Autorizado por la Comisión Estatal de Elecciones,
Núm. CEE-SA-12-5579

Esta página ha sido dejada intencionalmente en blanco

(Este folleto sustituye la publicación *Las Mejores Prácticas para la Adquisición y Utilización de la Tecnología de Información* de febrero de 2001)

Esta página ha sido dejada intencionalmente en blanco

Estado Libre Asociado de Puerto Rico
OFICINA DEL CONTRALOR

LAS MEJORES PRÁCTICAS PARA LA ADQUISICIÓN, DESARROLLO, UTILIZACIÓN Y CONTROL DE LA TECNOLOGÍA DE INFORMACIÓN

CONTENIDO

Esta página ha sido dejada intencionalmente en blanco

MENSAJE DEL CONTRALOR DE PUERTO RICO

Estimado lector:

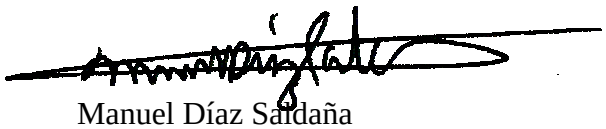
Una de las mejores prácticas de una sana administración pública es incorporar los cambios e innovaciones tecnológicas a las gestiones de cada entidad gubernamental con el objetivo de mejorar la calidad y productividad de éstas. Esto a su vez requiere disponer de criterios, normas y estándares que "*promuevan el uso efectivo y eficiente de los recursos del gobierno en beneficio de nuestro pueblo.*" Por lo tanto, los funcionarios públicos deben establecer prácticas para la adquisición, desarrollo, utilización y control de la tecnología de información de manera que se alcancen los objetivos de los proyectos.

Esta segunda edición del **Folleto sobre las Mejores Prácticas para la Adquisición, Desarrollo, Utilización y Control de la Tecnología de Información** amplía la lista de prácticas enumeradas en la primera edición y toma en cuenta las enmiendas a las leyes, normas, procedimientos y hallazgos de los informes de auditoría, relevantes para la tecnología de información y para el uso de la propiedad y de los fondos públicos. Las entidades gubernamentales deben verificar las disposiciones de ley específicas, y los reglamentos internos aplicables a su caso particular. Los organismos y entidades de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico y aquellas entidades gubernamentales que se beneficien de los servicios ofrecidos por la Oficina de Gerencia y Presupuesto (OGP), deben cumplir con las **Políticas de Tecnologías de Información Gubernamental** incluidas en la **Carta Circular Núm. 77-05**, emitidas por la OGP el 8 de diciembre de 2004. Aquellas entidades que no estén obligadas a regirse por estas normas, deben contar con normas de sana administración que incluyan todos los aspectos mencionados en esta publicación y, cualquier otro, que sea necesario en su caso particular.

En esta nueva edición, también incluimos la lista de publicaciones y otras referencias disponibles en la Internet que pueden ayudar a conocer aquellos aspectos que no se detallan en la misma. Esperamos que esta breve guía sea de utilidad para todos los involucrados en los procesos de adquisición y utilización de la tecnología de información en la administración pública.

Contamos con su cooperación para mejorar la fiscalización y la administración de la propiedad y de los fondos públicos.

Cordialmente,



Manuel Díaz Saldaña
Contralor de Puerto Rico
enero de 2006

Esta página ha sido dejada intencionalmente en blanco

INTRODUCCIÓN

La incorporación oportuna de la tecnología a los programas y servicios del gobierno es un valioso instrumento para reducir el tiempo de gestión y los costos de operación, y para hacer más accesibles los servicios que se prestan a los ciudadanos. Sin embargo, en toda institución, mantenerse al día sobre los adelantos tecnológicos requiere una inversión de recursos considerable. Anualmente las entidades gubernamentales invierten millones de dólares en el desarrollo, la adquisición, la implantación, la seguridad y el mantenimiento de los sistemas de información, y en la contratación de servicios profesionales de asesoría técnica en sistemas computadorizados. La inversión de fondos públicos en tecnología de información debe planificarse, de manera que se obtengan los beneficios esperados en un período de tiempo razonable, y que se pueda cumplir con la política gubernamental de interconexión entre los sistemas computadorizados de las entidades gubernamentales.

Los proyectos relacionados con la tecnología de información generalmente involucran distintas fases durante su "ciclo vital". Por ejemplo, el ciclo vital de un sistema computadorizado comienza con el análisis de las necesidades y termina cuando se remplaza por un nuevo sistema o se determina que deja de ser necesario. En términos generales, el ciclo vital de un proyecto de informática consta de las siguientes fases:

- Análisis y planificación
- Desarrollo y pruebas
- Implantación
- Operaciones
- Conservación y control de cambios

Cada una de estas fases conlleva la implantación de controles y de métodos de seguridad, así como la adquisición de servicios. Además, en cada etapa se recomienda establecer un proceso de revisión de calidad de los productos.

Aunque cada caso se debe examinar en su contexto, la Oficina del Contralor recomienda que se utilice una metodología de desarrollo modular y de tipo espiral. De esta manera se obtendrán resultados de forma rápida, se identificarán los requerimientos específicos de los usuarios, y se reducirá el riesgo de la inversión. También se recomienda emplear o contratar recursos profesionales altamente capacitados y con la experiencia necesaria en este campo. Esto debe hacerse de forma ponderada, de acuerdo con la inversión y la magnitud de cada proyecto.

Los organismos y las entidades de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico y aquellas entidades gubernamentales que se beneficien de los servicios ofrecidos por la OGP, deben cumplir con las **Políticas de Tecnologías de Información Gubernamental** incluidas en la **Carta Circular Núm. 77-05** emitida por la OGP el 8 de diciembre de 2004. Aquellas entidades que no estén obligadas a regirse por estas normas, deben contar con normas de sana administración que incluyan todos los aspectos mencionados en esta publicación y, cualquier otro que sea necesario en su caso particular.

A continuación se describen brevemente los criterios a considerarse para la adquisición, el desarrollo, la utilización y el control de la tecnología de información. La aplicación de éstos dependerá del tamaño y de la complejidad del proyecto. Además, se debe tener en cuenta que esto **no** constituye una metodología, sino más bien una guía breve de los varios aspectos a considerarse.

PROCESO DE ADQUISICIÓN Y DESARROLLO DE APLICACIONES

El proceso de adquisición consiste de varios pasos dirigidos a obtener los equipos y los programas de tecnología de información que puedan satisfacer las necesidades de la entidad gubernamental, a un costo razonable. Mediante este proceso se analizan y se identifican las necesidades a ser atendidas y la forma de atender las mismas.

A. Estudio de Necesidades

El estudio de las necesidades de la entidad gubernamental es el primer paso que se debe considerar en los procesos de adquisición de equipos y programas, y de desarrollo de aplicaciones. Dicho estudio debe estar enmarcado en la misión, las responsabilidades y los servicios de la entidad gubernamental y, estar acorde con la política de interconexión de los organismos para facilitar y agilizar los servicios al pueblo. Es importante que los gerentes y los usuarios participen activamente en este proceso para evitar la inversión en un sistema que no cumplirá con los requisitos de la entidad gubernamental. Dicha participación es necesaria para identificar todos los requerimientos o especificaciones del sistema, de manera que se logren los objetivos y los beneficios esperados.

Como parte del proceso de evaluación de las necesidades de la entidad gubernamental se efectúan un estudio preliminar y un estudio de viabilidad.

1. Estudio Preliminar

El estudio preliminar se realiza para identificar las necesidades básicas de los usuarios y las posibles soluciones. El informe que se obtenga como resultado de este estudio, se utilizará para tomar la determinación de continuar o detener el proyecto de computadorización.

2. Estudio de Requisitos y Viabilidad

Los requisitos específicos y detallados de los usuarios es tal vez el aspecto más importante de un proyecto de computadorización. Se debe definir o identificar tanto lo que se va a proveer como lo que **no** estará disponible. Los errores que se cometan en este proceso y las expectativas que se dejen de identificar podrían propiciar el fracaso o el sobrecosto del proyecto.

Una vez se identifican los requisitos, se evalúan los beneficios y los costos asociados a cada una de las soluciones potenciales identificadas en el

estudio preliminar. El estudio de viabilidad determinará si la inversión propuesta en el desarrollo o adquisición está de acuerdo con las metas y los objetivos de la entidad.

