2010

Reglamento para Usuarios Que manejan Sistemas de Tecnología de Información V2.0

Autoridad del Distrito del Centro de Convenciones de Puerto Rico
08/19/2010

Tabla de Contenido

Índice

Reglamento para Usuarios que manejan Sistemas de Tecnología de Información

ARTICULO 1 - TITULO

Este Reglamento se conocerá como el Reglamento para la Administración de Sistemas de Tecnología de Información de la Autoridad del Distrito del Centro de Convenciones (el "Reglamento").

ARTÍCULO 2 – BASE LEGAL

Este Reglamento se promulga en virtud de lo dispuesto en el Artículo 1.05 de la Ley Núm. 351 de 2 de septiembre de 2000, según enmendada, que crea la Autoridad del Distrito del Centro de Convenciones de Puerto Rico.

ARTÍCULO 3 – PROPÓSITO

El propósito de este Reglamento es establecer las políticas, normas y guías para la administración y el manejo de los sistemas de Tecnología de Información de la Autoridad, estableciendo controles internos en el uso de tales sistemas a los fines de proteger tanto la información que se genera, procesa o conserva en los mismos como los equipos y evitar con ello un manejo indebido de los mismos, bien sea por actos intencionales o accidentales.

ARTÍCULO 4 – INTRODUCCIÓN

Es necesario proteger todo tipo de información, particularmente la producida, guardada y transmitida en forma electrónica por sistemas de computadoras. Los controles de seguridad deben existir para minimizar la vulnerabilidad de la información y el daño a los equipos.

De no existir una seguridad adecuada estaríamos expuestos a:

A. Daños a equipos sofisticados que son propiedad del pueblo Puerto Rico, y, por consiguiente, la pérdida de dinero.

B. Daños a la reputación de la Autoridad del Distrito del Centro de Convenciones y al Gobierno de Puerto Rico.

C. Divulgación de información confidencial (accidental o intencional).

D. Uso indebido de los sistemas de computadoras.

E. Demandas por violación a la confidencialidad y privacidad.

F. Infección o entrada a los sistemas de virus, gusanos, "Spyware", "Adwares", "Hijacker", o personas no autorizadas (Internos o Externos).

Los usuarios de los Sistemas de Tecnología de Información de la Autoridad, deben seguir los cuatro principios básicos que se indican a continuación:

A. Como responsables de los equipos de sistemas de Tecnología de Información que nos son asignados para realizar nuestras tareas, debemos proveer protección a los equipos, programas y la información de las computadoras.

B. Como usuarios tenemos la responsabilidad de controlar esencialmente el uso de las computadoras y proteger las aplicaciones técnicas de la Administración, procesamiento de datos, modelos de hojas de trabajo electrónicas y programas computadorizados.

C. Como desarrolladores debemos incorporar los controles adecuados para la protección de los sistemas de computadoras.

D. Todo sistema de computadoras de Tecnología de Información y los servicios asociados tanto internos como externos, el sistema de correspondencia electrónica ("e-mail"), el Intranet o Portal y redes, el acceso a la Internet, los documentos y programas que existen en la misma, son propiedad de la Autoridad y del Gobierno de Puerto Rico; solo podrán utilizarse para propósitos lícitos, prudentes, responsables y dentro de las funciones o poderes de la Autoridad.

ARTÍCULO 5 – APLICABILIDAD

El Reglamento aplica a todo usuario de los sistemas de Tecnología de Información que le dan servicio a la Autoridad, como por ejemplo y que se entienda como una limitación, a los funcionarios y empleados de la Autoridad, funcionarios y empleados de la Compañía de Turismo de Puerto Rico, y/o empleados de otras agencias del Gobierno de Puerto Rico en asignación administrativa o especial en la Autoridad, consultores contratados, auditores de la Oficina del Contralor de Puerto Rico, auditores externos, y los proveedores de servicios profesionales.

ARTICULO 6 – DEFINICIONES

A los fines del presente Reglamento las siguientes palabras, frases o términos tendrán el significado que se detalla a continuación:

A. Ambiente – Área de la computadora designada para un uso específico. Para aplicaciones de computadoras que requieren desarrollo de código se deben establecer tres ambientes; desarrollo, prueba y producción. Para aplicaciones de tipo paquete (packaged software) sobre las que no se hace desarrollo de código y para otros tipos de aplicaciones, tales como telecomunicaciones, se pueden tener dos ambientes, el de prueba y el de producción. Es preferible, pero no obligatorio, tener los ambientes instalados en computadoras separadas.

B. Ambiente de desarrollo - Se utilizará para que los desarrolladores hagan cambios de programación, desarrollen código nuevo y hagan sus pruebas preliminares.

C. Ambiente de prueba – Se utilizará para emular el nuevo ambiente de producción. Aquí podrán hacerse las pruebas de aceptación de usuario y dar adiestramiento a estos.

D. Ambiente de producción – Es el ambiente para uso oficial. Aquí se llevan a cabo las funciones diarias y operacionales de la Autoridad. No se usa para propósitos de prueba o desarrollo. Cualquier cambio, entrada o eliminación de información afecta los archivos reales de la Autoridad.

E. Aplicación – Es el uso específico que se le da a una programación a través de una computadora. Algunos ejemplos de aplicaciones son las que manejan el archivo de asistencia, nóminas, las cuentas por pagar, compras, presupuesto, entre otros.

F. Autoridad – La Autoridad del Distrito del Centro de Convenciones de Puerto Rico.

G. Backup o Copia de Seguridad/Resguardo - Una copia de seguridad, resguardo o backup en informática es un archivo digital, un conjunto de archivos o la totalidad de los datos considerados lo suficientemente importantes para ser conservados. Fundamentalmente son útiles para dos cosas. Primero, recuperarse de una catástrofe informática. Segundo, recuperar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente o corrompido.

H. Banco/Base de Datos – Un banco o base de datos es una organización electrónica de datos e información. El banco de datos implica la integración de la información a través del ambiente en el cual se utiliza.

I. CD - El disco compacto (conocido popularmente como **CD** por las siglas en inglés de *Compact Disc*) es un soporte digital óptico utilizado para almacenar cualquier tipo de información (audio, imágenes, vídeo, documentos y otros datos). Hoy en día, sigue siendo el medio físico preferido para la distribución de audio. Esta tecnología fue más tarde expandida y adaptada para el almacenamiento de datos (CD-ROM), de video (VCD y SVCD), la grabación doméstica (CD-R y CD-RW) y el almacenamiento de datos mixtos (CD-i), Photo CD y CD EXTRA.

