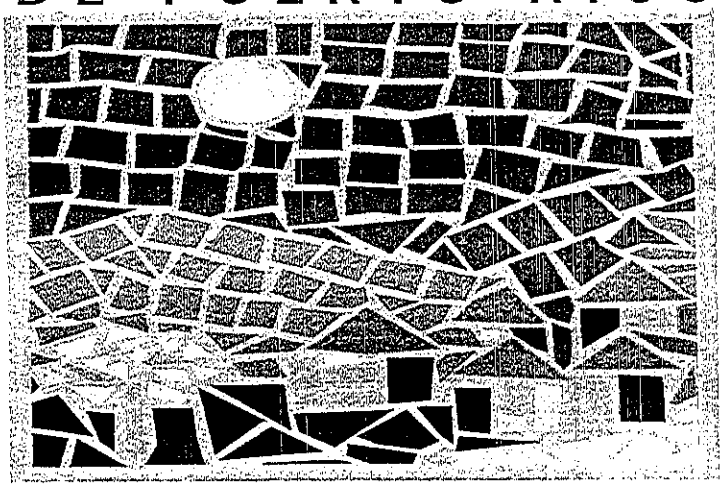
ESTADO LIBRE ASOCIADO
DE PUERTO RICO



MANUAL DE POLITICAS Y PROCEDIMIENTOS

COMUNIDADES ESPECIALES PUERTO RICO

AREA DE SISTEMAS DE INFORMACION

ESTADO LIBRE ASOCIADO DE PUERTO RICO
Oficina de Comunidades
Especiales de Puerto Rico

Julia Torres
COORDINADORA
GENERAL

8 de marzo de 2007

Héctor González
Director Interino

MANUAL POLÍTICAS Y PROCEDIMIENTOS
ÁREA DE SISTEMAS DE INFORMACIÓN

Incluyo copia del Manual de Políticas y Procedimientos a implantar en el Área de Sistemas de Información de la cual usted está a cargo.

Se incluyen además, formas que fueron diseñadas con su aval correspondiente a los procedimientos establecidos.

Falta por diseñar finalmente tres formas, las cuales discutiera con usted Nilda Díaz, Asesora en Administración y que están actualmente en uso. Las mismas son: Hoja de Cotejo Control de Calidad, Solicitud de Programación y Registro de Actividades del Sistema.

Es necesario que, para la implantación de los procedimientos contenidos en este manual, se realicen las gestiones pertinentes con el Área de Administración para la adquisición de los servicios necesarios de resguardo de cintas de "backups" y la adquisición de las cintas necesarias para producir los "backups".

Los procesos especificados, así como la Carta Compromiso que deben firmar los empleados, deben ser notificados por escrito a las áreas concernidas a la mayor brevedad, de forma que la implantación de los procesos sea la adecuada.

Cualquier duda sobre el particular puede comunicarse con la señora Díaz para discutir la misma.

Julia Torres Hernández

JTH/nidt

Cf. Ramonita Gaetán Peña
Subcoordinadora General

Madeleine Medina
Oficial Ejecutivo

#635 Ave. Fernández Juncos • San Juan, P.R. 00907
Tel. (787) 977-7060 • Fax: (787) 977-7058

I. BASE LEGAL:

Este Manual de Políticas y Procedimientos se promulga de conformidad con la ley que crea la Oficina del Coordinador General para el Financiamiento y la Autogestión de las Comunidades Especiales, conocida como Oficina de Comunidades Especiales de Puerto Rico (OCEPR), Ley Número 1 de marzo del 2001, y conforme a las cartas circulares emitidas por la Oficina de Gerencia y Presupuesto que regulan los sistemas y su utilización.

II. PROPOSITO:

Los programas de computadoras están protegidos por la Ley Federal de Derechos de Autor, la Ley de Propiedad Intelectual de Puerto Rico y otros tratados internacionales. La duplicación sin licencia o uso de cualquier programa no autorizado constituye una violación a estos reglamentos **y puede exponer al usuario** y a la Institución a responsabilidades civiles que van desde $100,000 y $250,000 y/o hasta cinco años de cárcel en caso de acción criminal.

El Manual de Políticas y Procedimientos presentado a continuación tiene como propósito definir en forma clara las responsabilidades del Área de Sistemas de Información de la OCEPR y su cumplimiento con las disposiciones estatales y federales.

La OCEPR tiene la obligación de asegurar la integridad y exactitud de la información de la agencia protegiéndola contra la divulgación, manipulación, modificación o destrucción no autorizada o accidental. Tanto los equipos de computadoras, los programas ("software") así como la información contenida en el banco de datos de la OCEPR ("network") son propiedad del Estado Libre Asociado de Puerto Rico.

Conforme a este Manual de Políticas y Procedimientos, la OCEPR requiere que su personal utilice correctamente los equipos de computadoras, así como los, programas y todas las piezas o aditamentos que se conecten a éstos (periferales) y que complementan su funcionamiento. Este personal tiene el deber de tomar las medidas necesarias para proteger el equipo y asegurar su funcionamiento óptimo.

Este consiste de dos tipos de documentos, políticas y procedimientos incluyendo una sección con muestras de los formularios a que se hacen referencia en los procedimientos.

Las políticas definen la filosofía general del Área de Sistemas de Información en diversos aspectos como lo son, las responsabilidades y prioridades que se deben establecer.

Por otro lado, los procedimientos los cuales se dividen en dos secciones, Procedimientos Administrativos y Procedimientos Operacionales, detallan los pasos que han de tomar los componentes del Área de Sistemas de Información para poder llevar a cabo sus responsabilidades específicas.

III. DEFINICIONES

A los efectos de este Manual de Políticas y Procedimientos, los siguientes términos y frases tendrán el significado que a continuación se indica:

1. OCEPR - Oficina de Comunidades Especiales de Puerto Rico Correo electrónico - Servicio de transmisión de mensajes a través de una red.

2. Internet - Es una red mundial con millones de servidores conectados. Estos pueden intercambiar información y establecer distintos servicios tales como visitar páginas de portales, correo electrónico, charlar por medio del teclado en los salones creados para este servicio, entre otros.

3. Coordinador(a) y Subdcoordinador(a) - El (la) Coordinador(a) y Subcoordinador(a) de la Oficina de Comunidades Especiales de Puerto Rico.

4. Empleados - Personal que labora en la OCEPR.

5. Sistema de Informática - Se refiere al uso y manejo de la información en los equipos electrónicos computadorizados que se utilizan como herramienta de trabajo en la OCEPR.

6. Oficinas - Oficinas de la OCEPR que utilizan el sistema de información computadorizado.

7. Periferales - Equipos electrónicos tales como terminales, impresoras, computadoras, entre otros.

IV. DISPOSICIONES GENERALES:

A. La Oficina de Comunidades Especiales de Puerto Rico (OCEPR) cuenta con acceso a computadoras, redes, servicios electrónicos internos y a la red Internet. Al hacer uso de estos equipos y de los servicios provistos a los empleados acatarán las siguientes normas:

a. La computadora, los servicios provistos tanto internos como externos, el sistema de correspondencia electrónica (e-mail), la Internet y los documentos y programas que existan en la misma son propiedad de la OCEPR y sólo podrán ser utilizados para propósitos lícitos, prudentes, responsables y dentro de las funciones inherentes a la agencia.

b. Toda información, dato, obra literaria o de arte, escrito, documento, programas, acción, privilegio, patente, derecho de autor o cualquier otro derecho que surja, se cree o modifique mediante el uso de una de las computadoras de la OCEPR será propiedad de la agencia, aunque la información, dato, obra literaria o de arte, escrito, documento, programa, acción, privilegio, patente, derecho de autor o cualquier otro derecho haya surgido mediante el esfuerzo personal del usuario.

c. La información contenida en la computadora, los servicios provistos tanto internos como externos, los mensajes de correspondencia electrónica (e-mail), información de la Intranet o la Internet y los documentos y programas existentes no podrán ser reproducidos o utilizados para fines ajenos a las funciones, y poderes de la OCEPR.

d. Se prohíbe el uso de programas o recursos para los cuales no exista una licencia o autorización de uso válido a nombre de la OCEPR. El (la) Director(a) del Área de Sistemas de Información velará por el

licenciamiento de los productos y registrará las licencias en sus respectivas compañías.

e. Se prohíbe copiar programas de computadora adquiridos por la OCEPR. Se prohíbe acceder a, o utilizar propiedad intelectual ("copyrighted information") que viole derechos de autor.

f. Se prohíbe instalar programas en las computadoras que no hayan sido adquiridos por la OCEPR, sin la autorización por escrito del (de la) Director(a) a través del Área de Sistemas de Información.

g. Se prohíbe el uso de los sistemas de computadoras y comunicaciones de la OCEPR para propósito personal, de recreo, para manejo de un negocio o asunto privado del usuario o para el recibo y envío de mensajes en cadena, para tener acceso a compras, juegos, concursos, encuestas, páginas de entretenimiento o cualquier otro asunto o servicio no oficial o ajeno a las funciones de la OCEPR.

h. El Área de Sistemas de Información podrá utilizar diferentes medios de programación para auditar y supervisar desde esta misma oficina el uso de cada equipo computadorizado.

Para garantizar la seguridad y protección de los equipos del sistema de informática, los usuarios cumplirán con las normas aquí establecidas.

B. Seguridad:

1. El uso de un código de acceso ("password") no impedirá que se audite el sistema y no significa que el usuario albergue expectativa de intimidad alguna con relación a la información almacenada en la computadora asignada o en cualquier otra. Las contraseñas deben mantenerse en estricta confidencialidad y se cambiarán cada treinta (30) días. La misma será de por lo menos 4 caracteres y no más 6 caracteres de longitud y podrá ser una combinación de caracteres alfanuméricos (letras, números, símbolos) en cualquier proporción o arreglo. La contraseña utilizada por el usuario no podrá repetirse cuando expire la validada en el sistema.

2. La OCEPR se reserva el derecho a auditar, vigilar y fiscalizar los sistemas de correspondencia electrónica y todos los servicios computadorizados para garantizar que su propiedad sea utilizada sólo para propósitos y gestiones relacionadas con el trabajo. Estas auditorias se realizarán periódicamente, al azar o cuando exista una investigación sobre una situación en particular. Al personal de la OCEPR no le alberga expectativa de intimidad con relación a cualquier información, documento, mensaje creado, recibido o enviado a través del sistema de correo electrónico (E-mail) de carácter personal.

3. Se prohíbe el envío fuera de la OCEPR de documentos electrónicos o mensajes por medio del correo electrónico (E- mail) que contengan información confidencial.

4. Se prohíbe el uso de computadoras portátiles ("Laptop") o cualquier otro equipo electrónico, por los empleados, para realizar trabajos en la OCEPR, si dichos equipos son de carácter personal, sin previa autorización del (de la) Coordinador(a) de la OCEPR.

5. Se prohíbe el envío o recibo de mensajes de correo electrónico entre el personal de la OCEPR y otras personas ajenas al mismo en los cuales se divulguen, comenten o expresen hechos, opiniones u otra situación o asuntos interno de la OCEPR, que puedan poner en entredicho la reputación y la imagen de la agencia.

6. Se prohíbe modificar los privilegios de acceso a las redes internas o externas para obtener acceso no autorizado a dichos recursos.

