



**GOBIERNO DE PUERTO RICO
COMPAÑIA DE PARQUES NACIONALES**

**REGLAMENTO PARA USUARIOS QUE
MANEJAN SISTEMAS DE INFORMACION
DE LA COMPAÑIA DE PARQUES NACIONALES**

OCTUBRE 2012

Contenido

ARTÍCULO 2 - TITULO.....	5
ARTÍCULO 3 - BASE LEGAL.....	5
ARTICULO 4 - PROPÓSITO	5
ARTÍCULO 5 - APLICABILIDAD	5
ARTICULO 6 - DEFINICIONES.....	6
ARTÍCULO 7 - NORMAS PARA LA ADMINISTRACIÓN Y MANEJO DE LOS SISTEMAS DE INFORMACIÓN.....	8
Sección 7.1 - Políticas Generales.....	8
Normas Relacionadas a los Equipos de Computadoras	9
Normas Relacionadas a los Accesos a los Diferentes Sistemas.....	10
Normas Relacionadas a la Información	11
Sección 7.2 - Responsabilidades de la “OSI” en Cuanto a la Administración e Implantación de las Políticas y Normas Contenidas en el presente Reglamento.....	12
Sección 7.3 - Políticas Dirigidas a Salvaguardar la Seguridad de Información	14
No Divulgación de Información Confidencial.....	14
Normas de Claves de Acceso (“ <i>username</i> ” y “ <i>password</i> ”).....	15
Sección 7.4 - Responsabilidades del Usuario en el Uso de los Sistemas y Equipos de Información.....	16
Sección 7.5 - Política para Envío y Recibo de Correo Electrónico, Correspondencia Interna y Servicio de Internet	20
ARTÍCULO 8 - SOLICITUD DE ACCESO Y MANEJO A LOS SISTEMAS DE INFORMACIÓN (CONTRASEÑA)	22
Sección 8.1 - Acceso.....	22
Sección 8.2 - Creación de Claves de Acceso	24
Sección 8.3 - Uso de la Contraseña.....	24
Sección 8.4 - Expedientes sobre Acceso a Sistemas de Información	25
Sección 8.5 - Accesos a las Aplicaciones de Producción y de Prueba	25
ARTÍCULO 9 - SEGURIDAD EN LOS EQUIPOS	26
Sección - 9.1	26
Inventario	26
Seguro	26

Sección 9.2 - Responsabilidades del Usuario para con los Diskettes, CD's, "Pen drive" o Cualquier Otro Medio para Almacenar Información	27
Sección 9.4 - Computadoras Portátiles	29
Sección 9.5 - Telecomunicaciones	30
ARTÍCULO 10 - PROTECCIÓN CONTRA LOS VIRUS	31
Sección 10.1 - Programa	31
ARTICULO 11- USO DEL CORREO ELECTRÓNICO Y SISTEMAS DE INTERNET	32
Sección 11.1 - Objetivo.....	32
Sección 11.2 - Utilización.....	32
Sección 11.4 - Aceptaciones	36
Sección 11.5 - Etiqueta en el Uso de Internet.....	36
ARTICULO 11 - PROHIBICIONES PARA USO DE EMAIL, SISTEMAS, INTERNET Y COMPUTADORAS	37
Sección 11.1 - Prohibiciones de Uso de Computadoras y Aplicaciones.....	37
Sección 11.2 - Prohibición de Correos Electrónicos (e-mails) e Internet.....	37
Sección 11.3 - Prohibiciones para el Uso de los Sistemas.....	38
ARTÍCULO 12 - CLAUSULA DE SALVEDAD.....	38
ARTÍCULO 13 - VIGENCIA Y APROBACIÓN.....	39

NOTA ACLARATORIA: Para propósitos de carácter legal en relación con la Ley de Derechos Civiles del 1964, el uso de los términos **empleados, supervisores, superintendentes, gerentes, directores** y cualquier otro que pueda tener referencia a ambos géneros, incluye tanto el masculino como el femenino.

ARTÍCULO 1 - INTRODUCCIÓN

La Compañía de Parques Nacionales de Puerto Rico, en adelante “la Compañía”, tiene como misión operar, desarrollar y preservar todos los parques naturales, recreativos e históricos declarados como parques nacionales; promoviendo la protección, conservación y uso recreativos de parques, playas, bosques, monumentos históricos y naturales para el disfrute de las presentes y futuras generaciones.

Como parte de los esfuerzos de la Oficina de Sistemas de Información, en adelante “OSI”, para establecer mejores medidas de seguridad que protejan a los sistemas de información administrativos, se produce este Reglamento para Usuarios que Manejan Sistemas de Información de la Compañía de Parques Nacionales de Puerto Rico. La “OSI” tiene como misión ofrecer los servicios electrónicos de manera segura y eficaz. Sin embargo, la dependencia de la tecnología crea serios riesgos a la seguridad, por lo que se requiere de unos mecanismos que eliminen o que reduzcan los riesgos a un nivel aceptable.

Este documento es una guía para los usuarios de los sistemas de información de la Compañía de Parques Nacionales de Puerto Rico. El mismo está basado en la Ley Núm. 151 de 22 de junio de 2004, según enmendada. Este incluye desde las responsabilidades de la “OSI” como custodio oficial de los equipos electrónicos, responsabilidades de los Usuarios hasta los procesos de decomisos de equipos electrónicos.

Si bien es cierto que hoy tenemos acceso a un mundo cibernético ilimitado llamado Internet, también es cierto que dicho mundo puede provocar serios problemas en nuestro sistema si no se toman las medidas de seguridad adecuadas. De igual manera que muchas personas utilizan el Internet en busca de información para enriquecimiento intelectual, hay quienes se dedican a crear programas y situaciones para destruir los sistemas de otros.

La “OSI”, en ánimo de mantener al usuario informado, provee estas normas con el fin de que cada Oficina de la Compañía cumpla con las mismas. Se espera que tanto el usuario individual, como las Oficinas e Instalaciones de la Compañía de Parques Nacionales aseguren el fiel cumplimiento de éstas. Este Reglamento ayudará a mantener el orden; prevenir el manejo inadecuado de los equipos de computadoras por parte de los usuarios;

establecer responsabilidades, tanto a los usuarios como a la “OSI” y establecer métodos de seguridad en los equipos y la red de telecomunicaciones.

De no existir una seguridad adecuada estaríamos expuestos a:

- Daños a equipos sofisticados, y por consiguiente, pérdida de dinero.
- Daños a la reputación de la Compañía de Parques Nacionales de Puerto Rico y el Gobierno de Puerto Rico. Divulgación de información confidencial (accidental o intencional).
- Uso indebido o mal uso de los sistemas.
- Demandas por violación a la confidencialidad y privacidad.
- Infección o entrada a los sistemas por virus o personas no autorizadas.

Los empleados, auditores externos e internos, consultores y servicios profesionales contratados, no solamente son usuarios simples de los sistemas de información, sino que en ocasiones desempeñan variadas funciones en el uso de los sistemas computadorizados, creadores de bases de datos, responsables de centros de información y responsables del manejo de información confidencial dependiendo de sus funciones.

Como usuarios de los equipos computadorizados, los empleados, auditores externos e internos, consultores, servicios profesionales contratados por la Compañía de Parques Nacionales o del Gobierno de Puerto Rico deben seguir los cuatro principios básicos señalados en este documento. Estos principios básicos son los siguientes:

1. Como responsables de los equipos de sistemas de información que nos son asignados para realizar nuestras tareas, debemos proveer protección a los equipos, programas y a la información de las computadoras.
2. Como usuarios tenemos la responsabilidad de controlar esencialmente el uso de las computadoras y cubrir extensamente las aplicaciones técnicas de la administración, procesamiento de datos, modelos de hojas de trabajo electrónicas y programas computadorizados.