J. Contraseña – Una **contraseña** (en inglés ***password***) es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña normalmente debe mantenerse en secreto ante aquellos a quien no se les permite el acceso. Aquellos que desean acceder a la información se les solicita una contraseña; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.

K. Computadora Personal o "PC" – Es aquella computadora (ya sea estilo torre, de escritorio o portátil) la cual ha sido adquirida por la Autoridad y asignada a un usuario con el propósito de mejorar su ambiente de trabajo, mecanizar funciones y procesar información oficial en las mismas.

L. Desktop o Computadora de escritorio - Es una computadora personal que diseñada para ser usada en una ubicación estable, como un escritorio (como su nombre indica), a diferencia de otros equipos personales como las computadoras portátiles. Es la herramienta de trabajo por excelencia; se trata de un elemento muy importante para la marcha de un negocio. El uso que se hace de las computadoras de escritorio está relacionado normalmente con las tareas productivas y administrativas de los empleados: creación de informes, presentaciones, memorandos, comunicación con otras empresas, contabilidad, gestión de tareas, etc.; por este motivo, la computadora de escritorio debe ser adecuadamente gestionada en el ámbito empresarial.

M. Director – El Director Ejecutivo de la Autoridad del Distrito del Centro de Convenciones de Puerto Rico.

N. DVD - Digital Video Disc (‘disco de video digital’), es un dispositivo de almacenamiento óptico. El nombre de este dispositivo hace referencia a la multitud de maneras en las que se almacenan los datos. Los DVD se pueden clasificar:

a. Según su contenido:
   - DVD-Video: Películas (vídeo y audio).
   - DVD-Audio: Audio de alta fidelidad.
   - DVD-Data: Todo tipo de datos.

b. Según su capacidad de regrabado:
   - DVD-ROM: Sólo lectura, manufacturado con prensa.
   - DVD-R y DVD+R: Grabable una sola vez. La diferencia entre los tipos +R y -R radica en la forma de grabación y de codificación de la información. En los +R los agujeros son 1 lógicos mientras que en los –R los agujeros son 0 lógicos.
   - DVD-RW y DVD+RW: Regrabable.
   - DVD-RAM: Regrabable de acceso aleatorio. Lleva a cabo una comprobación de la integridad de los datos siempre activa tras completar la escritura.
   - DVD+R DL: Grabable una sola vez de doble capa.
   - El DVD-ROM almacena desde 4,7 GB hasta 17 GB.

O. Drive o unidad de disco - En informática, el término unidad de disco se refiere a aquel dispositivo o aparato que realiza las operaciones de lectura y escritura de los medios o soportes de almacenamiento con forma de disco, refiriéndose a las unidades de disco duro, unidades de discos flexibles (disquetes: 5¼", 3½"), unidades de discos ópticos (CD, DVD, HD DVD o Blu-ray) o unidades de discos magneto-ópticos (discos Zip, discos Jaz, SuperDisk).

P. Jump Drive o USB de Memoria - Una memoria USB (de *Universal Serial Bus*; en inglés *pen drive*, *USB flash drive*) es un dispositivo de almacenamiento que utiliza memoria flash para guardar la información que puede requerir y no necesita baterías. Estas memorias son resistentes a los rasguños (externos), al polvo, y algunos al agua que han afectado a las formas previas de almacenamiento portátil, como los disquetes, discos compactos y los DVD.

Q. Notebook o Computador Portátil - Un computador portátil u ordenador portátil es una computadora personal móvil, que pesa normalmente entre 1 y 3 kg. Las computadoras portátiles son capaces de realizar la mayor parte de las tareas que realizan las computadoras de escritorio, con la ventaja de que son más pequeñas, más livianas y tienen la capacidad de operar por un período determinado sin estar conectadas a la electricidad. Su gran ventaja reside en la movilidad que los mismos permiten, ya que es posible llevarlos a donde se desee. Las computadoras portátiles también pueden realizar las mismas funciones que cualquier otra computadora.

R. Persona a cargo de un programa de aplicación de sistema– Es el usuario principal de la aplicación y es quien determina que información se incluye para que la aplicación ejecute.

S. Ejecución – Procesamiento de una transacción o grupo de transacciones en conjunto.

T. Nivel de Seguridad o de Acceso – Es el tipo de acceso que el usuario podrá tener a los recursos. Los niveles de acceso más utilizados son: LEER, ACTUALIZAR, CREAR, ELIMINAR.

U. Concienciar ("Awareness") – Es un programa de orientación el cual se ofrece periódicamente a todos los usuarios en todos los niveles. En este programa se resalta la importancia de mantener medidas de control adecuadas al utilizar la información. También se discute la política pública sobre Seguridad de Información y las reglamentaciones que nos exigen estos controles, así como el efecto que tendrá el no cumplir con ellos.

V. Recursos – Son las diferentes estructuras o formas de organización electrónicas a través de las cuales se puede almacenar información o accederla utilizando una computadora. Los recursos más conocidos son: TRANSACCIONES, PROGRAMAS, DATA-SET, LIBRERIAS, DISCOS, "STORAGE".

W. Virus – Es un programa que se copia automáticamente y que tiene por objeto alterar el funcionamiento normal de la computadora, sin permiso o con el consentimiento del usuario. Los virus son programas que se replican y ejecutan por sí mismos. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una PC, aunque existen también otros más benignos, que solo se caracterizan por ser molestos. Los virus informáticos tienen, básicamente, la función de propagarse replicándose, pero algunos contienen una carga dañina ('payload") con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas o bloquear las redes informáticas generando tráfico inútil. El funcionamiento de un virus informático es conceptualmente simple. Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario. El código del virus queda residente (alojado) en la memoria "RAM" de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse. El virus toma el control de los servicios básicos del sistema operativo, infectando de manera posterior, archivos ejecutables que sean llamados para ejecución. Finalmente se añade el código del virus al del programa infectado y se graba en disco, con lo cual el proceso de replicado se completa.

X. "Spywares" - Los "Spywares" tienen cierta similitud con los virus pero a diferencia de estos los "Spywares" no tienen código dañino para la PC, por lo tanto los antivirus comunes no lo pueden reconocer ni eliminar. Los "Spywares" son pequeños programas que se instalan en nuestro sistema con la finalidad de robar nuestros datos y espiar nuestros movimientos por la red. Luego envían esa información a compañías de publicidad de internet para comercializar con nuestros datos. Trabajan a modo de "background" (segundo plano) para que no nos percatemos de que están hasta que empiecen a aparecer los primeros síntomas.

