos de TI relacionados con infraestructura como servidores y hardware, además en aplicaciones y software, es decir un inventario general que se actualiza semestralmente. • Actualmente no cuentan con escenarios de desastres varios ni con respuestas a cada uno de ellos, sin embargo en lo relacionado a enlaces de comunicaciones se está implementado la contratación de un proveedor de respaldos para evitar fallar de comunicación e insatisfacción a los socios. • En cuanto a seguridad de personal, se encuentra dentro del contrato laboral. • De acuerdo a los requerimientos de la agencia reguladora como la SEPS[35], se encuentra en implementación del plan de contingencia como primer punto de garantizar la

[37] Superintendencia de Economía Popular y Solidaria

				continuidad de los servicios.
Políticas y procedimientos de la función de servicios de información relacionadas con marco referencial de continuidad, plan, filosofía, estrategia, plan de pruebas, los respaldos, y el entrenamiento de recuperación de desastres/continuidad. • Se tiene un marco de trabajo referencial de continuidad y de un plan para la función de servicios de información y áreas dependientes de los recursos de sistemas de información. • Roles y responsabilidades específicas para la planificación de continuidad, con pruebas, mantenimiento y requerimientos de actualización.			X	• No existe un marco de trabajo formal para la continuidad de todos los servicios de TI, pero el departamento de Sistemas se encarga de elaborar y definir alternativas para posibles emergencias con lo relacionado a servicios relevantes para el negocio con el objetivo de minimizar las perdidas en cuanto a costo-beneficio para la organización y evitar insatisfacción en los socios. • La responsabilidad para la definición de continuidad en los servicios de TI no están asignadas, pero son realizadas informalmente por el Jefe de sistemas y su departamento.
Los resultados de las pruebas de los planes de los usuarios relacionados con la continuidad y recuperación del negocio. • Programación de pruebas, los resultados de la última prueba y las acciones correctivas, que se realizan a partir de las pruebas anteriores. • Alternativas de reanudación del negocio para			X	• Solo existen programas de pruebas para los aspectos relacionados con el área de desarrollo de software en un ambiente de pruebas que son hechos antes de ser puestos en producción. • No se tienen alternativas para reanudar las actividades del negocio puesto que se tiene únicamente un servidor para la base de datos y de aplicaciones para el sistema Financial.

todos los usuarios, estableciendo sitios de trabajo alternativo cuando los recursos de información estén disponibles.				Sólo se tienen los respaldos en caso de necesitar acceder a la información crucial para la organización.
Metodología para determinar la priorización de aplicaciones para la recuperación. • Se tiene una priorización de las aplicaciones con respecto a los tiempos de recuperación y regreso a la operación normal y de las normas de desempeño esperadas.			X	• No se utilizan metodologías para priorizar las aplicaciones para la recuperación.
Contratos de los proveedores que dan soporte a los servicios de continuidad • Acuerdos de contrato formal con los proveedores de servicios en cuanto a la recuperación (instalaciones, respaldos) • Funciones y responsabilidades de la función de servicios de información, de los proveedores que prestan servicios de recuperación, de los usuarios de los servicios y del personal administrativo de soporte. • Funciones administrativas para comunicar y proporcionar servicios de soporte tales como beneficios, nómina, comunicación externa,		X		• Dentro de los contratos con los proveedores se establecen clausulas para que ellos sean los encargados de garantizar la continuidad de los servicios provistos. • No está especificadas las responsabilidades para los servicios de recuperación para los servicios de terceros. • En los acuerdos de niveles de servicio no se definen las funciones administrativas para los eventos de recuperación.

seguimiento de costos, etc. en el evento de requerirse la recuperación.				
Políticas de seguros por interrupción del negocio • Evaluación de riesgos, obtención de seguros por pérdidas del negocio en situaciones de continuidad.		X		• Se realiza un análisis de riesgos interno al departamento de Sistemas y por parte del Jefe de Sistemas con el fin de minimizar los riesgos y garantizar la continuidad de los servicios de TI relevantes para el negocio. Además de que existen seguros que son provistos por los proveedores de los servicios, y las garantías en cuanto a hardware. En lo que se refiere a software como los elementos de Office se cuenta con las licencias para su uso.

Tabla 2.18 Directrices de auditoría del DS4

2.3.3.5. DS5 Garantizar las Seguridad de los Sistemas

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Políticas y procedimientos globales para la organización referentes a seguridad y acceso a los sistemas de información. • Se tiene un plan de seguridad estratégico que proporcione dirección y control sobre la seguridad de sistemas y recursos de información y requerimientos de seguridad de usuarios. • Se tiene una organización de seguridad centralizada responsable de asegurar el acceso apropiado a los recursos del sistema. • Entrenamiento de los empleados sobre conocimiento y conciencia sobre seguridad, responsabilidades de los propietarios y protección contra virus.		X		• La Organización cuenta con políticas de seguridad de acceso físico, ambiental a nivel general que están definidos en el reglamento de seguridad de toda la organización, pero en lo que se refiere a TI, no existe un plan de seguridad de TI específico. En su lugar existen medidas implantadas por el Jefe de Sistemas para el control de los recursos de TI. • Actualmente, no se cuenta con una organización de seguridad responsable, esta función es delegada al personal del departamento de Sistemas. • Los empleados tienen el conocimiento de aspectos fundamentales sobre la seguridad de TI, pero no cuentan con un entrenamiento continuo sobre este tema por lo que sus funciones están restringidos a aspectos de inseguridad informática.
Procedimientos y políticas de TI relacionadas con		X		• La clasificación de datos es realizada y controlada por el sistema Financial, el cual

seguridad y acceso a los sistemas de información. • Se tiene una clasificación de datos en operaciones que indiquen que todos los recursos del sistema tiene un propietario responsable de su seguridad y contenido. • Se tienen perfiles de usuario y se hacen revisiones regulares a los perfiles por parte de la administración. • Se tienen reportes de fallas de seguridad (intentos autorizados y no autorizados de acceso al sistema, a los recursos del sistema, para consultar o modificar definiciones y reglas, entre otros) y procedimientos formales de solución. • Se tiene módulos criptográficos y procedimientos de mantenimiento de llaves y se administran usando estándares. • Se tienen mecanismos de autenticidad en uso (contraseñas no reutilizadas, autenticación múltiple, autenticación basada en políticas, autentificación basada en políticas o por demanda), con número de sesiones concurrentes limitadas. • Se tienen políticas de password (forzar el				garantiza que exista acceso restringido a la información de acuerdo a los perfiles de usuarios del sistema. • El departamento de Sistemas define perfiles de usuario de acuerdo a los cargos del personal y están sujetos a revisiones y actualizaciones periódicas. • Los reportes de fallas de seguridad son proporcionados por las funciones propias del Sistema Financial, pero no cuentan con procedimientos formales de solución. • No se utilizan estándares para la administración de llaves de seguridad. • Existen políticas internas en el Departamento de Sistemas que definen mecanismos de autenticidad para los perfiles de usuario. • Las políticas de contraseñas para el uso del sistema Financial son generadas automáticamente por un módulo de administración del mismo, previo a autorización del Jefe de Sistemas. En cuanto los perfiles de usuario para el uso de los equipos, se definen por parte del Jefe de Sistemas y se cambian periódicamente. • La configuración de Firewalls y proxys se

cambio de la contraseña en el primer uso, longitud mínima, frecuencia obligatoria de cambio). • Procedimientos para cambios frecuentes de firewalls de hardware y software para restringir el acceso a los activos y cambios frecuentes de claves de acceso y desactivación de claves de acceso de los empleados temporales. • Se utilizan rutas confiables para transmitir información sensitiva no encriptado. • Se establecen medidas de control preventivo para prevenir y detectar virus.				realizan por el personal de Sistemas, previa a la autorización del Jefe del departamento quien es el encargado de restringir su acceso a los usuarios de acuerdo al cargo que ocupen dentro de la organización, por ejemplo solo los jefes de los departamentos tienen acceso a sitios web. • El único medio de transmisión de la información sensitiva es la red que maneja la organización, a la que sólo tienen acceso el personal de la empresa y cuenta con las respectivas seguridades para no permitir el ingreso de intrusos. • Las medidas de control preventivo son realizadas por el personal de Sistemas instalando los respectivos antivirus en las máquinas, el bloqueo de puertos USB y restricción a sitios web no relacionados con las actividades laborales.

Tabla 2.19 Directrices de auditoría del DS5

2.3.3.6. DS7 Educar y entrenar a los usuarios

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Políticas y procedimientos generales para la organización con respecto sobre controles y conciencia de seguridad, programas de entrenamiento para los usuarios de servicios, instalaciones educacionales y requerimientos de educación continua profesional. • Los nuevos empleados tienen conocimiento y conciencia de la responsabilidad de seguridad y control con respecto a la utilización y custodia de los recursos de TI. • Existe disponibilidad de oportunidades y frecuencia de entrenamiento interno y externo, considerando la asistencia de los empleados.		X		• Dentro del programa de inducción se transmite lo estipulado en el reglamento interno de trabajo sobre las normas de seguridad generales que se deben cumplir, más no están especificadas medidas de seguridad de los recursos de TI. • Para el entrenamiento y capacitación del personal se planifican dentro de un cronograma cursos generales y específicos para cada área.
Programas, políticas y procedimientos de entrenamiento y de educación de TI relacionados con la concienciación en controles y seguridad. • Se tiene un programa de educación y entrenamiento enfocado a principios de		X		• No se tiene un programa de capacitación que se enfoque en el control de sistemas de información. Sólo se tienen talleres para capacitar al personal en el uso del sistema Financial. • El entrenamiento en cuanto a las seguridades

sistemas informáticos y control de sistemas de información. • Los entrenamientos incluyen principios generales de seguridad de sistemas, conducta ética de TI, prácticas de seguridad para protección contra daños por fallas que afecten a disponibilidad, confidencialidad, integridad y desempeño. • Políticas para evitar exposición de información sensitiva a través de conversaciones.				de los sistemas incluye la especificación de las restricciones que los usuarios tienen sobre los sistemas, equipos y áreas de sistemas. • La prohibición de exposición de información sensitiva no se tiene como una política establecida, pero sí se tiene un artículo dentro de la sección de obligaciones y prohibiciones del personal del reglamento interno del trabajo, además del reglamento para la custodia y manejo de la información institucional

Tabla 2.20 Directrices de auditoría del DS7

2.3.3.7. DS10 Administrar los problemas

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Políticas y procedimientos de la función de TI relacionados con la administración de problemas (registro, solución, escalamiento, seguimiento y reporte).		X		• No se tiene definida una administración de problemas, sin embargo para resolver los problemas relacionados con TI se tiene un formato de solicitud de requerimientos en la cual los usuarios especifican el problema que

• Los procedimientos de manejo de problemas definen e implementan un sistema de administración de problemas, registran, analizan y resuelven de manera oportuna los eventos no estándar, establecen reportes de incidentes para los eventos críticos y la emisión de reportes para usuarios. • Identificación de los tipos de problemas y metodología de priorización que permita soluciones tomando como base el riesgo. • Definición de controles lógicos y físicos para el manejo de problemas. • Aseguran la suficiencia de los seguimientos de auditoría para los problemas de sistemas.				tienen, su origen y el área, para que puedan ser solucionados lo más antes posible junto con la utilización de la herramienta mail corporativo. Por otro lado, también se tienen las disposiciones y memorándum que emite Gerencia General cuando se requiere corregir un problema de mayor magnitud, por lo que este tipo de problemas tienen una mayor prioridad para ser solucionados. • Los problemas sólo se identifican de acuerdo a la solicitud de requerimientos y se clasifican según el origen (interno y externo), el área del problema (Sistema Financial, equipo de computación), y la prioridad. • Para evitar ciertos problemas se han tomado medidas como el bloqueo de puertos USB, y para evitar el ingreso no autorizado al sistema Financial se ha restringido el número de ingresos de contraseñas erróneos. Sin embargo son medidas aisladas que se toman para prevenir problemas ya ocurridos anteriormente o por disposiciones de la

				Gerencia o de organismos de control, como la SEPS[38]. • Cuando ocurre un problema que es solucionado, antes de que la solución se pase a producción se tiene un informe de paso a producción, pero no se tiene documentación adicional para los seguimientos de auditoría interna.
Lista de los problemas reportados durante un período representativo de tiempo (fecha de ocurrencia, fecha de solución, tiempos de solución). • Determinar si la administración evalúa periódicamente el proceso de manejo de problemas en cuando a una mayor efectividad y eficiencia.			X	• No se administran los problemas y por tanto no se evalúan periódicamente, sin embargo el formato de solicitud de requerimientos va sufriendo mejoras cuando es necesario.
Lista de aplicaciones críticas para darles prioridad de solución.			X	• No se tiene listas ya que el único sistema crítico de la empresa es el Financial.
Conocimiento de aplicaciones de manejo de problemas, y métodos para asegurar que todos los problemas son capturados, resueltos y reportados.			X	• No se tienen aplicaciones específicas para el manejo de problemas, sólo se trabaja con la solicitud de requerimientos, la herramienta del mail corporativo y con los memorándum

[38] Superintendencia de Economía Popular y Solidaria

				emitidos por la Gerencia General.

Tabla 2.21 Directrices de auditoría del DS10

2.3.3.8. DS11 Administrar los datos

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Políticas y procedimientos organizacionales relacionados con la administración de base de datos. • Proceso de autorización de documentos fuente. • Procesos de recolección, seguimiento y transmisión de datos. • Procedimientos para asegurar la suficiencia, precisión, registro y transmisión de documentos fuente completo para su captura. • Procedimientos utilizados para identificar y corregir errores durante la creación de datos. • Métodos utilizados por la organización		X		• No se tiene un procedimiento para administración de los datos, simplemente se debe solicitar autorización para acceder a los documento fuente, dependiendo del grado de confidencialidad. • Los procesos de recolección, seguimiento y trasmisión de datos están especificados en el manual de operaciones de cada cargo. • Los procedimientos para asegurar la suficiencia, precisión, registro y transmisión de datos se especifican en el manual de funciones y en el manual de operaciones de cada cargo. • No se tienen procedimientos para identificar y corregir errores durante la creación de datos, simplemente se tienen establecidas reglas de

para retener documentos fuente (archivo, imágenes, etc.), para definir qué documentos deben ser retenidos, los requerimientos de retención legales y regulatorios, etc. • Contratos de proveedores para llevar a cabo tareas de administración de datos.				validación en el sistema. • Los documentos que, por disposición de organismos de control, deben ser retenidos durante un periodo de tiempo determinado se mantienen en archivadores en cada departamento, si es que son físicos, y los digitales se mantienen en el servidor de archivos. Hay que tener en cuenta que la mayoría de los documentos físicos no tienen un respaldo digital. • Los contratos con los proveedores no incluyen especificaciones relacionadas con la administración de datos.
Lista de todas las aplicaciones y documentación de usuario. • Módulos que lleven a cabo revisiones de precisión, suficiencia y autorización de captura en el ingreso de datos. • Funciones que lleven a cabo entradas de datos para cada aplicación. • Funciones que lleven a cabo rutinas de corrección de errores de entrada de datos. • Métodos utilizados para prevenir (por medios manuales y programados), detectar y corregir errores.		X		• Se tiene un módulo de administración de usuarios en el cual se implementan los permisos de cada uno de los usuarios del sistema con el fin de restringir el ingreso a módulos no autorizados. Por otro lado se tiene un módulo de administración del sistema en el cuál se incluyen las reglas del negocio necesarias para validar los datos que se ingresan. • De acuerdo a las reglas ingresadas en el sistema para la validación de datos, se pide que se corrijan los datos antes de ingresarlos al sistema para evitar ingresar datos inconsistentes en la base de datos.

• Edición y autenticación de la validación del procesamiento de datos tan cerca del punto de origen como sea posible. • Manejo y retención de salidas creadas por aplicaciones. • Revisión de la precisión de los reportes de salida y de la información. • Procedimientos de control de proveedores como terceras partes con respecto a preparación, entrada, procesamiento de salida.				• Si la información ingresada es válida pero proporciona una información errónea, se corrige después de realizar el cuadre de cuentas diario. Las correcciones se realizan con la autorización de Gerencia General y con la presencia del Jefe de Contabilidad. • No se tiene un manejo y retención de salidas creadas por aplicaciones. • La revisión de la precisión de los reportes de salida y de la información se realizan diariamente a través del cuadre de dinero diario. Si son correctos se remiten a Gerencia General, caso contrario se informa del problema y se realiza la corrección con la respectiva autorización. • No se tienen procedimientos de control de proveedores con respecto a preparación, entrada y salida de datos. Simplemente se cumplen con las clausulas estipuladas en cada contrato.
Políticas y procedimientos relacionados con la librería de medios y con el almacenamiento de datos externo. • Administración de la librería de medios y del sistema de administración de la librería. • Requerir la identificación externa de todos		X		• No se tiene una librería de medios, simplemente se tiene un servidor de archivos en el que se almacenan los documentos del personal. • Para evitar problemas de virus o de robo de información se han deshabilitado los puertos USB y las unidades de almacenamiento externo. Solo pueden habilitarse temporalmente con una

los medios. • Requerir el inventario actual de todos los contenidos y procesos para actividades de control. • Procedimientos de reconciliación entre registros actuales y registros de datos almacenados. • Reciclaje de datos y rotación de medios de datos. • Inventario de datos de prueba y pruebas de recuperación llevadas a cabo. • Medios y funciones del personal en el sitio alterno en el plan de continuidad..				autorización de Gerencia General y para una persona determinada. • No se tiene un inventario de los contenidos y procesos de actividades de control. • Sí se tienen procedimientos de reconciliación entre registros actuales y registros almacenados para hacer los reportes anuales del estado de la organización. • El reciclaje de datos se realiza una vez que se ha terminado el período de retención de la información establecido por las entidades de Control. Pero no se tiene un proceso documentado. • No se tiene un inventario de datos de prueba. Simplemente se tiene registros que se utilizan para la realización de los talleres de capacitación.
Políticas y procedimientos relacionados con cualquier repositorio central de base de datos de la organización. • Organización de la base de datos y diccionario de datos. • Procedimientos de mantenimiento y seguridad de bases de datos. • Procedimientos de control de cambios		X		• No se tiene el modelo de la base de datos documentado y tampoco se tiene diccionario de datos. • Se cuenta con procedimientos de mantenimiento y seguridad de base de datos. Se realiza el mantenimiento de manera periódica y para garantizar la seguridad se restringe el ingreso a la base de datos al resto de personal excepto al Jefe de Sistemas.

sobre el diseño y contenido de la base de datos. • Reportes administrativos y pistas de auditoría que definen actividades de bases de datos.				• Sí se tienen procedimientos de control de cambios sobre el diseño y contenido de la base de datos y para sus modificaciones se lleva un registro en un informe de Parametrización y paso a producción en el que se contemplan aspectos como su impacto para que estén sujetos a futras revisiones por los distintos organismos de control interno y externo. Cualquier cambio debe ir acompañado por un análisis de la razón para realizar una modificación y éstos deben ser autorizados por la Gerencia General.