3. Como desarrolladores debemos incorporar los controles adecuados a los sistemas.
4. Todo equipo de los sistemas de información y los servicios asociados tanto internos como externos, el sistema de correspondencia electrónica (“e-mail”), la Intranet o redes, el acceso a la Internet, los documentos y programas que existen en la misma, son propiedad de la Compañía de Parques Nacionales y del Gobierno de Puerto Rico, sólo podrán utilizarse para propósitos lícitos, prudentes, responsables y dentro de las funciones o poderes de la Compañía.

ARTÍCULO 2 - TITULO

Este documento se conocerá como el Reglamento para Usuarios que Manejan Sistemas de Información de la Compañía de Parques Nacionales de Puerto Rico.

ARTÍCULO 3 - BASE LEGAL

- Ley Núm. 114 de 23 de junio de 1961, según enmendada
- Ley Núm. 151 de 22 de junio de 2004, según enmendada

ARTICULO 4 - PROPÓSITO

El propósito de este Reglamento es establecer políticas, normas y guías para la administración y el manejo de los sistemas de información de la Compañía 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 de la Compañía y evitar con ellos un manejo indebido de éstos, bien sea por actos intencionales o accidentales.

ARTÍCULO 5 - APLICABILIDAD

Estas guías y normas aplican a todos los empleados, empleados de otras agencias del Gobierno del Estado Libre Asociado de Puerto Rico en destaque, auditores externos e internos, consultores y servicios profesionales contratados de la Compañía de Parques

Nacionales o del Gobierno de Puerto Rico que en sus funciones y deberes, entre otros, utilizan los sistemas de información de la Compañía. La Compañía y todos los usuarios que tengan acceso a los diferentes sistemas, son responsables por cumplir las reglas establecidas en este documento.

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 de Producción** - Es el ambiente que utilizan los usuarios para sus funciones diarias. Cualquier cambio, entrada o eliminación de información afecta los archivos reales de la Agencia.
- B. Ambiente de Prueba** - Se puede utilizar para el análisis de nuevos programas, experimentos en telecomunicaciones y para el desarrollo de aplicaciones por el grupo de programación.
- C. Aplicación (“Software”)** - 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.
- D. 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.
- E. Clave de Acceso o “Password”** - Código que utiliza el usuario para comunicarse con la computadora. La clave es cualquier grupo de caracteres que identifique a un usuario en el sistema computadorizado.
- F. Compañía** - La Compañía de Parques Nacionales de Puerto Rico, (CPNPR).
- G. Computadora Personal (PC)** - Es aquella computadora (ya sea estilo torre, de escritorio o portátil) la cual ha sido adquirida o forma parte de los activos de la Compañía y es asignada a un empleado, auditor externo o interno, consultor y proveedor de servicios profesionales contratados por la Compañía de Parques

Nacionales y/o el Gobierno de Puerto Rico con el propósito de mejorar su ambiente de trabajo, mecanizar funciones y procesar información oficial en las mismas.

- H. Correo Electrónico o “E-mail”** - Es la herramienta de comunicación que permite el envío de mensajes de forma rápida entre usuarios. Es una herramienta de trabajo oficial, la cual ningún empleado o Supervisor puede hacer mal uso de ella.
- I. Director** - El Director Ejecutivo de la Compañía de Parques Nacionales de Puerto Rico.
- J. Ejecución** - Procesamiento de una transacción o grupo de transacciones en conjunto.
- K. 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, entre otros.
- L. Oficina** - Cualquier instalación que responda a los intereses de la CPNPR.
- M. OSI** - Oficina de Sistemas de Información.
- N. Periférico** - Cualquier componente externo a los componentes regulares de una computadora. Ej. Impresoras, scanner, etc.
- O. Recursos** - Son las diferentes estructuras o formas de organización electrónicas a través de las cuales se puede almacenar información o acceder utilizando una computadora. Los recursos más conocidos son: TRANSACCIONES, PROGRAMAS, DATA-SET, LIBRERIAS, DISCOS, etc.
- P. Usuarios** - Todo empleado registrado por la Oficina de Recursos Humanos de la CPN a tiempo completo o parcial que requiera el uso de una computadora para realizar su trabajo y al que se le otorga una clave de acceso a los Sistemas.

ARTÍCULO 7 - NORMAS PARA LA ADMINISTRACIÓN Y MANEJO DE LOS SISTEMAS DE INFORMACIÓN

La Compañía tiene como política administrativa el que cada empleado o usuario de sus sistemas de información haga un uso adecuado de los mismos, observando en todo momento las normas que para el manejo de tales sistemas y de los equipos de la Compañía se establecen en el presente Reglamento.

El uso adecuado a que se extiende esta política, incluye pero no se limita a la 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 en los sistemas de información y equipo de la Compañía.

Sección 7.1 - Políticas Generales

- A. Todo empleado o usuario de los sistemas de información de la Compañía deberá suscribir un documento titulado: “Acuerdo de Confidencialidad, Seguridad de Información y Protección de Equipos”, que le será entregado por la Oficina de Recursos Humanos de la Compañía y donde se detallarán los deberes y responsabilidades de tal empleado o usuario, en el uso de los Sistemas de Información y en cuanto a la protección de los equipos que para tales fines cuenta la Compañía. Dicho documento una vez firmado será entregado a la “OSI” de Información que será su custodio. Copia de este documento se hará formar parte del Expediente Personal del Empleado en Recursos Humanos. Contemporáneo con la entrega y firma del antes mencionado documento el empleado o usuario recibirá una orientación en torno a las normas, políticas y reglamentos de la Compañía que rigen el uso de sus sistemas de información y equipos.
- B. Las normas, políticas y reglas contenidas en el presente Reglamento podrán ser enmendadas o modificadas periódicamente para atemperarlas a nuevas necesidades operacionales o de servicios y a cambios en las leyes o reglamentos aplicables. Copia de tales enmiendas, serán entregadas a los empleados, quienes deberán acusar recibo de las mismas, al igual que en el caso del Acuerdo de Confidencialidad.

Normas Relacionadas a los Equipos de Computadoras

1. El usuario tendrá acceso a una computadora de la CPNPR. Sin embargo, no necesariamente el equipo asignado será para su uso exclusivo. Limitaciones de espacio y equipo podrían ser causa para que más de un usuario tenga acceso a una misma computadora.
2. El equipo es propiedad de la CPNPR y solamente la Oficina de Sistemas de Información tendrá acceso a los componentes y/o configuraciones de éste.
3. Por ser el equipo propiedad de la CPNPR, el usuario no está autorizado a mover de lugar, trasladar dentro o fuera de las instalaciones de la CPNPR, llevar consigo o prestado un equipo de computadoras.
4. El usuario no está autorizado a desarmar para añadir, eliminar, modificar o cambiar cualquiera de los componentes, tanto los internos como externos del equipo. Esta tarea es responsabilidad del personal de la “OSI” u otro personal técnico autorizado por esa Oficina.
5. El usuario deberá colaborar para que el equipo no sea accesible de manera fácil, particularmente fuera de las horas laborables. La Oficina de Sistemas de Información dará protección al contenido de los servidores solamente, no así a la información que se grabe en el disco duro u otro medio de almacenamiento (CD’s o *pen drives, etc.*) de cada computadora.
6. Es responsabilidad del usuario dar buen uso a su equipo, protegerlo con relación al polvo, humedad y otras condiciones extremas. Apagar el equipo antes de salir de la oficina se considera mejor que dejarlo encendido toda la noche o por varios días. La limpieza exterior del equipo es responsabilidad del usuario.
7. La oficina que posee el equipo deberá adquirir el mobiliario necesario para que se instale en un lugar adecuado. La localización de los cables, toma eléctrica y periféricos será responsabilidad del usuario y de su oficina.

8. Por ser un equipo sensitivo a fluctuaciones eléctricas, éste debe estar aislado de motores, equipo de calor y equipos de alto consumo de electricidad o magnéticos, ya que éstos afectan la operación del equipo y eventualmente dañan las computadoras.
9. El usuario notificará a la “OSI” cualquier irregularidad en el funcionamiento de su equipo.