Para determinar la mejor opción entre el desarrollo interno de la programación del sistema computadorizado, la contratación de servicios o la adquisición de programas computadorizados disponibles comercialmente (COTS por sus siglas en inglés), se recomienda considerar los siguientes factores:

- Los recursos tecnológicos y humanos que se requieren para desarrollar el sistema, incluyendo la evaluación del conocimiento y la experiencia del personal disponible
- La fecha en que se requiere que el sistema esté funcionando
- El costo del desarrollo versus el costo de la contratación
- La disponibilidad de fondos necesarios para el proyecto
- La compatibilidad con los planes estratégicos de la entidad gubernamental
- La compatibilidad con la infraestructura tecnológica de la entidad gubernamental[1]
- Los probables requerimientos de cambios futuros al funcionamiento del sistema.

Para llevar a cabo un estudio de viabilidad, se recomienda constituir un comité compuesto por un representante de cada uno de los siguientes sectores: la alta gerencia, el área de Finanzas, el área de Tecnología de Información, los usuarios a quienes afectará la computadorización, y la Oficina de Auditoría Interna.

Las entidades del Estado Libre Asociado de Puerto Rico, como parte de su estudio de viabilidad, deben efectuar un análisis de costos y de procedencia de fondos, para determinar si los proyectos requieren la aprobación de la OGP (véase la **Política Núm. TIG-001** en la **Carta Circular Núm. 77-05**). De requerirse la aprobación de la OGP, la entidad debe iniciar el proceso de aprobación durante esta etapa. Aquellas entidades que no estén obligadas a regirse por estas normas, deben contar con normas de sana administración que incluyan todos los aspectos mencionados en esta publicación y, cualquier otro que sea necesario en su caso particular.

La documentación desarrollada durante el transcurso del estudio se utilizará para preparar las especificaciones del sistema y la solicitud de propuestas.

[1] Las entidades gubernamentales que utilicen los Sistemas Financieros del Departamento de Hacienda y que estén considerando adquirir o desarrollar un sistema computadorizado de nóminas, de finanzas o de recursos humanos, deben asegurarse de que éstos provean interoperabilidad e integración con los sistemas computadorizados del Departamento de Hacienda, según se establece en la **Política Núm. TIG-009** en la **Carta Circular Núm. 77-05**. Además, se deben garantizar la integridad y la seguridad de los datos transmitidos.

B. Plan de Desarrollo Tecnológico

El estudio de necesidades nos ayudará a preparar el **Plan de Desarrollo Tecnológico** y a establecer las prioridades entre unas necesidades y otras: áreas críticas y menos críticas. En este **Plan** se indica qué sistemas se van a computadorizar y cuáles son las prioridades, según la misión de la entidad y los servicios que brinda. También debe indicar el equipo y los programas necesarios para mecanizar estas áreas. Al ofrecer las especificaciones del equipo, se deben incluir los sistemas que serán computadorizados, y la debida información en cuanto a los datos de entrada y salida, los archivos, los informes, el uso, el volumen, los controles, etc. También es necesario indicar los requisitos mínimos del equipo, tales como: velocidad, capacidad de memoria y características específicas. Además, el **Plan** debe detallar las fases y las tareas de cada proyecto, las entregas de cada fase y las fechas de terminación.

Sugerimos a toda entidad gubernamental que adopte, como norma de sana administración, la práctica de segregar las tareas, de la persona o la firma que prepara o diseña el **Plan**, y la persona o la firma a quien se le asigna el desarrollo o la implantación del mismo.

Las entidades gubernamentales que tengan la responsabilidad de cumplir con la **Carta Circular Núm. 77-05** deben preparar y someter anualmente su **Plan de Tecnología**, según lo requiere la **Política Núm. TIG-12**. Aquellas entidades que no estén obligadas a regirse por la referida **Carta** deben contar con normas equivalentes que incluyan todos los aspectos mencionados en esta publicación y, cualquier otro que sea necesario en su caso particular.

C. Desarrollo o Adquisición de Programas y de Otros Componentes de Programación[2]

La entidad gubernamental debe asegurarse de que los programas desarrollados o adquiridos provean medidas de control o, de interoperabilidad con otros sistemas. Con este fin, el personal encargado del desarrollo o adquisición de programas o de otros componentes de programación debe tomar en cuenta que:

- Sean compatibles con el equipo existente o cumplan con las especificaciones mínimas del proponente de la programación.
- Los sistemas financieros tengan la capacidad de interfase con los sistemas del Departamento de Hacienda.
- Provean crecimiento, flexibilidad y adaptabilidad.
- Puedan operar entre sí, sean funcionales en arquitectura n-niveles y, si es necesario, tengan la capacidad de poder operar en navegadores de uso común en la industria.

[2] El componente de programación se define como aplicaciones, lenguajes de programación, bases de datos, programas de productividad y programas de utilidades.

- Existan maneras de controlar la creación y privilegios de los usuarios.
- Exista una garantía que asegure el funcionamiento apropiado de la programación, según los propósitos para los cuales fue desarrollada o adquirida.

1. Contratación para el Desarrollo de Sistemas

Los contratos para el desarrollo de sistemas y de programas deben contener los siguientes puntos, entre otros:

- Descripción específica de los productos que se van a entregar y sus costos
- Fechas para la entrega de los productos
- Compromiso de documentación, mantenimiento, actualizaciones y adiestramientos
- Descripción del apoyo que se brindará durante la instalación
- Criterios para la aceptación por el usuario
- Disposición para permitir un periodo razonable de pruebas de aceptación
- Programa de pagos vinculado con las fechas efectivas de entrega.

Además, dichos contratos deben incluir una cláusula donde se especifique que todos los programas desarrollados y su documentación son propiedad del Estado Libre Asociado de Puerto Rico y, que deben cumplir con la Ley de Derechos de Autor. Como parte de la documentación, se debe requerir a los contratistas que entreguen los códigos fuentes de los programas desarrollados. Dicha cláusula es esencial para adiestrar al nuevo personal y para facilitar el mantenimiento de las aplicaciones y sus programas. Se recomienda que un asesor legal de la entidad revise el contrato antes de firmarlo, para garantizar que incluye las cláusulas requeridas y se protege el interés público. La gerencia de la entidad gubernamental deberá asignar un administrador que posea la experiencia y los conocimientos técnicos necesarios, para velar por que se cumpla con las disposiciones del contrato.

Se considera una norma de sana administración que todo sistema de información en el que se haya invertido una cantidad considerable de fondos sea evaluado por el personal técnico de programación de la entidad concernida, con el propósito de determinar si se puede modificar, antes de comprometer recursos económicos adicionales en el desarrollo o adquisición de nuevos sistemas de información.

Las entidades gubernamentales requerirán a sus contratistas y a aquellas personas que soliciten fondos administrados por dichas entidades, que certifiquen que tienen sistemas y controles apropiados para asegurarse de no utilizar fondos públicos para adquirir, operar o mantener programas en

violación a las leyes federales y de Puerto Rico, las cuales rigen los derechos de autor y la propiedad intelectual.

2. Adquisición de Programas y Otros Componentes de Programación

La adquisición de aplicaciones, lenguajes de programación, bases de datos y programas de productividad y de utilidades, debe comenzar con una Solicitud de Propuesta **[Request for Proposal (RFP)]**, la cual utilizará como base la documentación desarrollada en el estudio de viabilidad.

El personal del Área de Tecnología de Información de la entidad gubernamental debe verificar que los programas sean compatibles con el equipo existente o solicitar las especificaciones mínimas del proponente de los programas. Los auditores deben participar en el proceso de adquisición de programas o aplicaciones para verificar que éstos incluyen los controles de seguridad necesarios para garantizar la integridad de los datos que serán procesados a través del sistema. El vendedor debe comprometerse a realizar los cambios necesarios a los programas, para ajustar el producto a las necesidades de la entidad gubernamental.

Al adquirir los programas disponibles comercialmente se debe verificar que todo programa incluya lo siguiente:

a) Un CD-ROM o disquete hecho por el fabricante
b) Contrato de Licencia
c) Certificado de Autenticidad **[Certificate of Authenticity (COA)]**
d) Manual de Uso
e) Tarjeta de Registro

Los programas se deben adquirir mediante un representante autorizado del fabricante para obtener el original de los programas y la documentación correspondiente.

D. Adquisición de Equipo y Componentes para la Red

Al evaluar las propuestas de los proveedores, la entidad gubernamental debe asegurarse de que se tomen en consideración todas las alternativas en el estudio preliminar y en el de viabilidad. Se deben considerar factores, tales como: costo del equipo, servicio de mantenimiento, servicios de resguardo de equipo y habilidad de la empresa seleccionada para entregar el mismo en la fecha establecida, entre otros.