Y. Gusanos o "Worms" – Los gusanos son programas que constantemente viajan a través de un sistema informático interconectado, de PC a PC, sin dañar necesariamente el "hardware" o el "software" de los sistemas que visitan. La función principal es viajar en secreto a través de equipos anfitriones recopilando cierto tipo de información programada (tal como los archivos de "passwords") para enviarla a un equipo determinado al cual el creador del virus tiene acceso.

Z. "Adwares" o "Advertising-Supported software" – Estos son programas creados con el propósito de mostrarnos publicidad, a diferencia de los "Spywares", suelen venir incluidos en programas "sharewares" y por lo tanto al aceptar los términos legales durante la instalación de dichos programas, estamos consintiendo su ejecución en nuestros equipos y afirmando que estamos informados de ello.

AA. Secuestrador o "Hijacker" – Tiene como función el secuestrar nuestro navegador de internet. Esta acción es posible debido a que sus programadores aprovechan las vulnerabilidades de la máquina de Java dentro del Internet Explorer. Aunque el secuestrador del navegador sólo puede darse si se visitan las páginas de este tipo de personas, el riesgo comienza a crecer con el envío de correos electrónicos con temas engañosos, los cuales piden al usuario a cambio de instalar un programa de supuesta utilidad al entrar a estos sitios.

ARTICULO 7 – POLITICA PARA LA ADMINISTRACION Y MANEJO DE LOS SISTEMAS DE TECNOLOGÍA DE INFORMACION

La política para la administración y manejo de los sistemas de Tecnología de Información es que cada usuario haga un uso adecuado de los mismos observando en todo momento las normas aplicables para el manejo de tales sistemas y de sus equipos.

El uso adecuado incluye pero no se limita, a seguridad de la información, envío y recibo de correo electrónico, correspondencia interna, uso de la Internet o cualquier otro método de comunicación, procesamiento o almacenamiento de datos.

Sección 7.1 – Acuerdo de Confidencialidad y Seguridad

Todo usuario tiene que suscribir un Acuerdo de Confidencialidad y Seguridad de Información y Protección de Equipos ("el Acuerdo") que detalla los deberes y responsabilidades del usuario en el uso de los sistemas de Tecnología de Información y en cuanto a la protección de los equipos que para tales fines cuenta la Autoridad.

El departamento de Recursos Humanos será responsable de custodiar y mantener en archivo los acuerdos firmados por los empleados de la Autoridad y de empleados de otras agencias en asignación administrativa. Como parte de la orientación de nuevos empleados, el representante oficial de Recursos Humanos le proveerá copia de este reglamento y le proveerá el Acuerdo para que suscriban el mismo en o antes de que comiencen sus labores.

El Director de Tecnología de Información será responsable de custodiar y mantener en archivo los acuerdos firmados por consultores, proveedores de servicios profesionales, auditores externos y visitantes a los que se le apruebe el uso de los recursos de Tecnología de Información de la Autoridad. A estos, la Oficina de Tecnología de Información le proveerá el Acuerdo para que suscriban el mismo en o antes de que comiencen sus labores.

No se podrá hacer uso de los Sistemas de Tecnología de Información y equipos de la Autoridad sin haber recibido una orientación en torno a las normas, políticas y reglamentos de la Autoridad que rigen el uso de sus sistemas de Tecnología de Información.

Sección 7.2 - Responsabilidades de la Oficina de Tecnología de Información en cuanto a la administración e implementación de las políticas y normas contenidas en el presente Reglamento

La Oficina de Tecnología de Información tendrá las siguientes responsabilidades en torno a la implementación y aplicación de las normas contenidas en este Reglamento:

A. Será responsable por la implementación, mantenimiento y revisión de éste reglamento.

B. Velará y orientará a los usuarios de sistemas de Tecnología de Información de las normas de seguridad, confidencialidad y protección de equipos que implica tal uso.

C. Tendrá a su cargo la administración de todo lo relativo al acceso a los sistemas de Tecnología de Información incluyendo crear la identificación del usuario y contraseña.

D. Establecer controles que garanticen el buen funcionamiento de los sistemas de Tecnología de Información a la hora de implementar nuevas aplicaciones o módulos en ambiente de producción.

E. Implementar controles de accesos al cuarto de computadoras centrales bajo las siguientes condiciones:

a. Debe proveer un control de acceso físico y;
b. Toda persona que visite las instalaciones deberá identificarse en un registro de visitas.

F. Trabajar en conjunto con el Auditor Interno y/o Recursos Humanos, para asegurarse que los usuarios están dando cumplimiento a lo establecido en este Reglamento en cuanto a la seguridad de información, el uso adecuado de los equipos y sistemas de Tecnología de Información para lo cual podrán, de tiempo en tiempo:

a. Conducir monitoreo periódico, así como cooperar con el Auditor en auditorías internas o externas.
b. Investigar cualquier acto ilegal o impropio en el uso de tales sistemas.
c. Revisar el que los servicios de Internet sean utilizados para fines legítimos de la Autoridad y en el desempeño de los deberes y responsabilidades del usuario.
d. Verificar que se le esté dando un uso apropiado al correo electrónico o cualesquier otro método de comunicación electrónica provisto dentro de los sistemas de Tecnología de Información de la Autoridad.

G. Examinar los equipos y sistemas en casos de fallas en el sistema o situación de emergencia.

H. Evaluar o actualizar la eficiencia y condición de los sistemas y equipos en la Autoridad.

I. Llevar a cabo y mantener copias de resguardo de la información residente en las computadoras centrales, los cuales residirán fuera de las facilidades de la Autoridad, con el propósito de poder recuperar la mayor cantidad de información posible en caso de un incidente o desastre.

J. Mantener periódicamente los Manuales Operacionales de sistemas de Tecnología de Información y de aplicaciones y el Plan de Recuperación en caso de desastre a fin de garantizar la continuidad de las operaciones de la Autoridad en un evento de emergencia.

K. Coordinar una revisión periódica de los accesos a los sistemas de la Autoridad en conjunto con la gerencia de las áreas aplicables. De esta forma se asegura que los accesos son correctos y vigentes.

L. Mantener un inventario actualizado de los programas instalados en las computadoras ya sean comprados o desarrollados internamente, existentes en todas las divisiones y oficinas de la Autoridad.