Normas Relacionadas a los Accesos a los Diferentes Sistemas

- El acceso a los sistemas es de manera continua 24/7 excepto cuando se están realizando tareas de mantenimiento preventivo al sistema, procesos de resguardo (backups) y/o corriendo los ciclos operacionales diarios; esto varía con relación a los sistemas o servidores. Generalmente se avisa al usuario para que haga los ajustes correspondientes.
- Aunque los sistemas permiten acceso durante las 24 horas del día, el acceso a éste dependerá de la disponibilidad de las facilidades físicas, particularmente fuera de días y horas laborables. La “OSI” provee acceso a los sistemas, sin embargo el acceso a las facilidades dependerá de la necesidad de las diferentes instalaciones, el puesto que ocupe y la autorización de su Supervisor. En el caso de ser un empleado temporero y/o de alguna propuesta estatal o federal como “*PathStone*”, la autorización estará sujeta a la aprobación de la Oficina de Recursos Humanos, Oficina del Director Ejecutivo, Oficina de Finanzas y Presupuesto y la Oficina de Sistemas de Información. Además, el que los sistemas estén activos 24 horas, no significa que el usuario este autorizado para entrar a los mismos en periodos que esté fuera de sus horas laborables.
- Como parte de los procesos de separación de empleo de la CPNPR, la Oficina de Recursos Humanos le entregará el formulario de Certificación de Terminación de Empleo el cual deberá completar para desactivar las cuentas de acceso. De igual modo la Oficina de Recursos Humanos deberá notificar a la “OSI” cuando se realicen cambios de oficina, renuncia, jubilación, etc.
- Las transacciones que realizan los usuarios en los sistemas de la CPNPR, son almacenadas por éste en un archivo de transacciones. Cualquier irregularidad que

se detecte en el sistema como consecuencia del mal uso por parte de algún usuario, éste será responsable del mismo. El acceso a áreas sensitivas de los sistemas, modificación, eliminación o cualquier operación no autorizada se considerará como una falta.

- La “OSI” tiene la responsabilidad de garantizar que el acceso a los sistemas sea uno seguro y que los sistemas locales estén protegidos en todo momento. En caso de una situación que coloque a los sistemas en algún tipo de riesgo, la OSI bloqueará o interrumpirá el acceso hasta que la situación sea corregida.
- La OSI podrá suspender temporalmente el acceso a los sistemas, si existen condiciones inapropiadas para el acceso como son: condiciones eléctricas, ambientales, falta de aire acondicionado o situaciones de seguridad. Esto también aplica al mantenimiento del sistema y otros eventos que requieran la supervisión de los servicios.

Normas Relacionadas a la Información

- El usuario deberá velar por el fiel cumplimiento de las normas establecidas en este Reglamento, para garantizar la confidencialidad de la información, así como la seguridad de ésta.
- El usuario deberá almacenar sus documentos en los servidores asignados para este propósito. La “OSI” se encargará de hacer los resguardos (backups) diarios. El servidor posee directorios para cada usuario por oficina o instalación y un directorio común por cada oficina. Todos los directorios están protegidos de forma que solamente tendrán acceso a éstos los usuarios autorizados.
- No se prohíbe, pero tampoco se fomenta el uso de “pen drives” para almacenar documentos oficiales, ya que los mismos se dañan con facilidad y son fáciles de hurtar. La “OSI” no se hace responsable del rescate de documentos archivados en estos medios. Es responsabilidad de la oficina y del usuario dueño del equipo el dar la seguridad a sus documentos almacenados localmente en cada computadora.
- Aunque cada computadora tiene espacio disponible para almacenamiento en su disco local (C:\ y algunos casos D:\), no se recomienda almacenar documentos en

éste. Toda vez que si la computadora se daña la probabilidad de recuperar la información de la computadora es de un 1%. La Oficina de Sistemas de Información no se responsabilizará por la recuperación de datos en las computadoras. Es total responsabilidad de los usuarios mantener un “backup” de los documentos guardados en los discos antes mencionados.

Sección 7.2 - Responsabilidades de la “OSI” en Cuanto a la Administración e Implantación de las Políticas y Normas Contenidas en el presente Reglamento

La Oficina de Sistemas de Información tendrá las siguientes responsabilidades en torno a la implantación y aplicación de las normas contenidas en este Reglamento.

- A. Será responsable por la implantación, mantenimiento, revisión de los Programas de Seguridad de Sistemas de Información de la Compañía.
- B. Orientar y concienciar a los empleados y usuarios de tales sistemas, de las normas de seguridad, confidencialidad y protección de equipos que implica su uso.
- C. Administrar todo lo relativo al acceso a los sistemas de información, incluyendo pero no limitándose a, crear la identificación del usuario y la contraseña para cada usuario de computadora y sus aplicaciones.
- D. Verificar si los empleados o usuarios están cumpliendo con lo establecido en este Reglamento, en cuanto a la seguridad de información, el uso adecuado de los equipos y sistemas de información para lo cual podrán periódicamente:
 - 1. Realizar vigilancia y/o auditorías internas o externas.
 - 2. Investigar cualquier acto ilegal o impropio en el uso de tales sistemas.
 - 3. Revisar que los servicios del Internet se utilicen para fines legítimos de la Compañía en el desempeño de los deberes y responsabilidades del empleado o usuario de la Compañía.

4. Verificar que se le esté dando un uso apropiado al correo electrónico o cualquier otro método de comunicación electrónica provisto dentro de los Sistemas de Información de la Compañía.
 5. Eliminar los equipos en casos de fallas en el sistema o situaciones de emergencia.
 6. Evaluar y actualizar la eficiencia, la condición de los sistemas y equipos en la Compañía.
- E. Establecer controles que garanticen el buen funcionamiento de los Sistemas de Información a la hora de implantar nuevas aplicaciones y/o módulos en ambiente de producción. La “OSI” será responsable de implantar controles de acceso al Centro de Cómputos bajo las siguientes condiciones:
1. Debe proveer un control de acceso físico como: cerradura electrónica o de llaves, entre otros.
 2. Toda persona que visite las instalaciones deberá identificarse en un registro de visitas, inclusive los empleados de la Compañía.
- F. La “OSI” será responsable de mantener periódicamente activos y actualizados el resguardo de los “backups” de la información residente en los Servidores. Éstos residirán fuera del Centro de Cómputos, con el propósito de poder recuperar la mayor cantidad de información posible.
- G. La “OSI” será responsable de mantener periódicamente activos y actualizados los Manuales Operacionales de los Sistemas de Información, de sus Aplicaciones, y el Manual del Plan de Contingencia, a fin de garantizar la continuidad de las operaciones de la Compañía en un evento de emergencia.
- H. La “OSI” y los directores de las Oficinas son responsables de proveer un ambiente propio y seguro para el manejo y distribución de la información que se genera en forma de reportes de los sistemas. Este medio de información deberá ser procesado en un área de acceso limitado y solamente para el personal autorizado para tal función.

- I. La “OSI” deberá adquirir el “*hardware*” y el “*software*” de computadoras que sea compatible y de acuerdo a los estándares establecidos por la Compañía, y regulado por los reglamentos, normas y cartas circulares.
- J. La “OSI” es responsable de cualquier movimiento de los equipos y deberá reemplazar todo “*hardware*” dañado en las computadoras.
- K. La “OSI” es responsable de mantener activos y actualizados los sistemas antivirus para la protección de la información y los equipos.
- L. La “OSI” se encargará de eliminar y remover equipos de comunicación, computadoras y aplicaciones que no estén autorizadas y hayan sido adquiridas y/o instaladas por los empleados o usuarios ya sea para uso oficial o personal.
- M. La “OSI” podrá determinar los horarios de acceso de los sistemas y a las estaciones a las que los usuarios pueden acceder éstos.