La adquisición de equipo o de componentes para la red debe cumplir con los requisitos mínimos detallados en la **Política Núm. TIG-010** incluida en la **Carta Circular Núm. 77-05**. La adquisición e implementación de componentes para la red debe promover una infraestructura que provea interoperabilidad y escalabilidad con el fin de mejorar las capacidades operacionales, la productividad y la ejecución

de las entidades gubernamentales, de modo que el resultado sea un servicio gubernamental de alta calidad. Las redes de comunicación de las entidades gubernamentales deben ser diseñadas y establecidas con sistemas redundantes y de tolerancia a fallas, para que se garantice la operación continua del sistema.

Aquellas entidades que no estén obligadas a regirse por la **Carta Circular Núm. 77-05**, deben contar con normas equivalentes que incluyan todos los aspectos mencionados en esta publicación y, cualquier otro que sea necesario en su caso particular.

E. Solicitud de Propuestas y Contratación

Se recomienda que las propuestas se soliciten en dos partes o sobres sellados, el primero debe contener la propuesta técnica y el segundo, la propuesta financiera. Además, se recomienda evaluar primero el contenido de todas las propuestas técnicas, y el cumplimiento de éstas con las especificaciones, antes de considerar la propuesta financiera.

Los contratos para la adquisición de equipo se deben revisar detalladamente desde el punto de vista legal, técnico y financiero, antes de ser firmados. Éstos deben contener, entre otras, cláusulas sobre apoyo técnico y mantenimiento del equipo.

Toda entidad gubernamental o municipio que interese suscribir contratos de arrendamiento para financiar la adquisición de equipos, computadoras y otros bienes muebles, deberá someterlos a la revisión y aprobación del Banco Gubernamental de Fomento para Puerto Rico (BGF). Este procedimiento se requiere para cumplir con la **Ley Núm. 265 de 3 de septiembre de 2003**.

F. Asignación de un Administrador de Proyecto

La gerencia debe nombrar un funcionario o contratar un profesional competente que será responsable de dirigir, coordinar y controlar el proyecto. Éste servirá de enlace entre los usuarios, el personal técnico y la gerencia. Además, se encargará de supervisar el proyecto y de velar por que se cumpla con el **Plan de Tecnologías**.

G. Desarrollo de Portales (Páginas Web) para Proveer la Integración y la Publicación de Transacciones Electrónicas Gubernamentales

Las entidades gubernamentales que planifican crear una *página web* (sitio en la Internet) deben seguir las recomendaciones sugeridas en la **Guía de Diseño y Contenido de Páginas Web** y cumplir con la **Política Núm. TIG-002** incluida en la **Carta Circular Núm. 77-05**. Para ello, la gerencia de la entidad debe asegurarse de que poseen la infraestructura necesaria para ofrecer los servicios en línea. Además, aquellas entidades que planifican ofrecer sus servicios a la ciudadanía a través de la Internet, deben cumplir con lo establecido en la **Política Núm. TIG-006** incluida en la referida **Carta**.

Aquellas entidades que no estén obligadas a regirse por la **Carta Circular Núm. 77-05**, deben contar con normas equivalentes que incluyan todos los aspectos mencionados en esta publicación y, cualquier otro que sea necesario en su caso particular.

Es importante que toda entidad u organismo gubernamental vele por que las leyes, los reglamentos y las órdenes administrativas se atemperen simultáneamente a los nuevos procesos electrónicos de transacciones gubernamentales. Además, deben proveerse los recursos necesarios para:

- Garantizar que las transacciones electrónicas se procesen inmediatamente, y que los empleados gubernamentales las atiendan en un tiempo razonable.
- Informar al ciudadano, por medios electrónicos, sobre el status de su transacción.

Las páginas para la *web* y los programas de aplicación que se desarrollen con el fin de brindar servicios al pueblo, deben incluir los controles de seguridad necesarios para proteger la confidencialidad de los datos personales de los ciudadanos y la integridad y la confidencialidad de los datos de la entidad. Además, es recomendable que como medida de control, durante el desarrollo de las páginas para la *web*, la gerencia incorpore procesos de calidad de datos, con el propósito de garantizar que la información publicada es correcta y confiable. Para evitar confusiones a los ciudadanos, es recomendable que cuando un sistema almacene datos provenientes de otras entidades gubernamentales, esos datos se validen y se comparen con los mantenidos por la entidad gubernamental gestora, antes de que se publiquen en las páginas para la *web*.

PROCESO DE PREIMPLANTACIÓN

Como parte de ese proceso, se identifican y se definen todas las tareas o actividades previas a la instalación del sistema, las cuales constituyen el plan de preimplantación. Este plan debe contener un estimado de tiempo para cada actividad, que permita medir el cumplimiento del itinerario de trabajo. Si el proyecto incluye la modificación o el desarrollo de sistemas, se debe considerar que los equipos computadorizados se adquieran *justo a tiempo*: cuando los programas sean necesarios para los usuarios y no antes.

PROCESO DE IMPLANTACIÓN

La implantación de un nuevo sistema es un proceso complejo que requiere la interacción de los usuarios, el equipo de desarrollo y el grupo de procesamiento de sistemas de información. Este proceso comprende la instalación del equipo y de los programas de sistemas (sistema operativo, compiladores, intérpretes, utilitarios), la instalación del sistema de información computadorizado que ha sido desarrollado, la conversión de los archivos, el adiestramiento de los usuarios y de los operadores del nuevo sistema, y la revisión y la actualización de la documentación en los casos requeridos. Durante el proceso de implantación, se establece el nuevo sistema de información y

se prueba si la operación es efectiva. La prueba de aceptación del usuario se lleva a cabo en esta etapa. Durante este proceso la entidad debe asegurarse de que los programas computadorizados funcionan de acuerdo con los propósitos para los cuales fueron desarrollados.

Los pasos que se deben seguir para la implantación son los siguientes:

A. *Establecer y llevar a cabo el Plan de Implantación*

B. *Establecer y llevar a cabo el Plan de Conversión* - La gerencia del departamento usuario debe participar en la conversión de la información del sistema actual al nuevo. El sistema debe ser aceptado y aprobado por la gerencia antes de iniciar la operación del mismo.

C. *Preparar respaldo y planes de recuperación para el nuevo sistema*

D. *Establecer una función de monitoreo* - La misma debe asegurar que los problemas asociados con las actividades del nuevo sistema se puedan identificar, documentar, diagnosticar y resolver rápidamente.

E. *Preparar la documentación del sistema*[3]- La documentación es esencial para el uso eficiente de cualquier sistema. Una documentación clara, completa y correcta debe utilizarse en cada etapa, desde el desarrollo hasta la operación del sistema, y debe actualizarse durante el mantenimiento del mismo. Ésta sirve como una herramienta de diagnóstico cuando el sistema no funciona como se esperaba. Por esa razón, debe estar orientada a proporcionar una comprensión clara y confiable del sistema computadorizado y, a facilitar el mantenimiento y las modificaciones requeridas posteriormente. De modo que se pueda cumplir dicho fin, es recomendable establecer normas para el desarrollo y el mantenimiento de la documentación.

F. *Adiestrar a los usuarios en la operación del sistema nuevo o revisado* - Se sugiere la capacitación de los usuarios *justo a tiempo* para poner en práctica el mismo y no antes.

G. *Establecer la operación del sistema paralelo* - El procesamiento en paralelo se ejecuta para el control efectivo de la conversión de los archivos viejos en nuevos y para ejecutar las operaciones iniciales de los nuevos sistemas. Además, para verificar que el nuevo sistema produce los mismos resultados que el sistema existente.

H. *Realizar una revisión postimplantación* - Esta revisión tiene el propósito de determinar si el proyecto alcanzó el éxito esperado.

[3] La documentación puede estar impresa o en sistemas de ayuda en línea. Podemos mencionar algunos tipos de manuales de documentación: de sistema, de usuario, de operación de computadoras, *help desk* y de control de redes, entre otros.

PROCESO DE POSTIMPLANTACIÓN

La evaluación postimplantación es la última fase del ciclo de desarrollo de sistemas y consiste en una revisión que se realiza después que los sistemas de información computadorizados hayan estado en operación durante un período razonable, bajo la responsabilidad del Administrador del Proyecto. Dicha evaluación debe realizarla un grupo compuesto por representantes de: los usuarios de los sistemas, los analistas, los operadores de sistemas y los auditores internos independientes del proceso de desarrollo del sistema. Éstos deben evaluar el proceso de implantación con el fin de determinar si se logró satisfacer los objetivos establecidos de acuerdo con la relación de beneficio-costo esperada.

