COSSEC
CORPORACIÓN PARA LA SUPERVISIÓN Y SEGURO
DE COOPERATIVAS DE PUERTO RICO
GOBIERNO DE PUERTO RICO

28 de octubre de 2011

CARTA CIRCULAR 2011-15

A TODAS LAS COOPERATIVAS DE AHORRO Y CRÉDITO

Wilfredo Torres Pinto, CPA, CFE
Presidente Ejecutivo

METODOLOGÍA Y REQUISITOS BÁSICOS PARA LA ADQUISICIÓN E IMPLEMENTACIÓN DE SISTEMAS DE INFORMACIÓN

La Corporación para la Supervisión y Seguro de Cooperativas de Puerto Rico (COSSEC) es el organismo regulador de las cooperativas y asegurador del sector de ahorro y crédito. Como parte de los requisitos del seguro de acciones y depósitos las cooperativas de ahorro y crédito deben poseer sistemas de información mecanizados.

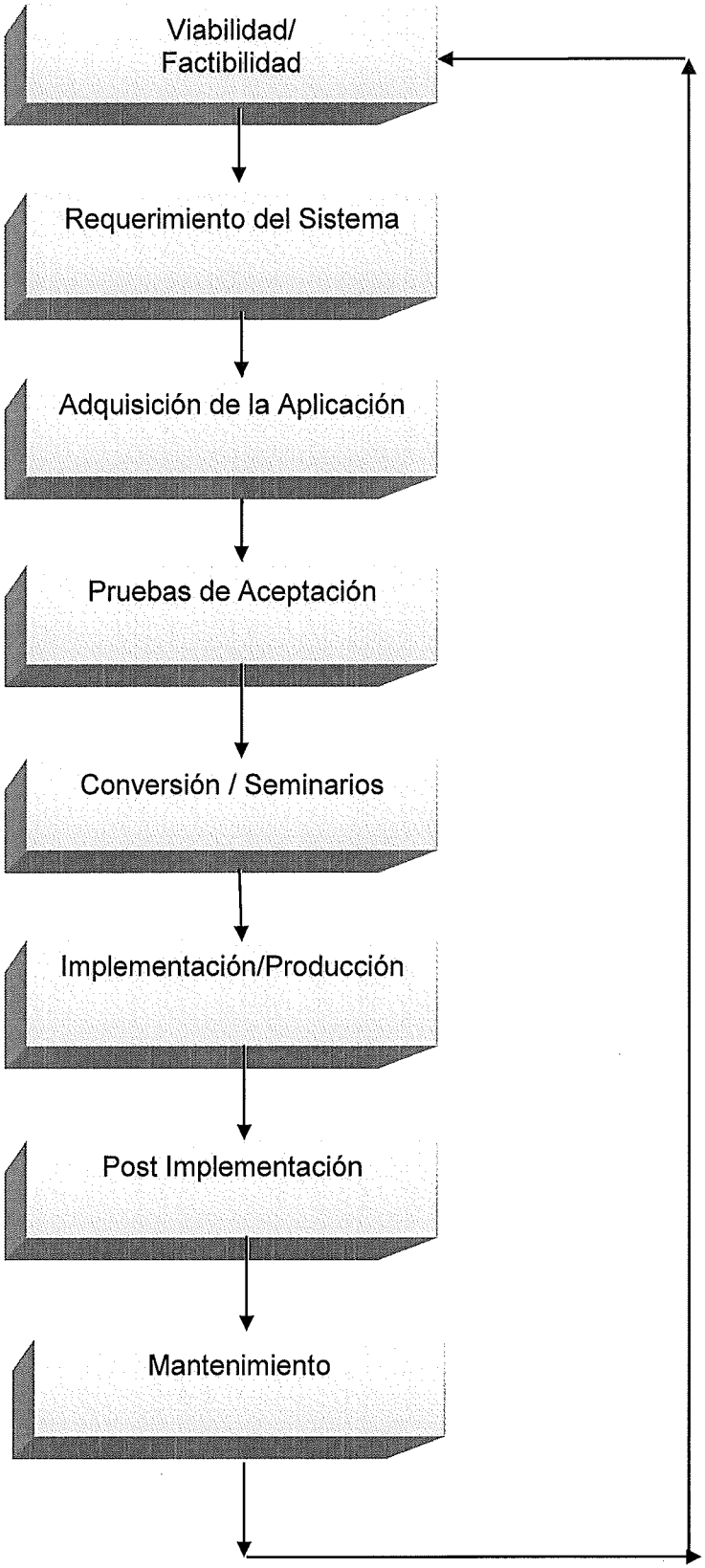
Con relación a este requisito, los sistemas deben ser efectivos, contar con una buena estructura de seguridad y controles internos, entre otros aspectos. Estos les permitirán operar eficientemente y salvaguardar la información de sus socios y depositantes.