7. No se podrá modificar ni archivar la información propiedad del la OCEPR con el propósito de impedir que alguien pueda leerlos, entenderlos o utilizarlos. Tampoco se podrá alterar el nombre del usuario u otra información que se utilice regularmente para identificar la información, mensajes o archivo. En caso de que algún usuario asigne contraseñas o codifique la información a fines de editar que otras personas puedan leerla, éste proveerá todos los datos para lograr acceso a los archivos al momento de su creación. La OCEPR está facultada para decodificar la misma o restituirla a su condición original.

8. Se prohíbe modificar los parámetros y configuración adoptada por el Área de Sistemas de Información en las computadoras de la OCEPR en

la capacidad de recibir llamadas telefónicas, conexión remota o cualquier otro tipo de acceso no autorizado en la red.

9. Todos los archivos que se creen en las computadoras serán guardados en el directorio asignado a cada usuario con el fin de protegerlos mediante los mecanismos de resguardo ("backup") existentes.

10. El sistema computadorizado estará disponible para los usuarios de lunes a viernes desde 7:30 AM hasta 6:00 PM. Los días feriados y fines de semana el personal autorizado a su uso deberá notificar al Área de Sistemas de Información con no menos de un (1) día de anticipación.

C. **Protección y Cuidado de Equipos Periferales (terminales, impresoras, computadoras, etc.)**

1. Ningún usuario realizará tareas de instalación de equipo, programas (software) ni de reparación. Solamente el personal autorizado por el Área de Sistemas de Información podrá instalar y configurar los equipos de computadoras.

2. Cuando el usuario detecte problemas en el funcionamiento del sistema deberá notificarlo rápidamente al Área de Sistemas de Información para que procedan a revisar el equipo, corrijan la falla o refieran para reparación. El servicio será solicitado mediante la Forma Solicitud de Servicio.

3. Ningún usuario llevará alimentos ni bebidas a las áreas de trabajo donde los equipos de computadoras estén localizados.

4. Cualquier movimiento de equipos así como de sus periferales deberá ser coordinado con el personal del Área de Sistemas de Información.

5. Con el fin de lograr la mayor uniformidad, antes de la adquisición de computadoras, redes, servicios electrónicos internos y programas deberá contarse con el asesoramiento de el Área de Sistemas de Información.

6. Al finalizar el día los usuarios deberán retirar sus claves de acceso de los terminales o computadoras y apagar todos los equipos electrónicos en su área de trabajo cuando el servicio así lo requiera.

En caso de emergencia cada usuario es responsable de tomar las medidas necesarias para proteger el equipo bajo su uso.

D. Correo Electrónico

1. Ningún empleado autorizado a usar Internet o correo electrónico podrá reclamar interés propietario o expectativa razonable de intimidad sobre comunicaciones utilizando dichos medios. El Área de Sistemas de Información tendrá acceso a los mensajes electrónicos e información de los espacios virtuales (Web) visitados por empleados en cualquier momento y los mismos serán considerados parte de los expedientes de la agencia.

2. Se prohíbe bajar información (download) de los servicios de Internet sin la debida autorización del (de la) Director(a) o de la persona que éste designe a cargo del sistema de informática. Se exceptúa de esta prohibición al personal técnico encargado de brindar mantenimiento a las computadoras, redes, servicios electrónicos internos y a la red Internet. El usuario deberá borrar por lo menos cada quince (15) días la correspondencia electrónica archivada de manera que se pueda utilizar al máximo el espacio en el disco de la computadora.

4. Se prohíbe utilizar el sistema para acceder y almacenar información oficial en cuentas de correo electrónico distintas a las cuentas oficiales provistas por la OCEPR, excepto al (a la) Coordinador(a), Subdcoordinador(a), Ayudantes del (de la) Coordinador(a), o cualquier otro personal autorizado.

5. Se prohíbe el envío de copias de mensajes de correspondencia electrónica con información confidencial sin el consentimiento del remitente original.

6. Se prohíbe a terceras personas leer, revisar, interceptar, modificar o destruir cualquier tipo de comunicación oficial y confidencial de la OCEPR o de cualquier otra persona o entidad, sin el consentimiento expreso del remitente y del destinatario de la comunicación.

7. Se prohíbe a los usuarios el suscribirse a listas de correo electrónico o que participen en grupos de noticias ("newgroups") que divulguen información o mensajes ajenos a las funciones y deberes de la OCEPR sin la debida autorización.

8. Se prohíbe guardar, enviar y recibir mensajes en exceso de la cuota asignada a cada usuario en el servidor de la OCEPR.

9. Se prohíbe la reproducción maliciosa o voluntaria de virus, envío de correo que no sea oficial, envío de material ofensivo, ilegal o pornográfico o de cualquier otra índole no autorizada. En caso de que así suceda, se disciplinará al empleado, según lo establezca el Reglamento de Personal.

10. Cada usuario será responsable de sus actos y conducta al acceder el Internet o al utilizar el correo electrónico, según dispuesto en la Certificación del Usuario Sobre Normas de Seguridad.

11. Se prohíbe el uso de programas de charlas ("chats").

12. La política adoptada sobre el uso de correo electrónico y sus auditorias será de igual aplicación para otros recursos de la Intranet e Internet.

13. La política adoptada para el uso de Internet será revisada periódicamente en caso de que surjan nuevas necesidades, únicas y particulares de la OCEPR. Estas se incorporarán y se hará formar parte de estas guías todos aquellos documentos, memorandos, instrucciones, manuales o políticas que se notifiquen de tiempo en tiempo y que estén relacionadas al uso de las computadoras de la OCEPR.

14. El uso de programas ("software") será autorizado por el Director de Área o su representante autorizado, por el (la) Coordinador(a) General. La utilización debe responder a los acuerdos establecidos en el contrato de utilización que la agencia negoció al momento de la compra. Ningún usuario utilizará programas que no estén respaldados por un contrato de utilización adquirido por la propia agencia.

15. El decomiso de los equipos electrónicos y periferales estará regulado por los reglamentos vigentes y aplicables de la Administración de Servicios Generales, en tanto la agencia determine regular este proceso, según lo establece el Reglamento Número 11 del Departamento de Hacienda, del 8 de abril de 2002, según enmendado.

16. La OCEPR se reserva el derecho a presentar la denuncia correspondiente por actuaciones que constituyan delitos estatales o federales aunque no estén expresamente prohibidas por estas condiciones para el uso de los equipos de computadoras.

17. Todo empleado será responsable de informar por escrito al (a la) Director(a) del Área o su representante autorizado sobre cualquier situación, incidente, problema de seguridad, acceso indebido o violación voluntaria o involuntaria de estas normas para el uso de las computadoras o redes de la OCEPR.

V. TABLA DE CONTENIDO DE POLÍTICAS, PROCEDIMIENTOS Y FORMAS:

A. POLÍTICAS ADMINISTRATIVAS	NÚMERO
Función de Servicio y Apoyo del Centro de Sistemas de Información	POL010
Políticas de Personal	POL020
Disponibilidad de Seguros Apropiados	POL030
Recomendación para la Adquisición de Equipo y Programación	POL040
Contratos de Mantenimiento	POL050
Prohibiciones en el Uso de Equipo y Programación	POL060
Labores del Auditor Interno con relación a Sistemas de Información	POL070

B. POLÍTICAS OPERACIONALES	NÚMERO
Políticas de Documentación	POL080
Políticas de Control de Calidad	POL090
Seguimiento de Políticas y Procedimientos y Procedimientos	POL100
Segregación de Tareas	POL110
Políticas de Interacción con Usuarios	POL120
Políticas de Adiestramiento	POL130
"Backups" (Resguardo de Datos)	POL140

Plan de Contingencia	POL150
Responsabilidades del Oficial de Seguridad	POL160
Registro de Actividades	POL170
Seguridad Física y Acceso al Área de Sistemas de Información	POL190
Separación del Fólder de Prueba y Producción	POL200
Políticas de Documentación	POL080
Políticas de Control de Calidad	POL090
Seguimiento de Políticas y Procedimientos y Procedimientos	POL100
Segregación de Tareas	POL110
Políticas de Interacción con Usuarios	POL120
Políticas de Adiestramiento	POL130
"Backups" (Resguardo de Datos)	POL140
Plan de Contingencia	POL150
Responsabilidades del Oficial de Seguridad	POL160
Registro de Actividades	POL170
Seguridad Física y Acceso al Área de Sistemas de Información	POL190
Separación de Fólder de Prueba y Producción	POL200
Procedimiento de "Backup"	PRO680

C. POLITICAS Y PROCEDIMIENTOS	NÚMERO
Otorgar Acceso al Sistema	PRO500
Prohibiciones del Uso del Internet	PRO510
Revocar Acceso al Sistema	PRO520
Acceso a Cintas	PRO530
Acceso a Documentación	PRO540
Devolución de Cintas	PRO550
Devolución de Documentación	PRO560
Copiar un "Source" al Fólder de Producción o al de Prueba	PRO570
Apagar o Bajar el Sistema Dell PowerEdge 2800	PRO590
Subir una PC	PRO620
Bajar o Apagar una PC	PRO630
Interacción con Usuarios	PRO640
Procedimiento para "Backups"	PRO680
Procedimiento para Restaurar Archivos	PRO690
Petición del Servicio	PRO700

D. FORMAS	NÚMERO
Hoja de Otorgar Acceso a la Red	
Certificación del Usuario a Seguir las	

Medidas de Seguridad Establecidas

Hoja de Requisición de Cinta

Hoja de Requisición de Documentación

Solicitud de Procesamiento de Data

Registro de Actividades del Sistema

Solicitud de Servicio

Registro de Llamadas del Usuario

Hoja de Notificación al Área de Sistemas de Información
Para dar de Baja o Alta a Empleados

Lista de Ex-empleados

Hoja de Registro de "Backups"

Hoja de Control de Llamadas de Servicio

VI. POLITICAS ADMINISTRATIVAS-AREA DE SISTEMAS DE INFORMACIÓN:

A. POLITICA 010: Función de Servicio y Apoyo

1. PROPOSITO:

El propósito de esta función es el de selección, dirección, planificación, instalación, operación, mantenimiento y supervisión de todos los recursos del Área de Sistemas de Información y la mejor y más efectiva utilización de éstos.

2. POLITICAS:

a. La preparación de un documento contentivo de las normas y reglas de organización y funcionamiento interno de dicha área. El mismo deberá incluir normas sobre la activación de sistemas, producción de copias de resguardo, normas de acceso y seguridad, de control y retención de archivos.

b. Adiestrar los usuarios en el uso correcto de equipo, aplicación y/o sistema.

c. Desarrollar y modificar aplicaciones o sistemas de acuerdo a las necesidades y especificaciones de los usuarios.

d. Implantar los sistemas o modificaciones desarrolladas, así como aplicaciones adquiridas en el mercado.

e. Proveer ayuda técnica a los usuarios según sea necesaria.

f. Crear Políticas y Procedimientos de documentación para los procesos de análisis, diseño y programación.

g. Proveer los manuales o procedimientos operacionales necesarios para el buen funcionamiento de los sistemas mecanizados.

h. Buscar los recursos necesarios para reparar equipo, haciendo llamadas para la garantía o mantenimiento del equipo a través del área de propiedad.

i. Llevar a cabo un análisis de las necesidades de equipo en la OCEPR antes de la adquisición de nuevo equipo.

j. Hacer los arreglos pertinentes para la compra y especificaciones de equipo o "software".

k. Velar por la privacidad, continuidad y desarrollo de los servicios del Área de Sistemas de Información.

l. Establecerá o fijará un área de biblioteca de archivo de datos y adoptará un manual de procedimientos a esos efectos.

m. Adoptará un plan de contingencia para el Área de Sistemas de Información e implantará los mecanismos monitores necesarios para asegurar el buen funcionamiento del mismo.

n. El (la) Director(a) del Área de Sistemas de Información reportará mensualmente al (a la) Subcoordinador(a) sobre las gestiones realizadas por el área.