Además, se deben asignar prioridades a las modificaciones y a otras necesidades identificadas durante el uso del nuevo sistema. Éstas permitirán alcanzar nuevos objetivos de forma alineada con las estrategias gerenciales.

REVISIÓN DE CALIDAD

La revisión de calidad consiste en examinar los resultados y los productos del proceso, tanto intermedios como al final de cada etapa del ciclo vital del sistema, de manera que se garantice el cumplimiento con los requisitos. Entre los atributos evaluados se incluyen la funcionalidad, la confiabilidad, la utilización, la eficiencia, el mantenimiento y la portabilidad.[4]

UTILIZACIÓN Y SEGURIDAD[5]

A. Normas y Procedimientos

Las entidades gubernamentales tienen la responsabilidad de desarrollar políticas y procedimientos de seguridad detallados, de acuerdo con los requisitos de seguridad establecidos en la **Política Núm. TIG-003** incluida en la **Carta Circular Núm. 77-05**. Aquellas entidades que no estén obligadas a regirse por dicha **Carta**, deben contar con normas equivalentes que incluyan todos los aspectos mencionados en esta publicación y en cualquier otro que sea necesario en su caso particular. Se recomienda, como norma de sana administración, desarrollar estrategias de orientación y adiestramiento continuo relacionados con las normas y los procedimientos de seguridad que los empleados y los contratistas deben seguir.

Las políticas, las normas y los procedimientos de seguridad establecidos deben estar de acuerdo con la legislación y los reglamentos vigentes.

---

[4] El **ISO 9126** provee la definición de las características y del el proceso asociado de evaluación de la calidad que se podría utilizar cuando se especifican los requerimientos y se evalúa la calidad de los productos de *software* en todo su ciclo vital.

[5] En la **Carta Circular OC-98-11** emitida por el Contralor de Puerto Rico el 18 de mayo de 1998 se incluyen algunas sugerencias sobre las medidas que se deben adoptar para controlar el uso de los equipos computadorizados y sus programas, y para proteger la información que se conserva en los mismos. En la **Carta Circular OC-2002-02** emitida por el Contralor de Puerto Rico el 16 de agosto de 2001 se establece la necesidad de advertir al usuario, en la pantalla inicial del sistema, sobre las normas principales para el uso del mismo.

B. Seguridad Física

La exposición a riesgos físicos y ambientales puede producir pérdidas financieras, tener repercusiones legales, causar pérdida de credibilidad o pérdida de competitividad. Las áreas que deben protegerse son las siguientes:

1. Área de Programación
2. Sala de la computadora principal
3. Consolas y terminales del operador
4. Biblioteca de los medios magnéticos de almacenamiento
5. Área de almacenamiento de las reservas fuera de los predios de la entidad gubernamental
6. Sala de control de entrada y salida
7. Cuarto de conexiones de comunicaciones (*Wiring Closet*)
8. Equipo de telecomunicaciones (radios, satélites, cableado, modems, etc.)
9. Microcomputadoras y computadoras personales
10. Fuente de energía eléctrica
11. Líneas telefónicas dedicadas
12. Equipo portátil (*escáneres*, lectores de código de barras, impresoras, y otros)
13. Impresoras en ubicaciones locales o remotas
14. Redes de comunicaciones

El acceso físico a las áreas mencionadas sólo se le permitirá al personal autorizado por la gerencia. Todas las personas que requieran acceso a las áreas indicadas lo harán bajo un control adecuado y acompañados del supervisor o funcionario autorizado del área de operación.

La seguridad física de los sistemas de información computadorizados requiere disponer de procedimientos y de medidas que contrarresten los riesgos a los daños que puedan causar el fuego, el agua, las interrupciones o las variaciones de la energía eléctrica que alimenta los equipos, así como la presencia de químicos y de otros elementos que afecten el ambiente normal de operación de las máquinas y el estado físico de los archivos magnéticos.

En atención a lo anterior, se debe disponer de dispositivos de detección de fuego y humedad, así como de extintores de fuego apropiados (manuales y sistemas de supresión de incendio), alarmas de incendio y detectores de humo, los cuales deben ser inspeccionados y probados periódicamente para asegurar su uso en el momento requerido. También deben ofrecer el adiestramiento necesario al personal para garantizar su adecuada utilización.

La sala de la computadora debe estar ubicada en una zona que no se exponga a riesgo de inundaciones y, separada de las áreas adyacentes con paredes resistentes al fuego. Fuentes de energía ininterrumpida (UPS por sus siglas en inglés), controladores y reguladores de las variaciones de la electricidad son también necesarias para procurar un procesamiento continuo y adecuado de los datos.

La inversión en medidas de seguridad debe ser proporcional al efecto de perder o comprometer la información contenida en los sistemas.

C. Seguridad Lógica

El acceso a los archivos de datos y a los programas instalados en las computadoras de la entidad gubernamental sólo se permitirá al personal autorizado para garantizar la integridad y la confidencialidad de los datos. Para mantener un control adecuado, es necesario emplear y hacer buen uso de programas de seguridad, los cuales deben:

1. Limitar, de acuerdo con las funciones del personal autorizado, el acceso a: archivos de información, terminales, programas de producción, tablas de claves de acceso, utilitarios y editores en línea
2. Definir las vías de acceso autorizadas y las funciones que puede llevar a cabo una persona
3. Controlar el sistema de claves de acceso y regular el cambio periódico de las contraseñas
4. Generar informes especiales sobre la violación de la seguridad lógica, para su revisión posterior
5. Prevenir y detectar de forma automática la instalación de programas no deseados
6. Prevenir y evitar ataques accidentales o intencionales desde las redes internas hacia otros sistemas de información externos, o viceversa.

Las tablas de autorización de las contraseñas definen quién está autorizado a actualizar, modificar, eliminar o ver datos. Los usuarios deben estar autorizados expresamente por la gerencia para acceder a áreas específicas de acuerdo con sus funciones y con las normas de la institución. Los formularios de autorización (en papel o electrónicos) establecen quién debe tener acceso a qué y, deben evidenciar la aprobación a nivel gerencial.

Será política de las entidades gubernamentales utilizar la información contenida en sus sistemas computadorizados con el propósito de realizar las operaciones propias del servicio público y de garantizar la confidencialidad de ésta de acuerdo con la ley y los reglamentos aplicables.

La implementación de los programas de seguridad debe ser complementada con normas y procedimientos que requieran considerar: la seguridad de la información durante la adquisición o el desarrollo de una aplicación, y la actualización periódica de los privilegios de acceso de acuerdo con las funciones y las cesantías del personal.

D. Administración de la Seguridad

La persona que lleve a cabo la función de Administrador de Seguridad debe velar por que los usuarios estén cumpliendo con las normas de seguridad de la entidad.

Además, debe asegurarse de que los controles son adecuados para prevenir el acceso no autorizado a los datos, los programas y el equipo. Las funciones del Administrador de Seguridad generalmente incluyen:

1. Mantener las normas de acceso a los archivos y recursos
2. Mantener la seguridad y la confidencialidad de la emisión y mantenimiento de las identificaciones y contraseñas de los usuarios autorizados
3. Investigar las violaciones de seguridad y tomar acción correctiva para asegurarse de que se está proporcionando la seguridad requerida
4. Revisar y evaluar periódicamente la política de seguridad y sugerir los cambios que sean necesarios.

E. Respaldo (backups) de Archivos y de Programas

Se mantendrán respaldos actualizados de los archivos y de los programas. Esos respaldos constituyen una necesidad para procurar la continuidad de las operaciones cuando se presenten interrupciones causadas por una destrucción significativa de los archivos o de los programas. En relación con los archivos de datos, es recomendable, mantener al menos tres generaciones de respaldos. De éstas **se debe mantener, al menos, una copia almacenada en un lugar seguro fuera del edificio donde está instalada la computadora principal, y que sea una localidad que ofrezca las condiciones ambientales y de seguridad necesarias.** El acceso de personas a estos medios será restringido y controlado. La Oficina de Sistemas de Información debe mantener un itinerario de respaldo que indique el ciclo de las cintas. Los procedimientos de respaldo deben estar documentados y regulados mediante la emisión de normas y procedimientos aprobados.