En las auditorías de sistemas de información llevadas a cabo por la Corporación hemos observado que varias de las instituciones aseguradas han cambiado sus sistemas de información sin llevar a cabo los pasos básicos que conlleva este proceso. La falta de planificación, supervisión y análisis han ocasionado en algunas instituciones pérdidas en la disposición de sus equipos y han afectado, adversamente, sus operaciones en diferentes aspectos.

La Corporación con el fin de disminuir los riesgos que puedan ocurrir en la adquisición o cambio de sus sistemas de información hemos establecido un protocolo de procesos y procedimientos que deben poner en práctica al identificar, analizar, evaluar e implementar nuevas alternativas informáticas que les ayuden a cumplir con las necesidades de la Institución y requerimientos de los usuarios.

La adquisición, desarrollo y mantenimiento de los nuevos sistemas de información deben asegurar que los requerimientos de la Cooperativa sean satisfechos. A continuación les presentamos un diagrama sobre los procesos que deben seguir al adquirir e implementar un nuevo sistema de información.

Diagrama de Flujo de la Metodología



A. Viabilidad/Factibilidad – En esta Fase, la Cooperativa debe iniciar un análisis para definir las necesidades e identificar alternativas para resolverlas. Entre los elementos más importantes se encuentran:

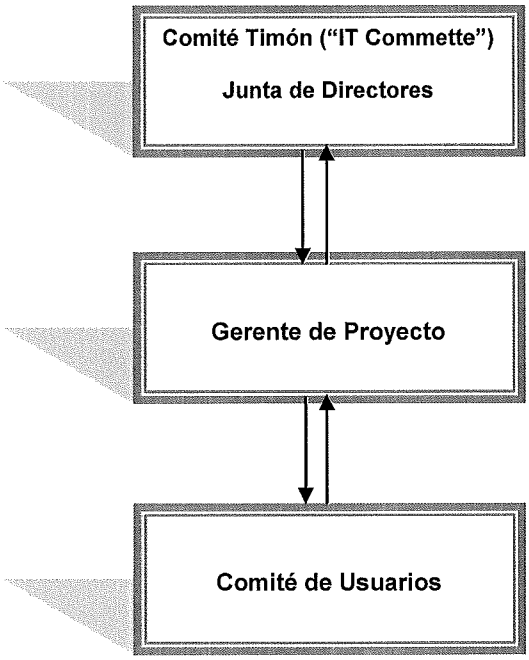
- ✓ Definir cuáles son las necesidades por la cual deben tomar la decisión de adquirir una nueva aplicación.
- ✓ Beneficios estratégicos de implementación (costo beneficio), tomando en cuenta el aumento en la productividad o en evitar costos futuros. Estos beneficios pueden ser tangibles e intangibles.
- ✓ Estimar la recuperación de los costos incurridos en la implementación de la nueva aplicación (Retorno de Inversión).
- ✓ Presupuesto disponible para la adquisición e implementación.
- ✓ Definir la infraestructura necesaria para la solución.
- ✓ Definir la fecha de implementación de la solución.
- ✓ Determinar cuál es la importancia del proyecto dentro de la Institución y como se relaciona con el Plan Estratégico vigente en ese momento.
- ✓ Mantener minutas y actas de todas las reuniones.