Sección 7.3 - Políticas Dirigidas a Salvaguardar la Seguridad de Información

No Divulgación de Información Confidencial

1. Queda terminantemente prohibido el divulgar a terceros información confidencial de la Compañía; bien haya sido obtenida de los diferentes sistemas de información, por razón de las funciones, deberes del empleado o usuario.
2. Se prohíbe además, divulgar información confidencial a aquellos empleados que por la naturaleza de sus funciones, deberes o tareas no tienen acceso a la misma.
3. Se entenderá por información confidencial, aquella información interna de la Compañía relacionada con sus operaciones; incluyendo, pero sin limitarse a la información sobre las finanzas o contabilidad de la Compañía, información del personal, planes y/o estrategias de mercadeo, promoción, planes de desarrollo y toda la información provista por los clientes de la Compañía.
4. La violación de esta norma podrá conllevar la imposición de medidas disciplinarias cuya severidad dependerá de las circunstancias de cada caso.

Normas de Claves de Acceso (“username” y “password”)

Cada usuario tiene una clave de acceso para entrar a los diferentes sistemas. Esta clave se compone de un “username” y un “password” dependiendo del sistema autorizado.

1. Los “passwords” que se utilizan para acceder a las computadoras y correo electrónico tienen una validez de 60 días. Luego de este periodo, el usuario deberá cambiar su contraseña siguiendo el procedimiento establecido e indicado por el propio sistema de su computadora.
2. Las claves de acceso (*username* y *password*) a los diferentes sistemas no pueden ser transferidas, prestadas o reveladas a otra persona en ningún momento y bajo ningún concepto.
3. La violación a esta norma podrá conllevar la imposición de medidas disciplinarias cuya severidad dependerá de las circunstancias particulares de cada caso.
4. La identificación de usuario y contraseña serán revocadas y/o transferidas el mismo día en que el usuario cese en sus funciones, sea transferido o cuando haya sido descendido o ascendido de su puesto y sus nuevas funciones no requieran el uso de la computadora.
5. La Oficina de Recursos Humanos se encargará de notificar a la “OSI” de éstos cambios en el estado de empleo para que se tomen las medidas pertinentes en los Sistemas de Información.
6. La clave de acceso a los sistemas no es un derecho sino una herramienta de trabajo que le otorga la CPNPR y la “OSI” al empleado cuya posición así lo requiera. Por lo tanto, el usuario deberá hacer buen uso de ésta. La “OSI” tiene la potestad de bloquear de manera temporera o permanente el acceso a los sistemas a determinado usuario si entiende que éste está dando uso indebido al Sistema de Información y su accesibilidad pone en riesgo la seguridad de los datos en el sistema.

Sección 7.4 - Responsabilidades del Usuario en el Uso de los Sistemas y Equipos de Información

1. El usuario deberá velar por el fiel cumplimiento de las normas para garantizar la confidencialidad de la información, así como la seguridad de ésta.
2. El usuario deberá almacenar sus documentos en el servidor designado para este propósito, ya que al contenido de éste se le hacen resguardos (“backups”) periódicamente. El servidor posee directorios para cada usuario, por oficina o departamento y un directorio común por oficina. Todos los directorios están protegidos de forma que solamente tendrán acceso a éstos los usuarios autorizados por el Director de cada oficina.
3. Aunque hay algunos servicios que están a través del Internet todo el tiempo, el uso de éstos está restringido a ser utilizado sólo en el horario de trabajo que le corresponde a los usuarios del mismo. Por otra parte, el empleado sólo está autorizado a utilizar fuera de horas laborales el correo electrónico (“*Outlook Web Acces*”).
4. No se prohíbe, pero tampoco se fomenta el uso de "pen drives" para almacenar documentos oficiales, ya que los mismos se dañan con facilidad y son fáciles de hurtar. La “OSI” no se hace responsable del rescate de documentos archivados en estos medios. Es responsabilidad de la oficina y del usuario dueño del equipo el dar la seguridad a sus documentos almacenados localmente en cada computadora.
5. Aunque cada PC tiene espacio disponible en su disco local (c: \, *my documents*, *desktop*, etc...), no se recomienda almacenar documentos en este disco. Cualquier persona que tenga acceso a la PC, puede tener acceso a todos los documentos que se encuentran en ésta localmente, lo que puede resultar en la fácil divulgación de información sensible.
6. El usuario no está autorizado a llevar consigo “*pen drives*” u otro método de almacenamiento que contengan datos o información oficial y/o sensible de la CPNPR, ya que esta práctica podría resultar en el hurto, pérdida, divulgación o daños a información confidencial. Si el propósito de tener copias fuera de la oficina es para

resguardos; el mismo deberá estar bajo la custodia del Director o persona con mayor jerarquía dentro de la oficina.

7. El usuario deberá almacenar en su directorio documentos relacionados a su área de trabajo, el tener información personal o no oficial extraída utilizando los sistemas de la CPNPR es considerado una falta y la “OSI” podrá referir el caso a la Oficina de Recursos Humanos para ser investigado y la imposición de sanciones disciplinarias.
8. El usuario que posea información cuyo contenido sea obsceno, ofensivo, de contenido sexual explícito, de doble sentido y/o de otra índole que en nada tenga que ver con la tarea que realiza y que viole los reglamentos de la CPNPR y/o las leyes locales o federales estará sujeto a sanciones.
9. El usuario no puede de ninguna manera instalar aplicaciones propiedad de la CPNPR para su uso en otro equipo de computadora. De igual forma, el usuario no está autorizado a añadir programas y/o modificar éstos. La violación de Derechos de Autor y la piratería de “*software*” representan grandes multas, convicción de delito grave en el plano personal y cancelación de fondos federales.
10. La “OSI” tiene la potestad para cotejar cualquier contenido físico de cada PC, así como el contenido de los discos y el directorio, en caso de duda o sospecha razonable y/o a petición de los Auditores internos o externos.
11. Se considera una falta grave el que un usuario instale aplicaciones compradas para su uso personal en la PC de su Oficina. El usuario que tenga una PC a su cargo y posea aplicaciones ilegales será referido a la Oficina de Recursos Humanos para investigación y la imposición de sanciones disciplinarias.
12. El uso de los recursos tecnológicos para beneficio personal o el beneficio de terceros es una violación a las normas y conlleva serias sanciones. Esto aplica al uso de los recursos de computadoras, Internet y/o correo electrónico, para lucro personal o de terceros.
13. El uso de los equipos y unidades del computador, los programas, información y los sistemas de información para uso personal queda terminantemente prohibido.

14. Sólo podrán utilizarse productos enlatados (programas) en las distintas áreas de trabajo siempre que:
 - a. Éstos hayan sido legalmente adquiridos por la Compañía o el Estado Libre Asociado de Puerto Rico.
 - b. Las licencias para su uso están vigentes.
 - c. La utilización de éstos sea para mejorar la realización de las tareas de la Compañía.
 - d. La utilización de estos productos enlatados debe responder a los acuerdos establecidos en el contrato de utilización que la Compañía negoció al momento de la compra o adquisición del Estado Libre Asociado de Puerto Rico.
15. No se deberá 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 protejan, aunque éstos hayan sido adquiridos por el usuario. Estos productos, incluyen: aquellos programas de entretenimiento “Screen Savers” y de utilidades para impresoras.
16. Está prohibido el reproducir o duplicar cualquier programa adquirido o desarrollado internamente por la Compañía.
17. 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 y/o “copyright”, es un acto ilegal que expone a demandas, reclamaciones y/o multas a la Compañía.
18. Todo usuario de los sistemas de información que realice funciones de pruebas o de desarrollo, deberá utilizar un ambiente y los recursos designados como ambiente de prueba en coordinación con la “OSI”.
19. Ningún usuario deberá modificar, instalar, reparar o mantener el equipo o los equipos de computadoras sin obtener para ello la debida autorización de OSI.
20. Todos los usuarios de computadoras personales y portátiles deben usar regularmente un programa de detección de virus para minimizar el daño que pueda ocasionar un

ataque de virus y para detectar cualquier virus que puedan tener los archivos que se introduzcan en la computadora. La forma principal de introducirse un virus a las computadoras es a través del uso del correo electrónico, en el uso del Internet o de “*diskette*” de una computadora a otra. Todo “*diskette*” a usarse en la PC debe ser pasado por un programa antivirus antes de grabarse o instalarse en la PC.