Tabla 2.22 Directrices de auditoría del DS11

2.3.3.9. DS12 Administrar el Ambiente Físico

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Políticas y procedimientos organizacionales relacionados con la administración, planos del sitio, seguridad, inventario de activos fijo e inventario de las instalaciones, así como adquisición. • Los procedimientos y prácticas de		X		• No se tiene acceso a las instalaciones con llaves magnéticas ni lectores de tarjetas. • Dentro del Reglamento Interno de Trabajo se especifican cuáles son las áreas restringidas y quiénes pueden ingresar a las mismas. Para

administración de llave y lectora de tarjetas son adecuados. • Políticas de acceso y autorización de entrada/salida, escolta, registro, pases temporales requeridos, cámaras de vigilancia son apropiadas para todas las áreas y especialmente para las áreas más sensibles. • Se llevan a cabo revisiones periódicas de los perfiles de acceso, incluyendo revisiones administrativas. • Se lleva a cabo una revisión de los registros de visitantes, asignación de pases, escolta, persona responsable del visitante, bitácora para asegurar los registros de entradas y salidas. • Se lleva a cabo una revisión de los procedimientos de aviso contra incendios, cambio de clima, problemas eléctricos y procedimientos de alarma, así como las respuestas esperadas. • Se tienen revisiones del proceso de alarma (prioridad de la alarma, respuestas, responsabilidades del persona, interacción con las autoridades locales, simulacros). • Entrenamiento y concienciación de seguridad.				garantizar la seguridad de estas áreas se tienen bitácoras de ingreso, guardias en las puertas de ingreso a la Organización, y cámaras de seguridad en puntos estratégicos. • Las claves de acceso al sistema se cambian periódicamente, además los perfiles de acceso son eliminados una vez que algún miembro del personal deje de pertenecer a la Organización. • Cada vez que una persona entra al departamento de Sistemas se registra la visita en una bitácora, sin embargo no siempre se revisa si los datos escritos con correctos. • Los procedimientos para asegurar la seguridad en casos de incendios, cambios de clima, problemas eléctricos y otros acontecimientos son proporcionados durante la capacitación de seguridad industrial que se realiza anualmente. • No se tienen procesos definidos de alarma cuando se produce algún acontecimiento. Además no se han realizado simulacros en los últimos 3 años. • Se tiene entrenamiento y concienciación de seguridad industrial, pero no de seguridad en

• Se cumplen con regulaciones de salud, seguridad y ambiente. • Los planes físicos son actualizados a medida que cambian la configuración, el ambiente y las instalaciones.				los sistemas. Las medidas de seguridad son tratadas en reuniones del Comité Ejecutivo y son comunicadas al resto de la Organización mediante disposiciones de gerencia. • Sí se cumplen con las regulaciones de salud, seguridad y ambiente. • No se tienen planes físicos, sólo cuentan con planos de las instalaciones que son revisados cuando se considera necesario hacer modificaciones en las instalaciones o en la infraestructura.
Políticas y procedimientos de TI relacionados con el plano de las instalaciones, seguridad física y lógica, acceso, mantenimiento, registro de visitas, salud, inventario de equipo, procedimiento de vigilancia, requerimientos regulatorios. • Los procedimientos de acceso lógico y físico son suficientes, incluyendo perfiles de seguridad de acceso para empleador, proveedores, equipo y personal de mantenimiento de las instalaciones. • Las medidas de control de seguridad y acceso incluyen a los dispositivos de información portátiles utilizados fuera del sitio.		X		• Se tienen perfiles de usuario en el sistema Financial para cada uno de los cargos. Además se cuenta con cámaras de seguridad para monitorear el acceso de personas no autorizadas a áreas restringidas. • Dentro de las medidas de control de seguridad y acceso no se incluyen medidas para dispositivos móviles, excepto la restricción de teléfonos celulares en las áreas de servicio al cliente. • El personal del departamento de Sistemas realiza revisiones para controlar que la temperatura y humedad sean adecuadas para el correcto funcionamiento de los servidores.

• Se lleva a cabo una revisión de los procedimientos de control de aire acondicionado, ventilación, humedad y las respuestas esperadas ante escenarios de pérdida o extremos no anticipados. • Coordinación de actividades que afecten en control de acceso lógico vía aplicaciones centralizadas o software de sistemas operativo. • Existen elementos de infraestructura alternativos para implementar seguridad como UPS, alternativas o reenrutamiento de líneas de comunicación, recursos alternativos de agua, gas, aire acondicionado y humedad.				Sin embargo no se cuenta con un procedimiento definido para la realización de la revisión. • Se coordinan actividades de mantenimiento del sistema de manera periódica, con previa autorización de Gerencia General, fuera de los horarios de atención al cliente. • Se tienen algunos elementos de infraestructura alternativos en caso de falla eléctrica, como UPS y un generador. Sin embargo no se tienen elementos en caso de falla de aire acondicionado, o falla de la línea de comunicaciones.
Lista de los individuos que tienen acceso a las instalaciones y planos del piso de instalación.	X			• Los individuos que tienen acceso a las instalaciones se controlan a través de bitácoras. Además, en el Reglamento Interno de Trabajo se encuentra estipulado el personal que está autorizado para ingresar a las áreas restringidas.
Lista de los acuerdos de desempeño, capacidad y nivel de servicios con respecto a las expectativas de desempeño de los recursos de TI.		X		• No se tienen acuerdos de desempeño, capacidad y nivel de servicio con respecto al desempeño de sistemas. • Cuando es necesario una ampliación de los

• Se llevan a cabo la actualización y negociación del contenido de los contratos de servicio. • Coordinación de pruebas de penetración física con proveedores y autoridades locales.				servicios con un determinado proveedor se revisan los contratos y se vuelven a negociar. • No se realizan pruebas de penetración física con proveedores, sin embargo estas pruebas sí son realizadas por los organismos de control.
Copia del documento de planificación de continuidad.			X	• No existe plan de continuidad.

Tabla 2.23 Directrices de auditoría del DS12

2.3.3.10. DS13 Administrar las Operaciones

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Políticas y procedimientos organizacionales relacionados con la administración de operaciones y el rol de sistemas de información en el cumplimiento de los objetivos de la organización.		X		• No se tienen políticas y procedimientos, pero las operaciones relacionadas con TI están establecidas en el manual de funciones. Además el rol del Departamento de Sistemas se especifica en el Plan Estratégico de la organización.
Políticas y procedimientos de la función de servicios de información relacionada con el rol operacional, las expectativas de desempeño,		X		• No se tienen estadísticas de cumplimiento de la programación de trabajos completos. La información que se posee respecto a trabajos

programación de trabajos, acuerdos de nivel de servicio, planificación de la continuidad y las operaciones de instalaciones remotas. • Estadísticas de cumplimiento de la programación de trabajos para confirmar el término completo de los requerimientos. • Estadísticas de desempeño para actividades operacionales sobre capacidad, utilización y desempeño de hardware y periféricos, de memoria, y de telecomunicaciones. • El personal de operaciones comprende los procedimientos de operación que están bajo su responsabilidad.				completos son las notificaciones a Gerencia General de los avances de los trabajos a realizarse. • Las estadísticas de desempeño sobre capacidad de los equipos se obtiene a través de las herramientas propias de los sistemas operativos correspondientes. No se tienen estadísticas de desempeño de las telecomunicaciones ya que estas son servicios de terceros. • Cada persona del departamento de Sistemas comprende cuáles son sus responsabilidades y las conoce a través del manual de funciones.
Instrucciones operacionales para la función general de inicio, termino, programación de carga de trabajo, acuerdos de servicio, procedimientos de correcciones de emergencia, bitácoras, seguridad lógica y física.			X	
Muestra seleccionada de instrucciones operacionales para aplicaciones clave como programación de actividades, entradas, tiempo de procesamiento, mensajes de error, procedimientos		X		• No se tienen bitácoras de operación. • No se tiene rotación de turnos en el departamento de Sistemas, sin embargo cada persona coordina sus vacaciones de manera que estén al cargo de las actividades del departamento al menos 2

de escalamiento de problemas. • Mantenimiento, retención y revisión periódicos de las bitácoras de operación se llevan a cabo periódicamente. • Rotación de turnos, disfrute de vacaciones y mantenimiento de competencia de los operadores.				personas.

Tabla 2.24 Directrices de auditoría del DS13

2.3.3.11. Síntesis global del dominio DS

La Organización es consciente de la necesidad de gestionar la entrega y soporte de los servicios de TI, ya que de éstos depende el cumplimiento de sus objetivos y de los del negocio, así como la satisfacción de los socios.

Las medidas que se toman para la gestión de este dominio consisten en establecer la responsabilidad de revisión y firma de los contratos a la Alta Gerencia, Comité Ejecutivo y Asesoría legal para la parte operativa y legal.

No existe un acuerdo de niveles de servicio como tal, en su lugar existe el contrato escrito en el que constan las condiciones del servicio prestado por el proveedor, enfocadas en el negocio y no en aspectos tecnológicos ni se especifican métricas para medir el desempeño del servicio.

El departamento de Sistemas cuenta con un inventario de todos los componentes de TI, pero no una clasificación de los que son críticos para el negocio, y menos con un plan de capacidad que permita a la Gerencia estar consciente del desempeño actual y futuro de los mismos. En su lugar existe un análisis de costo-beneficio, factibilidad y riesgos, que son desarrollados por el Jefe de Sistemas, de acuerdo a su experiencia y conocimientos, con el fin de comunicar a la Alta Gerencia de los nuevos requerimientos de capacidad y desempeño que la Organización debería adquirir para cubrir con las exigencias del negocio.

Además existen varias políticas de continuidad de los servicios de TI, pero no se encuentran documentadas ni integradas en un plan de continuidad. Por esta razón el departamento de Sistemas es el encargado de ejecutar las medidas de respaldos de información, comunicar a los proveedores de problemas de enlaces de comunicación, resolver problemas del Sistema Financial, entre otros. Para los problemas que identifican los usuarios, se tiene un formato de solicitud de requerimiento, el cual permite al Departamento de Sistemas resolverlos oportunamente para reducir el tiempo de interrupción del servicio y con ello causar la menor molestia a los socios de la Organización, además de la utilización de la herramienta institucional como es el mail corporativo.

En cuanto a seguridades de los sistemas, se toman medidas basadas en las recomendaciones de los organismos de control como la SEPS[39], las de Auditoría Interna y lo estipulado en el Reglamento para la Custodia y Manejo de la Información Institucional. También se toma en cuenta la seguridad industrial y la seguridad ambiental que por el momento es supervisado por Alta Gerencia.

Para mantener en curso las operaciones de TI junto con las del Negocio, el Jefe de Sistemas se encarga de coordinar las actividades del personal del departamento para cumplir con los objetivos expuestos en el plan Operativo anual. La capacitación del personal de Sistemas depende de la planificación del departamento de Talento Humano con respecto a los cursos generales y específicos. Adicionalmente, el Departamento de Sistemas se encarga de capacitar a los usuarios en lo que se refiere a módulos del Sistema Financial de cuerdo al surgimiento modificaciones en los requerimientos del negocio en el Sistema o a la incorporación de personal nuevo.

[39] Superintendencia de Economía Popular y Solidaria

2.3.4. MONITOREAR Y EVALUAR (ME)

2.3.4.1. ME1 Monitorear y Evaluar el Desempeño de TI

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Políticas, procesos y procedimientos para establecer prioridades y asignar responsabilidades en el monitoreo del desempeño y de la capacidad de prestación de servicios de TI. • Existen objetivos claros para llevar a cabo revisiones periódicas e iniciación de acciones correctivas. • Existe capacitación para la recolección, análisis de datos para la captura de la medición del desempeño.		X		• Existen revisiones y acciones correctivas basadas en medidas establecidas por el Jefe de Sistemas y son realizadas periódicamente. • No existe capacitación para la recolección de medición del desempeño, en su lugar existe recolección de datos procedentes de las herramientas propias del Sistema mientras que su análisis es realizado en base a la experiencia del personal del departamento de Sistemas.
Reportes de costo-beneficio, desempeño de los proyectos, desempeño de los procesos, satisfacción de usuarios. • Existe la traducción y comunicación de reportes de desempeño periódicos de los procesos para hacerlos reportes gerenciales (vinculación de la medición del desempeño de TI a los resultados del		X		• Los indicadores claves de rendimiento son porcentajes del procesamiento de transacciones y el costo del recurso humano, de manera que Gerencia sea consciente del impacto económico de la interrupción de los servicios para que pueda tomar decisiones oportunas. • No existe la identificación de procesos sobresalientes, por ende no existe un registro del

negocio), que pueden ser utilizadas para decisiones estratégicas y son discutidas en reuniones de alta gerencia analizando la contribución de TI al negocio (soluciones de TI) • Existe reducción del número de deficiencias de los procesos sobresalientes. • Existe un número de acciones de mejoramiento impulsadas por las actividades de monitoreo.				número de deficiencias de los mismos. • El Jefe de Sistemas propone a Gerencia las mejoras del desempeño de TI, avalado por un informe de costo-beneficio y factibilidad para su posterior análisis y aprobación.
Reportes del estado de los cambios. • Existe el registro de número de cambios a las metas para los indicadores de efectividad y eficiencia de los procesos de TI. • Existe recolección de los datos necesarios para el monitoreo así como su completitud, consistencia e integridad que aseguran el control de todos los cambios.			X	• No existen indicadores de efectividad y eficiencia debido a que no se tienen procesos definidos y documentados dentro del Departamento Sistemas. • No se controlan los cambios de TI, solo los considerados oportunos por parte del Jefe de Sistemas, por lo tanto no existe una documentación formal de los mismos.
Reportes de la efectividad de los controles de TI. • Existen número de métricas. • Existe el compromiso de los propietarios		X		• El Jefe de Sistemas establece internamente las métricas pero no tienen un enfoque general. • No existen procesos definidos y documentados, por lo tanto la propiedad de los procesos tampoco

de los procesos (actividades, funciones) que informe periódicamente sobre el desempeño del proceso en términos de las medidas definidas. • Existe retroalimentación con el monitoreo.				se encuentra asignada de manera formal. • No se tiene retroalimentación en el monitoreo del desempeño de TI.
Reportes sobre el cumplimiento de las actividades de TI respecto a requerimientos legales y regulatorios externos • Existe una falta de identificación oportuna de problemas relacionados con la informática y la alineación del negocio. • Establecer y mantener un sistema de control de TI que está ligado a las estrategias de negocio y facilita el control eficaz de las TI de apoyo a los objetivos. • Existe la comparación de valores de rendimiento con valores de la industria.		X		• Los problemas se identifican durante el periodo de desarrollo del plan estratégico, y se solucionan para que se adecúen a la alineación con el negocio. • No existe un sistema de control de TI ligado a las estrategias del negocio, en su lugar existen actividades realizadas por el Jefe de Sistemas en base a su experiencia. • No existen valores de rendimiento, por lo tanto no existe una comparación con los valores de la Industria.

Tabla 2.25 Directrices de auditoría del ME1

2.3.4.2. ME2 Monitorear y Evaluar el Control Interno

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Políticas, procesos y procedimientos para establecer controles internos de TI que son reportados a Gerencia. • Existe un sistema de controles internos documentado que está sujeto a emitir reportes de anomalías cuando se incumplen los controles internos y se determina sus acciones correctivas en base a gestión de riesgos, seguridad informática y cumplimiento de leyes y reglamentos. • El sistema de controles internos están sujetos a cambios o actualizaciones de acuerdo al entorno de control de la organización, los procesos del negocio relevantes y los riesgos de TI. • Está definida e implementada una política		X		• No existe un sistema de controles internos, por lo tanto no existen actualizaciones. Actualmente debido a la incorporación reciente del departamento de Auditoría Interna, por exigencia de la SEPS[40], el control interno se lleva a cabo con la utilización de herramientas ofimáticas. • No se tienen políticas en la Organización que definan la utilización de una metodología, sin embargo por la experiencia del Auditor Interno se está utilizando COSO para el monitoreo y evaluación del control interno a nivel de la Organización y no específicamente al Departamento de Sistemas. • Actualmente el encargado de fijar los controles internos es el departamento de Auditoría Interna. Anteriormente esta responsabilidad era llevada a cabo por el Consejo de Vigilancia a nivel de toda

[40] Superintendencia de Economía Popular y Solidaria

basada en los estándares y prácticas aceptadas en la industria, asociados a actividades de seguimiento y evaluación. • Está asignado un responsable para la definición formal de los controles internos, los cuales son comunicados a los propietarios de los procesos. • Se puede prever revisiones independientes para garantizar la objetividad de la autoevaluación y permitir el intercambio de buenas prácticas de control interno que son comparadas con estándares y buenas prácticas de la industria. • Existe una política que determine que las excepciones de control deben ser remediadas en línea con las necesidades del negocio. • Existe un método para priorizar y asignar la responsabilidad de todas las acciones correctivas del control de los propietarios de los procesos del negocio y de la alta dirección de TI.				la Organización. • Las revisiones independientes son realizadas por los Organismos de control externos como la SEPS[41], quienes pueden realizarlo en cualquier momento y de forma permanente. • No existe una política formal que determine que las excepciones de control deben ser remediadas en línea con las necesidades del negocio. • No cuentan con un método para priorizar y asignar la responsabilidad de todas las acciones correctivas del control de los propietarios de los procesos del negocio y de la alta dirección de TI. Está en proceso de implementación por parte del Departamento de Auditoría Interna.

[41] Superintendencia de Economía Popular y Solidaria

Reportes de efectividad de controles internos de TI. • Están documentados el número de debilidades identificadas para la mejora continua del control, es decir existen acciones oportunas para los problemas de control interno. • Existen requisitos de control interno establecido en los contratos con los proveedores tienen disposiciones de auditoria o revisión (certificaciones, acreditaciones) los cuales cumple con aspectos legales y reglamentarios.			X	• No existe documentación ni se tienen identificadas las debilidades que puedan afectar a la mejora continua de los controles • Únicamente existe control del cumplimiento de los contratos.