B. POLITICA 020: POLITICA DE PERSONAL

1. PROPÓSITO:

Establecer políticas relacionadas a la administración de personal con el objetivo de mantener un nivel de eficiencia óptimo en el Área de Sistemas de Información.

2. POLÍTICA:

a. Esta política está conforme al actual Reglamento de Personal de la OCEPR. Cualquier cambio que sea incorporado a dicho reglamento, también será incluido en este documento de ser necesario. En cualquier ambiente de computadoras siempre se busca personal competente, pero las cualidades de lealtad y honestidad muchas veces son pasadas por alto. El daño causado por un empleado deshonesto puede sobrepasar los daños causados por factores externos o personal incompetente. La práctica de obtener referencias para asegurar el conocimiento de la persona siendo considerada, ser complementará con referencias en el carácter personal del individuo, las cuales serán investigadas.

b. Los empleados tendrán las descripciones de sus puestos y responsabilidades y las medidas de seguridad correspondientes. Estas medidas le serán entregadas al momento de comenzar sus labores en el Área de Sistemas de Información por el (la) Director(a) de dicha área.

c. Violaciones y sanciones a las medidas de seguridad del Sistema implantadas, serán discutidas con el empleado, confirmadas por escrito claramente y permanecerá la copia en el expediente del empleado en el Área de Sistemas de Información.

d. Si algún empleado del Área de Sistemas de Información es despedido o somete su renuncia, se relevará inmediatamente de sus responsabilidades. Su contraseña y acceso al sistema se eliminará del sistema y la clave de acceso al cuarto de los servidores será cambiada inmediatamente.

e. Además, se evaluará el personal del Área de Sistemas de Información cada seis meses, en cuanto al desempeño de todas sus

responsabilidades y proyectos. Estas evaluaciones serán complementadas con una evaluación a fines del año fiscal que resuma el cumplimiento durante el año.

f. Todas las actividades relacionadas con la evaluación de empleados y la descripción de sus puestos y responsabilidades, serán realizadas de acuerdo al Reglamento de Personal vigente.

C. POLITICA 030: DISPONIBILIDAD DE SEGUROS APROPIADOS

1. PROPÓSITO:

Asegurar todo el equipo por un valor de sustitución comprar Área de Sistemas de Información al valor de compra.

2. POLÍTICA:

a. Todo equipo bajo la responsabilidad del Área de Sistemas de Información tendrá un seguro por daños relacionados con fuerzas fuera del control del área. El seguro será específico y comprensivo.

b. La obtención de este seguro es responsabilidad de la administración. El Área de Sistemas de Información se limitará a evaluar y ofrecer recomendaciones a la administración sobre los pormenores del seguro.

c. Además, se estudiará la adquisición de un seguro adicional para las siguientes causas:

1) Pérdida de información de valor,

2) Costos de restauración de programas e información,

3) Gastos adicionales incurridos en el restablecimiento de operaciones,

4) Costos por interrupciones fuera de control del Área de sistemas de Información,

5) Daños causados por acciones premeditadas de empleados o personas con acceso al sistema,

d. El Área de Sistemas de Información llevará un registro de todas las reclamaciones hechas al seguro para referencias futuras.

D. POLITICA 040: RECOMENDACIÓN PARA LA ADQUISICIÓN DE EQUIPO Y PROGRAMACIÓN

1. PROPÓSITO:

Establecer las responsabilidades del Área de Sistemas de Información en cuanto a la recomendación de equipo y programación a ser adquirida por la OCEPR.

2. POLÍTICA:

a. El Área de Sistemas de Información se hará responsable de analizar las necesidades de las áreas bajo su responsabilidad y de solicitar aquel equipo o "software" que sea necesario para el funcionamiento eficiente de las áreas de la OCEPR.

b. El trámite de requisición y adquisición de equipo se hará de acuerdo al Reglamento de Adquisición de Bienes y Servicios la OCEPR. El Área de Sistemas de Información será responsable además, de establecer especificaciones de equipo y evaluar todas las propuestas y alternativas. Para poder hacer una evaluación completa, los siguientes puntos se tomarán en consideración:

c. Recursos de área del Área de Sistemas de Información,

d. Necesidades identificadas en el área,

e. Eficiencia que pueda aportar las alternativas identificadas,

f. Costos de adquisición y mantenimiento,

g. Información existente,

h. Tiempo requerido para la implantación y otras prioridades,

i. Garantía del equipo o software,

j. Compatibilidad del equipo/programación,

k. Seguridad,

l. Contratos de mantenimiento y servicios relacionados.

m. El área de Compras debe trabajar en conjunto con el Centro para evitar compras de equipo que no cumpla con los requisitos de la OCEPR. Refiérase al Reglamento de Adquisición de Bienes y Servicios para más detalles sobre la adquisición de equipo y programación.

n. El área de Compras debe trabajar en conjunto con el Centro para evitar compras de equipo que no cumpla con los requisitos de la OCEPR. Refiérase al Reglamento de Adquisición de Bienes y Servicios para más detalles sobre la adquisición de equipo y programación.

E. POLITICA 050: CONTRATOS DE MANTENIMIENTO

1. PROPÓSITO:

Establecer políticas que ayuden al Área de Sistemas de Información a administrar efectivamente los contratos de mantenimiento de equipo y programación. Además, obtener un inventario de todos los contratos de mantenimiento activos y saber a ciencia cierta los pormenores de los mismos.

2. POLÍTICA:

a. El Área de Sistemas de Información es responsable de tramitar todos los contratos de mantenimiento de equipo de computadoras de la OCEPR de acuerdo al Reglamento de Adquisición de Bienes y Servicios.

b. Es responsable de catalogar todos los contratos de mantenimiento que estén vigentes. El inventario debe incluir los siguientes detalles:

c. Nombre, dirección, e-mail y número de teléfono del suplidor que provee el mantenimiento,

d. Lista del equipo: marca, número de serie, número de propiedad y año del equipo,

e. Además, es responsable de catalogar todos los contratos de mantenimiento que estén vigentes. El inventario debe incluir los siguientes detalles:

1) Nombre, dirección, e-mail y número de teléfono del suplidor que provee el mantenimiento,

2) Lista del equipo: marca, número de serie, número de propiedad y año del equipo,

3) Fecha de expiración del contrato,

4) Lista de piezas y descripción del servicio incluido en el contrato.

5) Fecha de última visita por el suplidor para llevar un registro de mantenimiento,

6) Requerir que se certifiquen las facturas,

7) Requerir que la persona que solicita el servicio sea el empleado autorizado.

F. POLITICA 060: PROHIBICIONES EN EL USO DE EQUIPO Y PROGRAMACIÓN

1. PROPÓSITO:

Establecer las prohibiciones relacionadas con los recursos del Área de Sistemas de Información, que afectan directamente al equipo y a los programas. Además, de recalcar el riesgo tomado cuando se utiliza una copia ilegal de un "software" y el uso indebido del Internet, correo electrónico.

2. POLÍTICA:

a. El uso ilegal de programación o "software" es un riesgo que no debe ser tomado. Se educará a los usuarios sobre los riesgos y las consecuencias negativas a los que la organización se expone cuando se utiliza una copia ilegal de un producto. Entre los riesgos se encuentra la posibilidad de una demanda por parte de los suplidores. Se le explicarán las consecuencias sobre el uso ilegal de programación no autorizada y las sanciones disciplinarias que esto conllevará a los empleados, para evitar el uso ilegal de programas.

b. Tiene que existir un "programa original" o licencia por cada usuario del mismo.

c. Los recursos del Área de Sistemas de Información, no podrán ser utilizados para los propósitos que se enumeran a continuación:

1) Grabar y producir mensajes con fines exclusivamente político partidista,

2) Grabar y producir transcripciones de conferencias de prensa o entrevistas radiales o televisadas, cuyo contenido sea exclusivamente político partidista,

3) Producir etiquetas engomadas ("Labels") para enviar comunicaciones con fines político-partidistas,

4) Suplir información de carácter confidencial a partidos políticos u otra entidad,

5) Preparar, almacenar, mantener y producir listas de nombres con propósitos electorales, incluyendo el almacenamiento de datos que identifiquen a dichas personas con determinados partidos políticos,

6) Producir y almacenar datos relacionados a actividades de recolección de fondos para beneficio de un partido político o candidato,

7) Realizar gestiones privadas para el beneficio de un partido político o candidato,

8) Producir y almacenar datos personales para beneficio personal,

9) Suplir información de carácter confidencial relativa al contenido de las librerías o a los archivos de documentos, sin estar debidamente autorizados a esos efectos,

10) Desarrollar trabajos de programación que no estén coordinados por el Área de Sistemas de Información y que no persigan los fines útiles de la OCEPR,

11) Realizar cualquier otra gestión que esté expresamente prohibida por ley o por reglamento,

12) Enviar o recibir información a través del correo electrónico que no tenga nada que ver con el trabajo de la agencia.

G. POLITICA 070: LABORES DEL AUDITOR INTERNO RELACIONADOS A SISTEMAS DE INFORMACION

1. PROPÓSITO:

Identificar las labores del auditor interno y sus responsabilidades con el Área de Sistemas de Información.

2. POLÍTICA:

a. La oficina de Auditoria Interna de la OCEPR proveerá la asistencia necesaria al Área de Sistemas de Información, en cuanto a las siguientes tareas:

1) Auditorias de controles internos,

2) Auditorias de aplicaciones,

3) Análisis de costos y tasación de equipo,

4) Hacer recomendaciones y comentarios sobre las actividades auditadas.

b. Para proveer la asistencia requerida, muchas actividades han de ser realizadas. A continuación un breve resumen de las mismas:

c. Auditoria de Controles Internos:

1) Revisar la seguridad del sistema en términos de acceso al mismo por usuarios y las limitaciones a dicho acceso impuesto por el sistema,

2) Revisar la seguridad física del Área de Sistemas de Información en términos de controles físicos, dispositivos contra fuego y la eficacia del Plan de Contingencia,

3) Revisar los controles internos en cuanto al acceso a los diversos sistemas, cintas, documentos y otras posesiones del Área de Sistemas de Información,

4) Revisar los controles internos en términos de segregación de tareas del personal del Área de Sistemas de Información,

5) Verificar el cumplimiento de los procedimientos, planes y políticas establecidas por el Área de Sistemas de Información,

6) Verificar la seguridad de toda la información producida por los sistemas.

3. AUDITORIAS DE APLICACIONES:

a. Revisar y estimar las aplicaciones de contabilidad, finanzas y otros controles administrativos y promover el control efectivo de la información a un costo razonable,

b. Revisar todos los sistemas desarrollados o adquiridos por el Área de Sistemas de Información que procesen correctamente la información financiera y los controles establecidos sean apropiados.

c. Revisar y estimar las aplicaciones de contabilidad, finanzas y otros controles administrativos y promover el control efectivo de la información a un costo razonable,

d. Revisar todos los sistemas desarrollados o adquiridos por el Área de Sistemas de Información que procesen correctamente la información financiera y los controles establecidos sean apropiados.