Antes de tomar alguna decisión, la Cooperativa deberá formar un Comité Evaluador/Implementador que analice las necesidades de la Cooperativa y recomiende, de ser necesario, la adquisición y/o implementación de un nuevo sistema de información. Este comité podrá estar compuesto por personal gerencial y administrativo, personal del departamento de información o por un recurso externo como consultor, proveedor y un representante de la Junta de Directores. La función del Comité será evaluar la adquisición de un nuevo sistema de información y evaluar las posibles compañías proponentes. El Comité Evaluador/Implementador hará las debidas recomendaciones a la Junta de Directores sobre la compañía a ser seleccionada para adquirir el nuevo sistema de información de la Cooperativa. De este comité recomendar la adquisición e implementación de un nuevo sistema de información, el mismo nombrará a un Gerente de Proyecto, que podría ser un recurso interno de la Cooperativa o un consultor externo y sería parte de este Comité.

El resultado debe presentarse en un Informe que incluya todos los elementos antes mencionados tomando en cuenta los costos, beneficios, riesgos, recursos requeridos e impacto en la Institución.

Una vez aprobado la adquisición e implementación de un nuevo sistema de información, el Comité integrado será responsable de dar seguimiento al proyecto de manera que el mismo sea auditado de manera contínua hasta ser completado a satisfacción de la Cooperativa y dentro del presupuesto.

Organigrama:



Es un representante de la Junta de Directores, preferiblemente con conocimiento en Sistemas de Información. Se compromete con el proyecto y aprueba los recursos necesarios. Este grupo se reunirá con el Gerente de Proyecto para el seguimiento del proyecto, de manera tal que el progreso del mismo sea auditado de manera continua.

Experiencia en la metodología de adquisición e implementación ("System Development Life Cicle"). Provee dirección general del proyecto, es la persona responsable de todos los informes, tales como: cronograma ("scheduling"), control del tiempo, entrenamiento de los usuarios, costos y es responsable que el proyecto permanezca en dirección. Esta persona reunirá y mantendrá informados a los Comités.

Es un representante de cada departamento impactado por el proyecto, el cual trabajará con la definición de los requerimientos del Sistema. Además, asistirá en la toma de decisiones en la adquisición y pruebas de aceptación antes de migrar a producción. Este grupo se reportará al Gerente de Proyecto.

B. Requerimientos del Sistema – Los requerimientos de los usuarios están identificados con la especificación de los requerimientos del Sistema.

La Cooperativa debe tomar en consideración los siguientes elementos:

- ✓ Documento de definición de requerimientos detallados por departamentos por el Comité de Usuarios u otros requisitos de la Cooperativa presentado al Gerente de Proyecto.
- ✓ Convertir los requerimientos del usuario en requerimientos del Sistema.
- ✓ Resolver conflictos entre los requerimientos y los recursos disponibles.
- ✓ Compromiso de la Alta Gerencia para patrocinar el proyecto.

- ✓ Los diagramas de flujo ("flowchart") de datos y el diseño representando gráficamente los requerimientos seleccionados.

Esta sección es la más importante en la selección de la aplicación.

C. Adquisición del Sistema - Deben comenzar la Fase de Adquisición una vez hayan identificado todos los requerimientos necesarios para adquirir la aplicación. Entre algunos de los elementos a considerar están los siguientes:

1. La Cooperativa debe enviar una Requisición de Propuesta *("Request for Proposal")* a más de dos proveedores que tengan disponibles aplicaciones dirigidas a instituciones financieras. En la requisición deben solicitarles a los Proveedores la siguiente información:

