AUTORIDAD DE DESPERDICIOS SÓLIDOS

GOBIERNO DE PUERTO RICO
AUTORIDAD DE DESPERDICIOS SÓLIDOS
SAN JUAN, PUERTO RICO

CARTA CIRCULAR NÚMERO: 2012-01

PARA ESTABLECER LA POLÍTICA DE LA AUTORIDAD DE DESPERDICIOS SÓLIDOS EN CUANTO A LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN; Y SOBRE EL USO DE SISTEMAS DE INFORMACIÓN, DE LA INTERNET Y DEL CORREO ELECTRÓNICO.

BASE LEGAL

Se promulga la presente CARTA CIRCULAR en virtud de la Ley Número 12 del 24 de julio de 1985, según enmendada y conocida como Ley de Ética Gubernamental; la Ley Núm. 151 de 22 de junio de 2004, según enmendada y conocida como Ley del Gobierno Electrónico"; la Política Número TIG-003 y la TIG-008, según estas han sido emitidas y enmendadas por el Área de Tecnologías de Información Gubernamental de la Oficina de Gerencia y Presupuesto, ambas del 15 de diciembre de 2004; y todas las leyes estatales y federales que regulan el uso de sistemas electrónicos de información y que protegen los derechos de autor.

ARTÍCULO 1: POLÍTICA PÚBLICA

1.1 La política pública del Gobierno de Puerto Rico es facilitar y agilizar los procesos operacionales de los numerosos organismos de la Rama Ejecutiva, aumentar la eficiencia y efectividad en la prestación de los servicios gubernamentales al público y viabilizar la interconexión tecnológica entre los organismos y agencias. La automatización de los procesos operacionales requiere regular el uso apropiado de sus componentes y equipos e implantar las medidas necesarias para garantizar la confidencialidad de la información. Conforme a lo anterior, resulta necesario establecer las políticas necesarias para garantizar el uso adecuado, efectivo y seguro de los sistemas de información y las herramientas de trabajo que éstos proveen.

Esta política tiene el objetivo de fijar las normas fundamentales que deben regir los controles básicos a ser establecidos por las agencias de manera que se garantice el uso adecuado de los recursos relativos a los sistemas de información.

1.2 Cónsono con dicha política pública, la Autoridad de Desperdicios Sólidos, (en adelante denominada "La Autoridad"), reconoce la importancia de la tecnología

electrónica como recurso valioso para lograr las metas y objetivos de esta Corporación Pública. La Autoridad, de igual forma, reconoce la importancia de las computadoras como herramientas para que sus empleados y funcionarios logren una mayor eficiencia operacional.

1.3 A esos efectos, La Autoridad establece la presente política pública de conformidad con las disposiciones y criterios establecidos por la Oficina de Gerencia y Presupuesto, Oficina de Ética Gubernamental y la Oficina del Contralor de Puerto Rico.

1.4 Esta política será aplicable a todo empleado de carrera, regular, irregular, transitorio, de confianza y funcionarios de La Autoridad. De igual forma aplica a cualquier consultor o contratado de La Autoridad, estudiantes practicantes u otros que por la naturaleza de su contrato y/o de su relación con La Autoridad necesite utilizar los sistemas de información. Será aplicable de igual forma a todos los servicios y sistemas, tanto internos como externos, correspondencia electrónica, información de la Intranet o la Internet y los documentos, programas y licencias propiedad de la Autoridad de Desperdicios Sólidos.

ARTÍCULO 2: USO, MANEJO Y CONSERVACIÓN DE LAS COMPUTADORAS

Sección 2.1 – Registro y continuidad

2.1.1 Será necesario un inventario de activos de los sistemas de información que incluya el equipo, los programas y los datos. Todos los activos deberán ser clasificados de acuerdo al nivel de importancia para la continuidad de las operaciones. En particular, los datos electrónicos deberán ser clasificados de acuerdo a su nivel de confidencialidad. Esto permitirá establecer qué es lo que se va a proteger.

2.1.2 Toda computadora adquirida por La Autoridad deberá ser registrada en la Oficina de Sistemas de Información, y en el Registro establecido por el Encargado de la Propiedad de La Autoridad conforme a las leyes y/o reglamentos aplicables. Dicho registro deberá contener el número de propiedad asignado, así como el usuario a quien se le asignó la misma.

2.1.3 Deberán identificarse las posibles amenazas contra los sistemas de información (i.e. robos, desastres naturales, fallas, virus, acceso indebido a los datos, etc.) junto con un análisis del impacto en las operaciones y la probabilidad de que ocurran esas amenazas. Esto permitirá establecer con qué se van a proteger los activos identificados.