4. ANÁLISIS DE COSTOS Y OTROS:

a. Verificar que todo el equipo del Área de Sistemas de Información esté asegurado adecuadamente,

b. Estimar la efectividad de los proyectos y responsabilidades asignadas,

c. Auditar la compra y utilización de equipo mecanizado. Se procederá a hacer una auditoria de los controles internos, así como una auditoria de aplicaciones, en forma anual para verificar que los procedimientos y políticas están siendo seguidos y asegurar que los controles establecidos para la seguridad no sean obsoletos,

d. Se procederá a hacer una auditoria de los proyectos terminados y en proceso trimestralmente para verificar que el nivel de calidad requerido ha sido mantenido. De haber alguna violación a los controles de calidad, ésta debe ser documentada y explicada por el programador, analista y el director del Área de Sistemas de Información,

e. En adición a estas auditorias periódicas, el auditor interno tiene la potestad de efectuar unas revisiones esporádicas de los controles y calidad de los proyectos del Área de Sistemas de Información,

f. El Auditor Interno efectuará una revisión semestral del Plan de Contingencia para asegurar que éste sea efectivo y eficiente en casos de emergencia y que todos los números de teléfono indicados son correctos. Evaluará las pruebas hechas por el (la) Director(a) del Área de Sistemas de Información para recomendar cambios o adiciones al plan.

H. POLITICA 080: POLÍTICAS DE DOCUMENTACIÓN

1. PROPÓSITO:

Establecer políticas de documentación de desarrollo y/o modificación de sistemas, así como documentación relacionada a manuales, procedimientos y políticas. Además, de indicar el uso correcto y mantenimiento de las instrucciones operacionales aplicables al (a la) Director(a), programadores y operadores.

2. POLÍTICA:

a. Todo sistema implantado, incluyendo sus características operacionales, estarán documentadas,

b. La documentación se protegerá contra uso no autorizado y desastres. En adición a ser requerida para mantenimiento o modificaciones, la documentación es indispensable para propósitos de recobrar información dañada o perdida.

c. Estos documentos incluyen la documentación técnica, procedimientos operacionales, manuales, así como pruebas y comunicaciones entre los usuarios y los programadores,

d. Incluye además, en esta documentación la aprobación por el usuario y el (la) Director(a) del Área de Sistemas de Información,

e. Para proveer un nivel satisfactorio de control, se puede clasificar la documentación de sistema en tres tipos:

   1) Confidencial I como lo son los manuales operativos del sistema,

   2) Confidencial II como lo son manuales de instalación de aplicaciones o documentación técnica de sistemas, y

   3) Público como son los casos de manuales de aplicación por suplidores.

f. Toda documentación será guardada en un anaquel a prueba de fuego, bajo llave, bajo la custodia del Oficial de Seguridad.

g. Copia de toda la documentación se guardará en la bóveda de una compañía contratada para resguardar estas cintas.

h. Muchas instalaciones de aplicaciones contienen librerías de documentación las cuales deben ser restringidas y controladas por el oficial de seguridad. La distribución de documentos reservados requiere atención especial. Se restringirá la distribución y la destrucción de estos documentos.

i. El auditor interno o la persona designada para revisar y mantener los controles de calidad establecidos, revisará periódicamente la documentación para asegurarse que los procedimientos y políticas establecidos han sido seguidos. La desviación de los procedimientos o políticas establecidos requerirá una explicación por parte del programador o analista a cargo, por escrito.

j. Instrucciones Operacionales:

1) Todas las instrucciones relacionadas con la operación de los computadores de la OCEPR estarán apropiadamente documentadas y accesibles a los Técnicos de Servicio y solamente a éstos. En adición, estas deben ser mantenidas periódicamente para asegurar que estén correctas.

I. POLITICA 090: POLÍTICAS DE CONTROL DE CALIDAD

1. PROPOSITO:

Definir el proceso a ser utilizado para asegurar que todos los trabajos desarrollados sean de óptima calidad y que hayan sido hechos con exactitud y a un nivel profesional.

2. POLÍTICA

a. El Control de calidad es un proceso continuo a través del ciclo de desarrollo y uso del sistema. Este proceso incluye las siguientes actividades:

b. Formalizar los Políticas y Procedimientos de sistema y programación,

c. Examinar el diseño de sistema y la documentación para asegurar que ha sido preparada de acuerdo con los Políticas y Procedimientos establecidos por la Oficina de Gerencia y Presupuesto y que el nuevo sistema tenga incorporado funciones adecuadas para control efectivo de calidad,

d. Revisar las pruebas de programación, sistema y las corridas pilotos para asegurar exactitud y cumplimiento con los Políticas y Procedimientos,

e. Revisar los procedimientos cada seis (6) meses para la conversión de data e información para exactitud y cumplimiento con los Políticas y Procedimientos,

f. Verificar que la metodología de sistema y programación está conforme a los Políticas y Procedimientos establecidos.

g. Garantizar que los controles apropiados, procedimientos de seguridad y pruebas de auditoria han sido especificadas y forman parte de la aplicación desarrollada, siguiendo la política de uso y manejo de información,

h. Las funciones arriba mencionadas deben ser consideradas como una actividad aparte por su proceso formal y deben de ser desempeñadas por el área de Auditoria Interna y el (la) director(a) del Área de Sistemas de Información,

i. Este tipo de revisión solamente puede ser llevada a cabo contra una estructura predefinida de Políticas y Procedimientos y procedimientos, i.e., metodología. Esto aseguraría que el producto final cumplirá con los controles y la seguridad requerida por la OCEPR,

j. Todo programador, técnico de servicio, analista y oficial de seguridad se compromete a mantener el nivel de calidad establecido por el Manual de Políticas y Procedimientos. Para ayudar a mantener este nivel de calidad se utilizará una **Hoja de Cotejo o de Control de Calidad.** Esta Hoja de Control de Calidad contendrá todos los documentos requeridos en el desarrollo o modificación de un sistema o aplicación. De faltar algún documento mencionado en la Hoja de Control de

Calidad, la persona responsable por la documentación deberá responder a esa violación.

J. POLITICA 100: SEGUIMIENTO DE POLÍTICAS Y PROCEDIMIENTOS

1. PROPÓSITO:

Establecer la responsabilidad de los componentes del Área de Sistemas de Información de obedecer los Políticas y Procedimientos y procedimientos establecidos en dicha área.

2. POLÍTICA:

a. Todo el personal del Área de Sistemas de Información tiene como deber el seguir los requisitos de programación y desarrollo establecidos en el Manual de Políticas y Procedimientos. Se llevará una revisión periódica de todos los Políticas y Procedimientos y procedimientos por el Auditor Interno de la OCEPR para asegurar que este seguimiento está siendo desempeñado,

b. De surgir algún cambio en el Manual de Políticas y Procedimientos, se hará llegar una copia del procedimiento nuevo o modificado con una explicación breve de su cambio a todo el personal del Área de Sistemas de Información y a la Oficina de Auditoria Interna. Este procedimiento debe ser incluido o sustituido en el Manual de Políticas y Procedimientos inmediatamente. Conjuntamente se notificará a todo el personal la fecha de adiestramiento para el nuevo o modificado estándar o procedimiento,

c. Pasada la fecha de efectividad del estándar o procedimiento, cualquier desviación del procedimiento establecido debe ser explicada e incluida en la documentación del desarrollo. De no cumplir, la persona en violación deberá corresponder directamente al (a la) Director(a) del Área de Sistemas de Información y/o al Auditor Interno de la OCEPR quienes tomarán las medidas necesarias.

K. POLITICA 110: SEGREGACIÓN DE TAREAS

1. PROPÓSITO:

Establecer la segregación de tareas para evitar que los usuarios, programadores, analistas y técnicos de servicio obtengan un nivel de acceso y comprensión que podría perjudicar el sistema y la integridad de su información.

2. POLÍTICA:

a. Responsabilidades y tareas de los usuarios:

b. Conocer el funcionamiento del sistema y tener acceso a su información. Sus privilegios son sumamente limitados,

c. No tendrán acceso a funciones de programación de sistemas operativos.

d. Responsabilidades y tareas de programadores:

1) Los programadores deben tener acceso a las herramientas de programación y pruebas,

2) Las actividades que ellos realicen deben ser limitadas a la prueba de programas y archivos con acceso a la programación de aquellos programas y archivos necesarios para el proyecto,

3) No tendrán acceso a archivos de producción.

4) En caso de que un programador necesite acceso a un archivo de producción deberá tener, por escrito, autorización del (de la) Director(a) del Área de Sistemas de Información o su representante autorizado.

5) No tendrán responsabilidades de usuario y el uso de utilidades tales como "dumping data" o backups debe ser restringida.

6) No operarán el sistema o accederán las librerías de aplicación.

e. Responsabilidades y tareas de los analistas:

1) Responsables por el diseño del sistema, incluyendo analizar las necesidades del sistema a desarrollar de acuerdo a los usuarios,

2) Diseñar los requisitos de seguridad,

3) Diseñar los archivos necesarios, pantallas e informes,

4) Definir los programas a desarrollar,

5) Documentar el sistema y hacer la demostración del sistema,

6) Son responsables por la programación, aunque ésta sea hecha por ellos directamente.

f. Responsabilidades y tareas del técnico de servicio:

1) Son responsables por la operación eficiente del sistema,

2) De hacer los "backups" semanal y cada seis meses y reportar fallas en el sistema o equipo de algún usuario,

3) No son responsables por los procedimientos de control ni el desarrollo de programas o aplicaciones,

4) Responsables de la eficiente operación del sistema y sus trabajos,

5) Se reportan directamente al supervisor que a su vez se reporta al (a la) Director(a) del Área de Sistemas de Información.

6) No son responsables de corregir procedimientos ni diseñar o programar aplicaciones o modificaciones,

7) Son responsables prender y apagar el sistema, hacer el backup requerido y registrar todo tipo de mantenimiento hecho por consecuencia de fallas en el sistema o en sus terminales/periferales y darle Apoyo técnico a los usuarios de la OCEPR.

L. POLITICA 120: POLÍTICA DE INTERACCIÓN CON USUARIOS

1. PROPÓSITO:

Establecer el nivel de interacción y responsabilidad de los usuarios hacia los sistemas desarrollados para su uso.

2. POLÍTICA:

a. Reconocer el compromiso hacia los usuarios para desarrollar un sistema que cumpla con sus necesidades del cual puedan hacerse responsables,

b. Asegurarse de que las aportaciones de los usuarios sean efectivas para cumplir en su totalidad con esos requisitos necesarios.

c. A su vez, los usuarios deben:

1) Asumir la responsabilidad del sistema por orden de jerarquía,

2) Participar en la definición de los requisitos del sistema, la etapa de prueba, adiestramiento e implantación del sistema,

3) Hacer repasos completos y periódicos de las opciones del sistema y determinar cómo este cumple con los objetivos del área.

M. POLITICA 130: POLÍTICAS DE ADIESTRAMIENTO

1. PROPÓSITO:

Establecer un Plan de Adiestramiento para los usuarios de la OCEPR para así promover el uso correcto del equipo y sus herramientas.

2. POLÍTICA:

a. Todo usuario debe ser adiestrado en el uso correcto del equipo y de las herramientas a la que tendrá acceso aprobado. De acuerdo a este propósito se estableció el Plan de Adiestramiento a revisarse anualmente para mejorar las funciones y entendimiento de los usuarios.

b. Los siguientes factores deben de considerarse al establecer un plan de adiestramiento:

1) Responsabilidad (quién) debe llevar a cabo los adiestramientos,

2) Recursos necesarios para llevarlos a cabo,

3) Cursos a ser provistos por el Centro.