Tabla 2.26 Directrices de auditoría del ME2

2.3.4.3. ME3 Garantizar el Cumplimiento con Requerimientos Externos

- **Checklist de entradas:**

Entradas	Si	Parcialmente	No	Observaciones
Políticas, procesos, procedimientos y catálogos de requerimientos legales y regulatorios relacionados con la prestación del servicio de TI. • Implementación de un proceso para identificar, evaluar y actualizar las leyes aplicables y requisitos reglamentarios (el de comercio electrónico), para determinar su impacto en lo referente a TI (recursos, sistemas, operaciones). • Asignación de un responsable para la identificación de requerimientos legales y regulatorios relacionados con TI y las operaciones de la organización. • Entrenamiento al personal de TI sobre la responsabilidad del cumplimiento regulatorio. • Minimizar el impacto al negocio de los eventos de cumplimiento dentro de TI. • Existe una revisión periódica de las políticas y		X		• A través de los reglamentos internos de la Organización, tanto la SEPS[42] como Auditoría Interna y Asesoría Legal identifican las leyes y regulaciones aplicables al negocio con respecto a TI, pero no se tiene un proceso definido para ello. Se lo realiza reactivamente de acuerdo a las leyes, resoluciones y circulares actuales. Al momento se han identificado los siguientes: Reglamento General de la Ley Orgánica de la Economía Popular y Solidaria y del Sector Financiero Popular y Solidario (Decreto Ejecutivo 1061), Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP), Normas generales para la aplicación de la ley general de instituciones del sistema financiero, Resolución para uso de claves de medios electrónicos a cargo de la SEPS[40], Circular No. SEPS-IR-DNRFPS-2013-01682 / Niveles de cumplimiento de seguridades en cajeros automáticos y canales electrónicos.

[42] Superintendencia de Economía Popular y Solidaria

normas para determinar la eficacia del cumplimiento regulatorio. • Existen regulaciones para las revisiones internas y externas así como de los controles internos. • Existe un procedimiento que asegure que los contratos con los proveedores de servicios de terceros requieren confirmación periódica de su cumplimiento de las leyes y reglamentos aplicables. • Existe un registro de la información corporativa sobre el cumplimiento legal, regulatorio en un repositorio histórico.				• El entrenamiento sobre el cumplimiento regulatorio relacionado con TI se realiza mediante reuniones con Auditoría Interna y los cursos obligatorios que proporciona la SEPS[41]. • Actualmente la Organización se encuentra estableciendo un proceso de Auditoría Interna, pero esta función no está contemplada en la estructura organizacional. • El procedimiento para asegurar que los contratos con los proveedores de servicios de terceros dan cumplimiento de las leyes y reglamentos aplicables es previamente realizado por la Asesoría legal de la Organización. No se lleva un control posterior a la firma del contrato. En el caso del servicio SPI, el proveedor Banco del Austro es el encargado de revisar el cumplimiento con las leyes aplicables e informar y realizar los cambios respectivos a la Organización a la que presta el servicio. • Gerencia General cuenta con un archivo físico de los informes que son emitidos por Auditoria Interna y los Organismos Control, mientras que los archivos digitales se encuentran en un servidor de archivos.
Reporte sobre el cumplimiento de las actividades de TI con los requerimientos legales y regulatorios.		X		• Cada vez que se realiza un cambio en las leyes los Organismos de Control comunican mediante reportes a la Organización para que se hagan las respectivas

• Documentación de publicación de una nueva ley o regulación lo que conlleva a una revisión de su cumplimiento. • Presentación de informes de las revisiones del cumplimiento. • Evaluar el impacto de los requisitos legales y reglamentarios en los contratos relacionados con las operaciones de TI, proveedores de servicios de terceros y socios comerciales. • Mantener un registro al día de todos los requisitos legales, reglamentarios y contractuales pertinentes cumplimiento; su impacto y acciones requeridas.				modificaciones según sea el caso. • Los Organismos de Control en base a las condiciones legales y regulatorias a las que se sujetan emiten informes periódicos y permanentes sobre las revisiones y sus hallazgos. • No se realiza una evaluación del impacto sobre los requisitos legales y reglamentarios, en su lugar se controla que cumplan con las leyes relacionadas con TI. • El registro de todos los requisitos legales, reglamentarios y contractuales es realizado por los Organismos de Control como son Consejo de Vigilancia, Auditoría Interna y los Organismos de Control externos.

Tabla 2.27 Directrices de auditoría del ME3

2.3.4.4. Síntesis global del dominio ME

La Organización es consciente de la necesidad de tener un proceso de monitoreo y evaluación en el área de TI para conocer cómo su desempeño está apoyando a los objetivos del negocio y llevar un control de todas las actividades que se realizan. También se reconoce la importancia de establecer un proceso definido que documente el control interno de TI para garantizar que se cumplan los objetivos del departamento de Sistemas junto con las regulaciones establecidas por los organismos de control externos.

De acuerdo a nuevas actualizaciones del organismo de control externo SEPS[43], la Organización por medio del departamento de Auditoría Interna se encuentra en la planificación de un proceso definido para el establecimiento de control interno en el departamento de Sistemas.

El cumplimiento regulatorio contractual y legal externos dependen de los organismos de control y el Consejo de Vigilancia, de acuerdo a las leyes, reglamentos, estatutos, circulares, normas establecidas. Los informes y reportes se generan para dar a conocer la situación actual de la Organización con respecto a las actualizaciones de las leyes y regulaciones y su cumplimiento.

[43] Superintendencia de Economía Popular y Solidaria

3. CAPÍTULO 3: PRESENTACIÓN DE LOS RESULTADOS

3.1. ANÁLISIS DE LOS RESULTADOS.

De acuerdo a la información recolectada en las tablas del capítulo 2 y la síntesis realizada por cada dominio, se continúa con la evaluación utilizando la herramienta Process Maturity Assessment Tool que facilita la determinación del nivel de madurez del proceso actual de los dominios de COBIT 4.1.

3.1.1. PROCESOS DEL DOMINIO PO

3.1.1.1. PO1. Definir un plan estratégico de TI

Análisis:

La Cooperativa cuenta con un plan estratégico definido de TI como parte del plan estratégico global. Se realiza bajo una metodología de causa-efecto que involucra a todo el personal, por lo tanto es conocido y comunicado a todos los participantes en reuniones con la Alta dirección.

No existe la definición de un proceso documentado para el desarrollo del plan estratégico de TI, pero si existe la definición del propósito, iniciativa estratégica, el coordinador y ejecutor del objetivo.

En cuanto a los riesgos, son identificados en base a un análisis costo-beneficio por iniciativa y experiencia del Jefe de Sistemas; son comunicados al Gerente General y comisiones de manera informal, sin seguir un proceso definido y documentado.

Los objetivos a corto y largo plazo que contempla el plan estratégico de TI tienen en cuenta las necesidades de Talento Humano, aspectos técnicos y financieros, regulaciones legales, además de tendencias tecnologías.

De acuerdo con el análisis realizado en el PO1 y la definición de niveles de madurez de COBIT, se concluye que este proceso está en el nivel TRES, como se observa en la Tabla 3.1.

PO1	Definir un Plan Estratégico de TI		
Nivel	Cumplimiento	Contribución	Valor
0	1,00	0,00	0,00
1	0,75	1,00	0,75
2	0,77	1,00	0,77
3	0,71	1,00	0,71
4	0,60	1,00	0,60
5	0,40	1,00	0,40
	Nivel de Madurez =		**3,22**

Tabla 3.1 Nivel de Madurez del PO1[44]

Para mayor información, consulte el ANEXO A

3.1.1.2. PO2. Definir la arquitectura de información

Análisis:

Dentro de la Organización se reconoce que es necesaria la definición de la arquitectura de información, sin embargo en la práctica este concepto está asociado a clasificar, organizar y almacenar los datos de los socios siguiendo un proceso no definido, razón por la cual no cuenta con procedimientos, políticas o documentación.

Toda modificación a la arquitectura de información como el desarrollo de nuevos componentes, es realizada en base al cambio de los requerimientos del negocio y ejecutados por el Jefe de Sistemas, quien es la única persona que tiene acceso a las configuraciones de la Base de Datos bajo previa autorización de Gerencia General.

De acuerdo con el análisis realizado en el PO2 y la definición de niveles de madurez de COBIT, se concluye que este proceso está en el nivel UNO, como se observa en la Tabla 3.2.

[44] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

PO2	Definir la Arquitectura de Información		
Nivel	Cumplimiento	Contribución	Valor
0	0,66	0,00	0,00
1	0,41	1,00	0,41
2	0,33	1,00	0,33
3	0,17	1,00	0,17
4	0,42	1,00	0,42
5	0,43	1,00	0,43
		Nivel de Madurez =	**1,75**

Tabla 3.2 Nivel de Madurez del PO2 [45]

Para mayor información, consulte el ANEXO A

3.1.1.3. PO3. Determinar la dirección tecnológica

Análisis:

La Gerencia entiende de la importancia de que la infraestructura tecnológica esté acorde a los requerimientos de la Organización y que sea de soporte para los servicios que ofrecen, sin embargo no existe la definición de un plan específico para ello; en su lugar se encuentra como parte del plan operativo anual de la Organización y satisface las necesidades actuales.

En el plan operativo se definen tanto los componentes tecnológicos como su implementación, que es llevada a cabo con un análisis de riesgos, impacto y factibilidad no documentado bajo la responsabilidad y experiencia del Jefe de Sistemas, es decir que no se cuenta con un proceso documentado y uso de metodología para su realización. Una vez que el plan operativo es definido puede ser modificado en base al cambio o aparición de nuevos requerimientos del negocio o tecnologías emergentes en la industria.

[45] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

Por último, la Gerencia recibe un informe sobre el análisis costo-beneficio para la organización que es revisado por el Comité Ejecutivo y finalmente aprobado por el Consejo de Administración.

De acuerdo con el análisis realizado en el PO3 y la definición de niveles de madurez de COBIT, se concluye que este proceso están en el nivel UNO, como se observa en la Tabla 3.3.

PO3	**Determinar la Dirección Tecnológica**		
Nivel	Cumplimiento	Contribución	Valor
0	0,55	0,00	0,00
1	0,54	1,00	0,54
2	0,34	1,00	0,34
3	0,22	1,00	0,22
4	0,21	1,00	0,21
5	0,43	1,00	0,43
	Nivel de Madurez =		**1,74**

Tabla 3.3 Nivel de Madurez del PO3 [46]

Para mayor información, consulte el ANEXO A

3.1.1.4. PO4. Definir los procesos, organización y relaciones de TI.

Análisis:

El establecimiento de una organización de TI se lleva a cabo por parte del departamento de Talento Humano, y cuenta con la definición de roles y responsabilidades para el personal del departamento de Sistemas, los cuales están establecidos en el manual de funciones. Sin embargo, en la práctica, el personal de Sistemas realiza todas las funciones del departamento en base a su disponibilidad de tiempo.

Existe un procedimiento de evaluación del desempeño del personal de TI que se realiza internamente por el Jefe de Sistemas, quien establece métricas de

[46] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

evaluación en base al cumplimiento de tareas y conducta. Posteriormente se entrega un informe de desempeño con un formato establecido al departamento de Talento Humano.

Cabe recalcar que el Jefe de Sistemas es el encargado de proponer de forma reactiva y proactiva nuevos requerimientos en cuanto a personal, que se presentan debido al crecimiento de la empresa y la demanda de prestación de servicios del departamento, los cuales son atendidos y revisados por Gerencia para una posterior aprobación.

A nivel de la empresa se tiene conocimiento de que las funciones prestadas por TI están para dar soporte al cumplimiento de los objetivos del negocio, es decir, que son consideradas indispensables y forman parte de todos los proyectos que emprenda la Organización durante su inicio, desarrollo y finalización.

De acuerdo con el análisis realizado en el PO4 y la definición de niveles de madurez de COBIT, se concluye que este proceso están en el nivel UNO, como se observa en la Tabla 3.4.

PO4	**Definir los Procesos, Organización y Relaciones de TI**		
Nivel	Cumplimiento	Contribución	Valor
0	0,66	0,00	0,00
1	0,15	1,00	0,15
2	0,33	1,00	0,33
3	0,40	1,00	0,40
4	0,30	1,00	0,30
5	0,19	1,00	0,19
		Nivel de Madurez =	**1,37**

Tabla 3.4 Nivel de Madurez del PO4[47]

Para mayor información, consulte el ANEXO A

[47] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

3.1.1.5. PO6. Comunicar las Aspiraciones y la Dirección de la Gerencia

Análisis:

Dentro de la Organización se ha reconocido la necesidad de establecer un conjunto de política, planes y procedimientos y cumplimiento de las actividades que se llevan a cabo para satisfacer los objetivos de negocio establecidos. Sin embargo, no se tiene definidas políticas y procedimientos, razón por la cual las actividades se llevan a cabo de manera intuitiva o por medio de la experiencia y práctica del personal de TI. Por tanto, se sabe que no se tiene documentación con respecto a este tema y tampoco se tiene definido un proceso que sea documentado para transmitir la información, aunque la responsabilidad de la transmisión de información sobre políticas recae sobre la Gerencia General. Las disposiciones de Gerencia son tomadas como políticas, pero éstas no se encuentran en un repositorio que esté a disposición del personal, ya que se sólo son comunicadas vía mail. Cabe tener en cuenta que estas disposiciones están basadas en las recomendaciones, en su mayoría relacionadas con seguridad informática, que proporciona el departamento de Sistemas.

De acuerdo con el análisis realizado en el PO6 y la definición de niveles de madurez de COBIT, se concluye que este proceso está en el nivel DOS, como se observa en la Tabla 3.5.

PO6	**Comunicar las Aspiraciones y la Dirección de la Gerencia**		
Nivel	Cumplimiento	Contribución	Valor
0	0,83	0,00	0,00
1	0,66	1,00	0,66
2	0,66	1,00	0,66
3	0,23	1,00	0,23
4	0,24	1,00	0,24
5	0,61	1,00	0,61
		Nivel de Madurez =	**2,40**

Tabla 3.5 Nivel de Madurez del PO6[48]

Para mayor información, consulte el ANEXO A

[48] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

3.1.1.6. PO7. Administrar Recursos Humanos de TI

Análisis:

En la Organización se tiene conciencia sobre la importancia de alinear la gestión de recursos humanos de TI con la planificación que realiza el Departamento de Sistemas. La persona responsable del personal de Sistemas es el Jefe de Talento Humano, quien se encarga de definir las responsabilidades de cada rol del Departamento de Sistemas. Sin embargo, el Jefe de Sistemas puede sugerir y solicitar más personal cuando se considere necesario.

El plan del personal de TI se establece en el plan general de Talento Humano de toda la Organización. No se contempla rotación de personal y se basa en la experiencia y práctica del Jefe de Talento Humano más que en estándares de la industria. Además es sensible a cambios según se requiera, ya sea para cumplir con medidas reglamentarias o por cambios en la tecnología de información del negocio.

Para la contratación de personal de TI se toma en cuenta los cambios en el negocio y de tecnología, puesto que es necesario que el nuevo personal esté preparado para asumir las responsabilidades que satisfagan los objetivos del negocio. De ser necesario, se tiene preparada capacitación general para el personal de TI para que se adecúe al funcionamiento de las tecnologías de información de la Organización. También se prepara capacitaciones específicas a través de cursos externos que permitan adquirir y reforzar el conocimiento del personal en áreas determinadas relacionadas con las tecnologías de información.

De acuerdo con el análisis realizado en el PO7 y la definición de niveles de madurez de COBIT, se concluye que este proceso está en el nivel DOS, como se observa en la Tabla 3.6.

PO7	Administrar Recursos Humanos de TI		
Nivel	Cumplimiento	Contribución	Valor
0	0,84	0,00	0,00
1	0,68	1,00	0,68
2	0,33	1,00	0,33
3	0,54	1,00	0,54
4	0,54	1,00	0,54
5	0,47	1,00	0,47
		Nivel de Madurez =	**2,56**

Tabla 3.6 Nivel de Madurez del PO7[49]

Para mayor información, consulte el ANEXO A

3.1.1.7. PO9. Evaluar y Administrar los Riesgos de TI

Análisis:

En la Organización se tiene conciencia de la importancia de llevar a cabo una gestión de riesgos. Sin embargo, el análisis actual se centra en mayor parte en los riesgos del negocio y no prestan la atención debida a los riesgos de TI que puedan afectar al negocio. Por esta razón sólo mantiene un análisis de riesgo interno por parte del Jefe de Sistemas cuando se requiere actualizar, cambiar o adquirir componentes de la infraestructura, el que es transmitido a quien corresponda mediante informes gerenciales. De este análisis se obtiene un reporte con los resultados y el posible impacto económico que puede tener la Organización de no mitigarse dichos riesgos. Esta documentación son recomendaciones que ayuden Gerencia General para la toma decisiones al respecto. En este documento se plantean las consecuencias de no mitigar el riesgo y se dan 3 posibles soluciones con un análisis de costo-beneficio, de las cuales una será seleccionada por la Alta Gerencia para ser considerada como medida de mitigación.

[49] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

El análisis de riesgo se realiza, en su mayoría, de manera reactiva y de acuerdo con la experiencia y práctica del Jefe de Sistemas sin seguir una metodología. Cabe destacar que esta actividad no está dentro de sus responsabilidades asignadas en el manual de funciones, y por tanto no se tiene una capacitación sobre gestión de riesgos de TI.

De acuerdo con el análisis realizado en el PO9 y la definición de niveles de madurez de COBIT, se concluye que este proceso está en el nivel UNO, como se observa en la Tabla 3.7.

PO9	**Evaluar y Administrar los Riesgos de TI**		
Nivel	Cumplimiento	Contribución	Valor
0	0,43	0,00	0,00
1	0,52	1,00	0,52
2	0,44	1,00	0,44
3	0,13	1,00	0,13
4	0,25	1,00	0,25
5	0,10	1,00	0,10
	Nivel de Madurez =		**1,44**

Tabla 3.7 Nivel de Madurez del PO9[50]

Para mayor información, consulte el ANEXO A

3.1.1.8. Análisis Global del Dominio PO

De acuerdo al análisis del Domino Planificar y Organizar, el nivel de madurez global se corresponde con el UNO: INICIAL/AD HOC del Modelo genérico de madurez de COBIT 4.1.