2.1.4 De igual forma, se registrará el acceso que La Autoridad le provea al usuario del uso del Internet y al Correo Electrónico, entendiéndose que el uso de los últimos dos es un privilegio que concede La Autoridad, no un derecho.

2.1.5 El análisis de riesgo antes mencionado debe servir de base para desarrollar un Plan de Continuidad de Negocios que incluya un Plan para Recuperación de Desastres y un Plan para la Continuidad de las Operaciones. Dichos planes estarán a cargo en su redacción por parte de la Oficina de Sistemas de Información de La Autoridad.

2.1.6 Deberán existir procedimientos para tener y mantener una copia de resguardo (backup) recurrente de la información y de los programas de aplicación y de sistema esenciales e importantes para las operaciones.

2.1.7 Las facilidades de sistemas de información deberán estar colocadas en un área donde sea menor la probabilidad de daños por fuego, inundaciones, explosiones, disturbios civiles y otras formas de desastres.

Sección 2.2 - Asignación

2.2.1 La Autoridad le proveerá computadoras a aquellos (as) empleados (as) o funcionarios (as) que las necesiten como herramienta para desempeñar las funciones de su puesto. La determinación de necesidad será única y exclusiva de La Autoridad.

2.2.2 La computadora, los servicios asociados, tanto internos como externos, el sistema de correspondencia electrónica, la Intranet, el acceso al Internet y los documentos y programas que existen en los mismos son todos propiedad de La Autoridad. Solo podrán utilizarse para propósitos lícitos, prudentes, responsables y dentro de los poderes y funciones de la Autoridad.

2.2.3 La Autoridad determinará las necesidades de equipo de cada usuario y se reserva el derecho de intercambiar las computadoras y equipo periférico según las necesidades de la Agencia.

Sección 2.3 Uso y Conservación

2.3.1 El usuario a quien se le asigne una computadora será el principal responsable del uso y conservación de ésta y del equipo periférico que se añada.

2.3.2 A cada usuario se le entregarán las unidades configuradas con aquellos programas autorizados por La Autoridad para el procesamiento de datos.

2.3.3 Ningún usuario está autorizado a instalar programas en las computadoras o a eliminar programas previamente instalados. Se prohíbe terminantemente utilizar programas o recursos para los cuales no exista una licencia o autorización válida a nombre de La Autoridad. Solamente estará autorizada la Oficina de Sistemas de Información a hacer cambios, modificaciones o instalaciones, incluyendo aplicaciones que contengan licencia de uso libre o gratuito.

2.3.3 Se prohíbe terminantemente copiar programas protegidos por las leyes de derecho de autor o tener instalados programas sin licencias. La Autoridad no requiere, solicita ni condona la duplicación o uso no autorizado de programas protegidos por derechos de autor.

2.3.4 Ningún usuario está autorizado a hacerle cambios a la configuración de la computadora asignada.

2.3.5 Ningún usuario está autorizado a conectar a una computadora equipo periférico que no haya sido aprobado o adquirido por La Autoridad.

2.3.6 Los usuarios no deben tomar alimentos en el área de la computadora, para así evitar daño al equipo propiedad de La Autoridad. Queda expresamente prohibido pegar afiches, logos o cualquier otro tipo de marca o identificación que no sean las establecidas por el Encargado de la Propiedad de La Autoridad y/o cualquier ley o reglamento aplicable a las unidades bajo su responsabilidad.

2.3.7 El usuario tendrá la obligación de notificar de inmediato a la Oficina de Sistemas de Información si el equipo requiere de reparación, instalación o modificación de cualquier tipo.

2.3.8 Cada equipo es responsabilidad de la persona a quien se le asigna. Si por alguna razón justificada, el equipo asignado a un usuario requiere ser removido, por ejemplo, por reparación, como préstamo a otra unidad, porque va a ser reemplazado, entre otros; es responsabilidad del usuario asegurarse que todo movimiento se tramite utilizando los procedimientos de transferencia de equipo que establezca el Encargado de la Propiedad de La Autoridad.

2.3.9 Si por alguna razón justificada, el equipo asignado a un usuario requiere ser utilizado fuera del área de trabajo a la cual fue asignado, es responsabilidad del usuario notificar a su Supervisor inmediato, a la Oficina de Sistemas de Información y al Encargado de la Propiedad para su autorización. No aplica a equipos que su naturaleza sea portátil.

2.3.10 A aquellos usuarios que se le asignen computadoras portátiles, éstos serán responsables de cuidar la unidad y protegerla de daño físico y robo. El usuario no deberá dejar el equipo en su automóvil, ni en ningún otro lugar que no ofrezca seguridad, en el cual pueda exponerse la propiedad de La Autoridad a robo, daño y/o pérdida.