M. Pasar juicio sobre toda adquisición de "hardware" y "software", para asegurarse que sea compatible con los sistemas y equipos de acuerdo a los estándares establecidos por la Autoridad y regulado por la Carta Circular 96-01.

N. Velar por que todo movimiento de los equipos este previamente autorizado por el Director de Tecnología de Información o su delegado. Que el mismo sea realizado en coordinación con el encargado de la propiedad que es la persona responsable de mantener control de los equipos asignados.

O. Establecer y mantener un sistema para manejo y control de cambios. Cambios se define como instalaciones, modificaciones o eliminaciones que alteran la infraestructura de producción de sistemas de información y su ambiente operacional. Esto se hace para minimizar las interrupciones de servicio a usuarios de sistemas de información de la Autoridad.

P. Instalar, modificar, reparar equipos de computadoras. Decomisar equipos se hará bajo la administración del departamento de Administración.

Q. Mantener activos y actualizados los sistemas anti-virus y "anti-spam" para protección de la información y los equipos.

R. Eliminar de las computadoras o equipos de la Autoridad programas no autorizados e instalados.

Sección 7.3 – Políticas dirigidas a salvaguardar la Seguridad de Información

A. No Divulgación de Información Confidencial

Está prohibido que los usuarios divulguen a terceros información confidencial de la Autoridad obtenida de los sistemas de Tecnología de Información o que los usuarios divulguen ningún tipo de información a persona alguna que debido a la naturaleza de sus funciones, deberes o tareas, no deben tener conocimiento o acceso a la misma.

Se entenderá por información confidencial aquella información interna de la Autoridad relacionada con sus operaciones incluyendo, pero sin limitarse, a información sobre recursos humanos, finanzas o contabilidad de la Autoridad, planes o estrategias de mercadeo o promoción y planes de desarrollo.

B. Contraseñas

Las contraseñas no pueden ser transferidas, prestadas o reveladas a otra persona en ningún momento.

La Oficina de Tecnología de Información revocará o transferirá la identificación de usuario y contraseña el mismo día en que el usuario cese en sus funciones (en el caso de funcionarios o empleados, el cese comprende el ser transferido, descendido, ascendido o ausencia con o sin licencia que excedan 30 días). Para ello, se cumplimentará él formulario "Notificación de Cese en el Servicio" por cada director de oficina o división; en el caso de empleados o funcionarios, corresponde a la Oficina de Recursos Humanos.

C. Revisión Periódica de Accesos

Al menos una vez al año, se hará una revisión de los privilegios de acceso aplicables a todos los usuarios de sistemas. Esta revisión será hecha por los directores de las áreas a las cuales pertenecen los usuarios, de manera que certifiquen que los accesos que tienen siguen vigentes y de acuerdo a los controles que deben estar establecidos por las áreas para evitar conflictos de responsabilidades.

Para esto, la oficina de Tecnología de Información, imprimirá y repartirá a los directores de área los reportes de acceso de los usuarios, distribuidos por sistema. Los directores de área, revisarán e identificarán cualquier cambio que sea necesario sometiendo la forma 340.17, "Solicitud de Acceso a Servicios de la Red Informática", debidamente aprobada, uno por cada usuario que requiera cambio en sus accesos, junto con el reporte de acceso revisado y firmado, a la Oficina de Tecnología de Información, en un período no mayor de 30 días calendario. La Oficina de Tecnología de Información actualizará los accesos en un período no mayor de 14 días calendario.

Sección 7.4 – Responsabilidades del usuario en el uso de los sistemas y equipos de información

A. El uso de los equipos, computadoras, programas, información y sistemas de información es exclusivamente para asuntos oficiales.

B. Solo podrán utilizar programas en las distintas áreas de trabajo siempre que:

a. Estos han sido legalmente adquiridos o desarrollados por la Autoridad o el Gobierno de Puerto Rico.
b. Las licencias para su uso están vigentes.
c. La utilización de estos es para mejorar la realización de las tareas de la Autoridad.
d. La utilización de estos productos enlatados debe responder a los acuerdos establecidos en el contrato de utilización que la Autoridad negoció al momento de la compra o adquisición del Gobierno de Puerto Rico.
e. Los mismos hayan sido previamente aprobados para instalación por el Director de Tecnología de Información.

C. No puede utilizar o copiar programas o productos protegidos por leyes de derecho de autor y/o licencias ("Copyright" y "License Restrictions") sin licencias correspondientes que los protegen.

D. No puede instalar programas de entretenimiento y/o utilidades, tales como "wall papers", "screen savers", entre otros, o cambiarlos fotografías o material no relacionado a la Autoridad.

E. Está prohibido el reproducir o duplicar cualquier programa adquirido por la Autoridad o desarrollado internamente. La reproducción o duplicación de programas a través del original o de copias del mismo con el propósito de obtenerlo sin sufragar los costos de licencia o "copyright" es un acto ilegal que expone a riesgo a la Autoridad de litigios o multas.

F. Todo usuario de los sistemas de información que realice funciones de pruebas o de desarrollo deberá utilizar un ambiente adecuado y coordinado con la Oficina de Tecnología de Información.

G. Todos los usuarios de computadoras personales y portátiles deben tener instalado y operacional el programa de detección/protección de virus y "spam" para minimizar el daño que pueda ocasionar un ataque de virus que puedan tener los archivos que se introduzcan en la computadora. La forma principal de introducir un virus a las computadoras es a través del uso del correo electrónico, en el uso del Internet, "CD" Disco Compacto o de "Jump Drive" de una computadora a otra. Todo "Jump Drive" o "CD" a usarse en la PC debe ser pasado por un programa anti-virus antes de grabarse o instalarse en la PC.

H. Todo documento creado electrónicamente se regirá por la Ley de Documentos Públicos.

I. Todo usuario guardará la información electrónica (datos) en los servidores designados o en sus correspondientes carpetas de usuario o carpetas compartidas por área. De esta forma se garantiza que será guardada como parte del proceso de creación de copias de resguardo ("backups") que hace el departamento de Tecnología de Información de forma periódica. El usuario será responsable de hacer copias de resguardo ("backups") de información o datos que no guarde en estos lugares designados en los servidores. Será su responsabilidad la seguridad de dicha información. Dichos "backups" de información deberán conservarse en un lugar seguro bajo llave o bóveda de seguridad en las facilidades de la división u oficina. El acceso a tales "backups" debe estar limitado y controlado que solo tenga acceso a los mismos el empleado o usuario que por motivo de sus funciones deba tener acceso a los mismos. El director de cada división u oficina estará encargado de velar por el cumplimento con lo antes indicado.