Para mayor información, consulte la Tabla 2.2

[50] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

3.1.2. PROCESOS DEL DOMINIO AI

3.1.2.1. AI1 Identificar soluciones automatizadas

Análisis:

La Organización está consciente de la importancia en definir requerimientos de TI para identificar soluciones automatizadas con respecto a hardware, software y servicios de TI que son relevantes para el negocio.

Esta responsabilidad recae sobre el Jefe de Sistemas quien, en base a la práctica adquirida, desarrolla un análisis interno en el departamento sobre la factibilidad tecnológica y riesgos; posteriormente realiza un análisis costo-beneficio sobre las necesidades funcionales y operativas, las cuales son expuestas en un documento de Solicitud de Requerimientos.

Todo este proceso de identificación de soluciones automatizadas se encuentra en el Manual de Adquisiciones de la Organización, sin embargo, no es específico para el departamento de Sistemas.

Una vez que el Jefe de Sistemas realiza este análisis, procede a emitir un informe con 3 posibles alternativas de proveedores para dar cumplimiento a la solución automatizada dependiendo del caso; este análisis es enviado a Gerencia, comité ejecutivo y por último para su aprobación al Consejo de Administración, dependiendo del monto de la solución tecnológica.

De acuerdo con el análisis realizado en el AI1 y la definición de niveles de madurez de COBIT, se concluye que este proceso está en el nivel DOS, como se muestra en la Tabla 3.8.

AI1	Identificar Soluciones Automatizadas		
Nivel	Cumplimiento	Contribución	Valor
0	0,83	0,00	0,00
1	0,56	1,00	0,56
2	0,74	1,00	0,74
3	0,57	1,00	0,57
4	0,37	1,00	0,37
5	0,16	1,00	0,16
		Nivel de Madurez =	**2,40**

Tabla 3.8 Nivel de Madurez del AI1[51]

Para mayor información, consulte el ANEXO B

3.1.2.2. AI2 Adquirir y mantener software aplicativo

Análisis:

La Organización reconoce la necesidad de tener un proceso definido sobre adquirir y mantener software aplicativo para cumplir con los requerimientos del negocio dentro de un tiempo y costo aceptable. Al momento cuentan con procedimientos internos al Departamento de Sistemas para conseguir resultados eficientes de mantenimiento y soporte de las aplicaciones para los usuarios.

En el departamento de Sistemas, esta responsabilidad está asignada al programador quien realiza estas tareas de soporte a las aplicaciones, bajo la supervisión del Jefe de Sistemas, y finalmente bajo la aprobación de Auditoría interna y el usuario que solicitó el requerimiento antes del paso a producción del software aplicativo.

No se utilizan metodologías para la consecución de este proceso, únicamente se basa en procedimientos establecidos por el Jefe de Sistemas, quien determina las actividades, recursos, tiempo y costos necesarios para su cumplimiento, los

[51] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

cuales son detallados en un informe de paso a producción y Parametrización para las aplicaciones.

De acuerdo con el análisis realizado en el AI2 y la definición de niveles de madurez de COBIT, se concluye que este proceso está en el nivel DOS, como se observa en la Tabla 3.9.

AI2	**Adquirir y Mantener Software Aplicativo**		
Nivel	Cumplimiento	Contribución	Valor
0	0,49	0,00	0,00
1	0,60	1,00	0,60
2	0,42	1,00	0,42
3	0,49	1,00	0,49
4	0,65	1,00	0,65
5	0,34	1,00	0,34
	Nivel de Madurez =		**2,50**

Tabla 3.9 Nivel de Madurez del AI2[52]

Para mayor información, consulte el ANEXO B

3.1.2.3. AI3 Adquirir y mantener infraestructura tecnológica

Análisis:

La Organización es consciente de que adquirir y mantener infraestructura tecnológica es de suma importancia para dar cumplimiento a los objetivos del negocio, por lo cual se cuenta con un manual de adquisiciones general. Se debe tener en cuenta que los aspectos tecnológicos se encuentran detallados en el plan operativo correspondiente al departamento de Sistemas.

En lo referente a adquisición y mantenimiento de infraestructura tecnológica relacionada con la información relevante del negocio, existe una baja amenaza de pérdida de información ya que existen respaldos físicos de la información sensible.

[52] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

Existe un ambiente para la realización de pruebas cuando se adquiere un nuevo componente de infraestructura tecnológica o cuando se realiza una modificación al mismo, pero no existe una documentación formal de este procedimiento ni algún tipo de plan de evaluación para el nuevo hardware y software.

En el caso del mantenimiento, se lo realiza periódicamente y de manera preventiva por el personal de Sistemas, teniendo en cuenta las necesidades de las aplicaciones que deben ser soportadas por la infraestructura tecnológica para brindar un funcionamiento óptimo. Sin embargo esta práctica no está documentada en ningún reglamento, sino que se realiza en base a la dirección del Jefe de Sistemas.

En cuanto a adquisición de infraestructura tecnológica de terceros existen contratados de arrendamientos o acuerdos de arrendamiento con opción de compra de hardware y software.

De acuerdo con el análisis realizado en el AI3 y la definición de niveles de madurez de COBIT, se concluye que este proceso está en el nivel DOS, como se observa en la Tabla 3.10.

AI3	**Adquirir y Mantener Infraestructura Tecnológica**		
Nivel	Cumplimiento	Contribución	Valor
0	0,66	0,00	0,00
1	0,18	1,00	0,18
2	0,80	1,00	0,80
3	0,75	1,00	0,75
4	0,58	1,00	0,58
5	0,60	1,00	0,60
	Nivel de Madurez =		**2,91**

Tabla 3.10 Nivel de Madurez del AI3[53]

Para mayor información, consulte el ANEXO B

[53] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

3.1.2.4. AI4 Facilitar la operación y el uso

Análisis:

Dentro de la Organización se reconoce la importancia que tiene la producción de documentación para los usuarios, manuales de operación y material de entrenamiento, por lo que la documentación que se suministra con los productos adquiridos no es la única que se utiliza en la Organización. Hay que tener en cuenta que para el desarrollo de la documentación que se genera no se utilizan estándares ni tienen un proceso documentado, sino que únicamente se cuenta con la experiencia y práctica de las personas responsables de esta actividad.

Los manuales de operación han sido creados con el fin de establecer los procedimientos que tiene que seguir el personal, de acuerdo a su área de trabajo o departamento, para desempeñar su actividad. Por otro lado, el material de entrenamiento se prepara para cada departamento con el fin de proveer al personal de una visión general del funcionamiento de su área de trabajo. Se debe tener en cuenta que esta documentación está desarrollada por el Jefe de Talento Humano en colaboración con el personal de cada área; ésta es actualizada anualmente, si es necesario, y es distribuida entre todo el personal, sobre todo cuando se incorporan a sus actividades por primera vez.

En cuanto al Departamento de Sistemas, se elabora documentación para los usuarios sobre los cambios o actualizaciones que se generan en el sistema Financial. Sin embargo, la documentación se desarrolla únicamente cuando se considera necesario. El responsable de esta actividad es la persona que está a cargo de realizar el cambio, y la calidad de la documentación generada es supervisada por el Jefe del departamento para su aprobación.

Finalmente, la documentación elaborada por el departamento de sistemas está almacenada en un servidor de archivos al que tienen acceso las personas a las que está destinada esta información, mientras que la información desarrollada por el departamento de Talento Humano se distribuye a través de documentos impresos.

De acuerdo con el análisis realizado en el AI4 y la definición de niveles de madurez de COBIT, se concluye que este proceso está en el nivel DOS, como se observa en la Tabla 3.11.

AI4	Facilitar la Operación y el Uso		
Nivel	Cumplimiento	Contribución	Valor
0	0,51	0,00	0,00
1	0,63	1,00	0,63
2	0,66	1,00	0,66
3	0,48	1,00	0,48
4	0,23	1,00	0,23
5	0,26	1,00	0,26
		Nivel de Madurez =	**2,25**

Tabla 3.11 Nivel de Madurez del AI4[54]

Para mayor información, consulte el ANEXO B

3.1.2.5. AI5 Adquirir recursos de TI

Análisis:

Dentro de la Organización, las adquisiciones se realizan de acuerdo a lo estipulado en el Manual de Adquisiciones. En él se establecen los requerimientos de TI para hacer la adquisición de cualquier recurso que sea necesario para mantener activas las operaciones del negocio, por tanto, se sabe que no se tiene un manual o una sección del manual que trate exclusivamente de recursos de TI.

El departamento de Sistemas, aun cuando no está involucrado directamente en la adquisición ni en la elaboración de los contratos con los proveedores, sí propone cuáles son las mejores alternativas relativas a las soluciones tecnológicas teniendo en cuenta un análisis de costo-beneficio y de factibilidad. También se toma en cuenta los riesgos que supone el hecho de no adquirir un recurso de TI, aunque este análisis sólo se realiza dentro del departamento de Sistemas. Una vez que la adquisición de recursos de TI se ha aprobado y

[54] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

ejecutado, en la mayoría de los casos, no se realizan pruebas documentadas para verificar si su funcionamiento es óptimo para apoyar a las actividades del negocio.

Con respecto a los proveedores, no se reconoce la necesidad de gestionar las relaciones con los proveedores, aunque sí se establecen buenas relaciones entre ambas partes. Por otro lado, los proveedores, sí definen las medidas de seguridad y soporte, sobre todo aquellos relacionados con recursos de TI arrendados por parte de la Organización.

De acuerdo con el análisis realizado en el AI5 y la definición de niveles de madurez de COBIT, se concluye que este proceso está en el nivel DOS, como se observa en la Tabla 3.12.

AI5	**Adquirir Recursos de TI**		
Nivel	Cumplimiento	Contribución	Valor
0	0,83	0,00	0,00
1	0,58	1,00	0,58
2	0,46	1,00	0,46
3	0,39	1,00	0,39
4	0,43	1,00	0,43
5	0,38	1,00	0,38
	Nivel de Madurez =		**2,25**

Tabla 3.12 Nivel de Madurez del AI5[55]

Para mayor información, consulte el ANEXO B

3.1.2.6. Análisis Global del Dominio AI

De acuerdo al análisis del Domino Adquirir e Implementar, el nivel de madurez global se corresponde con el DOS: REPETIBLE PERO INTUITIVO del Modelo genérico de madurez de COBIT 4.1.

Para mayor información, consulte el Tabla 2.2

[55] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

3.1.3. PROCESOS DEL DOMINIO DS

3.1.3.1. DS1 Definir y administrar los niveles de servicio

Análisis:

Dentro de este proceso la Organización está consciente de la importancia de definir los niveles de servicios de TI para lo cual se establecen contratos escritos entre el proveedor del servicio y el cliente, dentro de los cuales existen acuerdos que definen la descripción del servicio, fecha de inicio y de su terminación, entre otros, y un aspecto de suma relevancia como es la asignación de las responsabilidades y rendiciones de cuenta de los proveedores y clientes. Este es el medio de comunicación entre los involucrados de los servicios de TI.

Por otro lado, la Organización asigna la responsabilidad de supervisar los niveles de servicio a sus autoridades legales como son el Gerente General y Asesoría Legal, quienes realizan un análisis costo-beneficio de los servicios y ateniéndose al procedimiento de definición de niveles de servicio que se encuentra en el manual de adquisiciones. Posteriormente se mantiene cada contrato escrito archivado físicamente en Gerencia General de manera que sea de libre acceso y conocimiento para el resto del personal de la Organización.

Los contratos escritos no cuentan con métricas cuantitativas del desempeño del servicio de TI, solo con descripciones cualitativas mediante cláusulas relativas al incumplimiento de los servicios, así como de las modificaciones al contrato.

La notificación a Gerencia General sobre el desempeño de los servicios, así como de los niveles de servicio es llevada a cabo mediante la presentación de informes de actividades realizados por el Jefe de Sistemas sin detallar aspectos tecnológicos acerca de alguna anomalía del servicio o incumplimiento de los niveles de servicio.

De acuerdo con el análisis realizado en el DS1 y la definición de niveles de madurez de COBIT, se concluye que este proceso están en el nivel UNO, como se observa en la Tabla 3.13.

DS1	Definir y administrar los niveles de Servicio		

Nivel	Cumplimiento	Contribución	Valor
0	0,50	0,00	0,00
1	0,74	1,00	0,74
2	0,58	1,00	0,58
3	0,18	1,00	0,18
4	0,29	1,00	0,29
5	0,11	1,00	0,11

Nivel de Madurez =	**1,90**

Tabla 3.13 Nivel de Madurez del DS1[56]

Para mayor información, consulte el ANEXO C

3.1.3.2. DS2 Administrar los Servicios de Terceros

Análisis:

La Organización es consciente de la importancia que tiene en el negocio el definir, identificar, contratar y administrar los servicios de TI de terceros, para lo cual asignan responsables. En este caso intervienen el Jefe de Sistemas, quien se encarga de elaborar un informe o una proforma en el que constan una terna de proveedores para los servicios requeridos junto con un análisis de riesgos y costo-beneficio, posteriormente es revisado por Gerencia y los Consejos de Administración y Vigilancia que se encargan de aprobar la contratación del servicio de terceros de acuerdo a los montos establecidos en el manual de Adquisiciones. Por último, para finalizar la contratación del servicio interviene la Asesoría legal de la Organización, la cual evalúa las condiciones legales, mientras que el Jefe de Sistemas evalúa las condiciones operativas y de control que están expuestas en el contrato con el proveedor, para finalmente proceder a su firma.

En cuanto a las políticas y procedimientos de administración de servicios de terceros, la Organización se fundamenta en el manual de adquisiciones que indica

[56] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

las condiciones económicas que son establecidas en base a estándares planteados dentro de la Organización.

Los servicios de terceros emiten notificaciones del desempeño del servicio prestado, y a su vez informan sobre algún mal funcionamiento sin dar detalles cuantitativos (métricas) sobre los mismos, por lo que la Gerencia tiene un conocimiento general y superficial sobre la calidad del servicio prestado.

La supervisión del servicio de terceros es realizada periódicamente por el personal del departamento de Sistemas, quienes pueden detectar posibles problemas y comunicarlos a su Jefe para darle una solución oportuna. Además se cuenta con un informe de actividades realizadas por el Jefe de Sistemas, en el que se menciona el desempeño de algunos de los servicios de terceros.

La Organización no cuenta con procesos documentados para la administración de los servicios de TI con proveedores, por lo tanto no existe la asignación de un único responsable para su administración.

De acuerdo con el análisis realizado en el DS3 y la definición de niveles de madurez de COBIT, se concluye que este proceso está en el nivel DOS, como se observa en la Tabla 3.14.

DS2	**Administrar los servicios de terceros**		
Nivel	Cumplimiento	Contribución	Valor
0	0,94	0,00	0,00
1	0,61	1,00	0,61
2	0,69	1,00	0,69
3	0,60	1,00	0,60
4	0,49	1,00	0,49
5	0,46	1,00	0,46
		Nivel de Madurez =	**2,85**

Tabla 3.14 Nivel de Madurez del DS2[57]

Para mayor información, consulte el ANEXO C

[57] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

3.1.3.3. DS3 Administrar el Desempeño y la Capacidad

Análisis:

La Gerencia está consciente de que varios servicios claves del negocio pueden requerir de un mayor desempeño de los recursos de TI, razón por la cual se asigna al departamento de Sistemas la responsabilidad de definir bajo qué condiciones se administrarán todos los recursos de TI atendiendo a su desempeño y capacidad.

Sin embargo, a nivel de la Organización no se cuenta con un plan de la capacidad de los recursos de TI; en su lugar se maneja un inventario de todos los recursos de TI que es realizado semestralmente por el Departamento de Sistemas y bajo el cual se pueden determinar las posibles adquisiciones de otros recursos de TI para mejorar el desempeño actual y futura de los servicios clave que el negocio requiera.

Uno de los procedimientos que se realizan por parte del departamento de Sistemas es la revisión periódica de la infraestructura tecnológica y aplicaciones mediante herramientas propias del Sistema Operativo, con el objetivo de detectar posibles problemas en su desempeño y alternativas para sus soluciones, las cuales son analizadas y evaluadas por el Jefe de Sistemas y miembros del departamento, en base a las prácticas adquiridas y a las necesidades de TI para satisfacer los requerimientos del negocio que se presenten.

De acuerdo con el análisis realizado en el DS3 y la definición de niveles de madurez de COBIT, se concluye que este proceso está en el nivel UNO, como se observa en la Tabla 3.15.

DS3	Administrar el Desempeño y la Capacidad		
Nivel	Cumplimiento	Contribución	Valor
0	0,82	0,00	0,00
1	0,40	1,00	0,40
2	0,57	1,00	0,57
3	0,27	1,00	0,27
4	0,44	1,00	0,44
5	0,15	1,00	0,15
		Nivel de Madurez =	**1,82**

Tabla 3.15 Nivel de Madurez del DS3[58]

Para mayor información, consulte el ANEXO C

3.1.3.4. DS4 Garantizar la continuidad del Servicio

Análisis:

La Gerencia de la Organización está consciente de la importancia de identificar los riesgos, vulnerabilidades y amenazas en lo que se refiere a operaciones de TI así como en infraestructura, aplicaciones y en la relación que éstas tendrían con el negocio, pero no cuentan con un plan de continuidad. Actualmente se encuentran en el desarrollo de un plan de contingencia que pueda minimizar el impacto en caso de que se presente algún incidente o problema que pueda afectar a la continuidad de los servicios.

Cabe recalcar que la Organización cuenta con un procedimiento de copias de seguridad y respaldos de la información que genera y almacena el Sistema Financiero Financial. En lo que se refiere a enlaces de comunicación, se está implementando una red de contingencias para lo cual se está buscando un proveedor de este servicio para que pueda garantizar la continuidad del negocio.

La responsabilidad del desarrollo del plan de contingencia de los servicios de TI está asignada a los miembros del Departamento de Sistemas, quienes junto al

[58] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

representante de Auditoría Interna se encargarán de valorarlo y aprobarlo. Esta elaboración del plan de contingencias forma parte del plan estratégico actual de la Organización.