F. Plan de Continuidad de Negocios

Las entidades gubernamentales deben realizar un análisis de riesgos que servirá como base para desarrollar un Plan de Continuidad de Negocios que garantice la continuidad de la operación normal de los sistemas de información computadorizado cuando se presenten eventualidades inesperadas que afecten su funcionamiento, tales como: desastres naturales, robos, fallas de equipo, virus, acceso indebido a los datos, sabotaje, entre otros.

El Plan de Continuidad de Negocios forma parte de los procedimientos para la seguridad física y operacional del equipo, de los archivos y de los sistemas de información computadorizados. El referido Plan estará constituido por un Plan para la Continuidad de las Operaciones y por un Plan para la Recuperación de Desastres que deben abarcar todo lo relacionado con la programación, el equipo, los datos y las instalaciones físicas de la Entidad gubernamental. El primer Plan se refiere a los procedimientos necesarios para prevenir los riesgos presentes, y el segundo trata sobre los procedimientos a seguir cuando sucede el evento. El Plan de Continuidad de Negocios deberá estar actualizado y aprobado por la gerencia de la entidad.

Además, se deben realizar pruebas de forma periódica, de acuerdo con la frecuencia requerida por éste.

Un Plan de Continuidad de Negocios adecuado debe proveer, entre otras cosas, lo siguiente:

1. Las responsabilidades del personal asignado al área de Sistemas de Información durante y después de ocurrida la emergencia
2. Las responsabilidades de cada empleado al momento de ponerse en ejecución el plan
3. Una relación del personal clave, sus direcciones y números de teléfono donde pueden ser localizados
4. Procedimientos de desalojo del área del Sistemas de Información con orientación al personal sobre las salidas de emergencia
5. Procedimientos para la utilización de los respaldos del equipo, de los programas, de los archivos y de la documentación.
6. Una relación con los nombres, las direcciones y los números de teléfono de proveedores de equipo, programas y materiales
7. Los arreglos con otros centros de cómputos para el procesamiento y ejecución de los programas
8. Procedimientos para mantener actualizado el Plan de Continuidad de Negocios

Los equipos computadorizados estarán cubiertos por una póliza de seguro que garantice a las entidades gubernamentales poder reemplazar los mismos en caso de daños por causas fortuitas o actos delictivos. Para disminuir el riesgo de pérdida, las instalaciones de sistemas de información deben ser ubicadas en áreas donde la probabilidad de daños por fuego, inundaciones, explosiones, disturbios civiles y otras formas de desastres sea menor.

G. Uso, Control y Disposición de los Equipos

Las entidades gubernamentales deben preparar y mantener actualizado un inventario del equipo computadorizado que incluya, entre otras cosas, lo siguiente: la descripción, el costo y la localización. En el caso de equipo arrendado se deberá indicar el nombre del arrendador. Esto con el propósito de determinar los recursos disponibles, su utilización y sus necesidades. En la **Política Núm. TIG-004** incluida en la **Carta Circular Núm. 77-05** se requiere a las entidades gubernamentales mantener actualizado el Inventario de Equipo en Línea disponible a través del portal de apoyo: *http://g2g.gobierno.pr*.

El proceso de disposición de equipo debe efectuarse de conformidad con las reglas de la Administración de Servicios Generales. Durante este proceso deben utilizarse métodos, tales como *overwriting*, *degaussing* o destrucción física del medio, para remover toda la información gubernamental grabada y garantizar la confidencialidad.

Además, se deben establecer directrices para el uso de las microcomputadoras, las cuales permitan la utilización más efectiva y productiva de éstas; que se utilicen para asuntos estrictamente oficiales, y que faciliten los procesos para restablecer la continuidad de las operaciones en caso de emergencia. Es recomendable que todos los sistemas de las entidades gubernamentales incluyan una advertencia para que el usuario se comprometa a utilizar programas con licencias debidamente autorizadas.

Es responsabilidad de la gerencia establecer normas y procedimientos para reglamentar el uso y control de las microcomputadoras. Éstos deben incluir, entre otras, directrices para lo siguiente:

1. Protección de las microcomputadoras, sus periferales y los archivos de información en caso de desastres
2. Controles automáticos para la prevención de virus de computadoras y de accesos indebidos
3. Establecimiento y cambio periódico de contraseñas de acceso
4. Autorización y utilización de equipo fuera de la entidad gubernamental
5. Producción de listas de los programas, las aplicaciones y los usuarios de cada microcomputadora
6. Listas periódicas del contenido de los archivos de las microcomputadoras, para uso de la gerencia
7. Creación de nombres uniformes para la identificación de archivos y de documentos, con el propósito de identificar su contenido fácilmente
8. Preparación de hojas de trabajo y de modelos administrativos de uso común, con el propósito de compartir los mismos con otros usuarios de microcomputadoras
9. Protección de archivos con información confidencial y de los informes relacionados con éstos, así como de la disposición de los mismos
10. Controles sobre el uso de copias no autorizadas de programas

Para fomentar el uso adecuado de los sistemas de información el Área de Tecnología de Información de la entidad gubernamental debe establecer medidas para que las políticas y los procedimientos para el uso y control de los sistemas estén accesibles a todos los empleados, y para mantener un compromiso escrito de éstos de manera que se cumplan las referidas políticas y los procedimientos.

H. Uso y Control de las Licencias de Programas

Toda programación que se desarrolle internamente es propiedad del Estado Libre Asociado de Puerto Rico y no deberá ser divulgada, copiada o utilizada sin autorización. Está prohibida la reproducción de cualquier aplicación o producto sujeto a la Ley de Derechos de Autor.

Las entidades gubernamentales utilizarán programas computadorizados (*software*) en las distintas áreas de trabajo solamente si éstos han sido legalmente adquiridos, si las licencias para su uso están vigentes y si la utilización de éstos es para tareas

relacionadas con las funciones oficiales de cada unidad de trabajo. La utilización de programas debe responder a los acuerdos establecidos en el contrato de utilización que la entidad gubernamental negoció al momento de la compra. Ningún usuario deberá utilizar en los sistemas de la entidad gubernamental productos que no estén respaldados por un contrato de utilización de programas.

Los funcionarios gubernamentales a cargo de la Tecnología de Información deberán tomar las medidas de control necesarias para evitar la instalación de programas copiados o no autorizados. Los programas copiados no incluyen garantía ni servicios de apoyo técnico, no tienen derecho a actualizaciones o aplicaciones en línea y, como consecuencia, las máquinas pueden quedar expuestas y vulnerables a ataques de virus, *spamers*[6] o *hackers*[7]. Además, los discos falsificados y sin probar pueden dañar los lectores de discos, o estar infectados y dañar el disco duro o inutilizar una red, lo que podría implicar la pérdida total de toda la información almacenada.

La gerencia de toda entidad debe poseer y controlar las licencias de uso de todos los programas instalados en sus computadoras, así como de todas las copias autorizadas que tenga de los mismos. Esto para garantizar que se honren los derechos de autor correspondientes a dichos programas. Las entidades gubernamentales deben mantener un registro de todos los programas y de los componentes adquiridos.

Durante el proceso de disposición de equipo, debe notificarse al personal encargado de las licencias sobre el uso que se les dará a éstas, y se debe actualizar el inventario de las mismas.

I. Utilización de la Internet y del Correo Electrónico

Los medios de redes de comunicaciones y las computadoras personales para acceso a los servicios de la Internet se le proveerán a aquellos funcionarios asignados a labores específicas de investigación, estudio y adiestramiento para uso estrictamente oficial dentro y fuera de Puerto Rico. De igual forma, el correo electrónico será para uso estrictamente oficial del personal autorizado. Los funcionarios principales de las entidades gubernamentales son responsables de establecer la política administrativa y los procedimientos para el uso de la Internet y del correo electrónico.

[6] El término *spam* se refiere a mensajes electrónicos (habitualmente de tipo comercial) no solicitados y en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico.

[7] El término *hacker* es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con las Tecnologías de Información y las Telecomunicaciones: programación, redes de comunicaciones, sistemas operativos, hardware de red/voz, etc.

Las políticas administrativas y los procedimientos sobre el uso de la Internet deben incluir, entre otras cosas, lo siguiente:

1. Los usos permitidos y los no permitidos.
2. La descripción de los funcionarios autorizados a utilizar los servicios.
3. Las medidas disciplinarias que se adoptarán en caso del uso inaceptable de los servicios.
4. La obligación de los usuarios de respetar los derechos de propiedad intelectual de las obras, de los programas, y de las aplicaciones a los cuales se acceda a través de la Internet.
5. El derecho de la entidad gubernamental a intervenir y auditar los accesos a la Internet realizados por los usuarios a través del sistema de información de la entidad gubernamental.