4) Los cursos serán descritos en términos de tópicos a ser tratados, duración del curso, identificación de empleados/posiciones que ocupan para determinar si son los que deben tomarlo.

N. POLITICA 140: "Backups" (Resguardo de Datos)

1. PROPÓSITO

Establecer ciertas reglas para que se aproveche al máximo el proceso de "backup" y así asegurar la integridad de la data.

2. POLÍTICA:

1. El "backup" es un duplicado de una fuente de información, programa o archivo.

2. El "backup" se realizará diariamente y se guardará en una compañía que será contratada para esos propósitos.

3. Lo siguiente es una serie de reglas a seguir para aprovechar el "backup" a un máximo:

   1) Se mantendrán las copias de "backups" de la información, programas o archivos que sean de suma importancia.

   2) Se guardarán copias de éstas en la bóveda de la compañía contratada para el resguardo de los mismos, la cual será visitada todos los lunes.

   3) Se asegurará que los datos de los "backups" pueden ser recobrados con facilidad.

   4) Se harán las pruebas como se establece en los procedimientos del Plan de Contingencia para asegurar que la data pueda ser recobrada por ellos.

   5) Se utilizará el principio de padre-hijo para hacer "backups". De esta forma se asegurará que aquellos "backups" que contengan información esencial, no se utilizarán hasta que esta información no haya sido verificada mediante uso por parte del usuario.

4. Los "backups" de cierre de año se harán por períodos de más tiempo debido a los requisitos legales.

3. ROTULACIÓN DE CINTAS:

1. Para las cintas de "backups" se seguirá la siguiente rotulación:

   1) El backup completo "Full Backup"se ejecutará dos veces al año.

      Ej. DPVJUL04
      Ej. DPVDIC04

   2) XXX, primeras tres letras del nombre de la marca del equipo.

Ej. DPV = Dell Power Vault.
Ej. DPV-122T

3) XXX, primeras tres letras del nombre del mes.

Ej. DPVJUL04

4) XX, número del año en que se realiza el "backup".

2. Para backup diario del sistema, "Day Backup"

3. Las cintas se distribuirán en parejas o "set". Cada pareja contiene un "full backup" semanal y un incremento. El "full backup" semanal se corre los lunes de cada semana. Los incrementos corren de martes a viernes de cada semana.
Ej. SET-1-B, SET-1-I

4. La rotulación de las cintas se especifica de la siguiente manera:
XXX, primeras tres letras del nombre de la marca del equipo.
Ej. DPV = Dell PowerVault.
DPV seguido por un guión "– " y el modelo de los servidores.

Ej. DPV-122T
XXX, se asignará la abreviatura SET que identificará el SET a que pertenece la cinta semanal. Ej. SET-1-B

XX, Número del SET a que pertenece el Tape.

XX, Tipo de backup que se realiza.

NOTA: Estos "backups" se realizarán diariamente. Los lunes se utilizarán los tapes Set-1_B. De martes a viernes se utilizaran los Set-1_I que contiene toda la información de las áreas de trabajos y de las modificaciones de los usuarios, menos el sistema operativo. De estos existen doce (12) juegos, o sea que se puede obtener información para los usuarios de un (1) mes atrás.

5. Para backup anual del sistema, "HIS".

XXX, primeras tres letras del nombre de la marca del equipo.

Ej. DPV = Dell PowerVault.

XXX, se asignará la abreviatura HIS que identificará que es una cinta del "backup" Anual Histórico.

Ej. DPVHIS01.

XX, número de cinta del "backup" o de la semana en que se realiza el "backup".

O. POLITICA 150: PLAN DE CONTINGENCIA

1. PROPÓSITO:

Definir los procedimientos y políticas diseñadas para mantener o restaurar las operaciones después de una emergencia, falla de sistema o desastre.

2. POLÍTICA:

1. El Plan de Contingencia desarrollado para proveer los procedimientos y políticas necesarios en un caso de emergencia o desastre deberá:

   a) Identificar las aplicaciones críticas,

   b) Identificar lugares alternos donde las operaciones puedan continuar,

   c) Establecer estrategias a seguir en caso de desastre y la revisión periódica de éstas,

   d) Proveer el adiestramiento del personal del Área de Sistemas de Información en lo que respecta ha dicho plan,

   e) Crear los canales de comunicación para informar las emergencias y coordinar los esfuerzos,

f) Señalar el nombre, dirección y número de teléfono de los suplidores de equipo y materiales y de las personas encargadas de salvaguardar los archivos,

g) Indicar el número de teléfono y dirección de las oficinas y personas a quien se informará sobre el incidente ocurrido,

h) Contener un mapa que muestre las salidas de emergencia, localización de equipos para estos fines y la manera de desalojar el área.

i) Los procedimientos para la restauración de los archivos y programas,

j) Especificar los controles de seguridad necesarios durante dicha restauración,

k) Establecer la localización e identificación de resguardos de archivos y documentos,

l) Establecer un acuerdo formal con otro Área de Sistemas de Información por si fuese necesario poner en ejecución un plan de recuperación.

c. El Plan de Contingencia será reevaluado y ensayado periódicamente.

P. POLITICA 160: RESPONSABILIDADES DEL OFICIAL DE SEGURIDAD

1. PROPÓSITO

Detallar las responsabilidades del Director en conjunto con los técnicos de servicio para tener una segregación apropiada de tareas.

2. POLÍTICA

1. El Oficial de Seguridad tendrá las siguientes responsabilidades:

a. Asegurar que el sistema desarrollado cumpla con los requisitos de seguridad del Área de Sistemas de Información de la OCEPR,

b. Proveer protección a los programas siendo desarrollados o en la etapa de prueba,

c. Proveer acceso a los usuarios al igual que desactivar aquellos usuarios en violación a las medidas de seguridad o que ya no sean empleados de la OCEPR,

d. Asignar fólderes y tipo de protección a los usuarios,

e. Proveer acceso a cintas y documentación de aplicaciones o sistemas.

f. Será el guardián del disco de programas de producción,

g. Mantener el control adecuado del espacio en los discos del sistema.

Q. POLITICA 170: REGISTRO DE ACTIVIDADES

1. PROPÓSITO:

Registrar todo tipo de falla de sistema o del equipo asignado a los usuarios, de forma que se registren efectivamente las acciones tomadas y el tiempo requerido.

2. POLÍTICA:

a. Todos los técnicos de servicio llevarán dos tipos de registros: uno para registrar las fallas en el sistema y otro para registrar las fallas comunicadas por los usuarios,

b. Estos registros se revisarán en las reuniones de "status" hechas cada dos semanas,

c. El Registro de Llamadas de los Usuarios tendrá, por lo menos lo siguiente: número de llamada, oficina que llama, nombre del usuario, fecha, descripción del problema, comentario, fecha de solucionada la situación,

d. Los intentos hechos por personal no autorizado tratando de acceder al sistema serán registrados en el Registro de Actividades del Sistema. Este registro hecho por el sistema deberá ser revisado en casos de emergencias, por ejemplo, los accesos no autorizados o fallas en el sistema no comunes como lo son las fallas de energía eléctrica.

R. POLITICA 190: SEGURIDAD FÍSICA Y ACCESO AL AREA DE SISTEMAS DE INFORMACIÓN

1. PROPÓSITO:

Establecer una serie de medidas para mantener la seguridad física y de acceso al Área de Sistemas de Información al máximo.

2. POLÍTICA

a. La combinación de números establecida para permitir la entrada será cambiado una vez al mes por lo menos,

b. La presencia de cámaras de seguridad u otro mecanismo debe ser tomado en consideración en las facilidades en donde se encuentra equipo como terminales e impresoras. Todo tipo de equipo se alejará de ventanas, puertas abiertas o de cristal,

c. El acceso físico al Área de Sistemas de Información será restringido a sólo aquel personal autorizado y comprometido con las operaciones del mismo,

d. El (la) Director(a) del Área de Sistemas de Información será la persona responsable de mantener las medidas de seguridad del área,

e. El personal autorizado deberá tener la máxima precaución cuando se le permita la entrada a otra persona ajena al Área de Sistemas de Información de forma tal que no pueda copiarse la clave de acceso al mismo,

f. El acceso al cuarto de servidores será registrado en el Registro de Visitantes identificando el propósito de la visita. Conforme al propósito de la visita, se determinará si se le permite o no, el acceso al Área de Sistemas de Información,

g. Tanto en el área del computador como en todas las facilidades donde se encuentren terminales, se proveerá equipo contra fuego: extintores, Halon 1301, alarmas de fuego y detectores de humo,

h. Los cuartos de comunicación por piso y los paneles de distribución eléctrica del equipo deberán estar protegidas contra sabotaje.

i. Seguridad de Archivos, Programas y Formas será como sigue:

1) Todos los anaqueles y cajas de seguridad conteniendo las cintas de archivos, programas, documentación y formularios controlados estarán bajo llave para prevenir el uso por personas no autorizadas,

2) El (la) Director(a) mantendrá un registro de todas las salidas y entradas de las cintas, programas, documentación y formas en donde se indicará cuándo y quién removió y devolvió el material,

3) Versiones viejas de programas serán rotuladas para evitar confusión, guardadas bajo seguridad y cuando la nueva versión esté instalada se debe destruir la versión vieja lo antes posible,

4) Copia de todos los archivos, programas, aplicaciones, sistemas, documentaciones y formas deben ser guardadas en la bóveda de la compañía contratada para el resguardo de las cintas de "backups". De esta forma, se tendrá una copia segura.

S. POLITICA 200: SEPARACIÓN DE FÓLDER DE PRUEBA Y PRODUCCIÓN

1. PROPÓSITO:

Establecer los fólderes de prueba y producción como fólderes aparte que no deben ser mezclados.

2. POLÍTICA:

a. El directorio de producción estará accesible solo al (a la) Director(a). El (la) Director(a) será la persona responsable de copiar programas o archivos de sus fólderes de prueba para programar.-

b. Los programadores tendrán un directorio de prueba. En ella, podrán hacer las modificaciones o los desarrollos requeridos por los usuarios.

c. No será hasta que el usuario y la persona designada para mantener la calidad apruebe la prueba, que será autorizado el pasar a producción los cambios o el desarrollo nuevo. De esta forma, se asegura que un cambio que no haya sido autorizado forme parte del cambio solicitado y que el cambio no sea programado en el fólder de producción el cual puede ocasionar cualquier percance.

T. POLITICA Y PROCEDIMIENTO 500: OTORGAR ACCESO AL SISTEMA

1. PROPÓSITO:

Otorgar a un usuario autorizado acceso al sistema y a sus aplicaciones, conforme el nivel de seguridad permitido a cada usuario.

2. ALCANCE:

Este procedimiento aplica a todos los usuarios de la OCEPR.

3. FORMAS:

Hoja para Otorgar Acceso a la Red, Certificación de Usuario a Seguir las Normas y Procedimientos del Uso de los Equipos Electrónicos.