En caso de presentarse algún problema que limite la continuidad de los servicios de TI, los usuarios no emplean soluciones alternas como respuesta a la interrupción de los mismos sino que son realizadas por el personal del departamento de TI de forma reactiva en pocos casos, ya que por lo general se realizan de manera proactiva. Para garantizar la continuidad de los servicios en caso de fallas eléctricas, la Organización tiene adecuado un generador de respaldo así como dispositivos que aseguren a los equipos como son los UPS.

De acuerdo con el análisis realizado en el DS4 y la definición de niveles de madurez de COBIT, se concluye que este proceso está en el nivel UNO, como se observa en la Tabla 3.16.

DS4	**Garantizar la Continuidad del Servicio**		
Nivel	Cumplimiento	Contribución	Valor
0	1,00	0,00	0,00
1	0,26	1,00	0,26
2	0,43	1,00	0,43
3	0,25	1,00	0,25
4	0,17	1,00	0,17
5	0,10	1,00	0,10
	Nivel de Madurez =		**1,22**

Tabla 3.16 Nivel de Madurez del DS4[59]

Para mayor información, consulte el ANEXO C

[59] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

3.1.3.5. DS5 Garantizar las Seguridad de los Sistemas

Análisis:

La Organización está consciente de la importancia de la seguridad de los Sistemas, por ello reconoce la necesidad de desarrollar e implementar un plan de Seguridad de Sistemas que contemple todos los aspectos para mantener la integridad de la información y proteger los activos de TI. Actualmente no cuentan con dicho plan, únicamente existen algunas políticas de seguridad de acceso, datos, equipos, aplicaciones, las cuales son definidas por el Jefe de Sistemas según sea requerido. Además existen políticas de seguridad industrial a nivel de toda la Organización, que se enfoca en aspectos de seguridad ambiental, física, de personal entre otros.

La administración de seguridad de Sistemas está asignada al Jefe de Sistemas y demás personal del departamento de Sistemas, quienes deben garantizar que existan las mínimas brechas de seguridad. El cumplimiento de las políticas de seguridad se encuentra bajo la responsabilidad del personal de la Organización, quienes deben seguir las políticas establecidas. Además existe un monitoreo de seguridad continuo que es registrado y posteriormente analizado en los casos en los que ocurra de un fallo de seguridad.

En cuando al entrenamiento relacionado con seguridad de TI y del Negocio, se ofrece capacitación al personal de manera informal, sobre todo cuando se incorporan a la organización por primera vez.

En cuanto a seguridad de los servicios de terceros, las políticas de seguridad son establecidas por el proveedor del servicio dentro del contrato escrito, y ellos son los encargados de garantizar y emitir reportes sobre la seguridad de los mismos.

De acuerdo con el análisis realizado en el DS5 y la definición de niveles de madurez de COBIT, se concluye que este proceso está en el nivel DOS, como se observa en la Tabla 3.17.

DS5	Garantizar la Seguridad de los Sistemas		
Nivel	Cumplimiento	Contribución	Valor
0	0,72	0,00	0,00
1	0,62	1,00	0,62
2	0,53	1,00	0,53
3	0,52	1,00	0,52
4	0,34	1,00	0,34
5	0,15	1,00	0,15
		Nivel de Madurez =	**2,16**

Tabla 3.17 Nivel de Madurez del DS5[60]

Para mayor información, consulte el ANEXO C

3.1.3.6. DS7 Educar y entrenar a los usuarios

Análisis:

En la Organización se reconoce la importancia de crear un programa de capacitación y educación para los usuarios con respecto a los sistemas y herramientas que deben utilizar para desempeñar sus actividades laborales además de temas relacionados con el negocio. Por esta razón, el Departamento de Talento Humano se encarga de programar, anualmente, cursos para todo el personal, en los cuales se incluyen dos de carácter general y dos de carácter específico. Se debe tener en cuenta que estos cursos no tienen por objetivo tratar temas de conducta ética o seguridad de sistemas. Estos tópicos se transmiten a través de disposiciones de Gerencia General y reglamentos para que sean conocidos por todo el personal de la Organización.

Además, este departamento también se encarga de definir un manual de operaciones que el personal debe conocer sobre su área de trabajo y delega el entrenamiento sobre la tecnología al Departamento de Sistemas. Esta capacitación se lleva a cabo cuando se considera necesario, a través de talleres en un ambiente de prueba, donde el usuario maneja la herramienta o sistema. Estos talleres se desarrollan con estándares definidos por el Departamento de

[60] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

Sistemas, junto con la documentación necesaria para su ejecución. Tras finalizar la capacitación se realiza una evaluación teórica y práctica que permita conocer el nivel de conocimiento adquirido para valorar si el usuario está apto para utilizar el sistema en el ambiente de producción, y en base a la retroalimentación realizada con el usuario se estima si necesita más tiempo de capacitación.

De acuerdo con el análisis realizado en el DS7 y la definición de niveles de madurez de COBIT, se concluye que este proceso está en el nivel DOS, como se observa en la Tabla 3.18.

DS7	**Educar y Entrenar a los Usuarios**		
Nivel	Cumplimiento	Contribución	Valor
0	0,83	0,00	0,00
1	0,63	1,00	0,63
2	0,63	1,00	0,63
3	0,34	1,00	0,34
4	0,41	1,00	0,41
5	0,32	1,00	0,32
		Nivel de Madurez =	**2,32**

Tabla 3.18 Nivel de Madurez del DS7[61]

Para mayor información, consulte el ANEXO C

3.1.3.7. DS10 Administrar los problemas

Análisis:

En la Organización se tiene conciencia de la necesidad de la gestión de problemas de manera que se pueda identificar cuál es la causa de los problemas encontrados. Sin embargo, no se lleva una gestión de problemas propiamente dicha sino que se realiza un control de los problemas que se producen a nivel de sistemas mediante una solicitud de requerimientos por parte de los usuarios de los sistemas, memorándum por parte de la Gerencia General y mediante la utilización de la herramienta institucional como es el mail corporativo. Para dar una solución a los problemas que han comunicado los usuarios, se redirigen las

[61] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

solicitudes de requerimientos a las diferentes secciones del departamento de sistemas para que puedan ser atendidas, dependiendo de la prioridad que se les otorgue. Una vez solucionados los problemas, se hacen pruebas de aceptación con el usuario para comprobar que el problema ha sido solucionado de manera satisfactoria. De esta actividad la documentación emitida es la solicitud de requerimientos o los memorándum, y la información relacionada con los problemas la que sólo es comunicada a las personas afectadas.

Por otro lado, el Departamento de Sistemas, a través del monitoreo detecta problemas en el sistema, en las comunicaciones, servidores, seguridad, entre otros. Para solucionarlos, se comunica las causas, consecuencias y posibles soluciones a Gerencia General para que autorice la puesta en marcha de la solución propuesta.

Finalmente, hay que tener en cuenta que para la identificación y resolución de problemas no se utiliza ningún tipo de estándar escrito, sino que se depende de los procedimientos establecidos por Departamento de Sistemas, por lo que no existe documentación ni un sistema de gestión de problemas.

De acuerdo con el análisis realizado en el DS10 y la definición de niveles de madurez de COBIT, se concluye que este proceso está en el nivel DOS, como se observa en la Tabla 3.19.

DS10	**Administrar los Problemas**		
Nivel	Cumplimiento	Contribución	Valor
0	0,82	0,00	0,00
1	0,82	1,00	0,82
2	0,50	1,00	0,50
3	0,44	1,00	0,44
4	0,29	1,00	0,29
5	0,25	1,00	0,25
		Nivel de Madurez =	**2,30**

Tabla 3.19 Nivel de Madurez del DS10[62]

Para mayor información, consulte el ANEXO C

[62] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

3.1.3.8. DS11 Administrar los datos

Análisis:

La Organización reconoce que la información que posee es uno de sus activos más importantes para el negocio. Por esta razón se han asignado responsables y propietarios de los datos que se manejan en la Organización con el fin de que no sean accedidos ni alterados por personas no autorizadas. Para controlar la calidad e integridad de los datos, se hace un cuadre y cierre diario de las cuentas y transacciones realizadas para asegurar que la información sea correcta y confiable. Una vez que se realiza el cuadre se respalda la información y se la almacena en un servidor de respaldos, siguiendo el procedimiento propuesto por el Jefe de Sistemas para la realización de copias de seguridad/restauración y acuerdos de eliminación de residuos.

La información que se mantiene en el servidor de respaldos es entregada al Gerente General y una vez que los discos están a su máxima capacidad son almacenados en un lugar seguro. Las copias almacenadas se retienen el tiempo estipulado por los organismos de control como la SEPS[63].

Además, para implementar medidas que garanticen la seguridad de la información, se atienden a las recomendaciones que realizan la SEPS[43] y el Departamento de Auditoría Interna. Para dar a conocer al personal sobre seguridad de la información se realizan capacitaciones para transmitir las medidas de seguridad que se van a implementar para que cada uno contribuya con la protección de la información.

De acuerdo con el análisis realizado en el DS11 y la definición de niveles de madurez de COBIT, se concluye que este proceso está en el nivel TRES, como se observa en la Tabla 3.20.

[63] Superintendencia de Economía Popular y Solidaria

DS11	Administrar los Datos		
Nivel	Cumplimiento	Contribución	Valor
0	0,70	0,00	0,00
1	0,81	1,00	0,81
2	0,87	1,00	0,87
3	0,67	1,00	0,67
4	0,39	1,00	0,39
5	0,30	1,00	0,30
		Nivel de Madurez =	**3,05**

Tabla 3.20 Nivel de Madurez del DS11[64]

Para mayor información, consulte el ANEXO C

3.1.3.9. DS12 Administrar el Ambiente Físico

Análisis:

En la Organización se tiene conciencia de la necesidad de tener instalaciones adecuadas para proteger los activos tangibles e intangibles, además de ser conscientes de la necesidad de invertir en recursos informáticos que optimicen y apoyen a las funciones del negocio. Por esta razón, se supervisan y controlan factores ambientales que pueden afectar al negocio, como incendios, fallas eléctricas, calor excesivo, humedad entre otros. De esta actividad se encargan el Departamento de Sistemas para la protección del ambiente relacionado con los sistemas e infraestructura, los organismos de control físico como los bomberos y el Comité de Seguridad se encargan de la seguridad de las instalaciones y de la salud del personal.

Con respecto al Departamento de Sistemas, se restringe el acceso al personal no autorizado, sobre todo al área de servidores. Sin embargo, para autorizar el ingreso al departamento es necesario que la persona sea anunciada primero, y luego llene una bitácora de ingreso para tener constancia de su estancia en el departamento.

[64] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

Los procesos de protección física de las instalaciones no están definidos, ya que sólo se tienen disposiciones de Gerencia General y de organismos de control, o recomendaciones del Departamento de Sistemas y de Auditoría Interna para implementar medidas de seguridad física. Por tanto, como los enfoques de cada autoridad son distintos, no se tiene un estándar para la elaboración e implementación de las medidas en cuestión.

De acuerdo con el análisis realizado en el DS12 y la definición de niveles de madurez de COBIT, se concluye que este proceso está en el nivel DOS, como se observa en la Tabla 3.21.

DS12	**Administración del ambiente físico**		
Nivel	Cumplimiento	Contribución	Valor
0	1,00	0,00	0,00
1	0,75	1,00	0,75
2	0,32	1,00	0,32
3	0,69	1,00	0,69
4	0,60	1,00	0,60
5	0,49	1,00	0,49
		Nivel de Madurez =	**2,85**

Tabla 3.21 Nivel de Madurez del DS12[65]

Para mayor información, consulte el ANEXO C

3.1.3.10. DS13 Administrar las Operaciones

Análisis:

Dentro de la Organización se reconoce la importancia de dedicar tiempo y recursos para que el Departamento de Sistemas proporcione un servicio de soporte de TI que permita resolver los problemas y requerimientos de TI que le conciernen, en el menor tiempo posible y con la mejor relación costo-beneficio.

[65] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

Por esta razón el departamento de Talento Humano ha dividido las funciones concernientes al departamento de Sistemas en tres cargos: Jefatura, programador y help desk. Las responsabilidades de cada uno se encuentran detalladas en el Manual de Funciones de la Organización. Sin embargo, en este manual no se especifican procedimientos para llevar a cabo las responsabilidades de cada cargo, por lo cual el Jefe de Sistemas es el que se encarga de establecer los procedimientos para ejecución de las actividades del personal a su cargo. Estos procedimientos se encuentran detallados en el diagrama de procesos y disposiciones internas y son comunicados al personal a través de una capacitación práctica y disposiciones internas escritas, lo que hace que se dependa del personal actual del Departamento de Sistemas para ejecutar sus responsabilidades de acuerdo a los procedimientos establecidos.

De acuerdo con el análisis realizado en el DS13 y la definición de niveles de madurez de COBIT, se concluye que este proceso está en el nivel DOS, como se observa en la Tabla 3.22.

DS13	**Administrar las operaciones**		
Nivel	Cumplimiento	Contribución	Valor
0	0,66	0,00	0,00
1	0,48	1,00	0,48
2	0,63	1,00	0,63
3	0,52	1,00	0,52
4	0,48	1,00	0,48
5	0,51	1,00	0,51
		Nivel de Madurez =	**2,61**

Tabla 3.22 Nivel de Madurez del DS13[66]

Para mayor información, consulte el ANEXO C

[66] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

3.1.3.11. Análisis Global del Dominio DS

De acuerdo al análisis del Domino Entregar y Dar Soporte, el nivel de madurez global se corresponde con el DOS: REPETIBLE PERO INTUITIVO del Modelo genérico de madurez de COBIT 4.1.

Para mayor información, consulte Tabla 2.2

3.1.4. PROCESOS DEL DOMINIO ME

3.1.4.1. ME1 Monitorear y Evaluar el Desempeño de TI

Análisis:

La Organización y el departamento de Sistemas reconocen la necesidad de un proceso de monitoreo y evaluación del desempeño de TI, pero actualmente no lo tienen definido, por lo que es realizado internamente en el departamento de Sistemas siguiendo estándares propios.

Las métricas del desempeño de TI para aplicaciones e infraestructura tecnológica son proporcionadas por las herramientas propias del Sistema y son evaluadas de acuerdo a la práctica del Jefe de Sistemas, el mismo que crea un informe que se entrega Gerencia acerca del desempeño para la toma de decisiones en cuanto a nuevos requerimientos tecnológicos que surjan junto con un análisis de factibilidad y costo-beneficio.

De acuerdo con el análisis realizado en el ME1 y la definición de niveles de madurez de COBIT, se concluye que este proceso está en el nivel UNO, como se observa en la Tabla 3.23.

ME1	Monitorear y Evaluar el Desempeño de TI		
Nivel	Cumplimiento	Contribución	Valor
0	0,41	0,00	0,00
1	0,26	1,00	0,26
2	0,42	1,00	0,42
3	0,18	1,00	0,18
4	0,10	1,00	0,10
5	0,07	1,00	0,07
		Nivel de Madurez =	**1,03**

Tabla 3.23 Nivel de Madurez del ME1[67]

Para mayor información, consulte el ANEXO D

3.1.4.2. ME2 Monitorear y Evaluar el Control Interno

Análisis:

La Organización es plenamente consciente de la necesidad de implementar controles internos a TI, sin embargo actualmente no se cuenta con un proceso definido para su cumplimiento en el departamento de Sistemas. Sin embargo ciertas funciones críticas para el negocio como los cambios a la base de datos y aplicaciones son registradas en un documento llamado informe de paso a producción y Parametrización que cuenta con detalles como su nivel de complejidad, los involucrados, estimación de tiempos y costos, entre otros.

El Consejo de Vigilancia realizaba el monitoreo y evaluación del control interno a nivel organizacional sin tomar en consideración puntos de control específicos para TI. Actualmente el proceso control de TI está en planificación por parte del departamento de Auditoría Interna que se incorporó a la Organización recientemente.

Los reportes emitidos por el monitoreo y evaluación del control interno contemplan pocos aspectos tecnológicos, para ello existen informes de

[67] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

actividades periódicos que son realizados por parte del Jefe de Sistemas y se presentan a la Alta Gerencia con el fin de rendir cuentas del cumplimiento de los objetivos del departamento de Sistemas.

De acuerdo con el análisis realizado en el ME2 y la definición de niveles de madurez de COBIT, se concluye que este proceso están en el nivel UNO, como se observa en la Tabla 3.24.

ME2	**Monitorear y Evaluar el Control Interno**		
Nivel	Cumplimiento	Contribución	Valor
0	0,42	0,00	0,00
1	0,73	1,00	0,73
2	0,59	1,00	0,59
3	0,23	1,00	0,23
4	0,19	1,00	0,19
5	0,00	1,00	0,00
	Nivel de Madurez =		**1,74**

Tabla 3.24 Nivel de Madurez del ME2[68]

Para mayor información, consulte el ANEXO D

3.1.4.3. ME3 Garantizar el Cumplimiento con requerimientos externos

Análisis:

La Organización es consciente de dar a conocer y hacer cumplir las leyes, regulaciones y contratos con los proveedores. Por esta razón, se ha establecido el Consejo de Vigilancia para controlar los asuntos financieros, mientras que los organismos de control como la SEPS[69], auditoría interna y externa se encargan de asegurar tanto el cumplimiento financiero como el aspecto tecnológico. La evaluación del cumplimiento de los requerimientos regulatorios se realiza periódicamente con el fin de detectar las anomalías de cumplimiento de manera

[68] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool
[69] Superintendencia de Economía Popular y Solidaria

oportuna para corregirlas y evitar sanciones por parte de los organismos de control externos como la SEPS[44].

Con el fin de que todo el personal de la Organización cumpla con los requerimientos regulatorios se preparan cursos y reuniones con los organismos de control para comunicar las leyes y regulaciones y las medidas que se deben tomar para cumplir con las mismas.

Finalmente, cabe mencionar que Auditoría interna es un departamento que se incorporó recientemente a la Organización aunque aún no consta formalmente dentro de la estructura organizacional. No se tiene un proceso definido, políticas o procedimiento documentados para asegurar el cumplimiento de reglamentos y obligaciones contractuales y legales, sino que esta tarea se realiza basándose en la experiencia de los individuos de Auditoría Interna, Consejo de Vigilancia, y de Asesoría Legal.

De acuerdo con el análisis realizado en el ME3 y la definición de niveles de madurez de COBIT, se concluye que este proceso está en el nivel DOS, como se observa en la Tabla 3.25.