21. Los sistemas de información de la Compañía y sus equipos; no pueden ser utilizados para acceder, transmitir y almacenar material pornográfico o de contenido sexual.
22. Está prohibido el uso del correo electrónico y/o el servicio de Internet para enviar, acceder o transmitir material de contenido sexual, que pudiera ser ofensivo para otros empleados o personas externas.
23. El uso de los sistemas de información debe ser cónsono con la política contra el Hostigamiento Sexual en la Compañía de Parques Nacionales de Puerto Rico.
24. Todo documento creado electrónicamente se registrará por la Ley de Administración de Documentos Públicos de Puerto Rico, Ley Núm. 5 de 8 de diciembre de 1955, según enmendada.
25. Todo empleado o usuario deberá mantener periódicamente, activos y actualizados, el resguardo (“*backup*”) de la información en su estación de trabajo. Dichos resguardos (“*backups*”) de información deberán conservarse en un lugar seguro bajo llave o en un área designada para brindar esa seguridad.
26. El acceso a tales resguardos (“*backup*”) debe estar limitado y controlado de manera que sólo tenga acceso a los mismos, el empleado o usuario que por motivo de sus funciones deba acceder la data.
27. El Director de cada Oficina será responsable de velar por el cumplimiento de lo antes indicado.
28. No está permitido el uso en las computadoras y/o equipos de la Compañía, de programas y/o licencias obtenidas por el empleado o usuario para su uso personal.
29. La instalación de programas no autorizados por la “OSI” en las computadoras de la Compañía se considerará una violación a lo dispuesto en este Reglamento y puede conllevar la aplicación de medidas disciplinarias.

30. No está permitido que el usuario modifique, instale, repare o mueva el equipo de computadoras sin la debida autorización.

Sección 7.5 - Política para Envío y Recibo de Correo Electrónico, Correspondencia Interna y Servicio de Internet

1. Se utilizará el correo electrónico para el intercambio de correspondencia interna siempre que sea posible, disminuyendo así el manejo de documentos impresos, CD, "Pen Drives" u otros.
2. El correo electrónico y el servicio de Internet se utilizarán exclusivamente para propósitos oficiales de la Compañía y de las labores de los empleados dentro de la misma. **Se prohíbe su uso para propósitos personales, político-partidistas, o asuntos no relacionados a la Compañía.**
3. Todo correo electrónico "*E-mail*" se clasifica como una comunicación oficial.
4. 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 claves de acceso ("*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 transmitido 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, disseminación 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 NOTES"

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 by error, please notify the sender. “Thanks you for your cooperation”.

5. 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.
6. Todo 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 la correspondencia dentro de los parámetros establecidos.
7. Todo usuario deberá transferir al destinatario correspondiente toda correspondencia electrónica recibida por error y mantener la confidencialidad de la misma.
8. Se utilizará papel en blanco (sin timbrar) para imprimir los documentos de uso interno y papel timbrado con el logo de la Compañía de Parques Nacionales de Puerto Rico solamente para correspondencia externa.
9. La “OSI” 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 Compañía.
 - d. Realizar una investigación de un acto ilegal.
 - e. En caso de una falla en el sistema o emergencia.
 - f. Uso inadecuado del correo electrónico.

- g. Para revisar la utilidad de los servicios de Internet en las tareas afines al trabajo de los usuarios.
 - h. Utilización apropiada de los métodos de redes de comunicación electrónica.
10. La Compañía no permitirá o alentará 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 religiosas por parte de ningún empleado, no importa el puesto que ocupe. El uso indebido de un activo de la Compañía, puede conllevar acciones disciplinarias según se establece en el Manual de Medidas Disciplinarias de la Compañía de Parques Nacionales.
 11. La Oficina de Recursos Humanos será responsable de mantener informado a la “OSI” de reclutamientos, transferencias, promociones, renunciaciones, despidos, vacaciones y separación de los deberes de los empleados que estén autorizados a acceder sistemas de información, computadoras y programas con el propósito de cambiar o dejar sin efecto el nivel de acceso de éste.

ARTÍCULO 8 - SOLICITUD DE ACCESO Y MANEJO A LOS SISTEMAS DE INFORMACIÓN (CONTRASEÑA)

Sección 8.1 - Acceso

1. El acceso del empleado o usuario a los Sistemas de Información de la Compañía se determinará de acuerdo a las funciones, deberes y responsabilidades del puesto que ocupa.
2. El Director de la Oficina llenará los formularios de Solicitud de Creación de Cuentas para las diferentes aplicaciones.
3. La “OSI” evaluará la petición y otorgará los niveles de acceso necesarios para que el empleado pueda realizar efectivamente sus deberes y responsabilidades.

4. Al autorizar el acceso a una computadora, servicio de internet o alguna aplicación se determinará en primera instancia el nivel de acceso necesario para que el empleado pueda realizar efectivamente, tales deberes y responsabilidades.
5. De haber movimientos de personal en las oficinas o parques, el Director de la Oficina o el Superintendente del Parque en que se desempeña el usuario notificará a la “OSI” tal movimiento y autorizará cambios en los accesos de ser necesario.
6. La Oficina de Recursos Humanos será responsable de mantener informado a la “OSI” de los reclutamientos, transferencias, promociones, renunciaciones, despidos, vacaciones y separaciones de los deberes de los empleados que estén autorizados a acceder sistemas de información, computadoras y programas con el propósito de cambiar o dejar sin efecto el nivel de acceso del empleado concernido a los Sistemas de Información.
7. La “OSI” podrá denegar el nivel de acceso asignado a un usuario, en aquellos casos que tal nivel no corresponda, según la posición o el puesto del empleado. De ser el Director Ejecutivo, quien solicite el acceso para estos usuarios, la OSI procederá a otorgar el acceso según solicitado por el Director Ejecutivo.
8. Los Sistemas de Información de la Compañía están diseñados a operar de tal manera que todo usuario pueda tener acceso a los mismos. Cada usuario deberá identificarse adecuadamente al ingresar al sistema.
9. En el momento de ingresar al sistema, éste verifica la autorización de cada usuario para tener acceso al mismo, de manera que:
 - a. El sistema previene el que un usuario pueda tener acceso a más de una estación de trabajo a la vez.
 - b. Limita a los usuarios individuales a estaciones de trabajo con direcciones específicas.
 - c. Desconecta automáticamente a aquel usuario que continúa entrando una clave de acceso errónea al sistema después de dos (2) intentos.
 - d. Da acceso al sistema sólo en aquellos días en que los usuarios pueden tener acceso al mismo.

Sección 8.2 - Creación de Claves de Acceso

1. La “OSI” será responsable de proveer la solicitud o formulario en que se solicitan las claves de acceso a los sistemas.
2. El acceso del usuario al sistema puede brindarse en distintos niveles 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.
3. Todo usuario que reciba una clave de acceso será responsable de conocer y cumplir con los controles y políticas de la Compañía relacionadas al uso de los Sistemas de Información.
4. Dado que toda clave de acceso “contraseña” 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 “OSI” para que se proceda a cambiar la clave acceso.
5. Las claves de acceso serán renovadas periódicamente (cada sesenta (60) días) para lo cual la “OSI” establecerá el mecanismo correspondiente, las características de una clave de acceso son:
 - a. Debe tener mínimo de siete (7) caracteres.
 - b. Deberá contener al menos una letra, un número y carácter especial
 - c. No podrá re-utilizar la misma clave luego de diez (10) renovaciones.

Sección 8.3 - Uso de la Contraseña

1. **NO** divulgue, preste o transfiera su contraseña a otro usuario.
2. **NO** escriba, ni coloque la contraseña cerca o en el Terminal o Monitor.

3. **NO** use una contraseña que le asocie a usted, tal como, su fecha de nacimiento, su apodo, iniciales de una abreviación de su nombre, entre otros.