4. PROCEDIMIENTO:

PERSONA RESPONSABBLE	PASO	PROCESO
Director(a) del Área de Sistemas de Información	1	Prepara la hoja para solicitar acceso al sistema para el nuevo usuario, Forma Otorgar Acceso a la Red.
	2	Se asegura de que el usuario ha sido debidamente adiestrado en el funcionamiento correcto del equipo y sus aplicaciones.
	3	Firma la hoja para solicitar acceso al sistema, indicando el nivel de seguridad o autorización delegado al usuario.
	4	Envía la hoja al (a la) Director(a) del Área de Sistemas de Información.
Director (a) Área solicitante	5	Recibe la hoja del (de la) Director(a) del Área solicitante.
	6	Verifica que toda la hoja ha sido completada adecuadamente. De no ser así, se comunica con el Director de Área para que sea completada.
	7	Determina al grupo de acceso, aplicaciones y protección del nuevo usuario.
	8	Se reúne con el usuario para discutir las medidas de seguridad y las consecuencias obtenidas por causa de alguna violación incluyendo las medidas disciplinarias establecidas en el Reglamento de Personal.

Director(a) y Usuario	9	Verifica que el empleado haya sido adiestrado en la herramienta a utilizar.
	10	Elabora un adiestramiento sencillo sobre la operación y seguridad del equipo e información.
	11	Explica el proceso de acceso al sistema para que el usuario determine su contraseña.
	12	Obtiene la certificación del usuario de que no divulgará su contraseña o información confidencial a ninguna otra persona.
Ayudante Administrativo	13	Archiva la certificación y la hoja para otorgar acceso en el archivo para uso futuro.

U. POLITICA Y PROCEDIMIENTO 510: PROHIBICIONES EN EL USO DEL INTERNET

1. PROPÓSITO:

Establecer las prohibiciones relacionadas al uso indebido del Internet y controlar la contraseña de acceso al mismo.

2. POLÍTICA:

a. El acceso al Internet es una herramienta de trabajo que estará únicamente disponible a los usuarios que, por la naturaleza de sus funciones, deban acceder al mismo para realizar su trabajo. Se establecerá un control riguroso y se limitará a las personas según lo anteriormente establecido,

b. Este acceso deberá ser solicitado en la **Hoja de Acceso al Sistema Electrónico** de la OCEPR a través del (de la) Director(a) del Área de trabajo del usuario,

c. Los recursos del Internet **no** podrán ser utilizados para lo siguientes propósitos que se detallan a continuación:

1) Acceder y copiar información con fines exclusivamente político partidista.

2) Acceder áreas de "Chat".

3) Acceder "Website" o páginas con contenido sexual.

4) Hacer búsqueda de información que no tenga un propósito dentro del quehacer de la Agencia.

5) Copiar información gratis o pública en disquete o en el disco duro de la máquina, ya que se expone el equipo a copiar un virus durante el "download" o descargue.

6) Crear páginas de "Web" que no estén coordinadas por el Área de sistemas de Información y que no persigan fines útiles de la OCEPR.

7) Realizar cualquier otra gestión que esté expresamente prohibida por ley o reglamento.

8) Bajar aplicaciones que no estén autorizadas por el (la) Director(a) del Área de Sistemas de Información, para las cuales no se han pagado los derechos de uso.

V. POLITICA Y PROCEDIMIENTO 520: REVOCAR EL ACCESO AL SISTEMA

1. PROPOSITO

Revocar el acceso al sistema de cualquier usuario en violación a las medidas de seguridad establecidas o a una persona que ya no sea empleado de la OCEPR.

2. ALCANCE

Este procedimiento aplica a todo usuario de la OCEPR.

3. FORMAS y FORMULARIOS:

Hoja para Otorgar Acceso a la Red, Hoja de Notificación al Área de Sistemas de Información para dar de alta o baja a empleados, en el computador y Lista de Ex-Empleados.

4. PROCEDIMIENTO

PERSONA RESPONSABLE	PASO	PROCESO
Director(a) del Área de Recursos Humanos	1	Envía, **mensualmente**, el Listado de Ex-empleados de la OCEPR al oficial de seguridad.
Director(a) del Área de Sistemas de Información	2	Obtiene el listado de aquellos empleados que ya no forman parte de la OCEPR del (de la) Director(a) del Área de Recursos Humanos.
	3	Obtiene el listado de aquellos empleados que han violado las medidas de seguridad y serán desactivados del sistema.
	4	Va al sistema.
	5	Desactiva todos los empleados y los elimina del sistema.
	6	Va al archivo de usuarios.
	7	Obtiene del archivo de usuarios todos los empleados que han sido desactivados.

	8	Indica en la **Hoja de Otorgar Acceso** la fecha en que el empleado fue desactivado y la razón por la cual se desactivó.
	9	Archiva la Hoja de Otorgar Acceso en el archivo para uso futuro.

W. POLITICA Y PROCEDIMIENTO 530: ACCESO A CINTAS

1. PROPÓSITO:

Controlar el acceso a cintas para asegurar un mejor control sobre la manera en que se obtiene y se devuelve.

2. ALCANCE:

Este procedimiento aplica a todas las cintas de "backup disk" producidas en la OCEPR.

3. PROCEDIMIENTO

PERSONA RESPONSABLE	PASO	PROCESO
Director(a), Subdirector(a) u Operador(a)	1	Acceden a la Bóveda para obtener la cinta con los archivos necesarios.
	2	Envía la **Hoja de Requisición de Cinta** al (a la) Oficial de Seguridad para que éste se la provea.
Operador(a) o Director(a)	3	Recibe la hoja del (de la) programador(a) u operador(a).

	4	Verifica que la hoja ha sido completada adecuadamente. De no ser así, se comunica con el programador requiriendo la cinta.
	5	Va al archivo de cintas y localiza la cinta solicitada.
	6	Entrega la cinta al (a la) programador(a) que solicitó la misma.
Programador(a) u Operador(a)	7	Recibe la cinta del (de la) operador(a) o director(a) ó subdirector(a).
	8	Firma la **Hoja de Requisición de la Cinta** para indicar que fue recibida por él (ella) y anota la fecha y hora de entrega.
	9	Devuelve la Hoja de Requisición de Cinta al (a la) operador(a) o director(a), para archivar.
Operador(a) o Director(a)	10	Recibe la hoja de requisición firmada por el (la) programador(a).
	11	Verifica que la hoja indique la fecha y hora de la entrega de la cinta.
	12	De no indicar la fecha y hora de entrega, devuelve al (a la) programador(a) u operador(a).

	13	Archiva la hoja en el archivo de requisiciones de cinta, para luego ser completada al devolver la cinta.

X. POLITICA Y PROCEDIMIENTO 540: ACCESO A DOCUMENTACIÓN

1. PROPOSITO:

Controlar el acceso a documentación para asegurar un mejor control sobre la manera en que se maneja la documentación.

2. ALCANCE:

Este procedimiento aplica a toda documentación técnica de sistemas, manuales de usuarios, procedimientos y documentación de operación del equipo.

3. FORMAS:

Hoja de Requisición de Documentación.

4. PROCEDIMIENTO:

PERSONA RESPONSABLE	PASO	PROCESO
Programador(a), Analista o Usuario	1	Prepara la **Hoja de Requisición de Documentación** con el nombre de la documentación necesaria.
	2	Envía la **Hoja de Requisición de Documentación** al Oficial de Seguridad, para que éste se la provea.

Programador(a), Analista o Usuario	3	Recibe la documentación del (de la) Oficial de Seguridad.
Oficial de Seguridad	4	Recibe la **Hoja de Requisición de Documentación** del (de la) programador(a), analista o usuario.
	5	Verifica que la hoja haya sido completada en todas sus partes. De no ser así, se comunica con el (la) programador(a), analista o usuario requiriendo la documentación.
	6	Va al archivo de documentación para buscar la documentación solicitada.
	7	Entrega la cinta al (a la) Programador(a), Analista o Usuario.
	8	Firma la hoja de requisición para indicar que fue recibida por él con fecha y hora de entrega.
	9	Devuelve la hoja de requisición al (a la) Oficial de Seguridad, para archivar.
Oficial de Seguridad	10	Recibe la hoja de requisición firmada por el (la) programador(a), analista o usuario.
	11	Verifica que la hoja indique la fecha y hora de la entrega de la documentación.
	12	Archiva la hoja en el Archivo de Requisiciones de Documentación, para luego ser completada al devolver la documentación.

Y. POLITICA Y PROCEDIMIENTO 550: DEVOLUCIÓN DE CINTAS

1. PROPOSITO:

Controlar el acceso a cintas para asegurar un mejor control sobre la manera en que se obtiene y se devuelve.

2. ALCANCE:

Este procedimiento aplica a todas las cintas producidas en la OCEPR.

3. FORMAS:

Hoja de Requisición de Cinta.

4. PROCEDIMIENTO:

PERSONA RESPONSABLE	PASO	PROCESO
Programador(a) u Operador(a)	1	Devuelve la cinta al Oficial de Seguridad.
Oficial de Seguridad	2	Recibe la cinta del (de la) programador(a) u operador(a).
	3	Verifica que la numeración de la cinta sea la misma devuelta.
	4	Anota la hora y fecha de devolución en la Hoja de Requisición de Cinta, e inicializa al lado indicando el recibo.

	5	Entrega la hoja de Requisición de Cinta al (a la) programador(a) u operador(a), para que firme la hoja indicando que devolvió la cinta.
Programador(a) u Operador(a)	6	Recibe la Hoja de Requisición de Cinta para firmar que entregó la cinta en perfectas condiciones.
	7	Entrega la Hoja de Requisición de Cinta al oficial de seguridad para archivar.
Director(a) del Área de Sistemas de Información	8	Recibe la Hoja de Requisición de Cinta firmada por el (la) programador(a) u operador(a).
	9	Verifica que todas las partes de la hoja hayan sido totalmente complementadas.
	10	Archiva la hoja de Requisición de Cinta en el archivo de cintas devueltas, para uso futuro.

Z. POLITICA Y PROCEDIMIENTO 560: DEVOLUCIÓN DE DOCUMENTACIÓN

1. PROPOSITO

Establecer el procedimiento adecuado para la rápida y pronta devolución de documentación esencial.

2. ALCANCE

Este procedimiento aplica a toda documentación técnica de sistemas, manuales de usuarios, procedimientos y documentos de operación del equipo.

3. FORMAS

Hoja de Requisición de Documentación (CSIREQU2).

4. PROCEDIMIENTO

PERSONA RESPONSABLE	PASO	PROCESO
Programador(a), Analista o Usuario	1	Entrega la documentación prestada al oficial de seguridad.
Director(a) Área de Sistemas de Información	2	Recibe la documentación prestada del (de la) programador(a), analista o usuario.
	3	Busca en el Archivo de Requisiciones de Documentación, la Requisición de Documentación de la documentación en cuestión.
	4	Cuando la devuelve, verifica que la documentación sea la correcta.
	5	Anota la hora y fecha de devolución en la Hoja de Requisición de Documentación e inicializa al lado

		indicando el recibo.
	6	Entrega la **Hoja de Requisición de Documentación** al (a la) programador(a), analista o usuario para que la firme como constancia de que devolvió la documentación.
Programador(a), Analista o Usuario	7	Recibe la **Hoja de Requisición de Documentación** para firmar que entregó la documentación en perfectas condiciones.
	8	Entrega la **Hoja de Requisición de Documentación** al oficial de seguridad para archivar.
Director(a) Área de Sistemas de Información	9	Recibe la **Hoja de Requisición de Documentación** firmada por el (la) programador(a), analista o usuario.
	10	Verifica que todas las partes de la hoja hayan sido totalmente complementadas.
	11	Archiva la Hoja de Requisición de Documentación en el archivo de documentación devueltas para uso futuro.