ME3	**Garantizar el Cumplimiento con Requerimientos Externos**		
Nivel	Cumplimiento	Contribución	Valor
0	0,66	0,00	0,00
1	0,56	1,00	0,56
2	0,60	1,00	0,60
3	0,42	1,00	0,42
4	0,52	1,00	0,52
5	0,52	1,00	0,52
		Nivel de Madurez =	**2,62**

Tabla 3.25 Nivel de Madurez del ME3[70]

Para mayor información, consulte el ANEXO D

[70] Fuente: Extracto de la hoja de cálculo de la herramienta Process Maturity Assessment Tool

3.1.4.4. Análisis Global del Dominio ME

De acuerdo al análisis del Domino Monitorear y Evaluar, el nivel de madurez global se corresponde con el UNO: INICIAL/AD HOC de acuerdo al Modelo genérico de madurez de COBIT 4.1.

Para mayor información, consulte Tabla 2.2

3.2.PROPUESTA DE MEJORA.

En base al análisis de la evaluación y a los objetivos de control que COBIT 4.1 [**8**] ofrece para la mejora en la gestión de TICs, se han determinado una serie de propuestas que permita a la Organización mejorar la gestión de los procesos analizados y así aprovechar los recursos de TI para cumplir con los objetivos del negocio.

3.2.1. PROPUESTAS DE MEJORA DEL DOMINIO PO

PO1. DEFINIR UN PLAN ESTRATÉGICO DE TI	
Nivel de Madurez Actual TRES	**Nivel de Madurez Futuro** CUATRO
Propuestas: • Establecer una política que indique que la Gerencia debe monitorear el proceso de definición del plan estratégico de TI, de manera que pueda tomar decisiones basándose en este plan estratégico y en la medición de su efectividad. • Establecer el proceso de monitoreo para la asegurar la ejecución de los objetivos a corto y largo plazo. • Establecer procesos documentados para determinar los recursos internos y externos necesarios para el desarrollo y operaciones de los sistemas.	

Tabla 3.26 Plan de Mejora del PO1[71]

[71] Realizado por las autoras

PO2. DEFINIR LA ARQUITECTURA DE INFORMACIÓN	
Nivel de Madurez Actual UNO	**Nivel de Madurez Futuro** DOS
Propuestas: • Establecer un proceso documentado para llevar a cabo la definición, administración y mantenimiento de la arquitectura de información de la Organización basado estándares y buenas prácticas de la industria. • Asignar roles y responsabilidades para definir la arquitectura de información, cuyos responsables tengan la experiencia y capacitación apropiada. • Comunicar sobre la importancia y los componentes de arquitectura de información disponibles a todos los integrantes de la Organización.	

Tabla 3.27 Plan de Mejora del PO2[72]

PO3. DETERMINAR LA DIRECCIÓN TECNOLÓGICA	
Nivel de Madurez Actual UNO	**Nivel de Madurez Futuro** DOS
Propuestas: • Establecer un proceso definido para elaborar un plan específico para infraestructura tecnológica de acuerdo a los requerimientos del negocio y tecnologías emergentes. • Aplicar técnicas y estándares tecnológicos para el desarrollo de componentes de infraestructura tecnológica. • Realizar un análisis de las tecnologías emergentes que puedan utilizarse para la toma de decisiones. • Asignar un responsable para evaluar los cambios tecnológicos, que tenga las habilidades y experiencia necesarias para hacerlo.	

Tabla 3.28 Plan de Mejora del PO3[72]

[72] Realizado por las autoras

PO4. DEFINIR LOS PROCESOS, ORGANIZACIÓN Y RELACIONES DE TI	
Nivel de Madurez Actual	**Nivel de Madurez Futuro**
UNO	DOS

Propuestas:

- Replantear la ubicación del departamento de Sistemas en el organigrama funcional para que dé apoyo a las decisiones estratégicas de la organización.
- Realizar una evaluación de la organización del departamento de Sistemas para determinar la necesidad de contratar personal para que haya una mejor segregación de las funciones actuales.
- Comunicar las necesidades de implementar una gestión de proveedores para aprovechar las relaciones con terceros con el funde apoyar a los objetivos de la empresa.

Tabla 3.29 Plan de Mejora del PO4[73]

PO6. COMUNICAR LAS ASPIRACIONES Y LA DIRECCIÓN DE LA GERENCIA	
Nivel de Madurez Actual	**Nivel de Madurez Futuro**
DOS	TRES

Propuestas:

- Establecer políticas y procedimientos de control con la colaboración de la Gerencia para comunicar al personal todas las disposiciones y decisiones estratégicas, que esté sujeto a cambios y mantenimiento.
- Instaurar un proceso para la gestión de calidad que permita asegurar la entrega de los servicios que satisfagan las necesidades de los usuarios.
- Iniciar con programas de concienciación al personal de la organización acerca de temas relacionados con tecnologías de la información como seguridad informática y riesgos.
- Crear un plan de capacitación continua al personal de Sistemas para que administren adecuadamente el control de la información.

Tabla 3.30 Plan de Mejora del PO6[73]

[73] Realizado por las autoras

PO7. ADMINISTRAR RECURSOS HUMANOS DE TI	
Nivel de Madurez Actual TRES	**Nivel de Madurez Futuro** CUATRO
Propuestas: • Realizar una reevaluación del número de personas del departamento de Sistemas, y en base a sus resultados replantear su estructura organizacional así como sus funciones. • Crear una política, procedimiento y programa de capacitación que establezca a un responsable para suplir las funciones del Jefe de Sistemas en caso de su ausencia, y de esta manera evitar la dependencia funcional de este Departamento sobre una persona. • Plantear evaluaciones de desempeño acorde con estándares y mejores prácticas de la industria.	

Tabla 3.31 Plan de Mejora del PO7[74]

PO9. EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI	
Nivel de Madurez Actual UNO	**Nivel de Madurez Futuro** DOS
Propuestas: • Establecer un proceso de análisis, evaluación y gestión de riesgos tecnológicos basado en una metodología y estándares, a nivel organizacional que sea de conocimiento para todo el personal. • Asignar un responsable para la gestión de riesgos que cuente con la capacitación y experiencia adecuada. • Crear un plan de mitigación para los riesgos tecnológicos identificados que sea aplicado oportunamente.	

Tabla 3.32 Plan de Mejora del PO9[74]

[74] Realizado por las autoras

3.2.2. PROPUESTAS DE MEJORA DEL DOMINIO AI

AI1. IDENTIFICAR SOLUCIONES AUTOMATIZADAS	
Nivel de Madurez Actual DOS	**Nivel de Madurez Futuro** TRES
Propuestas: • Establecer un enfoque estructurado para identificar las soluciones de TI necesarias para el negocio de acuerdo a la experiencia y conocimiento del responsable de la función de TI, junto con una documentación que lo respalde. • Establecer un proceso documentado para determinar las soluciones de TI necesarias para satisfacer las necesidades del negocio. • Establecer un control de calidad de la documentación generada para la solución tecnológica antes y después de su implementación.	

Tabla 3.33 Plan de Mejora del AI1[75]

AI2. ADQUIRIR Y MANTENER SOFTWARE APLICATIVO	
Nivel de Madurez Actual DOS	**Nivel de Madurez Futuro** TRES
Propuestas: • Establecer un proceso definido para adquirir y mantener software aplicativo junto con una metodología estándar para que garantice su cumplimiento. • Adquirir todas las licencias del software aplicativo que esté en uso dentro de la Organización. • Poner especial atención en aspectos tecnológicos como disponibilidad y seguridad para la adquisición de software aplicativo.	

Tabla 3.34 Plan de Mejora del AI2[75]

[75] Realizado por las autoras

AI3. ADQUIRIR Y MANTENER INFRAESTRUCTURA TECNOLÓGICA	
Nivel de Madurez Actual DOS	**Nivel de Madurez Futuro** TRES
Propuestas: • Establecer un proceso definido y específico para adquirir y mantener infraestructura tecnológica. • Implementar un programa de mantenimiento de la infraestructura tecnológica que sea documentado.	

Tabla 3.35 Plan de Mejora del AI3[76]

AI4. FACILITAR LA OPERACIÓN Y EL USO	
Nivel de Madurez Actual DOS	**Nivel de Madurez Futuro** TRES
Propuestas: • Establecer un enfoque uniforme y definido para procedimientos de generación y actualización de la documentación de usuarios y de operación. • Involucrar a los usuarios en la mayor parte del proceso de generación de documentos para los usuarios y de operación, para mejorar la calidad de los mismos por medio de la retroalimentación. • Respaldar la documentación para usuarios y de operación en caso de desastres. • Emplear herramientas automatizadas para la generación y distribución de los procedimientos involucrados con la operación y el uso.	

Tabla 3.36 Plan de Mejora del AI4[76]

[76] Realizado por las autoras

AI5. ADQUIRIR RECURSOS DE TI	
Nivel de Madurez Actual DOS	**Nivel de Madurez Futuro** TRES
Propuestas: • Establecer un proceso definido junto con políticas y procedimientos para la adquisición de recursos de TI que estén alineados con el manual de adquisiciones y para proyectos de cualquier escala tecnológica. • Asignar roles y responsabilidades en el proceso de administración de adquisición y contrato de recursos de TI. • Implementar estándares en el proceso de adquisición de recursos de TI. • Establecer un proceso de administración de contratos que involucre a los proveedores de recursos de TI.	

Tabla 3.37 Plan de Mejora del AI5[77]

3.2.3. PROPUESTAS DE MEJORA DEL DOMINIO DS

DS1. DEFINIR Y ADMISTRAR LOS NIVELES DE SERVICIO	
Nivel de Madurez Actual UNO	**Nivel de Madurez Futuro** DOS
Propuestas: • Definir un proceso y utilización de estándares de la industria para el desarrollo de los acuerdos de niveles de servicio. • Establecer métricas cuantitativas para medir el desempeño de los niveles de servicio. • Generar reportes de los niveles de servicios que sean útiles para la Gerencia que le permita conocer el desempeño y su cumplimiento. • Asignar la responsabilidad de definir los niveles de servicio a un coordinador.	

Tabla 3.38 Plan de Mejora del DS1[77]

[77] Realizado por las autoras

DS2. ADMINISTAR LOS SERVICIOS DE TERCEROS	
Nivel de Madurez Actual DOS	**Nivel de Madurez Futuro** TRES
Propuestas: • Establecer un proceso definido de la supervisión de proveedores de servicios de terceros, atendiendo a los riesgos asociados. • Establecer las condiciones estándar para los convenios de la prestación de los servicios de terceros. • Definir un formato de reporte estándar que apoye a los objetivos del negocio.	

Tabla 3.39 Plan de Mejora del DS2[78]

DS3. ADMINISTRAR EL DESEMPEÑO Y LA CAPACIDAD	
Nivel de Madurez Actual UNO	**Nivel de Madurez Futuro** DOS
Propuestas: • Definir un proceso de planificación de la capacidad y desempeño de infraestructura, recursos y capacidades de TI. • Concienciar a los responsables del negocio sobre los beneficios acerca de la planificación de la capacidad de TI. • Establecer procedimientos periódicos para evaluar la capacidad y desempeños actual y futuro de los recursos de TI.	

Tabla 3.40 Plan de Mejora del DS3[78]

[78] Realizado por las autoras

DS4. GARANTIZAR LA CONTINUIDAD DEL SERVICIO	
Nivel de Madurez Actual UNO	**Nivel de Madurez Futuro** DOS
Propuestas: • Capacitar a los usuarios para que puedan solucionar problemas mínimos sobre los recursos de TI. • Establecer un plan de continuidad de los servicios de TI que contemplen todas las amenazas y abarque aspectos tecnológicos y del negocio. • Emitir reportes sobre la disponibilidad de los servicios, cuando sea requerido. • Clasificar los sistemas y componentes críticos dentro del inventario.	

Tabla 3.41 Plan de Mejora del DS4[79]

DS5. GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS	
Nivel de Madurez Actual DOS	**Nivel de Madurez Futuro** TRES
Propuestas: • Establecer un responsable que garantice la seguridad de los recursos de TI implementando un plan de seguridad en base a un análisis de riegos. • Documentar todos los procedimientos de seguridad de TI definidos por el departamento de Sistemas ateniéndose a las recomendaciones de los organismos de control y auditoria interna. • Desarrollar e implementar un programa de concienciación sobre la seguridad informática a todo el personal de la Organización. • Capacitar al personal de la Organización para que den cumplimiento a las políticas de seguridad establecidas. • Emitir reportes sobre incidentes y problemas relacionados con la seguridad de TI, para que Gerencia pueda autorizar las soluciones oportunas que sean planteadas por el Departamento de Sistemas y aplicar las respectivas sanciones.	

Tabla 3.42 Plan de Mejora del DS5[79]

[79] Realizado por las autoras

DS7. EDUCAR Y ENTRENAR A LOS USUARIOS	
Nivel de Madurez Actual DOS	**Nivel de Madurez Futuro** TRES
Propuestas: • Documentar todos los procedimientos de capacitación sobre los sistemas que hasta el momento son informales, y estandarizar los existentes. • Asignar un presupuesto, recursos, instalaciones e instructores que apoyen al proceso de capacitación y educación del personal sobre TI. • Definir un proceso de evaluación sobre los conocimientos y capacidades adquiridas de los usuarios para exista retroalimentación.	

Tabla 3.43 Plan de Mejora del DS7[80]

DS10. ADMINISTRAR LOS PROBLEMAS	
Nivel de Madurez Actual DOS	**Nivel de Madurez Futuro** TRES
Propuestas: • Establecer un proceso específico para la gestión de problemas que cuente con el apoyo de la Gerencia. • Estandarizar el procedimiento actual de resolución de problemas. • Registrar los problemas e incidentes identificados y sus soluciones para que en el futuro sean útiles para dar una respuesta ágil. • Realizar revisiones sobre el análisis de identificación y resolución de problemas para mejorar el proceso de gestión de problemas.	

Tabla 3.44 Plan de Mejora del DS10[80]

[80] Realizado por las Autoras.

DS11. ADMINISTRAR LOS DATOS	
Nivel de Madurez Actual TRES	**Nivel de Madurez Futuro** CUATRO
Propuestas: • Establecer un proceso para la Gestión de Datos con métricas que permitan medir su desempeño y utilidad en el negocio junto con procedimientos formales que lo apoyen y sean comunicados a todo el personal. • Asignar un responsable que controle la integridad y seguridad de la información de la Organización. • Establecer una capacitación para los miembros del personal sobre la Gestión de Datos y su importancia dentro de la Organización.	

Tabla 3.45 Plan de Mejora del DS11[81]

DS12. ADMINISTRAR EL AMBIENTE FÍSICO	
Nivel de Madurez Actual DOS	**Nivel de Madurez Futuro** TRES
Propuestas: • Mantener el ambiente del departamento de Sistemas despejado, de manera que el personal se pueda movilizar sin restricciones. • Utilizar estándares para garantizar la seguridad física del departamento de Sistemas. • Realizar un análisis de riesgos formal sobre el ambiente físico de manera que permita optimizar los costos de seguro mitigando los riesgos.	

Tabla 3.46 Plan de Mejora del DS12[81]

[81] Realizado por las Autoras.

DS13. ADMINISTRAR LAS OPERACIONES	
Nivel de Madurez Actual DOS	**Nivel de Madurez Futuro** TRES
Propuestas: • Documentar las instrucciones de qué hacer, cómo y en qué orden se deben realizar para mantener la continuidad de las operaciones. • Introducir el uso de herramientas para limitar la intervención del operador. • Desarrollar una política formal para reducir el número de eventos no programados.	

Tabla 3.47 Plan de Mejora del DS13[82]

3.2.4. PROPUESTAS DE MEJORA DEL DOMINIO ME

ME1. MONITOREAR Y EVALUAR EL DESEMPEÑO DE TI	
Nivel de Madurez Actual UNO	**Nivel de Madurez Futuro** DOS
Propuestas: • Establecer un proceso definido de monitoreo y evaluación del desempeño de TI, junto con reportes que informen acerca de la eficiencia del departamento y que apoyen a las decisiones gerenciales. • Asignar un responsable que cumpla con el rol de monitoreo y evaluación del desempeño de TI. • Involucrar al departamento de Contabilidad para el desarrollo y monitoreo de mediciones financieras básicas para TI.	

Tabla 3.48 Plan de Mejora del ME1[82]

[82] Realizado por las Autoras

ME2. MONITOREAR Y EVALUAR EL CONTROL INTERNO	
Nivel de Madurez Actual UNO	**Nivel de Madurez Futuro** DOS
Propuestas: • Establecer un proceso definido de control interno de TI, junto con puntos de control e indicadores de su efectividad y eficacia. • Asignar un responsable que garantice el cumplimiento del monitoreo y evaluación de la efectividad de los controles internos de TI. • Elaborar un listado de los controles internos críticos para que la Gerencia determine un monitoreo periódico de su efectividad.	

Tabla 3.49 Plan de Mejora del ME2[83]

ME3. GARANTIZAR EL CUMPLIMIENTO CON REQUERIMIENTOS EXTERNOS	
Nivel de Madurez Actual DOS	**Nivel de Madurez Futuro** TRES
Propuestas: • Realizar un monitoreo interno constante y permanente acerca de las nuevas regulaciones de requerimientos financieros y legislación de privacidad, con el fin de asegurar su cumplimiento. • Crear un programa de conciencia y entrenamiento sobre requisitos legales y regulatorios externos que afectan a la Organización. • Implementar políticas y procedimientos para garantizar el cumplimiento de los reglamentos y de las obligaciones contractuales y legales. • Desarrollar contratos pro-forma y procesos legales estándar para minimizar los riesgos asociados con las obligaciones contractuales.	

Tabla 3.50 Plan de Mejora del ME3[83]

[83] Realizado por las autoras

3.3.INFORME EJECUTIVO

Por medio del presente informe se agradece a la Cooperativa de Ahorro y Crédito “TEXTIL 14 DE MARZO”, por toda la colaboración prestada para realizar la evaluación de la Gestión Informática de la Unidad de TI de la Cooperativa de Ahorro y Crédito “TEXTIL14 DE MARZO” usando COBIT 4.1.