Todo usuario será responsable de sus acciones y de su conducta al acceder a la Internet. Se debe tener siempre presente que la Internet es un conjunto de redes de computadoras, por lo que su uso debe estar conforme a las normas establecidas por los diferentes administradores de éstas. Bajo ninguna circunstancia se realizarán actos que puedan considerarse ilegales, inmorales u ofensivos. Es responsabilidad de la gerencia supervisar rigurosamente el uso de las computadoras personales, así como la información y los documentos que se procesan en ellas.

Las políticas administrativas y los procedimientos sobre el uso del correo electrónico deben incluir, entre otras cosas, lo siguiente:

1. Uso sólo para asuntos oficiales.
2. Derecho de la entidad gubernamental a intervenir y auditar el uso del correo electrónico.
3. Normas relacionadas con el envío de información confidencial de la entidad gubernamental.
4. Medidas de seguridad sobre las cuentas de correo electrónico tales como códigos de acceso, contraseñas, normas de seguridad configuradas en el servidor, uso de sistemas de auditoría, y medidas de seguridad para el envío de información.

Las entidades gubernamentales deben cumplir con la **Política Núm. TIG-008** incluida en la **Carta Circular Núm. 77-05** relacionada con el uso de la Internet y del correo electrónico. Aquellas entidades que no vengan obligadas a regirse por la **Carta Circular Núm. 77-05**, deben contar con normas equivalentes que incluyan todos los aspectos mencionados en esta publicación y, cualquier otro que sea necesario en su caso particular.

HALLAZGOS MÁS COMUNES SEGÚN LAS AUDITORÍAS REALIZADAS POR LA OFICINA DEL CONTRALOR DE PUERTO RICO

A. Adquisición

1. Inversión realizada en equipos, programas y servicios profesionales, sin haber logrado los objetivos.
2. Contratación y adquisición del equipo computadorizado y de los servicios para el desarrollo e implantación del Sistema, sin haber sometido previamente a la evaluación y aprobación de la OGP el correspondiente Plan de Tecnología.
3. Falta de estudios previos y de un Plan de Tecnología, antes de solicitar propuestas para el desarrollo e implantación de un Sistema Computadorizado.
4. Adquisición de equipos y de servicios mediante contrato de arrendamiento con opción a compra, sin la celebración de subasta formal, y otras deficiencias relacionadas con el proceso llevado a cabo al contratar dicho arrendamiento.
5. Falta de información detallada en la solicitud de propuestas y contrato otorgado sin especificar en detalle los trabajos a realizar para la implantación del Plan de Tecnología de Información.
6. Subasta no adjudicada al mejor postor, adquisición de equipos sin celebrar subasta y sin solicitar cotizaciones, y otras faltas relacionadas.
7. Inversión de fondos para adquirir sistemas computadorizados cuyos componentes no se utilizaban en su totalidad ni se habían instalado completamente.
8. Adquisición de equipos de computadoras para el Sistema, que no se utilizaban.
9. Microcomputadoras almacenadas sin haberse considerado un uso alterno.
10. Falta de un estudio de necesidades para los equipos y los programas computadorizados adquiridos.
11. Falta de estudios previos y de un Plan de Tecnología, antes de solicitar propuestas para el desarrollo e implantación de un sistema computadorizado.
12. Programas y equipos sin uso.

B. Implantación

1. Atrasos en la implantación del Sistema y otras deficiencias relacionadas.
2. Deficiencias en la implantación del Sistema.
3. Falta de documentación de las aplicaciones desarrolladas.

4. Deficiencias relacionadas con la documentación de la Aplicación.
5. Documentación de la aplicación sin actualizar.
6. Falta de fiscalización de los procedimientos, de los controles y del funcionamiento de los sistemas de información.
7. Ausencia de auditorías internas de las operaciones de los centros de cómputos y, de los sistemas de información.
8. Falta de participación de los representantes de la entidad gubernamental en la evaluación de los procedimientos, de los controles y del funcionamiento del centro externo donde operan sus sistemas.
9. Deficiencias relacionadas con la documentación topológica de las instalaciones de la red de comunicaciones.
10. Instalaciones, modificaciones y configuraciones realizadas a los servidores de la red sin documentar, y sistema operativo del servidor principal que no tenía instalada la versión mínima requerida.
11. Falta de actualización del diagrama de la red de comunicación.

C. Contratos

1. Inversión en contratos de servicios profesionales y consultivos y en programas computadorizados, sin haber logrado los objetivos.
2. Deficiencias relacionadas con la contratación de servicios profesionales y con la adquisición de equipos para el desarrollo e implantación de un sistema de información.
3. Contratos con fechas retroactivas, incumplimiento de la Ley sobre el Registro de Contratos, falta de cláusulas importantes en los contratos de servicios y otras faltas relacionadas.
4. Uso de la Resolución de Reconocimiento de Deuda para el pago de servicios profesionales, e incumplimiento de la ley sobre el Registro de Contratos.
5. Contratos radicados tardíamente en la Oficina del Contralor de Puerto Rico.
6. Adquisición de equipo de computadoras mediante contrato de arrendamiento, sin obtener el asesoramiento requerido del Banco Gubernamental de Fomento para Puerto Rico.
7. Falta de cláusulas importantes y de certificaciones de los contratistas en los contratos de servicios relacionados.
8. Deficiencias en la formalización y en la administración de los contratos de servicios profesionales y consultivos.
9. Documentos no presentados para examen, pagos por tareas no relacionadas con las establecidas en el contrato de servicios profesionales

y consultivos, errores en el pago de una factura, tareas no detalladas en las facturas y atrasos en la presentación de las facturas.

10. Ausencia de cotizaciones para otorgar un contrato y deficiencias relacionadas con la administración de contratos de servicios profesionales y consultivos.
11. Costos adicionales a lo estipulado en un contrato, reembolso de gastos sin justificantes, pagos por tareas no contratadas y pagos sin retención de contribución sobre ingresos.
12. Subcontratista que prestó servicios sin estar incluido en la propuesta de la compañía contratada para el desarrollo e implantación del Sistema.
13. Contratación de servicios profesionales y consultivos con características propias de puestos regulares.
14. Posible conflicto de intereses en contratos con una firma de consultoría.

D. Procedimientos de Control de los Sistemas

1. Falta de normas de seguridad y de un manual de normas y procedimientos operacionales del centro.
2. Procedimientos de las operaciones del Centro, incompletos y sin actualizar.
3. Manual de procedimientos para regir las operaciones del centro, sin estar aprobado.
4. Falta de procedimientos para la documentación de las aplicaciones.
5. Falta de procedimientos escritos para el registro y el análisis de los datos en los sistemas de información.
6. Falta de procedimientos escritos y de controles adecuados para el manejo y la distribución de los informes.
7. Normas y procedimientos importantes no incluidos en la reglamentación aprobada para la seguridad y el uso de los sistemas de información computadorizados.
8. Ausencia de normas para establecer los parámetros de seguridad en el computador principal y para controlar las actualizaciones de las bases de datos.
9. Falta de normas y de procedimientos escritos para administrar, utilizar y modificar la red de comunicación, de un diagrama de sus componentes, y de la documentación necesaria sobre los cambios efectuados a la misma.
10. Falta de normas y de procedimientos para proteger los archivos con información confidencial procesada en las microcomputadoras.
11. Normas para reglamentar el uso de la Internet y del correo electrónico sin distribuir al personal que utiliza dichos servicios.

12. Ausencia de normas y de procedimientos para reglamentar el uso de las microcomputadoras y el acceso a la Internet.
13. Ausencia de normas para regir los procedimientos relacionados con el uso y el control de las piezas de microcomputadoras que se utilizaban como reemplazos.
14. Deficiencias en los procedimientos para preparar, custodiar y almacenar las cintas magnéticas.

E. Seguridad Física

1. Ausencia de un programa de adiestramiento sobre la seguridad de la información.
2. Seguridad física inadecuada del equipo computadorizado.
3. Controles de acceso al Centro inadecuados.
4. Falta de control sobre el acceso al área de la computadora central del Sistema.
5. Fallas de seguridad en el salón donde están localizadas las computadoras principales.
6. Seguridad física inadecuada en el área de la computadora del Sistema.
7. Medidas de seguridad inadecuadas en el área de la computadora del Sistema.
8. Falta de equipo para detectar y extinguir incendios.
9. Deficiencias relacionadas con la seguridad y con el acceso físico a las instalaciones de la red de comunicaciones.
10. Falta de seguridad en el área de los servidores.