AA. POLITICA Y PROCEDIMIENTO 570: COPIAR UN "SOURCE" AL FOLDER DE PRODUCCIÓN O AL DE PRUEBA

1 PROPOSITO:

Asegurar que solamente los "sources" autorizados son los que sean copiados al fólder de prueba o a la de producción.

2. ALCANCE:

Este procedimiento aplica a todos los sistemas mecanizados activos en el Área de Sistemas de Información.

3. FORMAS:

Hoja de Requisición de Archivos a Transferir.

4. PROCEDIMIENTO:

PERSONA RESPONSABLE	PASO	PROCESO
Programador(a) o Analista	1	Anota en el registro de "sources" copiados el nombre del "source" a ser transferido de fólder, al fólder al cual se copia y el propósito de la copia.
	2	Notifica al Oficial de Seguridad para que éste copie el source al fólder correspondiente.
Oficial de Seguridad	3	Recibe la solicitud del (de la) programador(a) o analista para la copia del "source".
	4	Copia el "source" deseado al fólder correspondiente. Si el "source" va a ser copiado al fólder de producción, verifica que éste haya sido aprobado por la persona designada a mantener el control de calidad. De estar aprobado el "source", elimina el "source" viejo para copiar el nuevo "source".
	5	Anota en el registro de "sources" copiados la fecha en la que se copió el mismo.

	6	Notifica al (a la) programador(a) o analista que el "source" ha sido copiado.
Programador(a) o Analista	7	Recibe la notificación del Oficial de Seguridad que el "source" ha sido copiado.
	8	Si el "source" fue copiado al fólder de producción, termina la documentación para ser archivada.
	9	Si el "source" fue copiado al fólder de prueba, comienza a modificar el "source" según la requisición del usuario.

BB. POLITICA Y PROCEDIMIENTO 580:
APAGAR O BAJAR EL SISTEMA DELL POWEREDGE 2800

1. PROPÓSITO

Instrucciones para bajar el Sistema Digital DECSYSTEM5000.

2. ALCANCE

Equipo Digital DECSYSTEM 5000/260.

3. PROCEDIMIENTO

PERSONA RESPONSABLE	PASO	PROCESO

Operador(a)

1. En la consola de Digital Dell PowerVault 122T:

2. Escribir "root" cuando la computadora está pidiendo algún "login" para entrar al sistema y luego oprimir la tecla "Enter."

3. Escribir el "password" de la cuenta "root" cuando la computadora lo pida y luego oprimir la tecla "Enter".

4. Una vez aparece el "prompt" OCEPR escribir "pcsamgr" y saldrá el menú del "PC Manager". Moverse con el cursor a la derecha hasta Message",bajar con el cursor hasta "Broadcast" y oprimir "Enter".

5. Escribir el mensaje que se enviará a los usuarios y oprimir "Enter" y cuando esté sobre la opción "Send" oprimir "Enter" nuevamente.

6. Oprimir las teclas "Alt+Q" a la vez

para salir del "box" del mensaje que se envió. Oprimir "Enter" sobre la opción Return" para volver al menú del "PC Manager".

7. Moverse con el cursor a la izquierda hasta "View", bajar con el cursor hasta "Exit" y oprimir "Enter".

8. Una vez aparece el "prompt" OCEPR escribir "shutdown – h now"* y luego oprimir la tecla "Enter" para que el sistema baje completamente en ese mismo momento.

* También puede escribir "shutdown +x" siendo "x" un número entero, para indicarle que el sistema baje sólo dentro de "x" minutos. También puede escribir "shutdown hh:mm" siendo "hh:mm" la hora (militar) y minutos en la que se quiere que el sistema sea bajado.

9. Esperar que la computadora baje ciertos programas del sistema y luego aparecerá en pantalla el "prompt" >>.

10. Poner en "Off" el botón en la parte izquierda posterior de la consola.

11. Poner en "Off" el botón en la parte izquierda inferior del frente del monitor.

12. Poner en "Off" los botones en la parte izquierda posterior de todas las unidades de disco.

13. Poner en "Off" el botón en la parte inferior posterior de la unidad de "tape backup".

14. Poner en "Off" el botón en la parte izquierda frontal de la unidad de cinta.

15. Poner en "Off" el botón en la parte izquierda frontal del "UPS".

CC. POLITICA Y PROCEDIMIENTO 590: SUBIR EL SISTEMA DELL POWEREDGE 2800

1. PROPÓSITO

Establecer los pasos a seguir para subir el sistema Dell PowerEdge 2800.

2. ALCANCE

Equipo Subir el sistema Dell PowerEdge 2800.

3. PROCEDIMIENTO

PERSONA RESPONSABLE	PASO	PROCESO
Operador(a)	1.	En la consola de la Digital DECSystem 5000:
	2..	Poner en "On" el botón en la parte de atrás de la consola.
	3.	Poner en "On" el botón en la parte izquierda inferior del frente del monitor.
	4.	Poner en "On" los botones en la parte izquierda posterior de todas las unidades de disco.
	5.	Poner en "On" el botón en la parte inferior posterior de la unidad de "tape backup".
	6.	Poner en "On" el botón en la parte izquierda frontal de la Unidad de cinta.
	7.	Poner en "On" el botón en la parte izquierda frontal del "UPS".
	8.	Esperar que la computadora suba ciertos programas del

sistema y luego aparecerá en pantalla el "prompt" >>.

9. Escribir "BOOT" y oprimir la tecla "Enter"

10. La computadora comenzará a subir los restantes programas del sistema, hará una revisión de los discos del mismo y luego aparecerá en pantalla el "prompt" "login". Esto indica que el sistema subió completamente y ya aquí se puede trabajar como de costumbre.

DD. POLITICA Y PROCEDIMIENTO 620: SUBIR UNA PC

1. PROPOSITO

Establecer el proceso a seguir para subir una PC.

2. ALCANCE

Equipo Digital PC o PC compatible.

3. PROCEDIMIENTO

PERSONA RESPONSABLE	PASO	PROCESO
Operador(a)	1.	En la consola de la PC: Poner en "On" el botón de encendido en la parte frontal derecha de la consola o es necesario encender la pantalla de la PC porque la

misma enciende automáticamente cuando se enciende la consola.

2. Esperar que la computadora suba ciertos programas del sistema y luego aparecerá en pantalla el mensaje "Enter user name:", aquí escribir su código de usuario del sistema y luego oprimir la tecla de Tab.

3. Aparecerá el mensaje "Enter your password" y entonces escribir su contraseña para entrar al sistema y luego oprimir la tecla "Enter".

4. La computadora comenzará a subir otros programas del sistema y luego entrará a Microsoft Windows XP Professional". Ya estando aquí ha entrado al sistema.

EE. POLITICA Y PROCEDIMIENTO 630: BAJAR O APAGAR UNA PC

1. PROPOSITO

Establecer el proceso a seguir para apagar una PC.

2. ALCANCE

Equipo Digital PC o PC compatible.

3. PROCEDIMIENTO

PERSONA RESPONSABLE	PASO	PROCESO
Operador(a)	1.	En la consola de la PC:
	2.	Salir de toda aplicación que esté utilizando en la computadora.
	3.	Una vez se encuentre en el "Desktop" de "Microsoft Windows" mover el "mouse" hasta apuntar en la palabra "Start" en la barra de la parte inferior. Una vez ahí oprimir el botón izquierdo del "mouse".
	4.	Mover el "mouse" hasta la opción "Shut Down" y oprimir el botón izquierdo del mismo.
	5.	Aparecerá en pantalla el mensaje "What do you want

the Computer to do?: Acompañado de tres opciones "shut down the computer". Escojer la opción "Shutdown" y oprimir el botón izquierdo del mismo.

6. Aparecerá en pantalla "shutting down the computer". Es necesario apagar la pantalla e la PC porque la misma no se apaga "automáticamente cuando se apaga el CPU.

FF. POLITICA Y PROCEDIMIENTO 640: INTERACCIÓN CON USUARIOS

1. PROPÓSITO:

Ayudar a los usuarios a resolver dificultades que tengan con el equipo y aclarar dudas sobre los programas existentes.

2. POLÍTICA:

El compromiso hacia los usuarios se traduce en ayudarles a cumplir con sus necesidades.

3. FORMAS

Hoja de Control de Llamadas de Servicio

4. PROCEDIMIENTO

PERSONA RESPONSABLE	PASO	PROCESO
	1.	Se reciben las llamadas de los diferentes usuarios.
	2.	Se anotan en el Registro de Llamadas de Servicio en el orden en que se reciben y se les asigna un número de control.
	3.	Estas llamadas se le asignan a los diferentes técnicos de servicio.

3a El técnico determina si puede asistir al usuario por vía telefónica o si es necesario presentarse a la oficina que solicita el servicio.

3.b El técnico informa al Área de Sistemas de Información desde la oficina en la que se encuentra si resolvió la llamada. Además, el técnico se comunica al área también si necesita algún tipo de orientación adicional o ayuda para poder resolver el problema.

3.c Luego de terminada la ayuda al usuario, el técnico lo informa a la persona encargada de llevar el registro de llamadas para completar el registro.

GG. PROCEDIMIENTO 680: PROCEDIMIENTO DE "BACKUP"

1. PROPOSITO

Establecer un procedimiento para hacer los "backups".

2. ALCANCE

Este procedimiento aplica a "backups" de todos los datos y sistemas existentes en el Área de Sistemas de Información en los diferentes computadores principales.

3. FORMAS

a. Hoja de Registro de "Backups"

4. PROCEDIMIENTO

PERSONA RESPONSABLE	PASO	PROCESO
Operador(a)	1.	Verifica en el Itinerario de "Backups" la fecha del último "backup" y que el Registro de "Backups" esté completo.
	2.	Hacer "log-on" en dominio OCEPR como administrador o con usuario que pertenezca a grupo "Domain Backup Users".
	3.	Seleccionar "Star->All Program-<Sumantec Backup Exec 10d for Windows Server".
	4.	Sacar todos los tapes de la rotación semanal de la unidad de "tape backup" e insertar el "tape" que va a usar para hacer el "backup".
	5.	En la pantalla principal de Veritas selecciones la pestaña de "Devices", bajo "Robotic Libraries", expanda la unidad de

tape "DELL", seleccione "Slots" con el botón derecho del Mouse y escoja "Inventory"... oprima el botón de "RUN NOW".

6. En la pantalla principal de Veritas seleccione la pestaña de "Backup" en la parte superior izquierda y se debe desplegar la pantalla de "Backup Job Properties".

7. En la Ventana de "Propierties" de la mano izquierda de la pantalla debe estar seleccionada la opción de "Selections". En la mano derecha expanda los discos para buscar los archivos a los cuales necesita hacer 'backup", en los discos locales del servidor bajo "Local Selections" o busque un servidor bajo "Remote Job Properties".

8. En la ventana de "Propierties" de la mano izquierda de la pantalla, seleccione "Device and Media"y asegúrese de que "Append to Meida, Overwrite if No Appendable Media is Availabe" y "Eject Media After Job", estén seleccionados.

9. En la ventana de "Properties" de la mano izquierda de la pantalla General, y bajo "Backup Method for Files", seleccione "Full-Back-Up-Files-Using Archive Bit (Reset

Archive Bit)" y asegúrese que bajo "Compression Type" tenga seleccionado "Hardware (if available, otherwise none).