El actual trabajo comenzó con la planificación de la evaluación para lo cual se definió el grupo evaluador conformado por el Gerente General, Jefe de Sistemas, Jefe de Operaciones, Jefe de Contabilidad y las evaluadoras. Con su ayuda se procedió a la recolección de la información de la Gestión informática del Departamento de Sistemas de la Organización. Con la información obtenida se realizaron análisis de la situación actual de la empresa y se determinaron los posibles problemas que afectan su desempeño. En base al marco de referencia COBIT 4.1 se seleccionaron los dominios y procesos más adecuados para la evaluación. Se analizaron los resultados obtenidos de la evaluación de los procesos que permitieron plantear recomendaciones y una propuesta de mejora para la Gestión Informática de Departamento de Sistemas.

Cabe mencionar que debido a circunstancias y la disponibilidad de tiempo de las personas requeridas para la recolección de información, fue necesario utilizar otras alternativas sugeridas por la Organización para poder proseguir con el avance del trabajo.

Al finalizar el trabajo, se obtuvieron las siguientes conclusiones y recomendaciones:

CONCLUSIONES

- Los procesos analizados fueron seleccionados en base a las necesidades actuales de la Organización y a la importancia que tienen para el cumplimiento de los objetivos del negocio.

- El resultado de la evaluación de la gestión de TICs de la Organización, será de utilidad para que la Alta Gerencia pueda conocer el estado actual de gestión llevada a cabo por del Departamento de Sistemas, y tomar acciones en base a las recomendaciones emitidas en las propuestas de mejora.

- La gestión de TICs del departamento de Sistemas mejorará mediante la utilización de estándares y metodologías, además de la utilización de este documento.

- La Organización tiene parcialmente establecido un modelo de arquitectura de información debido a que no conoce las ventajas de su utilización.

- La Organización incluye una perspectiva tecnológica dentro del plan operativo del departamento de Sistemas a corto plazo sin contemplar todos los aspectos de la infraestructura tecnológica para ese periodo.

- La falta de personal del departamento de Sistemas genera sobrecarga de trabajo entre el personal de Sistemas, lo que hace se cumplan tareas de acuerdo a la disponibilidad de tiempo del personal aunque no estén asignadas a su cargo esas actividades dentro del manual de funciones.

- Se tiene dependencia de la experiencia y conocimiento del personal de Sistemas para la realización de ciertas actividades que no constan en el Manual de Funciones y que son relevantes para dar soporte a la toma de decisiones de la Alta Gerencia.

- Las disposiciones de Gerencia relacionadas con aspectos tecnológicos son trasmitidas a todo el personal de la Organización mediante comunicados físicos y electrónicos, pero no siempre se confirma el entendimiento de dichas disposiciones.

- El análisis de riesgos que se realiza en la Organización en su mayoría se centra en aspectos financieros más no en los tecnológicos, por lo que no existe garantía de la mitigación de los riesgos ni de su impacto en el negocio.

- Para la identificación de soluciones automatizadas y la adquisición de software y hardware se mantiene un proceso organizado en base al manual de adquisiciones general de la Organización, de manera que se puede obtener un análisis de riegos, costos y factibilidad tecnológica que sea útil a la Gerencia para la toma de decisiones.

- No se tiene un proceso documentado del mantenimiento preventivo y correctivo para las aplicaciones e infraestructura tecnológica, sin embargo si se tiene un plan de mantenimiento de estos recursos para su cumplimiento.

- A pesar de que el departamento de Sistemas no cuenta con procesos documentados, existe una administración inicial de las actividades necesarias para dar cumplimiento a los objetivos del negocio con la mayoría de las exigencias actuales y futuras.

- Se tiene documentación como manuales de operación, manuales de usuario y material de entrenamiento para los usuarios, pero estos no se actualizan periódicamente, lo que conlleva a la dependencia de una persona para su explicación.

- A pesar de que Gerencia General reconoce la importancia de Gestión de TICs, no se ha tomado medidas para garantizar una adecuada gestión de los recursos tecnológicos, lo que supone una cierta deficiencia en algunos aspectos del departamento de Sistemas.

- El departamento de Sistemas no aplica la definición de niveles de servicio cuando se adquieren soluciones tecnológicas, en su lugar se tiene un

contrato escrito en el cual se establecen términos legales para asegurar su cumplimiento de acuerdo a las clausulas estipuladas.

- Existe una relación con los proveedores de los servicios de TI para garantizar su funcionamiento, sin embargo no sigue un proceso definido.

- El departamento de Sistemas es consciente de la necesidad de un alto rendimiento que requieren los servicios de TI para cumplir los objetivos del negocio sin embargo no existe una planificación de la capacidad.

- La organización actualmente está contemplando aspectos relevantes para dar continuidad a los servicios de TI que cumplan los objetivos del negocio y satisfagan a sus clientes, pero no son tomados como prioridad para su realización ni especificados dentro de un plan de continuidad del negocio.

- A pesar de que no está documentado un plan de seguridad de la información y sistemas, existen políticas desarrolladas por parte del departamento de Sistemas que sirven como guía para mitigar y minimizar aspectos que puedan atentar contra la seguridad de la información.

- No se tiene proceso documentado para la gestión de problemas, pero esta tarea se realiza bajo un procedimiento establecido interno al departamento de Sistemas.

- Actualmente las condiciones físicas del departamento de Sistemas cumplen con los requerimientos mínimos para garantizar su correcto desempeño.

- Para la recolección de la información fue necesario involucrar a varias áreas de la Organización, ya que para el cumplimiento de los objetivos generales del negocio todas las áreas deben estar apoyadas por los procesos del Departamento de Sistemas.

- Debido a la falta de documentación acerca de la gestión de TICs, la mayor parte de la recolección de la información fue utilizando fuentes directas de información como entrevistas y observación de las actividades del departamento de Sistemas.

- El departamento de Sistemas reporta su desempeño mediante la presentación de informes de actividades a Alta Gerencia cuando periódicamente, permitiendo a las autoridades evaluar su cumplimiento y tomar las medidas oportunas.

- Actualmente la Alta Gerencia está tomando medidas para cumplir con los requerimientos de los Organismos de Control Externos con la colaboración de auditoria interna y asesoría legal, lo que garantiza evitar sanciones al respecto y contar con la confianza de los socios.

RECOMENDACIONES

- Realizar el levantamiento de procesos del departamento de Sistemas para establecer una gestión de TICs en base a estándares y buenas prácticas de la industria que garanticen la seguridad e integridad de los servicios de TI.

- Identificar los recursos de TI críticos para el negocio con el fin de administrarlos adecuadamente para que puedan satisfacer óptimamente a los requerimientos del negocio actuales y futuros.

- Contratar personal para el departamento de Sistemas para reducir la carga de trabajo actual del equipo. Permitiendo dar el cumplimento a las funciones correspondientes a cada cargo.

- Evaluar e incluir todas las actividades y responsabilidades del departamento de Sistemas que hasta el momento no se encuentran definidas en el manual de funciones de la Organización.

- Revisar detalladamente el análisis realizado en el presente trabajo, para la futura implementación de las propuestas de mejora del departamento de Sistemas con el fin de mejorar la gestión de TICs.

- Utilizar estándares para cubrir las diferentes áreas, por ejemplo ISO 27001 para seguridad de sistemas informáticos, ITIL v3 para la gestión de servicios de información, entre otros.

- Comunicar a todo el personal de la Organización acerca de la importancia de definir procesos en la Gestión de TICs y promover su aceptación mediante programas de concienciación.

- Concienciar al personal del departamento de Sistemas sobre la importancia de llevar un proceso de documentación de todas las tareas y actividades relacionadas con las funciones de TI y del negocio, con el fin de facilitar la prestación de los servicios a los usuarios y a su vez disminuir el tiempo de entrenamiento del nuevo personal y la dependencia del personal actual para este fin.

- Reestructurar el orgánico funcional de la Organización de manera que refleje que el departamento de Sistemas apoya a la Alta Gerencia a la toma de decisiones con respecto al negocio.

- Instaurar el concepto de Gobierno de TI para garantizar que existe alineación de los objetivos de TI con los del negocio, de manera que todos los recursos se utilicen de la manera más eficiente y den cumplimiento a requisitos regulatorios, operativos y del negocio.

- Desarrollar un análisis del impacto de las tecnologías actuales sobre el negocio para la definición de un plan de contingencias y recuperación de desastres (DRP) que garanticen la continuidad del negocio.

- Conocer los beneficios que tiene la implementación de un modelo de arquitectura de información, para que pueda ser aplicado con el fin de mejorar la administración de la información.

- Implementar un proceso actualización y de control de versiones de la documentación que sirve como material de entrenamiento y manuales de usuarios.

- Conocer los beneficios de definir niveles de servicios para facilitar la relación entre cliente y proveedor, tanto en los servicios que proporcionan a sus clientes como en los servicios de TI con proveedores de terceros.

4. CAPÍTULO 4: CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES

- Los procesos analizados fueron seleccionados en base a las necesidades actuales de la Organización y a la importancia que tienen para el cumplimiento de los objetivos del negocio.

- El resultado de la evaluación de la gestión de TICs de la Organización, será de utilidad para que la Alta Gerencia pueda conocer el estado actual de gestión llevada a cabo por del Departamento de Sistemas, y tomar acciones en base a las recomendaciones emitidas en las propuestas de mejora.

- La gestión de TICs del departamento de Sistemas mejorará mediante la utilización de estándares y metodologías, además de la utilización de este documento.

- A través del uso del marco de trabajo COBIT 4.1, se ha logrado identificar cual es el nivel de madurez de los procesos seleccionados en del Departamento de Sistemas y cuáles son las aspectos que deberían tomarse en cuenta para mejorar su nivel actual.

- Las directrices de auditoría de COBIT 4.1, son una guía para la planificación de la evaluación que ofrecen alternativas para determinar las posibles actividades que se realizarán dentro la evaluación de TI, mas no son una herramienta obligatoria que ofrece COBIT 4.1 para la realización de la evaluación de los procesos.

- La planificación y ejecución de la Auditoría y Evaluación depende del criterio del auditor, el que se puede basar en distintas herramientas o guías que el marco de trabajo COBIT ofrece.

- Existe un proceso de planificación estratégica que incluye el aspecto tecnológico lo que permite definir los objetivos de TI para apoyar al cumplimiento de los objetivos del negocio.

- La Organización tiene parcialmente establecido un modelo de arquitectura de información debido a que no conoce las ventajas de su utilización.

- La Organización incluye una perspectiva tecnológica dentro del plan operativo del departamento de Sistemas a corto plazo sin contemplar todos los aspectos de la infraestructura tecnológica para ese periodo.

- La falta de personal del departamento de Sistemas genera sobrecarga de trabajo entre el personal de Sistemas, lo que hace se cumplan tareas de acuerdo a la disponibilidad de tiempo del personal aunque no estén asignadas a su cargo esas actividades dentro del manual de funciones.

- Se tiene dependencia de la experiencia y conocimiento del personal de Sistemas para la realización de ciertas actividades que no constan en el Manual de Funciones y que son relevantes para dar soporte a la toma de decisiones de la Alta Gerencia.

- Las disposiciones de Gerencia relacionadas con aspectos tecnológicos son trasmitidas a todo el personal de la Organización mediante comunicados físicos y electrónicos, pero no siempre se confirma el entendimiento de dichas disposiciones.

- El análisis de riesgos que se realiza en la Organización en su mayoría se centra en aspectos financieros más no en los tecnológicos, por lo que no

existe garantía de la mitigación de los riesgos ni de su impacto en el negocio.

- Para la identificación de soluciones automatizadas y la adquisición de software y hardware se mantiene un proceso organizado en base al manual de adquisiciones general de la Organización, de manera que se puede obtener un análisis de riegos, costos y factibilidad tecnológica que sea útil a la Gerencia para la toma de decisiones.

- No se tiene un proceso documentado del mantenimiento preventivo y correctivo para las aplicaciones e infraestructura tecnológica, sin embargo si se tiene un plan de mantenimiento de estos recursos para su cumplimiento.

- A pesar de que el departamento de Sistemas no cuenta con procesos documentados, existe una administración inicial de las actividades necesarias para dar cumplimiento a los objetivos del negocio con la mayoría de las exigencias actuales y futuras.

- Se tiene documentación como manuales de operación, manuales de usuario y material de entrenamiento para los usuarios, pero estos no se actualizan periódicamente, lo que conlleva a la dependencia de una persona para su explicación.

- A pesar de que Gerencia General reconoce la importancia de Gestión de TICs, no se ha tomado medidas para garantizar una adecuada gestión de los recursos tecnológicos, lo que supone una cierta deficiencia en algunos aspectos del departamento de Sistemas.

- El departamento de Sistemas no aplica la definición de niveles de servicio cuando se adquieren soluciones tecnológicas, en su lugar se tiene un contrato escrito en el cual se establecen términos legales para asegurar su cumplimiento de acuerdo a las clausulas estipuladas.

- Existe una relación con los proveedores de los servicios de TI para garantizar su funcionamiento, sin embargo no sigue un proceso definido.

- El departamento de Sistemas es consciente de la necesidad de un alto rendimiento que requieren los servicios de TI para cumplir los objetivos del negocio sin embargo no existe una planificación de la capacidad.

- La organización actualmente está contemplando aspectos relevantes para dar continuidad a los servicios de TI que cumplan los objetivos del negocio y satisfagan a sus clientes, pero no son tomados como prioridad para su realización ni especificados dentro de un plan de continuidad del negocio.

- A pesar de que no está documentado un plan de seguridad de la información y sistemas, existen políticas desarrolladas por parte del departamento de Sistemas que sirven como guía para mitigar y minimizar aspectos que puedan atentar contra la seguridad de la información.

- No se tiene proceso documentado para la gestión de problemas, pero esta tarea se realiza bajo un procedimiento establecido interno al departamento de Sistemas.

- Actualmente las condiciones físicas del departamento de Sistemas cumplen con los requerimientos mínimos para garantizar su correcto desempeño.

- Para la recolección de la información fue necesario involucrar a varias áreas de la Organización, ya que para el cumplimiento de los objetivos generales del negocio todas las áreas deben estar apoyadas por los procesos del Departamento de Sistemas.

- Debido a la falta de documentación acerca de la gestión de TICs, la mayor parte de la recolección de la información fue utilizando fuentes directas de

información como entrevistas y observación de las actividades del departamento de Sistemas.

- El departamento de Sistemas reporta su desempeño mediante la presentación de informes de actividades a Alta Gerencia cuando periódicamente, permitiendo a las autoridades evaluar su cumplimiento y tomar las medidas oportunas.

- Actualmente la Alta Gerencia está tomando medidas para cumplir con los requerimientos de los Organismos de Control Externos con la colaboración de auditoria interna y asesoría legal, lo que garantiza evitar sanciones al respecto y contar con la confianza de los socios.

4.2.RECOMENDACIONES

- Realizar el levantamiento de procesos del departamento de Sistemas para establecer una gestión de TICs en base a estándares y buenas prácticas de la industria que garanticen la seguridad e integridad de los servicios de TI.

- Identificar los recursos de TI críticos para el negocio con el fin de administrarlos adecuadamente para que puedan satisfacer óptimamente a los requerimientos del negocio actuales y futuros.

- Contratar personal para el departamento de Sistemas para reducir la carga de trabajo actual del equipo. Permitiendo dar el cumplimento a las funciones correspondientes a cada cargo.

- Evaluar e incluir todas las actividades y responsabilidades del departamento de Sistemas que hasta el momento no se encuentran definidas en el manual de funciones de la Organización.

- Revisar detalladamente el análisis realizado en el presente trabajo, para la futura implementación de las propuestas de mejora del departamento de Sistemas con el fin de mejorar la gestión de TICs.

- Utilizar estándares para cubrir las diferentes áreas, por ejemplo ISO 27001 para seguridad de sistemas informáticos, ITIL v3 para la gestión de servicios de información, entre otros.

- Comunicar a todo el personal de la Organización acerca de la importancia de definir procesos en la Gestión de TICs y promover su aceptación mediante programas de concienciación.

- Concienciar al personal del departamento de Sistemas sobre la importancia de llevar un proceso de documentación de todas las tareas y actividades relacionadas con las funciones de TI y del negocio, con el fin de facilitar la prestación de los servicios a los usuarios y a su vez disminuir el tiempo de entrenamiento del nuevo personal y la dependencia del personal actual para este fin.

- Reestructurar el orgánico funcional de la Organización de manera que refleje que el departamento de Sistemas apoya a la Alta Gerencia a la toma de decisiones con respecto al negocio.

- Instaurar el concepto de Gobierno de TI para garantizar que existe alineación de los objetivos de TI con los del negocio, de manera que todos los recursos se utilicen de la manera más eficiente y den cumplimiento a requisitos regulatorios, operativos y del negocio.

- Desarrollar un análisis del impacto de las tecnologías actuales sobre el negocio para la definición de un plan de contingencias y recuperación de desastres (DRP) que garanticen la continuidad del negocio.

- Conocer los beneficios que tiene la implementación de un modelo de arquitectura de información, para que pueda ser aplicado con el fin de mejorar la administración de la información.

- Implementar un proceso actualización y de control de versiones de la documentación que sirve como material de entrenamiento y manuales de usuarios.

- Conocer los beneficios de definir niveles de servicios para facilitar la relación entre cliente y proveedor, tanto en los servicios que proporcionan a sus clientes como en los servicios de TI con proveedores de terceros.

BIBLIOGRAFÍA

[1] COAC Textil 14 de Marzo. (2013) Cooperativa de Ahorro y Crédito "TEXTIL 14 DE MARZO". [Online]. http://www.14demarzo.fin.ec/cooperativa_de_ahorro_y_credito/

[2] Asamblea General Extraordinaria de Representantes de la Coac TEXTIL 14 DE MARZO LTDA., Estatuto de la Cooperativa de Ahorro y Crédito TEXTIL 14 DE MARZO LTDA., 2013.

[3] Cooperativa de Ahorro y Crédito "TEXTIL 14 de Marzo", "Manual de Funciones Actualizado de la Coac. "TEXTIL 14 de Marzo"," Coac. "TEXTIL 14 de Marzo", Quito, Manual de Funciones.

[4] IT Governance Institute, *COBIT 4.1*. Estados Unidos: IT Governance Institute, 2007.

[5] Cooperativa de Ahorro y Crédito 14 de Marzo, "Plan Operativo 2012-2014," Cooperativa de Ahorro y Crédito 14 de Marzo, Quito, Plan Operativo 2012.

[6] Diana Pamela Sango Pillajo, Diseño y estandarización de los procesos operativos de la Cooperativa de Ahorro y Crédito "Santa Ana de Nayón", 2010.