Sección 2.4- Controles Generales

2.4.1 La Oficina de Sistemas de Información de La Autoridad deberá instalar controles automáticos para la prevención y detección de programas no deseados (i.e. *virus, spyware, adware y updates* automáticos).

2.4.2 La seguridad de la información deberá ser parte integral del diseño de cualquier programa de aplicación que adquiera o desarrolle La Autoridad para facilitar las operaciones de la agencia y/o mejorar el servicio a los ciudadanos.

2.4.3 La información y los programas de aplicación utilizadas en las operaciones de La Autoridad deberán tener controles de acceso para su utilización de tal manera que solamente el personal autorizado pueda ver los datos que necesita ver, o usar las aplicaciones (o la parte de las aplicaciones) que necesita utilizar. Estos controles deberán incluir mecanismos de autenticación y autorización (ver la sección de Definiciones).

2.4.4 Todos los mecanismos de autenticación deberán incluir una contraseña combinada de números y letras, no menor de seis (6) caracteres.

2.4.5 Los privilegios de acceso de los usuarios deberán ser reevaluados regularmente.

2.4.6 Deberán existir procesos que permitan monitorear las actividades de los usuarios en aquellos activos sensitivos que lo ameriten.

2.4.7 Si se va a disponer de equipo que contiene información sensitiva deberá hacerse de forma segura con un método que no permita acceder los datos una vez el equipo esté fuera de las facilidades de La Autoridad.

2.4.8 La Oficina de Sistemas de Información adoptará los controles necesarios para evitar que de forma intencionada o accidental se inicien ataques desde sus redes internas hacia otros sistemas de información externos.

Sección 2.5- Personal

2.5.1 La Autoridad establecerá controles en el reclutamiento del personal de sistemas de información de tal manera que se verifique su conocimiento en el área técnica y su reputación en el área profesional y firmará acuerdos por escrito de no divulgación antes de exponerlo a datos confidenciales u otros activos sensitivos.

2.5.2 Deberán establecerse controles para el manejo de la terminación de empleados en La Autoridad de tal manera que estas circunstancias no afecten la seguridad de la información ni de los sistemas. Para esto deberán establecerse procedimientos que incluyan una comunicación efectiva entre el área de Recursos Humanos, el área en que trabaja el empleado y el área de Sistemas de Información.

ARTÍCULO 3: PROTECCIÓN Y SEGURIDAD DE INFORMACIÓN

Sección 3.1 – Fiscalización

3.1.1 Toda información, dato, obra, escrito, documento, programa, acción, privilegio, patente, derecho de autor, o cualquier otro derecho que surja, se cree o modifique, mediante el uso de las computadoras y relacionada al curso operacional de La Autoridad, será propiedad de ésta aunque la información, dato, obra, escrito, documento, programa, acción, privilegio, patente, derecho de autor haya surgido mediante el esfuerzo personal del usuario. Deberá mantenerse el carácter confidencial de la misma de acuerdo a la legislación y reglamentación vigente y aplicable a los Departamentos y entidades públicas del Gobierno de Puerto Rico.

3.1.2 La información contenida en las computadoras, sistemas, correspondencia electrónica, documentos, programas y servicios asociados, tanto internos como externos es para uso oficial. Su reproducción y uso deberá ser cónsono con esto; sin menos cavar las disposiciones del Artículo 6 de esta Carta Circular.

3.1.3 La Oficina de Sistemas de Información de La Autoridad, asignará las claves de acceso a la red de las unidades asignadas a los usuarios, para asegurar que otra persona no pueda acceder a la información allí contenida.

3.1.4 Si el usuario tiene que abandonar el área de trabajo por tiempo prolongado, deberá apagar la unidad, para evitar dejar documentos u hojas de trabajo abiertos y accesibles.

3.1.5 La Autoridad se reserva el derecho de auditar, vigilar y fiscalizar los sistemas de correspondencia electrónica y todos los servicios computadorizados para garantizar que su propiedad se utilice para los propósitos y gestiones relacionadas con el trabajo. Estas auditorías se realizarán periódicamente o al azar, o cuando exista una investigación sobre una situación en particular. La Oficina del Contralor de Puerto Rico y otras agencias con jurisdicción, podrán realizar auditorías a los sistemas de información, con previo aviso.