10. Oprima el botón de "Run Now", para ejecutar el trabajo de "Backup".

11. Una vez termina de ejecutar el "Backup", saque el tape de la unidad y reinserte los tapes de la rotación semanal.

12. Vuelva a ejecutar el paso número 5 de este procedimiento, para que Veritas vuelva a reconocer los tapes de la rotación.

HH. POLITICA Y PROCEDIMIENTO 690: PROCEDIMIENTO PARA RESTAURAR ARCHIVOS

1. PROPOSITO

Establecer el procedimiento para restaurar archivos correctamente.

2. ALCANCE

Este procedimiento aplica a los datos de todos los sistemas existentes en el Área de Sistemas de Información.

3. FORMAS

Hoja de Requisición de Cinta.

4. PROCEDIMIENTO

PERSONA RESPONSABLE	PASO	PROCESO
Operador(a)	1.	Prepara la Forma **Hoja de Requisición de Cinta** según el procedimiento Acceso a Cinta. Se comunica con el oficial de seguridad para que éste busque la cinta o disco necesario.
Oficial de Seguridad	2.	Recibe del operador la requisición para restaurar un archivo.
	3.	Verifica las **Hojas de Registro de "Backups"** y la cinta o disco en donde el archivo se encuentra.
	4.	Entrega al operador la cinta o el disco correcto.
Operador	5.	Recibe el disco o la cinta dependiendo en donde está localizado el archivo.
	6.	Hacer "Log-On" en dominio OCEPR, como administrador o con usuario que pertenezca a grupo de "Domain Backup Users".
	7.	Selecciona "Start->All Program->Sumantec Backup Exec 10d for Windows Server".
	8.	En la pantalla principal de Veritas selecciona la pantalla de "Restore Job Properties".

9. En la ventana de "Properties" de la mano izquierda de la pantalla debe estar seleccionada la opción de "Selections". En la ventana de la mano derecha, asegúrese que "View By Resource" esté seleccionado. Escoja el archivo o los archivos que quiere recuperar seleccionándolo(s) en la pantalla donde están listados los servidores. Tome nota del nombre del "Tape" donde se encuentra el archivo o los archivos y búsquelo en su librería de "Tapes".

10. Saque todos los "Tapes" de la rotación semanal de la unidad de "Tape Backup" e inserte el "tape" que va a usar para hacer el "restore". Como medida d de protección, use la pestaña de "Write Protect" del "tape" para evitar que se borre accidentalmente.

11. En la pantalla principal de "Veritas", seleccione la pestaña de "Devices", bajo "Robotic Libraries", expanda la unidad de "tape" DELL , seleccione "Slots" con el botón derecho del Mouse escoja "Inventory"...oprima el botón de "Run Now".

12. Cuando termine la ejecución del inventario, haga otra vez el paso 9 para buscar el (los) archivo(s) y selecciónelos.

13. Si va a restaurar los archivos a un lugar diferente de donde estaban localizados originalmente, escoja "File

	Redirection" bajo "Properties"en la pantalla de "Restore Job Properties". Seleccione "Redirect File Sets" y escoja el lugar donde quiere que "Back-up Exec" restaure los archivos.
	14. Una vez termine de ejecutar el "Restore", saque el "tape' de la unidad y reinserte los "tapes" de la rotación semanal.
	15. Vuelva a ejecutar el paso número 10 de este procedimiento para que Veritas vuelva a reconocer los "tapes" de la rotación.
Oficial de Seguridad	16. Recibe el disco o la cinta del operador.
	17. Guarda la cinta o el disco en los anaqueles bajo llave localizados en la oficina antes del cuarto de computadoras.

II. POLITICA Y PROCEDIMIENTO 700: PETICIÓN DEL SERVICIO MEDIANTE EL "SYSTEM REQUEST"

1. PROPOSITO

Establecer los procesos a seguir para la requisición y aprobación de modificaciones o desarrollo de sistemas.

2. ALCANCE

Este procedimiento aplica a toda requisición de servicio recibida en el Área de Sistemas de Información.

3. FORMAS

Solicitud de Programación.

4. PROCEDIMIENTO

PERSONA RESPONSABLE	PASO	PROCESO
Usuario Programación para	1.	Prepara la Forma Solicitud de solicitar un cambio a un sistema o programa o desarrollar un sistema o programa nuevo.
	2.	Entrega la Forma Solicitud de Programación al (a la) supervisor(a) o director(a) del área para que éste apruebe el cambio o sistema solicitado.
Director(a) de Área de Sistemas de Información	3.	Recibe la **Forma Solicitud de Programación del usuario.**
	4.	Verifica que la solicitud concuerda con los cambios o especificaciones requeridas y discutidas de antemano.
	5.	Firma la **Forma Solicitud de Programación** y la envía al (a la) Director(a) del Área de Sistemas de Información.
Director(a) Área de Sistemas de	6.	Recibe la **Forma Solicitud de** Información **Programación** del (de la) supervisor(a) o director(a) de área.

7. Verifica que la hoja ha sido debidamente complementada y firmada.

8. Analiza las especificaciones requeridas y su validez.

9. Aprueba la solicitud y asigna a un (una) programador(a) o analista disponible para el desarrollo.

10. Si no aprueba la solicitud, se comunica con el (la) supervisor(a) o director(a) de área para discutir las razones por la decisión tomada.

11. Notifica al (a la) supervisor(a) o director(a) de área sobre la aprobación y el nombre del (de la) programador(a) o analista asignado(a).

12. Entrega la Forma Solicitud de Programación al (a la) programador(a) o analista asignado(a) para que éste comience la documentación.

Programador(a) o Analista

13. Recibe la **Forma Solicitud de Programación** del (de la) Director(a) de Sistemas de Información.

14. Analiza las especificaciones requeridas por el usuario. De haber alguna duda, se comunica inmediatamente con el usuario, el (la) supervisor(a) o director(a) de área.

15. De surgir algún cambio a la solicitud Original, esta debe ser escrito por parte del usuario y discutida con el director del Área de Sistemas de Información.

16. Comienza a programar según los Políticas y Procedimientos y políticas establecidas en el Manual de Políticas y Procedimientos del Área de Sistemas de Información.

IX. VIGENCIA:

Este Manual de Políticas y Procedimientos será efectivo el 15 de marzo de 2007.

Julia Torres Hernández,
Coordinadora General

ESTADO LIBRE ASOCIADO DE PUERTO RICO
OFICINA DEL COORDINADOR GENERAL
PARA EL FINANCIAMIENTO SOCIOECONOMICO Y LA AUTOGESTION

COMUNIDADES ESPECIALES PUERTO RICO

ÁREA DE SISTEMAS DE INFORMACIÓN
HOJA DE REQUISICIÓN DE CINTAS

FECHA:
DD/ MM / AAAA

NOMBRE: **POSICIÓN:**

CINTAS SOLICITADAS		
NÚM. CINTA	**PROPÓSITO**	**FECHA DEVUELTA**

FIRMA SOLICITANTE

A SER COMPLETADO POR EL OFICIAL DE SEGURIDAD

☐ **ENTREGADA** ☐ **NO ENTREGADA**

RAZÓN:

NOMBRE OFICIAL DE SEGURIDAD

FIRMA OFICIAL DE SEGURIDAD

FECHA ENTREGADA

FORMA OCEPR-SI-0002-2007

ESTADO LIBRE ASOCIADO DE PUERTO RICO
OFICINA PARA EL FINANCIAMIENTO SOCIOECONOMICO Y LA AUTOGESTION

COMUNIDADES ESPECIALES PUERTO RICO

ÁREA DE SISTEMAS DE INFORMACIÓN
HOJA DE OTORGAR ACCESO A LA RED

FECHA:
DD/ MM / AAAA

NOMBRE: **TELÉFONO: ( )- - EXT.:**

DIRECCIÓN FISICA: **ÁREA/OFICINA:**

ACCION A TOMAR		
☐ OTORGAR ACCESO	FECHA: DD/MM/AAAA	NOMBRE USUARIO:
☐ DESACTIVAR	FECHA: DD/MM/AAAA	UNIDAD ORGANIZACIONAL:

EQUIPO EN USO O A ASIGNAR	MARCA	NÚMERO DE SERIE	NÚMERO DE PROPIEDAD
TORRE ☐ LAPTOP ☐			
MONITOR			
BATERÍA			
OTRO:			

CONFIGURACIÓN	PROGRAMA
☐ CREAR CUENTA EN ACTIVE DIRECTORY O LOCAL	☐ ANTIVIRUS
☐ IP DINÁMICO (DHCP)	☐ OFFICE 2003
☐ REGISTRAR WINDOWS XP	☐ VNC
☐ INTEGRARLA AL DOMINIO	☐ ACROBAT READER 7
☐ COMPUTER NAME = (NUM. PROPIEDAD)	☐ WIN WP SP2
☐ CREAR MAPPING DRIVES	☐ OFFICE SP2
☐ INSTALAR IMPRESORAS	☐ WIN 2000 SP4
☐ CONFIGURAR EL OUTLOOK	☐ MICROSOFT DEFENDER
☐ DES-INSTALAR JUEGOS	☐ FIREWALL CLIENT NETWORK (ISA)
☐ ACCESO INTERNET	

NOMBRE DIRECTOR AREA/OFICINA: **FIRMA:**_____

ESTADO LIBRE ASOCIADO DE PUERTO RICO
COMUNIDADES ESPECIALES PUERTO RICO

ESTADO LIBRE ASOCIADO DE PUERTO RICO
OFICINA DEL COORDINADOR GENERAL
PARA EL FINANCIAMIENTO SOCIOECONOMICO Y LA AUTOGESTION

ÁREA DE SISTEMAS DE INFORMACIÓN
HOJA DE REQUISICIÓN DE DOCUMENTOS O PROGRAMAS

FECHA:
DD/ MM / AAAA

NOMBRE: **POSICIÓN:**

DOCUMENTOS / PROGRAMAS SOLICITADOS	
DOCUMENTO / PROGRAMA	PROPÓSITO SOLICITUD

FIRMA SOLICITANTE

A SER COMPLETADO POR EL OFICIAL DE SEGURIDAD

☐ ENTREGADO ☐ NO ENTREGADO

RAZÓN:

NOMBRE OFICIAL DE SEGURIDAD FIRMA OFICIAL DE SEGURIDAD

FECHA ENTREGADO

FORMA OCEPR-SI-0004-2007

ESTADO LIBRE ASOCIADO DE PUERTO RICO
OFICINA DEL COORDINADOR GENERAL
PARA EL FINANCIAMIENTO SOCIOECONOMICO Y LA AUTOGESTION

COMUNIDADES ESPECIALES PUERTO RICO

ÁREA DE RECURSOS HUMANOS
HOJA DE NOTIFICACIÓN

FECHA:
DD/ MM / AAAA

PERSONAL DADO DE ALTA O BAJA		
NOMBRE EMPLEADO	ALTA O BAJA	FECHA ACCIÓN

Nombre Director Área Recursos Humanos
o su Representante Autorizado

Firma Director Área Recursos Humanos
o su Representante Autorizado

A SER COMPLETADO POR EL ADMINISTRADOR DE SISTEMA

☐ DADO DE ALTA ☐ DADO DE BAJA FECHA:
DD/ MM / AAAA

RAZÓN:

NOMBRE ADMINISTRADOR DE SISTEMA

FIRMA ADMINISTRADOR DE SISTEMA

FECHA COMPLETADO PROCESO

FORMA OCEPR-SI-0005-2007