Sección 7.5 – Política para envío y recibo de correo electrónico, correspondencia interna y servicio de Internet

A. Se utilizará el Correo Electrónico para el intercambio de correspondencia interna siempre que sea posible, disminuyendo así el manejo de documentos impresos y el uso de "CD's", Jump Drive, DVD y cualquier otro medio externo.

B. El Correo Electrónico y el servicio de Internet se utilizará exclusivamente para asuntos oficiales relacionados con las labores de los usuarios.

C. Toda correspondencia intercambiada a través del Correo Electrónico se considera confidencial entre el remitente y su(s) destinatario(s) al igual que un documento impreso, y como tal debe mantenerse su privacidad y seguridad. Para ello es necesario que se conserve el buen uso de las contraseñas ("password") al Correo Electrónico. Todo correo electrónico llevará el siguiente mensaje al final de cada comunicación la versión en español y la versión en inglés:

"NOTA DE CONFIDENCIALIDAD"

Esta comunicación y cualquier archivo transmitidos con ella pueden contener información que es confidencial, privilegiada y/o privada bajo la ley aplicable. Se utilizará solamente para el uso del individuo o entidad a que se dirige. Si usted no es el destinatario intencional, se le notifica a usted por la presente que cualquier uso, diseminación o copia de esta comunicación se prohíbe estrictamente. Si usted ha recibido esta comunicación por error, por favor notifique al remitente. Gracias por su cooperación.

"CONFIDENTIALITY NOTE"

This communication and any files transmitted with it may contain information that is confidential, privileged and exempt from disclosure under applicable law. It is intended solely for the use of the individual or entity to which it is addressed. If you are not the intended recipient, you are hereby notified that any use, discrimination or copying of this communication is strictly prohibited. If you have received this communication in error, please notify the sender. Thank you for your cooperation.

D. Se considerará evidencia de recibo y lectura por parte del destinatario el récord electrónico que se crea al utilizar las opciones de "Delivery, Receipt Read y Receipt" del "Tracking Options" del menú de Microsoft Outlook. Estas opciones deben utilizarse en todo mensaje electrónico enviado.

E. El usuario del correo electrónico es responsable de acceder el sistema al llegar a su oficina y mantenerlo activo durante todo el día de trabajo para el envío y recibo de su correspondencia dentro de los parámetros establecidos.

F. El usuario deberá transferir al destinatario correspondiente toda correspondencia electrónica recibida por error y mantener la confidencialidad de la misma.

G. Se utilizará papel en blanco (sin timbrar) para imprimir los documentos de uso interno y papel timbrado con el logo de la Autoridad solamente para correspondencia externa.

H. La Oficina de Tecnología de Información podrá revisar el correo electrónico y acceso a las páginas de Internet de cada empleado bajo las siguientes situaciones:

a. Encontrar mensajes o correspondencia perdida o extraviada.
b. Llevar a cabo monitoreo, auditorías internas o externas.
c. Evaluar la eficiencia del sistema de la Autoridad.
d. Realizar una investigación de un posible acto ilegal.
e. En caso de una falla en el sistema o emergencia.
f. Uso inapropiado del correo electrónico.

g. Verificar la utilización de los servicios de Internet para las tareas afines al trabajo de los usuarios.
h. Utilización apropiada de los métodos de redes de comunicación electrónica.

I. Está prohibido el uso del correo electrónico y el servicio de Internet como instrumento para prácticas o mensajes discriminatorios por razón de raza, color, sexo, nacimiento, edad, origen, condición social o por ideas políticas o religioso por parte de ningún empleado.

J. Está prohibido el uso del correo electrónico para envío de mensajes en cadena.

Sección 7.6 – Violación a la Política para la Administración y Manejo de los Sistemas de Tecnología de Información

En caso de que se cometa alguna violación este Reglamento, se aplicará la sanción correspondiente según el manual de Disciplina de División de Recursos Humanos.

ARTICULO 8 – SOLICITUD DE ACCESO Y MANEJO A LOS SISTEMAS DE INFORMACIÓN

Sección 8.1 - Acceso

El acceso a los sistemas de información de la Autoridad se determinará en atención a las funciones, deberes o responsabilidades del puesto que se ocupa.

El Director de Área, División u Oficina determinará en primera instancia el nivel de acceso necesario para que el empleado pueda realizar efectivamente tales deberes o responsabilidades. Para ello, el Director del Área, División u Oficina en que se desempeña el potencial usuario cumplimentarán el formulario "Solicitud de Acceso a Servicios de la Red Informática" Forma 340.17 y autorizará tal acceso y enviará el formulario aprobado a la División de Sistemas de Información. De necesitar acceso al Sistema de Oracle tiene que además llenar la Forma 340.17A. De necesitar acceso al Sistema SATT, debe llenar la Forma 340.17B. Si requiere acceso al Sistema de HR Sense debe llenar la Forma 340.17C.

La Oficina de Tecnología de Información podrá procesar las peticiones de acceso solo cuando estas están debidamente autorizadas. No se podrán procesar accesos sin la debida documentación. Además, la Oficina de Tecnología de Información podrá denegar el nivel de acceso solicitado al empleado en aquellos casos que, después de verificar, entienda que tal nivel no corresponda según la posición o el puesto del empleado.

Los sistemas de información de la Autoridad están diseñados para operar de tal manera que todo usuario autorizado pueda tener acceso a los mismos. Para ello, debe identificarse adecuadamente al acceder el sistema.

En el momento de acceder el sistema, éste verifica la autorización del usuario para acceder al mismo de suerte que:

A. Desconecta automáticamente a aquel usuario que continúa entrando una clave de acceso errónea al sistema después de tres intentos.