ARTÍCULO 4: USO Y MANEJO ADECUADO DEL SISTEMA DE INFORMACIÓN

Sección 4.1 Uso, Manejo y Acceso a Internet

4.1.1 Los sistemas de comunicación y acceso al Internet son propiedad de La Autoridad y se ofrecerán a los usuarios como herramienta de trabajo en el desempeño de sus funciones; sin menospreciar las disposiciones del Artículos 6 de esta Carta Circular. Se prohíbe terminantemente el uso de los sistemas de computadoras y comunicaciones de La Autoridad para propósitos personales. Ver Artículo 6 "USOS RAZONABLES DEL SISTEMA DE INFORMACIÓN".

4.1.2 El acceso a Internet será autorizado única y exclusivamente por el Director Ejecutivo o el Oficial Principal de Informática de la Oficina de Sistemas de Información o, en su defecto, la persona que el Director Ejecutivo autorice.

4.1.3 El Internet, como privilegio, requiere respetar los derechos de otros usuarios, respetar la integridad de los sistemas y recursos físicos relacionados y observar las leyes, reglamentos y obligaciones contractuales relativamente. Se prohíbe modificar los privilegios de acceso a las redes de información, internas o externas, para obtener acceso no autorizado a dichos recursos.

4.1.4 El usuario de Internet es responsable por el uso de su cuenta y es responsable de salvaguardar su contraseña y no divulgarla. En todo momento se presumirá que el acceso a toda información, dato, obra, escrito, documento, programa, acción, y/o sistema interno o externo lo realiza el usuario mediante cuya contraseña se obtuvo acceso al uso de las computadoras, salvo prueba en contrario.

4.1.5 Se prohíbe codificar, asignar contraseñas, o modificar de manera alguna la información, mensajes de correo electrónico, o archivos propiedad de La Autoridad, con el propósito de impedir que alguien pueda leerlos, entenderlos o utilizarlos o con el propósito de falsear o alterar el nombre del usuario, la fecha de creación o modificación u otra información que se utilice regularmente para identificar la información, mensajes o archivos, si no obtiene previamente el consentimiento por escrito del Director Ejecutivo. En el caso de que por razones de seguridad se permita codificar, asignar contraseñas o modificar alguna información a fines de evitar que otras personas puedan leerla, La Autoridad estará facultada en todo momento para decodificar la misma y restituirla a su estado original y el usuario será responsable de proveer todos los datos para lograr acceso.

4.1.6 Se prohíbe que los usuarios modifiquen los parámetros o configuración de las computadoras de La Autoridad para darle capacidad de recibir llamadas telefónicas o cualquier otro tipo de acceso o conexión remota que permita intrusiones no autorizadas a la red de La Autoridad, sin mediar consentimiento previo, por escrito, del Director Ejecutivo.

4.1.7 En aquellas áreas remotas donde La Autoridad no pueda suplir acceso al Internet, solo podrán ser utilizadas cuentas de acceso al Internet tramitadas por la Oficina de Sistemas de Información o su representante autorizado.

4.1.8 Queda expresamente prohibido acceder o instalar programas obtenidos a través del Internet, aunque sean gratis, de prueba o por tiempo limitado. Solamente estará autorizado a acceder o instalar programas obtenidos a través del Internet la Oficina de Sistemas de Información luego de una evaluación de la licencia por el Oficial Pricipal de Informática y con una autorización del Director Ejecutivo o su representante autorizado. De igual forma, se prohíbe utilizar el Internet para copiar, acceder o enviar programas protegidos por las leyes de derecho de autor.

4.1.9 El acceso a información o a una cuenta ajena sin autorización, obtenido mediante la modificación de privilegios de acceso o la interceptación de información en cualquier otra manera está prohibido, por lo que tal conducta se castigará conforme a la legislación local y federal vigente y a las normas aplicables que rigen la conducta de los empleados.

4.1.10 La comunicación con Internet desde adentro de la agencia deberá estar controlada por un *firewall* (Servidor de Seguridad de Computadoras y Redes).

4.1.11 Si existe la necesidad de acceder a la red interna desde afuera de las facilidades de La Autoridad (por ejemplo, para que un empleado realice un trabajo en un

programa de aplicación desde Internet), deberán existir los controles de autenticación, autorización, confidencialidad, integridad y monitoreo necesarios para proteger los sistemas y la información.

4.1.12 Si se determina que hay datos sensitivos pasando a través de redes que no son seguras (como Internet o redes inalámbricas), se deberán tener los controles necesarios para garantizar la confidencialidad, como por ejemplo, el uso de encripción.