   - ✓ Cumplimiento de la aplicación con los Requerimientos de Leyes, Regulaciones Estatales y Federales para las Cooperativas de Ahorro y Crédito de Puerto Rico.
   - ✓ Requerimientos del Comité Evaluador/Implementador
   - ✓ Referencias de clientes
   - ✓ Estados Financieros de los Proveedores.
   - ✓ Cumplimiento con SSAE 16, (Anteriormente SAS 70), el estándar para auditar organizaciones de servicios,
   - ✓ Documentación completa de la aplicación por escrito y con antelación a la decisión.
   - ✓ Soporte técnico del vendedor incluyendo el grupo de trabajo.
   - ✓ Disponibilidad del Código Fuente ("Software Escrow Agreement")
   - ✓ Número de años de experiencia en el Sistema.
   - ✓ Lista de actualizaciones recientes en el Sistema.
   - ✓ Certificaciones de aceptación del Sistema.

   La Cooperativa debe evaluar cada uno de estos elementos solicitados en las propuestas y seleccionar solo los proveedores que se destaquen entre los demás y solicitarles presentaciones de sus productos. El Comité de Usuarios debe estar presente para evaluar las aplicaciones.

2. Evaluación de Proveedores - El Comité Evaluador/Implementador y el Gerente de Proyecto, como una medida deseable y de ser posible, deberán visitar alguna Institución Financiera que tenga instalada la aplicación para verificar cómo funciona la misma y conocer la ejecución de la aplicación en un ambiente en producción. Algunas de las preguntas más relevantes son:

- ✓ Grado de satisfacción de la institución financiera con la aplicación.
- ✓ Tiempo de implementación requerido.
- ✓ Proceso de implementación.
- ✓ Cumplimiento del presupuesto.
- ✓ Tiempo y calidad de respuesta en el Área de Soporte.
- ✓ Si la Cooperativa recomienda la aplicación.

3. El Comité de Usuarios, debe presentarle al Gerente de Proyecto todas las observaciones obtenidas en las presentaciones para así seleccionar la aplicación. Previo a la selección de la aplicación deseada, es importante presentarles al Proveedor todas las observaciones obtenidas del Comité de Usuarios para asegurar que puedan ser consideradas al momento de obtener la aplicación, específicamente, si el Proveedor puede cumplir con los cambios sugeridos por el Comité de Usuarios.

4. El Comité de Usuarios debe presentar un Informe al Gerente de Proyecto de las observaciones encontradas.

5. Seleccionar Proveedor - El paso final para la adquisición es firmar un Contrato de Adquisición que especifique los siguientes puntos:

   - ✓ Descripción especifica de los productos que se van a entregar.
   - ✓ Fechas de compromisos para la entrega de la aplicación. Esto incluye cualquier cambio que se vaya a realizar en la aplicación presentada en la Fase de Requerimiento por el Comité de Usuarios antes de la instalación. Pueden establecer una cláusula en el contrato donde penalicen al Proveedor por no cumplir con el tiempo determinado en la implementación del Sistema.
   - ✓ Compromiso de entrega de documentos, flujo grama ("flowchart") de la aplicación, licencias, manuales, seminarios, "upgrade", entre otros.
   - ✓ Garantías de los códigos fuentes de la aplicación por si el Proveedor dejare de existir ("Software Escrow Agreement").[1]
   - ✓ Descripción del Soporte Técnico que se brindará una vez terminada la instalación.
   - ✓ Garantía de poder copiar el Sistema y Mantenerlo en otro ambiente con el propósito de Continuidad de Negocios y Plan de Recuperación a Desastres.

[1] "Software Escrow Agreement" – es un contrato entre el Proveedor, un tercero de confianza y la Cooperativa sobre la garantía de los códigos fuentes de la aplicación, por si el Proveedor dejare de existir.

- ✓ Acuerdos de mantenimiento.
- ✓ Compromisos de pagos por la Cooperativa de acuerdo a cada Fase finalizada por los Proveedores "pagos por fases".
- ✓ El contrato debe ser negociado reduciendo los costos y tiempo de entrega. Al iniciar el proceso de negociación, deben tener presente lo siguiente:

    - ➲ Mantenga otras propuestas recibidas de otros proveedores para así poder negociar.
    - ➲ Analizar el contrato y asegurarse que incluya todo lo prometido durante el proceso de la compra.