Sección 8.4 - Expedientes sobre Acceso a Sistemas de Información

La “OSI” mantendrá en archivo todas las solicitudes de accesos a los sistemas de la CPNPR. Estas solicitudes contendrán la información del solicitante, puesto que ocupa, fecha de solicitud, el nombre y la firma del Director de la Oficina que está solicitando el acceso.

Dicho expediente incluirá, pero no se limitará a:

- a. Solicitudes de acceso al Internet y correo electrónico
- b. Solicitudes de acceso al Sistema de Ventas
- c. Solicitudes al Sistema de Intercambio de Ingresos
- d. Solicitudes al Sistema ABS
- e. Solicitudes a Oracle y sus módulos de Compras, Recursos Humanos, Propiedad, “General Ledger”, Finanzas y Contabilidad
- f. Recibo de entrega del Reglamento para Usuarios que Manejan Sistemas de Información de la Compañía de Parques Nacionales de Puerto Rico

Esta información estará bajo la custodia de la “OSI” y sólo será compartida para propósitos de auditorías.

Sección 8.5 - Accesos a las Aplicaciones de Producción y de Prueba

1. La “OSI” permitirá el acceso a las aplicaciones 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.
2. Todo usuario que realice funciones de prueba o desarrollo deberá utilizar el ambiente y los recursos designados para tal propósito (ambiente de prueba). Sólo tendrán acceso a tales recursos, aquellos empleados que por la naturaleza de sus funciones requieren del mismo.

3. Solamente aquellas transacciones que se generen como parte del flujo normal de los servicios que ofrece la Compañía, podrán alterar la información oficial contenida en el archivo.
4. Las tareas de prueba y desarrollo deberán llevarse a cabo en un ambiente separado y no podrán afectar o alterar en ninguna manera la información oficial de la Compañía. Aquellos usuarios que ejecutan trabajos que utilizan aplicaciones de producción se les otorgará acceso sólo para leerlas. Estos usuarios podrán crear nuevas aplicaciones como parte de sus tareas, pero bajo los parámetros de nombre designados para el ambiente de prueba y desarrollo.
5. Por definición, los usuarios actualizarán la información oficial de los archivos a través de los programas creados para tales propósitos. El Sistema de Seguridad se implantará de tal forma que no permitirá a los usuarios leer o modificar códigos de las aplicaciones.

ARTÍCULO 9 - SEGURIDAD EN LOS EQUIPOS

Sección - 9.1

Inventario

La "OSI" en adición de la División de Propiedad de la Compañía preparará y mantendrá actualizado un inventario del equipo electrónico de la Compañía, que incluirá:

1. La descripción del equipo
2. Localización del mismo
3. Número de propiedad

Seguro

Los equipos de procesamiento electrónicos de la Compañía estarán cubiertos por una póliza de seguros cuya cubierta se extenderá a daños al equipo por eventos fortuitos, actos delictivos o aquellas circunstancias que provea tal cubierta.

El equipo en cuestión se asegurará por el costo original (costo de reemplazo).

Estarán asegurados además, los programas de la Compañía que estén disponibles en el mercado, como por ejemplo; programas de aplicación tales como MS-Office, FoxPro, MS-Project, entre otros.

Sección 9.2 - Responsabilidades del Usuario para con los Diskettes, CD's, "Pen drive" o Cualquier Otro Medio para Almacenar Información

1. Todo usuario será responsable de velar por el uso adecuado de los "diskettes", CD's, "Pen drive" o cualquier otro medio y de la información contenida en ellos. Para esto deberá:
 - a) Rotular adecuadamente con las etiquetas provistas para ello.
 - b) Cambiar las etiquetas siempre que borre o cambie la información en el "diskette", CD's, "Pen drive" o cualquier otro medio utilizado para guardar la información.
 - c) Guardar en un lugar seguro, bajo llave fuera del área de trabajo, si es necesario. Puede utilizar la bóveda de Sistemas de Información.
 - d) Mantener por lo menos a un mínimo de doce (12) pulgadas de distancia de imanes y dispositivos electromagnéticos, tales como: teléfonos, beeper y celulares.
 - e) Hacer copias regularmente.
 - f) Antes de disponer de ellos deberá reformatearlos para borrar la información o romperlos.

2. Al utilizar los métodos de almacenamiento, todo usuario observará las siguientes normas:
 - a) Brindar a los "diskettes", CD's, "Pen drive" o cualquier otro medio la misma protección en términos de confidencialidad que a los documentos que contienen la información.
 - b) No enviar los discos duros a reparar fuera sin antes reformatear los mismos.
 - c) Evitar tocar las áreas sensitivas del "diskette", CD's, "Pen drive" o cualquier otro medio (centro), ya que podría causar daños y perder información.
 - d) Evitar escribir directamente sobre ellos, o colocar presillas "clips".

- e) Evitar colocar los “*diskettes*”, CD’s, “*Pen drive*” o cualquier otro medio cerca de líquidos solventes.
- f) No doblar los “*diskettes*”, CD’s, “*Pen drive*” o cualquier otro media, ni colocar objetos pesados sobre ellos.
- g) Evitar exponer los “*diskettes*” a los rayos del sol, tampoco permitirá que éstos se mojen con algún líquido.

Sección 9.3 - Protección y Cuidado de Equipos Periféricos

1. La Compañía utilizará equipos electrónicos (terminales, impresoras, PC’s portátiles, CD Drivers, etc.) para facilitar el flujo de tareas en las distintas divisiones y oficinas. La Compañía 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.
2. El personal debidamente adiestrado de la “OSI” son los únicos autorizados a hacer cualquier tipo de instalación de equipos computadorizados y/o de aplicaciones a los equipos. Ningún usuario deberá realizar tareas de instalación o movimiento de equipos por sí mismo.
3. Cualquier mal funcionamiento que el usuario detecte en los equipos deberá notificarlo rápidamente a la “OSI” para que los revisen, corrijan la falla de ser necesario, y para ordenar la reparación de las mismas. Ningún usuario deberá reparar los equipos; esta tarea sólo puede realizarla el personal autorizado por la OSI.
4. Los usuarios no deberán llevar alimentos o bebidas a las áreas de trabajo donde existan equipos periféricos.
5. Al finalizar el día, los usuarios deberán retirar sus claves de acceso de las computadoras y deberán apagar todos los equipos electrónicos en su área de trabajo.
6. Los usuarios no deberán colocar equipos, tales como: radios, celulares o electromagnéticos cerca del CPU.
7. Los usuarios no deberán colocar plantas o tuestos sobre la computadora ni pegar papeles de notas en las partes de ventilación de la computadora.

8. Los usuarios no deberán trabajar con grapas o sujetadores de papel sobre el teclado, ni forzar un CD para que entre o salga de la unidad de CD.
9. Toda solicitud de servicio para la instalación, reparación, movimiento, sustitución o eliminación de equipos, tales como: monitores, impresoras y computadoras; deberá dirigirse por escrito a la Oficina de Sistemas de Información. Todas las solicitudes deben ser originadas por el Director de la Oficina en la cual se encuentra y se utiliza el equipo.

Sección 9.4 - Computadoras Portátiles

1. Las medidas de seguridad que incluimos a continuación son para todos los empleados o usuarios que utilicen computadoras portátiles ("*Laptops*") o "*LAN file servers*" y la red de computadoras. Debido a que las computadoras "*Laptops*" o portátiles corren un alto riesgo de ser hurtadas, cada unidad debe estar protegida con "programas" de control de acceso y "claves de accesos" para activar o prender la máquina siempre y cuando sea factible o práctico. La clave de acceso para activar o prender la máquina protege el artefacto en contra de que se use un '*diskette*' DOS o de Sistemas para esquivar el programa de control de acceso del sistema.
2. Se prohíbe estrictamente guardar números telefónicos de módem del network o claves de accesos del network en computadoras personales (PC) o individuales ("*Laptops*") que no estén protegidas.
3. Todos los programas y archivos de la Compañía que se encuentren en medios móviles deben almacenarse bajo llave cuando no se están utilizando o deben mantenerse en áreas que se cierran con llave cuando no se utilicen.
4. El usuario que tenga asignada una ("*Laptop*"), no podrá llevar la misma a su hogar. Éstas podrán ser sacadas de las inmediaciones de la CPNPR sólo para hacer trabajos en las instalaciones, al final del día el usuario deberá regresar la misma a su lugar de trabajo y guardarla en un lugar bajo llave. El Personal de la Oficina de Sistemas de Información y las personas autorizadas por el Director Ejecutivo podrán llevar las ("*Laptops*") a sus residencias para realizar trabajos de la CPN.