4.1.13 Las operaciones realizadas a través de la Internet pueden generar responsabilidad por parte de las entidades gubernamentales del Gobierno de Puerto Rico, por lo que los usuarios que tengan acceso al Internet a través de La Autoridad no tienen expectativa de privacidad alguna con relación al uso y los accesos realizados a través de la Internet. La Autoridad se reserva el derecho a intervenir y auditar los accesos realizados por los usuarios a través de su sistema de información, el acceso a la Internet y el contenido de lo accedido.

4.1.14 La Autoridad no se responsabiliza por la validez, calidad, contenido o corrección de la Información contenida en la Internet.

4.1.15 La publicación de información de la entidad gubernamental a través de la Internet deberá ser debidamente autorizada por el Director Ejecutivo o la persona a quien éste delegue.

4.1.16 En caso de que La Autoridad determine brindar servicios de la agencia a los ciudadanos a través de Internet deberán tomarse en cuenta los siguientes elementos en el estudio de viabilidad para la implantación del programa:

a. Un diseño de seguridad.

b. La integración de mejores prácticas de seguridad en programación para evitar el acceso no autorizado y/o malicioso a través de Internet.

c. Un *firewall* (Servidor de Seguridad de Computadoras y Redes) que permita controlar el acceso al programa desde Internet.

d. Asegurar que si el servicio que está disponible maneja datos sensitivos sea instalado en una red alterna. En este caso el programa deberá funcionar en una red alterna y segura que permita el acceso desde Internet y a la misma vez permita un acceso controlado a la red interna para el intercambio controlado y monitoreado de datos.

e. Cerciorarse que si el servicio ofrecido a través de Internet maneja datos sensitivos, se haya implantado un sistema de detección de intrusos.

Sección 4.2 **Uso y Manejo Adecuado del Correo Electrónico**

4.2.1 Los sistemas de comunicación electrónica y toda información contenida en los mismos son propiedad de La Autoridad. Por esta razón, toda la información y mensajes creados y enviados, a través de los sistemas se consideran documentos de La Autoridad; sin menoscabar las disposiciones del Artículo 6 de esta Carta Circular.

4.2.2 Las cuentas individuales de acceso al correo electrónico las asignará la Oficina de Sistemas de Información o su representante autorizado.

4.2.3 Los usuarios del correo electrónico están obligados a respetar los derechos de otros usuarios, respetar la integridad de los sistemas y recursos físicos relacionados y observar las leyes, reglamentos y obligaciones contractuales relevantes.

4.2.4 El usuario de correo electrónico es responsable por el uso de su cuenta y es responsable de salvaguardar su contraseña y no divulgarla.

4.2.5 En aquellas áreas remotas donde La Autoridad no pueda suplir acceso al Internet, solo podrán ser utilizadas cuentas de acceso al Internet tramitadas por la Oficina de Sistemas de Información o su representante autorizado.

4.2.6 Queda expresamente prohibido utilizar el correo electrónico para enviar mensajes que puedan considerarse irresponsables, molestosos, hostigantes, u ofensivos, incluyendo pero no limitados a comentarios o imágenes de contenido sexual, racial y/o que pueda contener lenguaje ofensivo o soez.

4.2.7 Queda expresamente prohibido utilizar el correo electrónico para recibir o enviar programas protegidos por las leyes de derecho de autor.

4.2.8 Se prohíbe leer, revisar o interceptar cualquier tipo de correspondencia electrónica de persona no autorizada por el Director Ejecutivo para fiscalizar el uso adecuado del sistema de información, sin el conocimiento o consentimiento expreso del remitente y del destinatario.

4.2.9 Se prohíbe que los usuarios se suscriban a listas de correo electrónico o que participen en grupos de noticias que divulguen información o mensajes ajenos a las funciones y deberes a los que se desempeñan en La Autoridad.

4.2.10 La Oficina de Sistemas de Información deberá establecer claramente una norma con relación a enviar por medio del correo electrónico documentos que contengan información confidencial de la agencia o que contengan información en los cuales se comenten asuntos internos de la agencia que no deben ser divulgados, conforme a las normas que rigen la conducta de los empleados. De ser necesario enviar tal información sensitiva, la misma deberá ser cifrada (*encrypted*) para evitar su divulgación. De sospecharse la interceptación o divulgación de tal información, se deberá informar a la Oficina de Sistemas de Información inmediatamente, de manera que puedan tomar las medidas cautelares que procedan.

4.2.11 Los usuarios no podrán utilizar o acceder a cuentas de correo electrónico distintas a las cuentas oficiales de la agencia, a menos que estén autorizados a tal uso.

Sección 4.3 - <u>Disposiciones Adicionales sobre el Uso Adecuado de los Equipos y el Sistema de Información</u>

4.3.1 Los equipos y sistemas de La Autoridad son propiedad de esta Agencia y solo podrán utilizarse para propósitos lícitos, prudentes, responsables y dentro de las funciones o poderes designados.