F. Seguridad Lógica

1. Acceso a archivos del sistema de información, concedido indebidamente a consultores.
2. Control inefectivo de los códigos de acceso al Sistema.
3. Falta de actualización de los formularios de solicitud de acceso al sistema.
4. Fallas en los controles de acceso y en la asignación de niveles de seguridad de los sistemas.
5. Configuración inadecuada de los privilegios de acceso lógico y, de las propiedades de los archivos y de los directorios de la red de comunicación local.
6. Deficiencias en los parámetros de seguridad y en los controles de acceso lógico de los servidores de la red de comunicación.

G. Producción y Revisión de los Registros del Sistema

1. Falta de un registro computadorizado para el control de las operaciones diarias.
2. Falta de revisiones de las bitácoras o registros computadorizados de los sistemas.
3. Deficiencias relacionadas con las revisiones periódicas de la capacidad y el funcionamiento de la red y, con el registro de los eventos de los servidores principales.
4. Falta de monitoreo de las líneas de comunicación de la red.

H. Respaldo de Archivos, Programas y Equipo

1. Deficiencias relacionadas con la preparación, la custodia y el almacenamiento de las copias de reserva.
2. Fallas de control de las reservas de los archivos y de los programas.
3. Falta de resguardos de archivos, programas y datos fuera del Centro.
4. Falta de producción de un inventario de las cintas y cartuchos de resguardo y, de un registro sobre el uso de éstos.
5. Falta de equipo de reserva para casos de emergencia.
6. Falta de acuerdos por escrito para mantener un Centro Alterno de recuperación de sistemas de información.
7. Fallas relacionadas con el equipo de reserva.

I. Plan de Contingencia

1. Necesidad de establecer un plan de contingencias.
2. Plan de Contingencias sin actualizar.
3. Deficiencias relacionadas con el Plan de Recuperación de Desastres y, con los correspondientes procedimientos y documentos operacionales.
4. Fallas en el Plan de Contingencias.
5. Falta de aprobación de un Plan de Contingencias.

J. Uso y Control de los Equipos

1. Necesidad de adiestramiento sobre el uso y la seguridad de los sistemas computadorizados.
2. Falta de un contrato de mantenimiento preventivo para el equipo computadorizado.
3. Falta de información en los formularios de solicitud de servicio.
4. Falta de registros para los servicios de apoyo al Sistema.
5. Microcomputadoras utilizadas para fines ajenos a la gestión pública, y falta de controles para prevenir y detectar la instalación de programas no autorizados o la remoción de programas ya instalados.
6. Deficiencias en los recibos de la propiedad emitidos para los equipos computadorizados, y en la localización física según inventario de los equipos.
7. Falta de actualización y deficiencias de control en el inventario de equipos computadorizados.
8. Equipo de computadoras dañado, obsoleto o sin uso alterno.
9. Faltas por no informar la desaparición de equipo a la Oficina del Contralor de Puerto Rico.
10. Desaparición de propiedad informada tardíamente a la Oficina del Contralor de Puerto Rico.
11. Incumplimiento de disposiciones sobre desaparición de propiedad.

K. Uso y Control de las Licencias de Programas

1. Ausencia de un registro de los programas instalados en cada microcomputadora.
2. Falta de controles relacionada con los programas de computadoras, las licencias y la documentación de las aplicaciones.
3. Inventario de programas y aplicaciones sin actualizar.
4. Programas instalados en las microcomputadoras sin las licencias de uso.

L. Uso de la Internet

1. Microcomputadoras y cuentas para acceder a la Internet utilizadas para fines ajenos a la gestión pública.
2. Fallas de controles relacionadas con los códigos de acceso a la Internet.

M. Mantenimiento y Control de las Aplicaciones

1. Errores e información incompleta y no actualizada en los archivos del Sistema..
2. Deficiencias relacionadas con el Archivo Maestro del Sistema.
3. Récords duplicados en los archivos computadorizados del Sistema.
4. Atrasos en el proceso de registro de datos, y falta de controles internos efectivos para agilizar dicho proceso
5. Deficiencias relacionadas con la validación y el procesamiento de los datos registrados en el sistema.
6. Atrasos en el procesamiento de transacciones.
7. Faltas de control en la actualización de la base de datos de la aplicación.
8. Falta de un registro histórico de las transacciones diarias procesadas mediante el Sistema.
9. Uso limitado del Sistema.
10. Deficiencias en la producción, verificación y distribución de los informes producidos por el Sistema.

REFERENCIAS

Para obtener información adicional relacionada con los temas discutidos en este folleto informativo puede referirse a las siguientes páginas electrónicas en la Internet:

http://www.ogp.gobierno.pr

http://www.g2g.gobierno.pr

http://www.w3c.org/WAI

http://www.bsa.org

http://www.gsa.gov/itpolicy

http://www.gao.gov

http://www.whitehouse.gov/OMB/inforeg/index.html

http://www.section508.gov

http://www.isaca.org

NORMAS DE CONDUCTA SUGERIDAS POR LA OFICINA DEL CONTRALOR PARA REGIR LA RELACIÓN CON LOS PROVEEDORES

El personal encargado de la adquisición y de la contratación de la tecnología de información debe actuar siempre correctamente al administrar la propiedad y los fondos públicos. Esa exigencia de corrección en la conducta de todo servidor público se extiende al ámbito de la apariencia. Una impresión equivocada no solamente puede manchar el buen nombre de una persona noble y digna, sino el de su entidad gubernamental y el de sus compañeros de trabajo. Esta Oficina emitió el 19 de junio de 1998, el **Memorando OCP-98-440** en el cual se establecen las normas de conducta que deben exhibir el personal de compras de la Oficina del Contralor y los proveedores, así como la relación que debe existir entre éstos. La adopción de éstas o de cualesquiera otras normas que promuevan la ética en el trabajo y que propendan a mantener una sana administración pública es recomendable. Consideremos que estas normas ayudan a promover el uso más efectivo y eficiente de los recursos del Gobierno, en beneficio de nuestro pueblo.

Las normas de conducta sugeridas para el personal a cargo de la adquisición y de la contratación de la tecnología de información son las siguientes:

A. Adoptar un trato profesional y respetuoso hacia todos los proveedores, y exigir lo mismo de éstos en todo momento.

B. Divulgar toda la información necesaria para que los proveedores puedan emitir un juicio informado.

C. Proveer iguales términos y condiciones a todos los proveedores.

D. Utilizar los mismos criterios para evaluar los productos o los servicios.

E. Rechazar gratificaciones, privilegios o favores.

F. Procesar los pagos con prontitud.

G. Cumplir con todas las leyes y los reglamentos aplicables a la adquisición y a la contratación de tecnología de información.

H. No intervenir en asuntos en los que tiene interés personal o económico, o en asuntos que puedan provocar un conflicto de intereses o la apariencia de tal conflicto.

Las normas de conducta sugeridas para el proveedor son las siguientes:

A. Cumplir con las normas de ética establecidas por la empresa para la cual trabajan.

B. Exhibir un trato profesional y respetuoso.

C. Cotizar a base de precios justos.

D. Ofrecer productos y servicios de calidad.

E. Entregar los productos y servicios antes de la fecha límite.

F. Honrar las garantías ofrecidas para los productos y servicios.

G. Rehusar trato preferencial o discriminatorio.

H. Abstenerse de ofrecer gratificaciones, privilegios o favores.

I. Rechazar solicitudes de gratificaciones, privilegios o favores.

J. Notificar al funcionario de mayor jerarquía de la entidad gubernamental cualquier conducta impropia de parte del personal de la entidad y de cualquier fuente, inclusive posibles conflictos de intereses de servidores públicos y competidores.

K. Colaborar con los auditores en las investigaciones.

L. Incluir en su factura la siguiente certificación:

> **Ningún servidor público de (Entidad Gubernamental) es parte o tiene algún interés en las ganancias o beneficios producto del contrato objeto de esta factura y de ser parte o tener interés en las ganancias o beneficios producto del contrato, ha mediado una dispensa. La única consideración para suministrar los bienes o servicios objeto del contrato ha sido el pago acordado con el representante autorizado de la entidad gubernamental. El importe de esta factura es justo y correcto. Los productos han sido entregados (los servicios prestados) y no han sido pagados.**

M. Además, en toda orden de compra emitida deberá incluirse en forma impresa lo siguiente:

> **Se emite esta orden de compra con el entendimiento de que el (la) proveedor (a) ha cumplido o cumplirá con las normas emitidas por (Entidad Gubernamental), las cuales le fueron suministradas mediante (documento por el cual se establecen las normas)**.