Sección 9.5 – Telecomunicaciones

1. Es política de la CPNPR que la utilización de los equipos de comunicaciones (equipos telefónicos y de datos) sea exclusivamente con propósitos oficiales de la Compañía 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 intereses para sus usuarios. Toda transmisión de información deberá corresponder siempre a los mejores intereses de la Compañía.
2. Toda computadora personal dejada conectada por el usuario en la red de telecomunicaciones, pasada la hora de trabajo del empleado, deberá ser desactivada de la red por el Administrador de la Red o por los operadores del centro.
3. Todo acceso a la red de telecomunicaciones por personas ajenas a la Compañía (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 equipo asociados a la Red de Telecomunicaciones.
4. Es política de la CPNPR mantener en funcionamiento óptimo la red de telecomunicaciones de nuestro sistema de información. Para esto es necesario que el mantenimiento a los equipos asociados a la red, sea realizado por recursos adiestrados en estas técnicas.
5. Toda solicitud de servicio para la instalación, reparación, movimiento, sustitución o eliminación de equipos tales como: monitores, impresoras y computadoras; deberá dirigirse por escrito a la Oficina de Sistemas de Información. Todas las solicitudes deben ser originadas por el Director de la Oficina en que se encuentra localizado el equipo.
6. Toda solicitud de servicio para la instalación, reparación, movimiento, sustitución o eliminación de equipos, tales como: monitores o terminales, impresoras, computadoras personales y líneas de comunicación; deberá dirigirse por escrito a la unidad responsable para el funcionamiento de la red. Todas las solicitudes deben ser

originadas por el Director de la Oficina en la cual se está utilizando el equipo. Ningún empleado por su propia iniciativa está autorizado a realizar tareas de instalación, reparación, entre otros, a los equipos asociados a la red de telecomunicaciones.

ARTÍCULO 10 - PROTECCIÓN CONTRA LOS VIRUS

Sección 10.1 - Programa

1. Para minimizar el que las computadoras personales (PC's) se infecten de virus, en el equipo tecnológico propiedad de la CPNPR sólo se pueden usar programas autorizados y con la debida licencia. Los programas autorizados son aquellos aprobados por la Compañía.
2. La "OSI" instalará un programa anti-virus a nivel de Red para:
 - a. Garantizar la protección contra desastres en las PC's.
 - b. Monitorear las PC's remotamente.
 - c. Restaurar los discos dañados.
3. Toda información relevante a problemas de virus encontrados en computadoras de usuarios se mantendrá en la base de datos del servidor. De esta forma la "OSI" podrá cotejar con el usuario sobre el uso de CD's, "Pen Drives" o cualquier otro medio infectados con virus, su procedencia y a la misma vez, comentarles sobre los métodos de seguridad a seguir.
4. El programa debe proveer, entre otros, la siguiente información:
 - a. Informe y estadísticas de computadoras conectadas a la red.
 - b. Problemas de virus.
5. El Administrador de la Red y/o sus técnicos deben, periódicamente, hacer un diagnóstico de cada computadora.

6. El programa debe configurarse para que ejecute cuando el usuario se conecte a la red una vez por día/semana. Cuando el programa ejecuta, graba la dirección del **nodo**, la identificación del usuario, problema de virus, hora y fecha.
7. Para evitar o poder recuperarse de un ataque de virus u otro desastre, se implantarán procedimientos rutinarios de “*backup*” (copia) para el programa y los archivos de la Compañía en las PC’s a Lan’s, según se dispone en este Reglamento.

ARTICULO 11- USO DEL CORREO ELECTRÓNICO Y SISTEMAS DE INTERNET

Sección 11.1 - Objetivo

La Compañía 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:

1. Agilizar nuestra comunicación interna y externa.
2. Minimizar la impresión en el sistema de recibo de la correspondencia.
3. Mantener registro en el sistema del recibo de la correspondencia.
4. Acelerar el envío y recibo de la correspondencia interna.
5. Disminuir interrupciones por llamadas telefónicas.
6. Transferir archivos y documentos sin necesidad de utilizar “diskettes” u otros medios de almacenamiento.
7. Reducir los costos de impresión de documentos y de uso de “diskettes” u otros medios de almacenamiento.
8. Estandarizar el tipo de papel a usar para correspondencia interna y externa.
9. Agilizar el método de trabajo y que este sea de manera eficiente.
10. Agilizar el acceso a la información.

Sección 11.2 - Utilización

1. La Compañía requiere que se utilice el correo electrónico siempre que sea posible, sustituyendo el documento impreso por un mensaje electrónico.

2. El usuario 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 o PowerPoint utilizando la opción “*File/Send*” en estos programas. Esto elimina el uso de papel.
3. Todas las personas con acceso al correo electrónico aparecen en el listado incluido en el sistema en la opción Directorio (“*Address Book*”).
4. Si el destinatario de su correspondencia (no aparece en este listado, envíe la correspondencia al Secretario (a), Asistente Administrativo u Oficial Administrativo de la División u Oficina correspondiente, quien podrá imprimirlo y entregarlo al destinatario. Este proceso no elimina la impresión del documento, pero si acelera el envío y entrega del mismo.
5. Como regla general, un mensaje enviado por correo electrónico no debe repetirse por escrito.
6. Cada Director de la Compañía designará una persona en su Oficina, conforme sea necesario, para enviar mensajes informativos a otras oficinas o parques de la Compañía. Se dispone que todo mensaje que tenga como destinatario a todos los empleados de la Compañía, deberá transmitirse por conducto del Director (a) de la Oficina de Sistemas de Información y en caso de que el mismo no esté presente, un representante autorizado. Las únicas personas autorizadas a enviar un mensaje a todos los empleados de la Compañía son: el Director Ejecutivo y el Director de la Oficina de Sistemas de Información o representante autorizado, en caso de que los mismos no estén presentes. Esto para evitar duplicidad del mensaje, ahorro en tiempo y mantiene cierto estilo de uniformidad en la redacción de los mensajes.
7. 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 registro se puede retener como un acuse de recibo de la correspondencia enviada.

8. Todo usuario deberá archivar sus mensajes en sus cartapacios ("*folder*"), por lo menos una vez al mes de acuerdo a la acción posterior que requieren de su parte. Cuando éstos sean propiamente atendidos, los eliminará del cartapacio.
9. Ningún destinatario podrá enviar copia de la correspondencia electrónica recibida a otras personas sin el conocimiento del remitente. A éste, se le deberá notificar por lo menos con copia.
10. Toda impresión de documentos de uso interno se hará en papel blanco. Si el usuario desea que el logo de la Compañía aparezca en sus documentos, puede incluirlo como parte del mismo. La "OSI" enviará el membrete a su máquina, a través del correo electrónico en documentos de Word. **Sólo se utilizará papel timbrado para correspondencia externa.**
11. Evite poner fondos u otros elementos "decorativos" innecesarios, ya que el mensaje perderá formalidad (sobre todo en el ámbito profesional). Además, al agregar "decoración", se aumenta el número de *bytes* a transmitir y esto puede ser un problema para personas con conexiones a Internet lentas.
12. Verificar la ortografía y utilice correctamente las reglas gramaticales y de puntuación, tal y como si estuviera escribiendo un comunicado o una carta en papel.
13. NO escribir correos electrónicos (*e-mails*) en mayúsculas sostenidas. Además, de que es de mal gusto, en Internet eso significa GRITAR.
14. Cuando se intercambie un mismo mensaje varias veces a manera de una conversación, el usuario debe asegurarse de incluir toda la serie de mensajes anteriores que se ha ido acumulando en el mismo. Esto le facilita a todos los involucrados seguir la conversación. Esto es particularmente útil para todos los que reciben muchos mensajes al día.
15. Evitar "frases motivacionales"; lo único que se logra es distraer al lector del propósito principal del mensaje.
16. Asegurarse de que debajo de su firma aparezcan todos los datos necesarios para que el receptor lo identifique y se pueda poner en contacto con usted. Esto debe incluir: el

nombre de la Compañía, el puesto, teléfono, dirección postal, página Web y cualquier otra información pertinente.