B. Dará acceso al sistema solo en aquellos días en que los usuarios que están autorizados a usar el mismo.

Sección 8.2 – Creación de Contraseñas

La Oficina de Tecnología de Información dará el acceso al usuario de acuerdo al nivel autorizado, a saber:

A. Acceso a la computadora (antes de subir a la red).

B. Acceso a la red.

C. Acceso a los productos/aplicaciones/programas.

D. Acceso específico a leer, escribir, borrar y ejecutar archivos.

Las contraseñas deben cumplir con los siguientes requisitos mínimos:

A. Largo mínimo de 6 caracteres.

B. Debe incluir letras mayúsculas, números y letras minúsculas.

C. Debe expirar al menos cada 45 días como máximo.

D. Se debe mantener un historial de al menos 6 contraseñas sin reusar.

E. La cuenta del usuario será suspendida luego de 3 intentos inválidos.

Dado que toda clave de usuario (User-ID) y contraseña (“password”) es para el uso exclusivo del usuario, si la misma llega a conocimiento de cualquier otro empleado o usuario, el empleado concernido deberá notificar este hecho de inmediato a la Oficina de Tecnología de Información para que se proceda a cambiar la contraseña.

Sección 8.3 – Expedientes sobre acceso a sistemas de información

La Oficina de Tecnología de Información mantendrá la documentación pertinente (formas 340.17 y documentos de revisión periódica de accesos) que contienen los datos de la asignación y/o cambios y utilización de los accesos a los sistemas de información de la Autoridad.

Estos documentos serán mantenidos en carpetas y guardados en un lugar seguro.

Sección 8.4 – Accesos a las Aplicaciones de producción y de prueba

La red de computadoras permitirá el acceso a las aplicaciones en ambiente de producción únicamente a aquellos usuarios que generan transacciones como parte del flujo normal de los servicios ofrecidos. Estos accesos deberán ser regulados de acuerdo con el nivel de seguridad que cada usuario necesite para realizar sus funciones.

Todo usuario que realice funciones de prueba o desarrollo deberá utilizar el ambiente y los recursos designados para tal propósito. Solo tendrán acceso a tales recursos aquellos empleados que por la naturaleza de sus funciones requieran del mismo. Para realizar cambios o modificaciones en ambiente de producción se debe cumplir con el PROCEDIMIENTO DE MANEJO DE CAMBIOS.

Las tareas de desarrollo y pruebas deberán llevarse a cabo en un ambiente separado y no podrán afectar o alterar en ninguna manera la información oficial en el ambiente de producción de la Autoridad.

Sección 8.5 – Uso de la contraseña

A. NO divulgue, preste o transfiera su contraseña a otro usuario.

B. NO escriba ni coloque la contraseña cerca del terminal.

C. NO use una contraseña que lo asocie a usted, tal como su fecha de nacimiento, su apodo, iniciales a una abreviación de su nombre.

ARTÍCULO 9 – SEGURIDAD EN LOS EQUIPOS

Sección 9.1 - Inventario

El área de Propiedad, bajo Servicios Generales de la Oficina de Administración, con la ayuda de la Oficina de Tecnología de Información, preparará y mantendrá actualizado un inventario del equipo electrónico de la Autoridad que incluirá:

A. La descripción del equipo

B. Costo por unidad

C. Localización del mismo

D. De ser arrendado tal equipo, se expresará el nombre del acreedor

Sección 9.2 - Seguro

Los equipos de procesamiento electrónico de la Autoridad estarán cubiertos por una póliza de seguros cuya cubierta se extiende a daños al equipo por eventos fortuitos, actos delictivos o aquellas circunstancias que mejor protejan los intereses de la Autoridad.

El equipo en cuestión se asegurará por el costo original.

Sección 9.3 – Responsabilidades del usuario para con los Discos Compactos, DVD, Jump Drive o cualquier otra media.

A. Todo usuario será responsable de velar por el uso adecuado de los Discos Compactos, DVD, Jump Drive o cualquier otra media y la información contenida en ellos. Para esto deberá:

a. Rotularlos adecuadamente con las etiquetas provistas para ello, utilizando bolígrafos suaves.
b. Cambiarle las etiquetas siempre que borre o cambie la información en el Discos Compactos, DVD, Jump Drive o cualquier otra media.
c. Guardarlas en un lugar seguro, bajo llave afuera del área de trabajo, si es necesario. Puede utilizar la bóveda de Tecnología de Información.
d. Mantenerlos por lo menos a doce pulgadas de imanes y dispositivos electromagnéticos tales como teléfonos, beeper y celulares.
e. Hacerles copias regularmente.
f. Disponerlos de los mismos borrando la información o parta los mismos cuando vaya a tirar de ellos.

B. Todo usuario observará las siguientes normas con relación a los Discos Compactos, DVD y/o Jump Drives:

a. Brindará a los Discos Compactos, DVD, Jump Drive o cualquier otro medio la misma protección en términos de confidencialidad que a los documentos que contienen la información.
b. No se enviarán los discos duros fuera de la Autoridad, sea por reparación, venta o donación sin reformatear los mismos.
c. Evitará tocar las áreas sensitivas de Discos Compactos, DVD, Jump Drive o cualquier otra media, que podría hacer daño y perder información.
d. Evitará escribir directamente sobre ellos, ni colocar presillas “clips”.
e. Evitará colocar los Discos Compactos, DVD, Jump Drive o cualquier otra media cerca de líquidos solventes.
f. No doblará los Discos Compactos, DVD, Jump Drive o cualquier otra media ni colocará objetos pesados sobre ellos.
g. Evitar exponer los media a los rayos del sol, ni permitirá que se mojen con ningún líquido.

Sección 9.4 – Uso, protección y cuidado de Computadoras y sus equipos periferales.

A. La Autoridad utilizará equipos electrónicos (impresoras, PC's portátiles, CD's, etc.) para facilitar y agilizar el flujo de tareas en las distintas divisiones y oficinas. La Autoridad requiere de sus empleados o usuarios que utilicen estos equipos correctamente y que tomen las medidas necesarias para protegerlos y mantenerlos funcionando en óptimas condiciones, de esta forma evitar daños y averías. Los equipos serán instalados por la Oficina de Tecnología de Información. Ningún usuario deberá realizar tareas de instalación de equipos por sí mismo.

B. Cualquier mal funcionamiento que el usuario detecte en los equipos deberá notificarlo rápidamente a la Oficina de Tecnología de Información a través del Escritorio de Servicio (Help Desk), accesible llamando al 787-721-2400, extensión 1000, para que los revisen, corrijan la falla, de ser necesaria, o para ordenar la reparación de las mismas.

C. Está prohibido, para empleados de la Autoridad, usar computadoras que no sean propiedad de la Autoridad o de cualquier organización gubernamental con la que no exista un acuerdo inter-agencial en los predios de la Autoridad para uso personal o de trabajo. Las computadoras deben ser utilizadas solo para propósitos oficiales de la Autoridad.