[7] Comité Directivo de COBIT y el IT Governance Institue, *COBIT Directrices de Auditoría*, Tercera ed., 2000.

[8] IT Governance Institute, *COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance*, Segunda ed., 2007.

[9] Jaime Naranjo, Metodología para la evaluación del desempeño de una unidad informática. Proyecto de titulación de Maestría en Computación e Informática, 2000.

[10] Pablo Del Hierro and Pablo Trujillo, Auditoría del sistema informático del hospital del sur "Enrique Garcés", 2012.

[11] Carla Corrales and Diana Vallejo, Evaluación del nivel de madurez de la Gestión de las TICs en la empresa “ASTAP”, 2008.

[12] Pablo Cilio and Javier Muñoz, Evaluación y propuesta de mejora de los procesos de TI pertenecientes al dominio de entrega y soporte del modelo COBIT 4.1 en el departamento de tecnologías de la información de una empresa comercial, 2012.

[13] Mayra Carrión and Luz Coronado, Auditoría de la Gestión de las TIC’s para la empresa DIPAC utilizando COBIT, 2008.

[14] David Callay and Luis Sánchez, Auditoria Informática a los servicios de red de TransElectric, 2012.

[15] SEPS. (2013) Superintendencia de Economía Popular y Solidaria. [Online]. http://www.seps.gob.ec/web/guest/resoluciones_sector_financiero

[16] ITIL. (2013) ITILv3. [Online]. http://itilv3.osiatis.es/gestion_servicios_ti.php

[17] ISACA. (2013) ISACA. [Online]. http://www.isaca.org/cobit/pages/default.aspx

GLOSARIO DE TÉRMINOS

Arquitectura de Información: se encarga del análisis, organización, disposición y estructuración de la información, así como su selección y presentación de los datos en los sistemas de información interactivos.

CMM (Capability Maturity Model): Modelo de Capacidad y madurez para determinar el grado de formalidad y optimización de los procesos claves agrupados en KPA (Key Process Área) mediante la utilización de buenas prácticas como definir procedimientos documentados, que sean ejecutados de modo sistemático, universal y uniforme.

COAC: Cooperativa de Ahorro y Crédito.

COBIT: Objetivos de control para las tecnologías de la información relacionadas, marco de trabajo para la administración y establecimiento de un gobierno de TI.

Control Interno: Políticas, procedimientos, buenas prácticas que están diseñadas para garantizar que los objetivos del negocio se están cumpliendo y que las anomalías serán detectadas y corregidas.

COSO (Committee of Sponsoring Organizations of the Treadway Commission): Modelo de control de negocios que mediante la utilización de un estándar permite evaluar los procesos de control y determinar la mejora de los mismos dentro de la Organización.

Directrices de Auditoría: son guías que permiten determinar las actividades relacionadas con la evaluación de TI.

DRP: Plan de recuperación de desastres. Es un proceso de recuperación de información, hardware y software considerado crítico para que una organización pueda reiniciar sus actividades y operaciones en caso de que ocurra algún desastre, ya sea de carácter natural o causado por humanos.

Financial Bussines System: Sistema Financiero de la Cooperativa “Textil 14 de Marzo”

Gobierno TI: el conjunto de acciones que realiza el área de TI en coordinación con la alta dirección para movilizar sus recursos de la forma más eficiente en respuesta a requisitos regulatorios, operativos o del negocio.

ISACA: es un líder mundialmente reconocido, proveedor de conocimiento, certificaciones, comunidad, apoyo y educación en seguridad y aseguramiento de sistemas de información (SI), gobierno empresarial, administración de TI así como riesgos y cumplimiento relacionados con TI.

ISO 27001: es un estándar que se centra en la seguridad de la información con el fin establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información.

ITIL: Information Technology Infraestructure Library. Es un conjunto de conceptos y buenas prácticas enfocadas en la gestión de servicios de tecnologías de la información, su desarrollo y las operaciones relacionadas con las mismas

Metodología: Conjunto de métodos que siguen varias reglas y varias técnicas adicionales utilizadas para alcanzar un conjunto de objetivos.

Niveles de Servicio: son niveles de calidad en los que deben operar los servicios que ofrece una determinada organización.

Plan Operativo: es un documento formal en el que la Alta Gerencia expone los objetivos y directrices que se cumplirán a corto plazo.

Proceso: conjunto de actividades que se llevan a cabo de manera consecutiva o simultánea para conseguir un determinado fin.

Proceso definido: es aquel en el que el proceso, los recursos, los roles y responsabilidades se encuentran documentados y formalizado.

Riesgos de TI: es la probabilidad de que una amenaza de naturaleza informática se convierta en un desastre causando pérdidas de cualquier índole a la organización.

SEPS: Superintentendencia de Economía Popular y Solidaria. Es una entidad técnica cuyas funciones supervisar y controlar las organizaciones que pertenecen

a la economía popular y solidaria, y que tiene como propósito el desarrollo, estabilidad, solidez y correcto funcionamiento del sector económico popular y solidario.

SLA(Service Level Agreement): Acuerdos de nivel de Servicio son contratos escritos entre el proveedor del servicio y el cliente para fijar el nivel acordado para la calidad del servicio.

SPI: Sistema de pagos interbancario.

TI: Tecnologías de Información.

TICs: Tecnologías de Información y Comunicación. Es el conjunto de recursos, procedimientos y técnicas que se usan para el procesamiento, almacenamiento y transmisión de información.

ANEXOS

ANEXO A – NIVEL DE MADUREZ DEL DOMINIO PO

Se encuentra en el CD en la ruta *Anexos\Nivel de Madurez Dominio PO.docx*

ANEXO B – NIVEL DE MADUREZ DEL DOMINIO AI

Se encuentra en el CD en la ruta *Anexos\Nivel de Madurez Dominio AI.docx*

ANEXO C – NIVEL DE MADUREZ DEL DOMINIO DS

Se encuentra en el CD en la ruta *Anexos\Nivel de Madurez Dominio DS.docx*

ANEXO D – NIVEL DE MADUREZ DEL DOMINIO ME

Se encuentra en el CD en la ruta *Anexos\Nivel de Madurez Dominio ME.docx*

ANEXO E - MANUAL DE FUNCIONES DEL DEPARTAMENTO DE SISTEMAS [3]

PERFIL DE CARGO DEL JEFE DE SISTEMAS

IDENTIFICACIÓN DEL CARGO
DENOMINACIÓN: JEFE DE SISTEMAS SUPERVISA A: HELP DESK, PROMAGRADOR REPORTA A: GERENCIA GENERAL NÚMERO DE PUESTOS: 1 NOMBRE DEL AREA O DIVICION: DEPARTAMENTO DE SISTEMAS

MISIÓN DEL CARGO	
Analizar, planificar, organizar, dirigir, controlar, implementar, evaluar el sistema Financiero de la Cooperativa, permitiendo la prestación oportuna de los servicios financieros que brinda la cooperativa a sus clientes.	
ACTIVIDADES BÁSICAS DEL CARGO	
ACTIVIDADES PRINCIPALES	**FRECUENCIA**
Participar en la formulación del Plan Estratégico de la Cooperativa.	d
Revisión de requerimientos.	d
Revisión del cajero automático con tarjeta de seguridad y el software.	d
Revisión de enlaces de comunicación externa, matriz y las diferentes Agencias.	d
Revisión del funcionamiento de los servidores.	d
Revisión del e-mail institucional.	d
Cierre de sistema financiero.	d
Generación de trasporte de Transacciones SPI.	d
Soporte Técnico a usuarios de equipos de computación y software.	d
Soporte administrativo a usuarios.	d
Retención de enlaces Cooperativa Banco del Austro.	d
Verificación de cajas cerradas y afectaciones antes del cierre.	d
Verificación que no exista inversiones pendientes antes del cierre.	d
Control y administración del Fider Wall.	d

Respaldo base de datos de la cooperativa antes y después del cierre.	d
Respaldo base de datos SPI.	d
Configuración de acceso de conexión del servidor de archivo para los usuarios.	d
Coordinación con HelpDesk y área de programación de los requerimientos levantados por los usuarios.	d
Proceso de reclamo de tarjetas de Débito y SPI al banco de Austro.	d
Seguimiento y coordinación, directamente con el personal del Banco de Austro el IESS escalando jerarquías, para dar una resolución satisfactoria a los reclamos de tarjetas de Débito y SPI.	d
Monitoreo de la red de comunicación entre todas las oficinas de la cooperativa.	d
Supervisión del buen funcionamiento del sistema informático de la cooperativa.	d
Administración de la base de datos del sistema financiero de la cooperativa.	d

CUALIFICACIÓN	FRECUENCIA	Diaria (d)

ACTIVIDADES PERIÓDICAS Y OCASIONALES	FRECUENCIA
Administración de las cuentas de correo electrónico.	o
Revisión de reportes de Virus GDAT.	s
Revisión y control de inventarios de toners.	m
Acreditación de intereses, debito, fondo de asistencia social, fondo mortuorio a los socios y retención del 25% sobre inversiones de clientes jurídicos.	t
Acreditación de intereses certificados de aportación a los socios.	a
Cierre anual contable en el sistema.	a
Inventarios de equipos de comunicación anual.	a
Coordinación con los proveedores externos de comunicación por caída de enlaces de comunicación.	o
Coordinación con los proveedores externos de Western Unión, SOAT, PRODUBANCO para la creación de contraseña y servicio a terceros.	o

Creación de usuarios para el sistema de tarjetas de Débito.	o
Creación de usuarios y contraseñas para el sistema financia.	o
Participación en la elaboración del plan estratégico de la cooperativa.	a
Configuración de parametrizaciones en el sistema Financia según autorización de Gerencia General.	o
Pruebas de desarrollo con el programador de los requerimientos utilizados por el usuario.	o
Coordinación y ejecución del paso a producción de los requerimientos solicitados y aprobados por el usuario.	o
Reuniones de trabajo interna con las áreas de HelpDesk y Programación.	s
Elaboración del plan operativo y presupuesto del Dpto. de Sistemas con las áreas de HelpDesk y programación.	a
Revisión del plan operativo de las áreas HelpDesk y Programación.	m
Revisión de informes y actividades trimestrales de las áreas HelpDesk y Programación.	t
Revisión y actualización de equipos de computación activos del Dpto. de Sistemas.	s
Revisión ya actualización del inventario de equipos para bajo contable de matriz y coordinación para baja contable con las Agencias.	s
Revisión y actualización de equipos de respaldo para la cooperativa.	t
Revisión y actualización de inventarios de equipos para donación.	s
Revisión y actualización de inventarios para destrucción.	s
Coordinación con la Gerencia General Contabilidad, Auditoria Interna, para el proceso de entrega como reciclaje de los equipos dados para destrucción.	s
Informe a la Gerencia General de los suministros de equipos de computación y comunicación para la aseguradora.	o
Elaboración y entrega de informes trimestrales al consejo de administración.	t
Emisión de actas de entrega de equipos de computación, Toners u otros	o

equipos.	
Emisión y entrega de diferentes reportes solicitados por la Gerencia General, Consejo de Vigilancia, Consejo de Administración.	o
Coordinación con la empresa Alta Tronic y Agencias Oficinas para el mantenimiento de la UPS.	o
Análisis y aprobación de los cuadros comparativos para adquisición de equipos de computación de acuerdo a lo aprobado por la Gerencia General.	o
Asesoramiento a Gerencia General el ala implementación de sistemas, métodos, procedimientos técnicos administrativos que permitan optimizar la gestión empresarial, asegurando la confidencialidad de la información.	o
Capacitación a usuarios de temas administrativos a nuevo personal.	o
Revisión y control de equipos de computación de acuerdo al mantenimiento realizado por HelpDesk.	o
Coordinación con el área de sistemas y Contabilidad los procesos necesarios parar la realización del proceso de cierre de sistema anual.	a
Coordinación el mantenimiento los sistemas de Hardware y Software.	s
Coordinación con Talento Humano la capacitación de Dpto. de Sistemas.	o

CUALIFICACIÓN	**FRECUENCIA**	Ocasional (o)	Semanal (s)	Mensual (m)	Trimestral (t)
		Semestral (c)	Anual (a)		

PERFIL DE CARGO DE HELP DESK

IDENTIFICACIÓN DEL CARGO
DENOMINACIÓN:HELP DESK SUPERVISA A: NINGUNO REPORTA A:JEFE DE SISTEMAS NÚMERO DE PUESTOS: 1 NOMBRE DEL ÁREA O DIVISIÓN: HELP DESK

MISIÓN DEL CARGO

Atender los requerimientos que se presentan en el día a día de todos los usuarios de la cooperativa.

ACTIVIDADES BÁSICAS DEL CARGO	
ACTIVIDADES PRINCIPALES	**FRECUENCIA**
Brindar el soporte técnico de sistemas y programas y mantenimiento preventivo de Hardware a las diferentes áreas operativas a fin de optimizar el proceso automático de datos y desarrollo de los reportes de gestión.	d
Monitoreo y actualizan de antivirus.	d
Monitoreo de las redes de comunicación de la Cooperativa LAN- WAN.	d
Monitoreo de servidores.	d
Cambio de TONERS.	d
Administrar y mantiene organizado los archivos de respaldo de información del sistema Finacial y mapas de redes LAN.	d

CUALIFICACIÓN	**FRECUENCIA**	Diaria (d)

ACTIVIDADES PERIÓDICAS Y OCASIONALES	**FRECUENCIA**
Cambio de equipos de computación.	a
Mantenimiento preventivo y correctivo.	c
Inventario de los equipos de computación.	c
Formateo de equipos.	m
Instalación de programas.	s

CUALIFICACIÓN	FRECUENCIA	Ocasional (o)	Semanal (s)	Mensual (m)	Trimestral (t)
		Semestral (c)	Anual (a)		

CONOCIMIENTOS	
INSTRUCCIÓN FORMAL	
NIVEL	**ESPECIALIDAD**
Tecnólogo	Título profesional acorde a la finalidad de la

	Cooperativa como: Tecnólogo en sistemas y telecomunicaciones o Lic. Informático.	
CONOCIMIENTOS ESPECÍFICOS	**ADIESTRAMIENTO**	**CAPACITACIÓN**
Telecomunicaciones		✓
Informática básica	✓	
Redes	✓	
Cableado estructurado	✓	✓
Electricidad y electrónica		✓

EXPERIENCIA		
EN CARGOS DE LA MISMA DENOMINACIÓN	6 meses	HELP DESK
EN CARGOS SIMILARES (EQUIVALENCIA)	1 año	Auxiliar de sistemas o telecomunicaciones

Perfil de cargo del Programador

IDENTIFICACIÓN DEL CARGO
DENOMINACIÓN:HELP DESK SUPERVISA A: NINGUNO REPORTA A:JEFE DE SISTEMAS NÚMERO DE PUESTOS: 1 NOMBRE DEL ÁREA O DIVISIÓN: HELP DESK

MISIÓN DEL CARGO
Colaborar en las actividades de desarrollo, implementación, evaluación y mejoramiento de los sistemas computacionales, genera respaldos de información del sistema además mediante su función apoya en la prestación oportuna de los servicios del sistema financiero.

ACTIVIDADES BÁSICAS DEL CARGO	
ACTIVIDADES PRINCIPALES	**FRECUENCIA**
Cierre de sistemas financieros para tener listos y actualizados para el próximo día.	d
Soporte a técnicos abarca, sistema, comunicaciones, aplicación de escritorio, equipos programas como; Hardware, Software.	d
Soporte a usuarios cuando hay erros de los Departamentos.	d
Soporte operativo en el manejo d sistema como: Hardware, Software.	d

Administra operativamente el Sistema Financial		d
CUALIFICACIÓN	FRECUENCIA	Diaria (d)

ACTIVIDADES PERIÓDICAS Y OCASIONALES	FRECUENCIA
Analiza, Diseña, desarrolla y evalúa las diferentes incidencias del sistema Financial	m
Coordina con Jefe de Sistemas, la planificación de módulos del sistema Financial	o
Evalúa las herramientas de desarrollo PUNTO NET y Base de Datos SQL. Server	s
Colabora en las actividades de desarrollo, implementación, evaluación y mejoramiento de sistemas computacionales	s
Genera respaldo de información de Base de datos.	o

CUALIFICACIÓN	**FRECUENCIA**	Ocasional (o)	Semanal (s)	Mensual (m)	Trimestral (t)
		Semestral (c)	Anual (a)		

CONOCIMIENTOS		
INSTRUCCIÓN FORMAL		
NIVEL	**ESPECIALIDAD**	
Tercer nivel	Título profesional acorde a la finalidad de la Cooperativa como: Ing. En Sistemas o afines.	
CONOCIMIENTOS ESPECÍFICOS	**ADIESTRAMIENTO**	**CAPACITACIÓN**
Conocimiento Visual Estudio 2003	✓	
Conocimiento SQL Server 2008		✓
Conocimiento ASP Para desarrollo Web		✓
Microsoft Windows Server 2003	✓	
Lite Speed		✓
EXPERIENCIA		
EN CARGOS DE LA MISMA DENOMINACIÓN	1 año	Programador
EN CARGOS SIMILARES (EQUIVALENCIA)	2 año	En actividades similares.

ANEXO F – LISTADO DE DOCUMENTACIÓN PROPORCIONADA POR LA ORGANIZACIÓN

Documentos
Estatuto de la Cooperativa de Ahorro y Crédito “TEXTIL 14 DE MARZO”
Plan Operativo 2012-2014
Planificación Estratégica 2012-2014
Reglamento para la Custodia y Manejo de la Información Institucional.
Reglamento Interno de Trabajo
Reglamento Interno de la Cooperativa
Políticas de Evaluación del Desempeño Laboral
Manual del Usuario Sistema –Financial Buiness System- Administración
Reglamento de Ética y Conducta
Manual de Servicios
Manual de Procedimientos de Personal
Manual de Control de Acceso a Áreas Restringidas
Manual de Funciones y Clasificación de Puestos
Reglamento General de la Ley Orgánica de la Economía Popular y Solidaria y del Sector Financiero Popular y Solidario.
Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP),
Normas generales para la aplicación de la ley general de instituciones del sistema financiero.
Normas generales para la aplicación de la ley general de instituciones del sistema financiero.
Resolución para uso de claves de medios electrónicos a cargo de la SEPS
Circular No. SEPS-IR-DNRFPS-2013-01682 / Niveles de cumplimiento de seguridades en cajeros automáticos y canales electrónicos.