Ejemplo de firma,

Nombre
Puesto que ocupa
Oficina
Compañía de Parques Nacionales de Puerto Rico
Tel.787-622-5200 Ext.
www.parquesnacionalespr.com



Por favor considere el ambiente antes de imprimir este mensaje. consider the environment before printing this message.

“NOTA DE CONFIDENCIALIDAD”

Esta comunicación y cualquier archivo transmitido 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 NOTES”

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 by error, please notify the sender. “Thanks you for your cooperation”.

Sección 11.3 - Monitoreo de Correo Electrónico e Internet

1. El correo electrónico y el Internet son de uso oficial de la Compañía. La Compañía podrá auditar el contenido de los mensajes y el acceso a las páginas de Internet, para determinar 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 Compañía 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 ambas herramientas se proveen a los usuarios para funciones oficiales de la Compañía.

2. En el caso del correo electrónico, el mensaje posee como particularidad la identificación de la Compañía, lo cual le hace instrumento de carácter representativo de la Compañía. Por otro lado, cada acceso a las páginas de Internet nos identifica como Compañía 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 Compañía.
3. El acceso a las páginas de internet será monitoreado a través de una aplicación que se especializa en esta labor.

Sección 11.4 - Aceptaciones

Los siguientes son algunos ejemplos de los usos aceptados del correo electrónico y del servicio de Internet:

1. Intercambio de correo electrónico para realizar funciones de trabajo con agencias del Gobierno del Estado Libre Asociado de Puerto Rico, ciudadanos, compañías turísticas, y agencias de viajes en cualquier parte del mundo con el propósito de promover y brindar información de nuestros parques y bellezas turísticas para dar a conocer a Puerto Rico como un destino turístico tanto local como internacional.
2. Promover a través de páginas de Internet nuestros centros vacacionales, parques, balnearios y otros lugares de interés a los turistas internos e internacionales, incitando a la unión familiar mediante el disfrute de nuestros recursos; además, de promover a Puerto Rico como destino turístico.

Sección 11.5 - Etiqueta en el Uso de Internet

1. Todo usuario es responsable por sus acciones y conductas al acceder el Internet. Siempre debe tener presente que el Internet es un conjunto de redes, por lo que su uso debe ser correcto y conforme a las políticas establecidas en este Reglamento.

Bajo ninguna circunstancia se realizarán actos que puedan considerarse ilegales, inmorales u ofensivos.

ARTICULO 11 - PROHIBICIONES PARA USO DE EMAIL, SISTEMAS, INTERNET Y COMPUTADORAS

Sección 11.1 - Prohibiciones de Uso de Computadoras y Aplicaciones

1. NO utilice programas de origen desconocido y/o ilegal, o que se ofrecen gratis, aún cuando estos hayan sido provistos por algún amigo.
2. NO utilice programas que no están relacionados directamente con las funciones de su equipo o la Compañía (juegos, otros).
3. NO instale aplicaciones en las computadoras, sin autorización de OSI.
4. NO borre, formatee o altere el sistema operativo.
5. NO use herramientas que permita traspasar la seguridad de las computadoras o la red de datos.
6. NO llevarse para sus hogares las computadoras y/o "*laptops*" que tengan asignadas.

Sección 11.2 - Prohibición de Correos Electrónicos (e-mails) e Internet

1. De ninguna manera se permitirá a los usuarios, utilizar el correo electrónico y el servicio de Internet para lo siguiente:
 - a) Uso para actividades con fines de lucro - Uso de los equipos y herramientas de la Compañía para actividades con fines de lucro, tales como: trabajo para consultoría con paga, compra o venta de productos, negocios privados, entre otros.
 - b) Impacto Negativo - Uso para actividades que influyen, afectan o van en detrimento de la imagen de la Compañía y sus empleados, cualquier persona, organización o instrumentalidad del Gobierno de Puerto Rico.

- c) Manejo de Archivos Voluminosos - Transferencia de archivos voluminosos a los sistemas de la Compañía, sin la previa aprobación de la persona responsable de esos recursos.
 - d) Actos maliciosos - Actos maliciosos incluyendo la replicación de virus, envío de correo no oficial o político partidista, material ofensivo, pornográfico u otros actos ilegales que puedan afectar de forma adversa el funcionamiento de los sistemas de la Compañía.
 - e) NO debe escribir el mensajes en mayúsculas sostenidas. Además, de que es de mal gusto, en Internet eso significa GRITAR.
2. El uso de Internet es sólo para realizar las labores correspondientes a su trabajo. Está prohibido el uso de Redes Sociales, estaciones de radio a través de internet, juegos online entre otras.

Sección 11.3 - Prohibiciones para el Uso de los Sistemas

- 1. **NO** divulgue, preste o transfiera su contraseña a otro usuario.
- 2. **NO** escriba, ni coloque la contraseña cerca o en el Terminal o Monitor.
- 3. **NO** use una contraseña que le asocie a usted, tal como, su fecha de nacimiento, su apodo, iniciales de una abreviación de su nombre, entre otros.
- 4. **No deberá permitir que otro usuario utilice su cuenta de accesos a los diferentes sistemas y/o computadora.**

ARTÍCULO 12 - CLAUSULA DE SALVEDAD

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

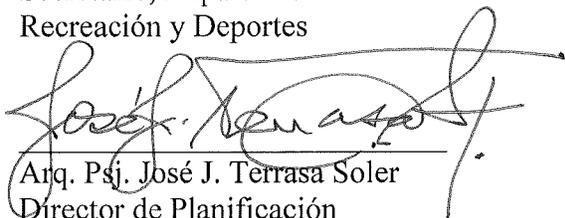
ARTÍCULO 13 - VIGENCIA Y APROBACIÓN

Este Reglamento comenzará a regir inmediatamente luego de su aprobación por la Junta de Directores de la Compañía de Parques Nacionales de Puerto Rico.

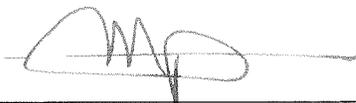
Aprobado en San Juan, Puerto Rico, el 10 de octubre de 2012.



Hon. Henry Neumann Zayas
Presidente, Junta de Directores
Secretario, Departamento
Recreación y Deportes



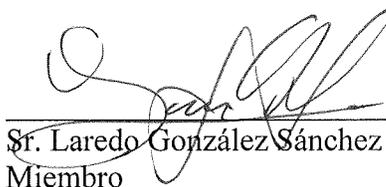
Arq. Psj. José J. Terrasa Soler
Director de Planificación
Compañía de Turismo



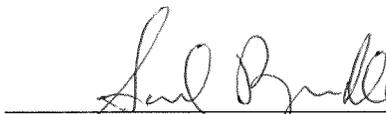
Arq. Psj. Jorge A. Palou Pujós
Miembro

Sr. Luis C. Maldonado Padilla
Miembro

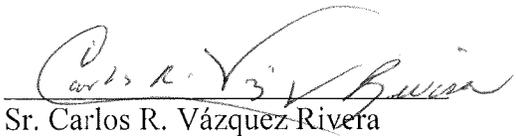
Sr. Saúl Rodríguez Pabón
Ayudante del Secretario
Departamento de Educación



Sr. Laredo González Sánchez
Miembro



Prof. Samuel Brindle Quiroga
Miembro



Sr. Carlos R. Vázquez-Rivera
Miembro