D. Consultores podrán utilizar computadoras propias siempre que tengan la autorización previa del Director de la Oficina de Tecnología de Información. La Autoridad no se hará responsable de la pérdida o daño a equipo que no es propiedad de la Autoridad. Cada consultor es responsable de velar por la seguridad y el cuidado de su equipo. Estos deben evidenciar que su equipo tiene un anti-virus al día y que cualquier jump drive a utilizar está libre de virus.

E. Los usuarios no deberán llevar alimentos o bebidas a las áreas de trabajo donde existan equipos periféricos. Al finalizar el día, los usuarios deberán retirar sus contraseñas de las computadoras y deberán apagar todos los equipos electrónicos en su área de trabajo.

F. Los usuarios no deberán colocar equipos tales como radios o cualquier equipo que emita radiaciones electromagnéticas cerca del CPU.

G. Los usuarios no deberán colocar plantas o tiestos sobre las computadoras ni pegar papeles de notas en las partes de ventilación de la computadora.

H. Los usuarios no deberán trabajar con líquidos, grapas o sujetadores de papel sobre el teclado ni forzar algún medio para que entre o salga de su "drive".

I. En caso que el usuario se tenga que ausentar por orden del Fondo del Seguro del Estado con una Licencia de Descanso o solicite una Licencia sin sueldo o tenga una Licencia por enfermedad prolongada y tenga asignado algún equipo de computadoras o telefonía tendrá que entregar el mismo (o los mismos) a la Oficina de Tecnología de Información.

Sección 9.5 – Computadoras portátiles

A. Debido a que las computadoras portátiles corren un alto riesgo de ser hurtadas, cada unidad debe estar protegida con "programas" de control de acceso y contraseñas para activar o prender la máquina siempre y cuando sea factible o práctico.

B. Se prohíbe estrictamente guardar números telefónicos de módem del network o contraseñas de la red de computadoras personales (PC) o individuales ("desktops" o "notebooks") que no estén protegidas.

C. Todos los programas y archivos de la Autoridad que se encuentren en medios móviles deben almacenarse bajo llave cuando no se están utilizando o deben mantenerse en áreas que se cierren con llave cuando no se utilicen.

Sección 9.6 – Telecomunicaciones

A. La utilización de los equipos de comunicaciones (equipos telefónicos y de datos) será exclusivamente con propósitos oficiales de la Autoridad y siempre deberán cumplir con las reglamentaciones y aspectos legales relacionados con el uso de la tecnología. Además la utilización de los equipos para la transmisión de datos no deberá representar conflicto de interés para los usuarios de los mismos. Toda transmisión de información deberá corresponder siempre a los mejores intereses de la Autoridad.

B. Toda computadora personal dejada conectada, por el usuario, en la red de telecomunicaciones, pasada la hora de trabajo del empleado, podrá ser desactivada de la red por el personal de la Oficina de Tecnología de Información.

C. Todo acceso a la red de telecomunicaciones por personas ajenas a la Autoridad (consultores y/o técnicos de mantenimiento y servicio) deberá ser autorizado adecuadamente para asegurar su buen uso y/o poder restaurar la configuración de las computadoras a su estado original. Estas personas deben ser incluidas en la Lista de Acceso de equipos asociados a la Red de Telecomunicaciones.

D. Para el funcionamiento óptimo la red de telecomunicaciones de nuestro sistema de información es necesario que el mantenimiento a los equipos asociados a la red, sea realizado por recursos adiestrados en estas técnicas.

E. Toda solicitud de servicio para la instalación, reparación, movimiento, sustitución o eliminación de equipos tales como: impresoras, computadoras personales y líneas de comunicación, deberá dirigirse por escrito a la unidad responsable de Tecnología de Información. Todas las solicitudes deben ser originadas por el director de área.

ARTÍCULO 10 – PROTECCIÓN CONTRA VIRUS

Sección 10.1 – Programas

A. Para minimizar el que las computadoras personales (PC's) se infecten de virus, solo se pueden usar programas autorizados y con la debida licencia. Los programas autorizados son aquellos aprobados por la Autoridad que se obtengan de acuerdos gubernamentales y/o suplidores autorizados.

B. La Oficina de Tecnología de Información instalará un programa anti-virus a nivel de Red y hará copias de resguardo ("backups) periódicamente para proteger contra pérdida de información en las PC's.

C. La instalación programas debe incluir su optimización en el uso y mantenerse activos. Las facilidades de estos programas deben incluir el rescate automático de los archivos críticos infectados que son necesarios para el funcionamiento de la computadora o sus programas en caso de eventos de fallas.

D. El programa debe proveer, entre otros, la siguiente información:

a. Informes y estadísticas de computadoras conectadas a la red.
b. Problemas de virus.
c. Que computadoras han sido liberadas de contaminación viral y cuál fue el problema.

E. El programa debe configurarse para que ejecute cada vez que el usuario se conecte a la red, al menos, una vez por día/semana. Cuando el programa ejecuta, graba la dirección del nodo, la identificación del usuario, problema de virus, hora y fecha.

F. Para evitar o poder recuperarse de un ataque de virus u otro desastre, se implementarán procedimientos rutinarios de "backup" (copia de resguardo) para el programa y los archivos de la Autoridad en las PC's a LAN's según se dispone en este Reglamento.

Sección 10.2 – Prohibiciones

A. NO prenda su máquina con un Jump Drive, CD o DVD desconocido insertado en los periferales de entrada.

B. NO utilice discos de programas de demostración que usted no ha solicitado de un suplidor desconocido.

ARTICULO 11 – USO DEL CORREO ELECTRÓNICO Y DE INTERNET

Sección 11.1 – Objetivo

La Autoridad tiene como objetivo maximizar la utilización adecuada del envío y recibo de correspondencia a través del Correo Electrónico y del servicio de Internet, la cual implica:

A. Agilizar nuestra comunicación interna y externa.

B. Minimizar la impresión en el sistema del recibo de la correspondencia.

C. Mantener récord en el sistema del recibo de la correspondencia.

D. Acelerar el envío y recibo de la correspondencia interna.

E. Disminuir interrupciones por llamadas telefónicas.

F. Transferir archivos y documentos sin necesidad de utilizar discos.

G. Reducir los costos de impresión de documentos y de uso de discos.

H. Estandarizar el tipo de papel a usar para correspondencia interna y externa.

Sección 11.2 – Utilización

A. La Autoridad exhorta a que se utilice el Correo Electrónico siempre que sea posible, sustituyendo el documento impreso o en disco por un mensaje electrónico.