- ✓ El asesor legal de la Cooperativa debe revisar el contrato antes de que éste sea firmado. Luego debe ser firmado por la Junta de Directores.

D. Pruebas - Las pruebas se utilizan para validar y verificar que el sistema de información seleccionado realiza las funciones por las cuales fue adquirido. La Cooperativa debe asegurarse, como parte del proyecto de desarrollo, implementación o modificaciones del sistema de información, que se conserve la documentación de los resultados de las pruebas del sistema adquirido.

Algunas de las pruebas más importantes se encuentran:

1. Pruebas de Seguridad – Pruebas diseñadas para asegurarse que en la nueva aplicación se incluyeron controles de acceso apropiado y no contenga alguna debilidad de seguridad que pudiera comprometer otros sistemas.

2. Prueba de Estrés/ Volumen – Probar una aplicación con cantidades sustanciales de datos para evaluar su rendimiento en horas picos, *como por ejemplo días de cobros, fin de mes.*

3. Pruebas Paralelo - Introducir datos de pruebas en dos sistemas: la aplicación modificada y una aplicación original y comparar los resultados tomando en cuenta el costo beneficio de la prueba.

4. Pruebas de Validación/Funcionabilidad – Probar la funcionabilidad de la aplicación contra los requerimientos detallados para asegurarse que la aplicación haya sido construido este acorde con los requerimientos de la Institución.

5. Pruebas de Integración/Interface – Viabilidad de que el Sistema sea lo suficientemente flexible como para poder compartir información con otros Sistemas, según las necesidades y requerimientos definidos.

6. Prueba de Controles de Calidad – Esta prueba se realiza para asegurar que la aplicación mantiene controles de calidad incluyendo lo siguiente:

   - ✓ Funcionabilidad,
   - ✓ Seguridad,
   - ✓ Portabilidad,
   - ✓ Tolerancia a Fallas,
   - ✓ Estabilidad.

   Se recomienda que certifiquen o acrediten la aplicación antes de pasarla a producción para determinar la efectividad de la aplicación y así lograr sus objetivos y establecer un nivel apropiado de controles y seguridad en la aplicación.

7. Pruebas de Aceptación Final *("User Acceptance Testing")* - Es una prueba de aceptación donde el Comité de Usuarios evalúa todos los cambios realizados por el Proveedor de acuerdo a los requerimientos, especificaciones, seguridad y requisitos sometidos por los usuarios de la Cooperativa en la Fase de Requerimientos. Deberán asegurar, como parte de las pruebas de aceptación final o de aseguramiento de calidad de sistemas de información nuevos o modificados, una evaluación y aprobación formal de los resultados de las pruebas por parte de la Gerencia de los departamentos usuarios afectados y de Sistemas de Información. Las pruebas deben cubrir todos los componentes del sistema de información (software de aplicación, instalaciones. Sin la aceptación de esta prueba, la aplicación no puede ir a producción.

E. Conversión- En esta Fase se debe requerir que el plan de conversión de datos esté preparado, definiendo los métodos de recolección y verificación de los datos que serán convertidos e identificando y resolviendo cualquier error encontrado durante la conversión. Las pruebas a ser desarrolladas incluyen la comparación, del archivo original, y el convertido, revisión de la compatibilidad de los datos transformados con el nuevo sistema, revisión de los archivos maestros después de la conversión para asegurar la precisión de los datos de los archivos maestros y así asegurar que las transacciones realizadas actualicen tanto a los archivos maestros antiguos como los nuevos durante el periodo entre la conversión inicial y la implementación final. También deben verificar detalladamente, los procesos iniciales del nuevo sistema para confirmar una implementación exitosa tomando en cuenta lo siguiente:

- ✓ Determinar cuáles datos deben ser convertidos mediante la ejecución de programas y cuáles deben ser procesasdos, manualmente.