DISPOSICIONES LEGALES RELEVANTES

Incluimos una lista de algunas disposiciones legales las cuales consideramos que pueden ser relevantes o de aplicación dentro del contexto del proceso de adquisición y utilización de la tecnología de información. La misma debe utilizarse como referencia y no constituye la totalidad de las disposiciones que regulan dicho proceso. Las corporaciones públicas deben estar atentas a sus leyes habilitadoras y a la reglamentación aplicable.

A. Constitución del Estado Libre Asociado de Puerto Rico

1. **Artículo VI, Sección 9** - Establece que sólo se dispondrá de las propiedades y de los fondos públicos para fines públicos y para el sostenimiento y funcionamiento de las instituciones del Estado y, en todo caso, por autoridad de ley (1 L.P.R.A. §9).

2. **Artículo VI, Sección 16** - Dispone que todos los funcionarios y los empleados del Estado Libre Asociado, sus agencias, instrumentalidades y subdivisiones políticas prestarán, antes de asumir las funciones de sus cargos, juramento de fidelidad a la Constitución de los Estados Unidos de América y a la Constitución y a las leyes del Estado Libre Asociado de Puerto Rico (1 L.P.R.A. §16).

B. Leyes

1. **Ley Núm. 96 de 15 de julio de 1988**, según enmendada, **Ley de Propiedad Intelectual** - Esta **Ley** ofrece protección al autor de una obra literaria, científica, artística y/o musical, el cual tiene el derecho de beneficiarse de ella y las prerrogativas exclusivas de atribuirse o retractar su autoría, disponer de su obra, autorizar su publicación y proteger su integridad. Establece, además, la creación de un registro de las obras. (31 L.P.R.A. §401)

2. **Ley Núm. 81 de 30 de agosto de 1991**, según enmendada, **Ley de Municipios Autónomos del Estado Libre Asociado de Puerto Rico de 1991** - En su **Artículo 8.010** dispone que el Comisionado, en coordinación con los municipios, será responsable de diseñar o aprobar la organización fiscal, el sistema uniforme de contabilidad computadorizado y los procedimientos de pagos, de ingresos y de propiedad de todos los municipios de conformidad con los principios de contabilidad generalmente aceptados. (21 L.P.R.A. §4360)

3. **Ley Núm. 259 de 29 de diciembre de 1995**, **Bonos, Sistemas de Informática Electrónica** - Esta **Ley** provee para el diseño, la adquisición y la actualización de los sistemas computadorizados. (23 L.P.R.A. §111)

4. **Ley Núm. 265 de 3 de septiembre de 2003, Ley para Reglamentar Ciertos Contratos Gubernamentales de Financiamiento y Arrendamiento de Bienes Muebles** - Esta **Ley** establece un mecanismo para darle mayor control al Banco Gubernamental de Fomento para Puerto Rico sobre el otorgamiento de contratos de arrendamiento financiero, y sobre otros tipos de contratos análogos relacionados con bienes muebles, los cuales comprometen los recursos futuros de dichas entidades gubernamentales. (3 L.P.R.A. §8161)

5. **Ley Núm. 229 de 2 de septiembre de 2003, Ley para garantizar el acceso de Información a las Personas con Impedimentos** - Esta **Ley** establece que las personas con impedimentos tendrán derecho de tener acceso pleno a la información y hacer uso de los servicios que ofrece el Gobierno del Estado Libre Asociado de Puerto Rico, a través de las páginas electrónicas de las entidades del Estado. A tales fines, se adopta una política pública dirigida a garantizar que todas las agencias, corporaciones públicas e instrumentalidades públicas del Estado cumplan con dichos propósitos. (3 L.P.R.A. §8310)

6. **Ley Núm. 151 de 22 de junio de 2004**, **Ley de Gobierno Electrónico** - Dispone que la Oficina de Gerencia y Presupuesto tendrá facultad para instrumentar y emitir la política pública a seguir y las normas que regirán la adquisición e implantación de los sistemas, equipos y programas de información tecnológica para los organismos gubernamentales, con el objetivo primordial de lograr la interconexión de los organismos, para así facilitar y agilizar los servicios del pueblo. (3 L.P.R.A. §991)

C. Reglamentos

1. **Reglamento 5518 del 27 de noviembre de 1996**, emitido por la Oficina del Comisionado de Asuntos Municipales, trata sobre la implantación del sistema mecanizado

2. **Reglamento 5859 del 17 de septiembre de 1998**, emitido por la Oficina del Comisionado de Asuntos Municipales, trata sobre la dispensa del Sistema Uniforme de Contabilidad Computadorizado Municipal

D. Órdenes Ejecutivas

1. **Boletín Administrativo Núm. OE-2003-45 del 30 de junio de 2003** - Mediante esta **Orden** se crea el Programa de Gobierno Electrónico, adscrito a la OGP, desde el cual se administrarán los sistemas de información y se implantarán las normas y procedimientos, a tenor con la legislación vigente. La misma también dispone que las agencias e instrumentalidades del Gobierno deberán desplegar una página electrónica que contenga la información necesaria para que todo ciudadano pueda conocer los servicios que se ofrecen.

E. Cartas Circulares y Memorandos

1. Oficina del Contralor de Puerto Rico

    a. **Carta Circular Núm. OC-98-11 del 18 de mayo de 1998** - Establece sugerencias sobre normas y controles para el uso de los sistemas computadorizados.

    b. **Carta Circular Núm. OC-2002-02 del 16 de agosto de 2001** - Hace referencia a la **Carta Circular Núm. OC-98-11** y establece la necesidad de advertir al usuario, en la pantalla inicial del sistema, sobre las normas principales para el uso del mismo.

2. Oficina de Gerencia y Presupuesto

    a. **Carta Circular Núm. 77-05 del 8 de diciembre de 2004** - Dispone las normas fundamentales que deben seguir las entidades gubernamentales al establecer sus controles y procedimientos

internos, de manera que se garantice la adquisición y el uso adecuado, efectivo y seguro de los sistemas de información, así como la confidencialidad de la información. Dicha **Carta Circular** se acompaña con las siguientes 12 Políticas para la Adquisición e Implantación de los Sistemas, Equipos y Programas de Información Tecnológica:

1) Política TIG-001 - Aprobación de Proyectos de Tecnología
2) Política TIG-002 - Desarrollo y Mantenimiento de Sitios Web Agenciales (Websites)
3) Política TIG-003 - Seguridad de los Sistemas de Información
4) Política TIG-004 - Servicios de Tecnología
5) Política TIG-005 - Notificación de Proyectos de Tecnología
6) Política TIG-006 - Desarrollo, Integración y Publicación de Transacciones Electrónicas Gubernamentales
7) Política TIG-007 - Disposición de Equipo y Licencias
8) Política TIG-008 - Uso de Sistemas de Información, de la Internet y del Correo Electrónico
9) Política TIG-009 - Integración de Sistemas Financieros
10) Política TIG-010 - Adquisición de Equipo para Sistemas Computadorizados de Información
11) Política TIG-011 - Mejores prácticas de Infraestructura Tecnológica
12) Política TIG-012 - Plan de Tecnologías

b. **Memorando General Núm. 338-04 del 28 de agosto de 2003** – Establece la importancia de que las entidades gubernamentales utilicen el programa de antivirus y que actualicen el mismo. También advierte la facultad de la OGP para suspender el servicio de Internet a aquellas entidades gubernamentales que no cumplan con lo dispuesto en este **Memorando**.

F. Leyes Federales

Copyright Law - 17 USCA, §101 y ss.

Le invitamos a que visite nuestra página de la Internet o que se comunique con nuestra Oficina para orientación e información adicional.

Dirección postal:	*Oficina del Contralor de Puerto Rico* *Área de Estrategias Contra la Corrupción* *PO Box 366069* *San Juan, Puerto Rico 00936-6069*
Dirección física:	*Oficina del Contralor de Puerto Rico* *Ave. Ponce de León 105* *Esq. Calle Pepe Díaz* *Hato Rey, Puerto Rico*
Fax:	*(787) 756-0931*
Teléfono:	*(787) 250-3316, 754-3030 ext. 2750*
Página en la Internet:	*http://www.ocpr.gov.pr*
Correo electrónico:	*ocpr@ocpr.gov.pr*