4.3.2 Todos los equipos y sistemas de La Autoridad deberán estar protegidos por códigos de usuarios y contraseñas.

4.3.3 Por razón de que todos los sistemas y equipos pertenecen a La Autoridad y deberán ser utilizados de la forma que especifica esta carta circular, los usuarios del sistema no albergan expectativa de intimidad con relación a cualquier información, documento, archivo texto, o mensaje creado, recibido o enviado a través del sistema de correo electrónico, aunque los mismos sean creados conforme a las normas de usos razonables que se contienen en esta circular.

4.3.4 La Autoridad tiene sistemas de registros de los accesos a los equipos y sistemas de su propiedad. Estos registros anotan toda actividad de los usuarios de los mismos, para fines de verificar el cumplimiento de estas normas y toda la reglamentación y legislación aplicable.

4.3.5 Todos los archivos que se creen en los equipos y sistemas deberán ser guardados en el directorio asignado a cada usuario dentro de la Intranet con el propósito de protegerlos adecuadamente mediante los mecanismos de resguardo (*"backup"*).

4.3.6 La Autoridad se reserva todo derecho de auditar, incautar o remover los equipos y sistemas para garantizar que los mismos se utilicen de manera cónsona con todas las normas aplicables.

4.3.7 Se prohíbe la posesión, manejo, distribución o instalación de cualquier programa, aplicación, utilidad o recurso de los utilizados y creados para burlar aditamentos y parámetros de seguridad de los equipos y sistemas electrónicos.

4.3.8 El Director Ejecutivo podrá ordenar que se realice una auditoría interna cuando exista una investigación en contra de cualquier funcionario sobre alguna violación a las disposiciones aplicables de los Reglamentos de La Autoridad y Cartas Circulares.

4.3.9 La Oficina de Sistemas de Información de la Autoridad deberá desarrollar procedimientos para detectar, reportar y responder a incidentes de seguridad incluyendo límites para esos incidentes en términos de tiempo máximo y tiempo mínimo de respuesta. Todos los empleados y contratistas deberán conocer los procedimientos para informar los diferentes tipos de incidentes.

4.3.10 La Oficina de Sistemas de Información de la Autoridad es responsable de diseñar procedimientos que permitan que los cambios a la seguridad de los sistemas sean realizados y documentados adecuadamente y que esta documentación a su vez sea asegurada.

4.3.11 La Oficina de Sistemas de Información de la Autoridad es responsable de proveer adiestramientos a toda la gerencia y los supervisores de La Autoridad para que estén al tanto de los controles de seguridad y los beneficios correspondientes.

4.3.12 El personal de Oficina de Sistemas de Información de la Autoridad deberá estar adiestrado y con conocimientos actualizados sobre los aspectos de seguridad de sus áreas.

4.3.13 La Oficina de Sistemas de Información de la Autoridad es responsable de crear mecanismos de capacitación para todos los empleados conozcan los procedimientos de seguridad que le apliquen.

4.3.14 El acceso a las facilidades de sistemas de información deberá estar controlado para que solamente el personal autorizado pueda utilizarlas.

4.3.15 Cualquier equipo usado fuera de la agencia deberá estar autorizado por La Autoridad y deberá haber procedimientos para controlar su utilización, los

cuales serán adoptados por medio de un formulario que a esos efectos se cree por la Oficina de Sistemas de Información previa autorización del Director Ejecutivo.

4.3.16 Los contratos hechos con terceros deberán incluir la salvaguarda de los activos sensitivos, especialmente cuando los servicios contratados incluyen el manejo de estos activos fuera de las facilidades de La Autoridad. De hecho, si el servicio suministrado por terceros incluye que parte de los procesos corren en las facilidades de los contratistas deberán establecerse controles de mutuo acuerdo para proteger la información y estos acuerdos deberán ser parte del contrato.

4.3.17 El titular de los derechos relativos a las creaciones de funcionarios gubernamentales o por encargo de éstos es el Gobierno de Puerto Rico. Los usuarios de los sistemas de información están obligados a respetar los derechos de propiedad intelectual de los autores de las obras, programas, aplicaciones u otros, manejadas o accedidas a través de dicho sistema.

4.3.18 Los programas y recursos utilizados en los sistemas de información de La Autoridad deben tener su correspondiente licencia vigente o autorización de uso para poder ser utilizadas. Dichos programas sólo podrán ser instalados por personal autorizado a tales efectos. Además, no podrán instalarse programas sin la previa autorización de la Oficina de Sistemas de Información, aunque sean programas libres de costos.