- ✓ Depuración de datos innecesarios, incompletos o incorrectos, *por ejemplo, Nombre, Direcciones, Campos de Fechas, Campos de Seguro Social, Número de Socio, entre otros.*

- ✓ Reportes de excepciones que registren cualquier data que no pueda ser convertido automáticamente.

- ✓ Control de totales de los archivos maestros de la aplicación original a la nueva aplicación.

F. Seminarios - Todos los usuarios que utilizarán la aplicación deben tomar seminarios antes de su implementación. El Gerente de Proyecto debe preparar un cronograma ("schedule") de los seminarios que deben tomar los usuarios. Deben asegurar que desarrollen materiales de entrenamiento adecuados como parte de cualquier proyecto de desarrollo, implementación o modificación de sistemas de información. Estos materiales deberán enfocarse al uso del sistema en la práctica diaria.

G. Implementación - En esta Fase todas las pruebas, migración, seminarios deben haber sido realizados exitosamente. Si la aplicación no recibió cambios en programación, se debe certificar realizando una prueba de aceptación del usuario antes de la implementación.

H. Post – Implementación – Luego que la nueva aplicación haya estado operando, por lo menos durante un periodo de seis meses a un año, deben evaluarlo para determinar si la aplicación ha logrado lo siguiente:

- ✓ Los requerimientos adquiridos en especial atención a la utilización y la satisfacción de los usuarios.

- ✓ Luego de un periodo de tiempo, deben evaluar las medidas del costo beneficio o el Retorno de la Inversión (ROI) presentado en la primera Fase **(Viabilidad/Factibilidad)**.

- ✓ Someter recomendaciones de las deficiencias encontradas en la aplicación una vez ha sido implementado.

- ✓ Mantener las solicitudes de cambios a los programas que se han realizado después de la implementación.

- ✓ Se debe llevar a cabo una auditoría externa posterior a la implementación dirigida a los controles de los procesos de desarrollo e implementación.

I. **Mantenimiento** - Es la última Fase donde se debe contemplar un mejoramiento continuo de la aplicación hasta que nuevamente la Cooperativa tomará la decisión de adquirir una nueva aplicación.

   Desde que una aplicación es puesta en producción, se realizan mantenimiento y cambios los cuales deben tener en cuenta unos procedimientos para realizar y registrar estos cambios **"Procedimientos de los Cambios en Aplicaciones".** Este procedimiento debe incluir:

   1. Autorización de los cambios a los programas de producción.

   2. Mantener las solicitudes de cambios almacenadas con la documentación del programa modificado. Las solicitudes de cambios deben contener, como mínimo, la siguiente información:

      - ✓ Número de control de la solicitud.
      - ✓ Fecha de Solicitud.
      - ✓ Nombre del Solicitante.
      - ✓ Departamento
      - ✓ Descripción del cambio.
      - ✓ Razón por la que está solicitando los cambios.
      - ✓ Justificación del cambio (Costo-Beneficio).
      - ✓ Aprobación del Usuario.
      - ✓ Aprobación del Supervisor.

   3. Documentación de los programas modificados.

   4. Reportes de auditoría de cambios o manejo de versiones de los programas.

   5. Controles de acceso a los programas de producción. Debe existir un control de acceso a los programas de producción, estos controles generalmente son manejados por el programa de acceso a los servidores o equipo relacionado.

Como parte de nuestra función de educar y ofrecer ayuda técnica a las cooperativas, en nuestra asamblea anual de 2011, la cual llevaremos a cabo la última semana de octubre, ofreceremos un seminario a todas las cooperativas sobre el contenido de esta Carta Circular.

Si poseen alguna duda sobre los procesos aquí detallados, pueden comunicarse a nuestras oficina con el Sr. Gabriel Cordero Morales (CISA), Supervisor de Auditoría de Sistemas de Información, al teléfono (787) 622-0957 o vía correo electrónico, gcordero@cossec.gobierno.pr.