B. Usted puede redactar su mensaje en el Correo Electrónico utilizando la opción provista por la aplicación para ello. También puede transmitir un documento preparado en Word, Excel, PowerPoint u otros programas incluyendo los archivos al correo para economizar papel y el uso de medios externos.

C. Todas las personas con facilidades de Correo Electrónico aparecen en el listado incluido en el sistema en la Opción Directorio (“Address Book”).

D. Un mensaje que se envía por Correo Electrónico como regla general no debe repetirse por escrito.

E. Cada director de la Autoridad designará una persona en su división u oficina, conforme sea necesario, para enviar mensajes informativos a otras divisiones u oficinas de la Autoridad. Se dispone que todo mensaje que tenga como destinatario a todos los empleados de la Autoridad, deberá transmitirse como primer opción por conducto del(a) Director(a) de Administración. Las únicas personas autorizadas a enviar un mensaje a todos los empleados de la Autoridad son el (la) Director(a) Ejecutivo(a), el (la) Director(a) de Administración y el Director la Oficina de Tecnología de Información o sus representantes autorizados en caso de que los mismos no estén

presentes. Esto evita duplicidad del mensaje, ahorro en tiempo y mantiene cierto estilo de uniformidad en la redacción de los mensajes.

F. Todo remitente deberá mantener acuse de recibo y lectura del mensaje electrónicamente. De esta manera se asegura que el destinatario recibió y lee la correspondencia. Este record se puede retener como un acuse de recibo de la correspondencia enviada.

G. Ningún destinatario podrá enviar copia de la correspondencia electrónica recibida a otras personas sin el conocimiento del remitente. A este, se le deberá notificar por lo menos con copia.

H. Toda impresión de documentos de uso interno se hará en papel blanco. Si el usuario desea que el logo de la Autoridad aparezca en sus documentos, puede incluirlo como parte del mismo. La Oficina de Tecnología de Información enviará los logos a su máquina, a través del Correo Electrónico en documentos de Word. Solo se utilizará papel timbrado para correspondencia externa.

Sección 11.3 – Monitoreo

El correo electrónico y el Internet son de uso oficial de la Autoridad. El contenido de los mensajes y el acceso a las páginas de Internet, determinarán si el uso es adecuado o impropio. Si se determina que el uso ha sido inapropiado, se podrán imponer medidas disciplinarias a tono con la gravedad del caso. La Autoridad monitoreará los mensajes electrónicos y el acceso a las páginas de Internet con el propósito de cerciorarse que se esté usando correctamente. Este proceso no conlleva violación a la privacidad debido a que ambos se proveen a los usuarios para funciones oficiales de la Autoridad.

En el caso del correo electrónico, el mensaje posee como particularidad la identificación de la Autoridad lo cual la hace instrumento de carácter representativo de la Autoridad. Por otro lado, cada acceso a las páginas de Internet nos identifica como Autoridad en los diferentes proveedores de servicios de Internet, haciendo que cada acceso sea de carácter oficial, el cual pudiera beneficiar o perjudicar la imagen de la Autoridad.

Sección 11.4 – Aceptaciones

Los siguientes son algunos ejemplos de los usos aceptados del Correo Electrónico y del servicio de Internet:

A. Intercambio de correo electrónico para realizar funciones de trabajo con agencias del Gobierno de Puerto Rico, ciudadanos, compañías, turistas o agencias de viajes en cualquier parte del mundo con el propósito de promover y brindar información de nuestras bellezas turísticas para promover a Puerto Rico como un destino turístico.

B. Promover a través de páginas de Internet nuestras facilidades turísticas, hoteles, paradores, mesones astronómicos y otros lugares de interés a los turistas, agencias de viajes o desarrolladores turísticos que promuevan a Puerto Rico como destino turístico.

Sección 11.5 – Prohibiciones

No se permitirá utilizar el Correo Electrónico y el servicio de Internet para el manejo de archivos voluminosos (mayores de 10MB) sin la previa autorización de la Oficina de Tecnología de Información.

ARTÍCULO 12 – CLAUSULA DE SALVEDAD

Si cualquier disposición de este Reglamento fuere declarada nula o inconstitucional por foro competente, prevalecerá la determinación tomada, pero esto no afectara el resto del procedimiento ni la aplicación del mismo.

ARTÍCULO 13 – INCLUMPLIMIENTO

La violación de cualquiera de las disposiciones de este Reglamento podrá conllevar la imposición de medidas disciplinarias cuya severidad dependerá de las circunstancias de cada caso. Las medidas disciplinarias se impondrán de acuerdo al Manual de Disciplinas de Recursos Humanos.

ARTÍCULO 14 – HISTORIAL DEL DOCUMENTO

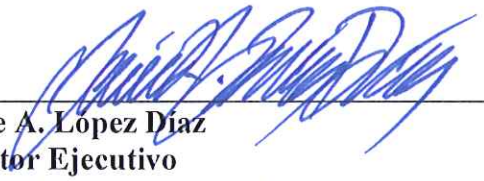
Se detallan las áreas, artículos y secciones que fueron enmendados en esta revisión.

Fecha de Actualización	Numero Versión	Autor	Descripción
08/23/2010	2	José R. Valdez	Se re-escribe el Reglamento para sincronizar el contenido con el de la Compañía de Turismo de Puerto Rico. Se cambia el Título. El anterior era “Reglamento para usuarios que manejan sistemas de información”.

ARTÍCULO 15 – VIGENCIA Y APROBACIÓN

Este Reglamento entrará en vigor en la fecha que lo firme y apruebe el Presidente de la Junta de Directores de la Autoridad.

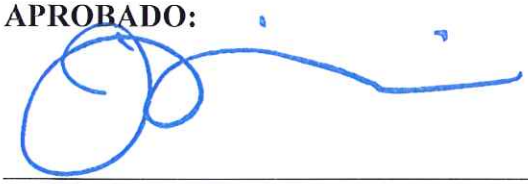
RECOMENDADO:



FECHA: 09/10/2010

Jaime A. López Díaz
Director Ejecutivo
Autoridad del Distrito del Centro de Convenciones de Puerto Rico

APROBADO:



FECHA: 9-14-2010

Lcdo. José R. Pérez Riera
Presidente Junta de Directores
Compañía de Turismo de Puerto Rico
Autoridad del Distrito del Centro de Convenciones de Puerto Rico