4.3.19 Los programas y aplicaciones contenidos en los sistemas de información no podrán reproducirse sin autorización o ser utilizados para fines ajenos a las funciones o poderes de la entidad gubernamental; sin menoscabar lo dispuesto en el Artículo 6 de esta Carta Circular.

ARTÍCULO 5: POLÍTICAS ANTIDISCRIMEN

Sección 5.1 Prohibiciones

5.1.1 Existe una prohibición absoluta y cero tolerancia a la utilización de la computadora o del sistema de correo electrónico para enviar, recibir, o crear mensajes o documentos de contenido discriminatorio por razón de raza, género, credo, ideas políticas u origen social o nacional, o que puedan ser catalogados como hostigamiento sexual.

5.1.2 Está prohibido el manejo o transmisión de información de material obsceno, profano u ofensivo a través del sistema de computadoras y/o del sistema de comunicación electrónica de La Autoridad. Esto incluye, mas no se limita a, todo

tipo de información, mensajes o imágenes de contenido sexual o pornográfico, bromas de cualquier forma o cualquier chiste o comentario que pueda violar la política contra el discrimen u hostigamiento sexual promulgada por La Autoridad.

5.1.3 Queda expresamente prohibido utilizar el sistema de información electrónico en forma irresponsable, molestosa, hostigante u ofensiva, y utilizar lenguaje impropio para ejecutar las funciones asignadas a cada usuario del sistema.

5.1.4 Se prohíbe la divulgación por cualquier medio de cualquier tipo de opinión personal específica con relación a raza, origen nacional, sexo o género, orientación sexual, edad, ideas o creencias religiosas o políticas, así como opiniones sobre personas con impedimentos físicos o mentales.

ARTÍCULO 6: USOS RAZONABLES DEL SISTEMA DE INFORMACIÓN

Sección 6.1 – Definición

Se entenderá uso razonable, prudente y moderado de los equipos y sistemas de La Autoridad para propósitos personales, fuera de horas laborables y dentro de los espacios de tiempo dispuestos para estas diligencias, o mediando una autorización del Director Ejecutivo, siempre y cuando su utilización no viole alguna de las normas establecidas en esta carta circular, ni la reglamentación o legislación aplicable.

Sección 6.2 - Usos Razonables del Sistema y Equipos

6.2.1 Acceder a páginas de Internet para propósitos de estudios, desarrollo personal o profesional. Esto incluye publicaciones seriadas, periódicos, servicios académicos y educativos.

6.2.2 Acceder a cuentas personales de correo electrónicas no creadas por La Autoridad fuera de horas laborables y en una manera cónsona con las normas establecidas en estas normas.

6.2.3 Utilizar los programas de procesamiento de palabras, hojas de cómputos, u otros que estén instalados en los equipos y sistemas de la Autoridad que no contengan información confidencial; con propósitos de estudios o desarrollo personal o profesional.

6.2.4 El hecho de que un usuario utilice los equipos y sistemas de La Autoridad bajo las disposiciones de este artículo, no lo exime de la facultad de La Autoridad

para fiscalizar, evaluar y disciplinar el uso de los mismos conforme a estas normas, ni le confiere el derecho o excepción alguna que lo distinga de un usuario regular que utilice el sistema o los equipos durante horas laborables.

ARTÍCULO 7: MEDIDAS ADICIONALES

Sección 7.1 – Medidas por Violación a las Disposiciones de esta Carta Circular

7.1.1 Se tomarán las medidas disciplinarias, administrativas, civiles y/o criminales que correspondan conforme las leyes, reglamentos, normas y otros aplicables; contra los usuarios que violen las normas establecidas por esta Carta Circular.

7.1.2 En cualquier momento se podrá impedir, restringir, limitar o modificar los accesos de un usuario a los equipos y sistemas de La Autoridad con el propósito de conducir una investigación, de llevar a cabo una auditoría, mejorar la seguridad, o tomar medidas de precaución en la protección de lo recursos de esta Agencia.

7.1.3 La Autoridad se reserva el derecho de presentar acusaciones criminales por las actuaciones que constituyan delito federal o estatal aunque no estén expresamente prohibidas por las normas que se establecen en esta Carta Circular. No obstante, podrá radicar querellas o solicitar la intervención de las agencias pertinentes, como por ejemplo la Oficina de Ética Gubernamental, entre otras.

7.1.4 A los fines de esta Carta Circular, una actuación o conducta imprudente, irresponsable o abusiva significa cualquier acción que ponga en riesgo la seguridad, integridad, y confiabilidad de los equipos, redes, programas, sistemas, información, mensajes de correo electrónico, o archivos propiedad de la Autoridad. Además incluye cualquier actuación que pueda causar u ocasionar daños físicos, morales, problemas interpersonales, menoscabo a la reputación de empleados o funcionarios de La Autoridad o personas ajenas a esta Agencia, el Director Ejecutivo o a esta institución.

7.1.5 Es obligación de todo usuario de los recursos de La Autoridad comunicar al Director Ejecutivo o su representante designado, cualquier situación incidente o problema de seguridad, acceso indebido o violación voluntaria o involuntaria de estas normas.

ARTICULO 8: DEFINICIONES

1. *Adware* – Es un programa que se instala inadvertidamente en una computadora y que su principal propósito es desplegar ante el usuario anuncios y propaganda pero también puede tener un comportamiento como el spyware.

2. Antivirus - Programa que protege a los sistemas de los ataques de virus conocidos.

3. Autenticación – Es el proceso por el cual una persona presenta información que lo identifica ante un sistema de información y el sistema compara la información contra su base de datos para validarla.

4. Autorización – Es el proceso por el cual se adjudican privilegios específicos a una persona para el uso de recursos en los sistemas de información.

5. Cifrar - Proceso en el cual los datos se convierten a un formato que no puede descifrarse fácilmente por personas no autorizadas a acceder los mismos.

6. Confidencialidad – Es la característica que se le da a una información para que pueda ser vista solamente por personas autorizadas.

7. Contraseña - Secuencia de caracteres que se utiliza para comprobar que el usuario que está requiriendo acceso a un sistema es realmente ese usuario.

8. Datos sensitivos – Datos que contienen información financiera, de los ciudadanos, de los recursos humanos u otra información crítica para la operación de la agencia.

9. Encripción – Es el proceso por el cual unos datos se transforman en información no entendible por aquellos que no están autorizados a verlos.

10. *Firewall* (Servidor de Seguridad de Computadoras y Redes) – Aplicación, equipo o conjunto de ambos que protege los recursos de la red de accesos no autorizados. En el caso de las aplicaciones son programas que reside en una computadora o en un equipo especializado y que permiten controlar el tráfico de información entre varias redes. Tradicionalmente protegen la red interna de una entidad del acceso indebido de usuarios que vienen de Internet.

11. Integridad – Es el proceso que permite proteger información de alteraciones indebidas.

12. Lenguaje Discriminatorio - Expresiones que podrían percibirse como ofensivas, ya sea por razones de raza, sexo, origen, nacionalidad, orientación sexual, edad, impedimento, religión o ideales políticos.

13. Programa – Conjunto de instrucciones que permite que una computadora lleve a cabo una función. Puede haber programas de sistema que controlan el funcionamiento de las computadoras y de las redes de informática y también programas de aplicación que facilitan y/o automatizan las operaciones de una entidad para que no tengan que ser llevadas a cabo de forma manual.

14. Sistema de Detección de Intrusos – Es un programa que reside en una computadora o en un equipo especializado y que permite detectar ataques o intentos indebidos de acceso hacia un sistema de información.

15. Seguridad de Informática – Protección de los sistemas de información en contra del acceso o modificación física o electrónica de la información; protección en contra de la negación de servicios a usuarios autorizados o de la disponibilidad de servicios a usuarios no autorizados; las políticas, normas, medidas, proceso y herramientas necesarias para detectar, documentar, prevenir y contrarrestar los ataques a la información o servicios antes descritos; los procesos y herramientas necesarias para la restauración de la información o los sistemas afectados por las brechas en la seguridad; disponibilidad y protección de los recursos requeridos para establecer dicha seguridad.

16. *Spyware* – Es un programa que se instala inadvertidamente en una computadora y que propaga sin autorización información sobre el usuario de la computadora y sus hábitos de utilización de Internet.

17. Usuario - Empleado del gobierno o contratista que tiene acceso autorizado a los sistemas.

18. Virus - Programa de computadora cuyo fin es hacerle daño a la computadora donde reside.

ARTICULO 9: INFORMES

El Director de la Oficina de Sistemas de Información deberá preparar y presentar ante el Director Ejecutivo informes semestrales sobre la implantación y cumplimiento con las disposiciones de la presente Carta Circular y la política pública dentro de las cuales están enmarcadas. Dichos informes deberán ser presentados ante el Director Ejecutivo

en los meses de enero y julio de cada año, haciéndose la salvedad de que se podrán requerir informes adicionales según sea necesario.

En San Juan, Puerto Rico a 21 de marzo de 2012

Antonio Ríos Díaz
Director Ejecutivo
Autoridad de Desperdicios Sólidos