

3.5.2 Periferales y Otro Equipo

Los equipos periferales son unidades que están unidas externamente a los servidores a través de la red administrativa (LAN) de la JGS911.

Los siguientes periferales afectan directamente el servicio que ofrece el CSI al componente administrativo de la JGS911.

<u>Unidad</u>	<u>Área Afectada</u>
Impresoras	
HP Color Laser Jet Modelo 5500dtn Total: 6 Descripción: Impresión de los informes y cartas oficiales de la Agencia	Todas las áreas
HP LaserJet 4200 dtns B/W Total: 5 Descripción: Impresión de los informes y cartas oficiales de la Agencia	
OKI Microline 591 24 Pin Printer Total: 1 Descripción: Imprimir Reportes de Contabilidad	
Lexmark T630 Total: 2 Scanner, Impresora, Fotocopiadora Impresión de los informes, fotocopias y cartas oficiales de la Agencia	
Fax Sharp FO 5700 Total: 1	
Reloj Ponchador –Kronos (3) 1er piso, 2do piso y CRL	Recursos Humanos
Equipo Multifuncional Ricoh Aficio CL7000 Scanner, Impresora, Fotocopiadora Total: 1 Descripción: Impresión de los informes, fotocopias y cartas oficiales de la Agencia	Todas las áreas

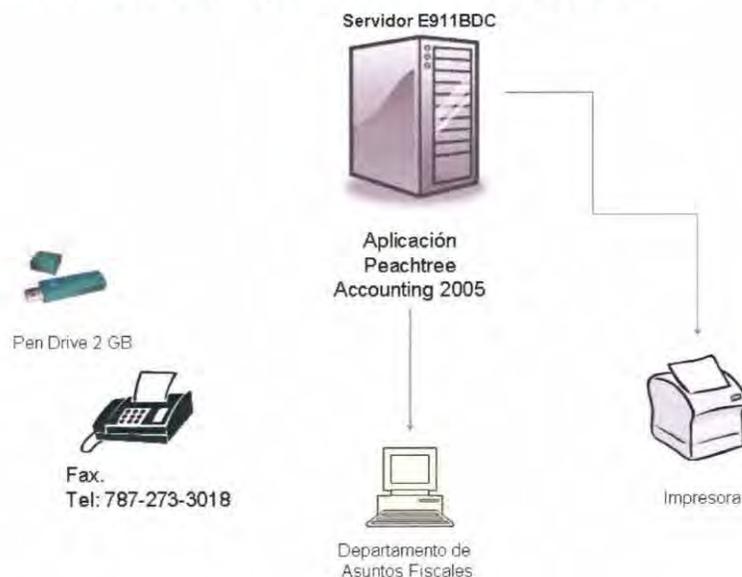
Si la falla del sistema computadorizado que apoya el componente administrativo se prolonga por mucho tiempo en un área específica, los usuarios de esta área se verán seriamente afectados. Un Plan de Contingencia se debe preparar para cada unidad crítica.

A continuación se presenta el Plan de Contingencia para las siguientes unidades críticas:

3.5.3 Plan de Contingencia para Equipo Periferal – Oficina de Asuntos Fiscales de la JGS911

La JGS911 tiene un contrato con la compañía Hewlett Packard para el mantenimiento de los servidores y el equipo periferal de la red de microcomputadoras que apoya el componente administrativo. Dicho contrato ofrece el servicio en las facilidades físicas de la JGS911 (on site) y su tiempo de respuesta a una llamada de servicio no es mayor de cuatro "4" horas para llamadas urgentes y no mas tarde del próximo día para servicios no urgentes.

Equipo Periferal que utiliza esta oficina:



Por otro lado la JGS911 mantiene contratados los servicios para la administración técnica de dicha red con la compañía ARJ Professional & Consulting Services Inc. Este contrato incluye los servicios de apoyo técnico a los usuarios de la red.

Procedimiento para solicitar servicios de reparación a equipo periferal

Handwritten signature in blue ink.

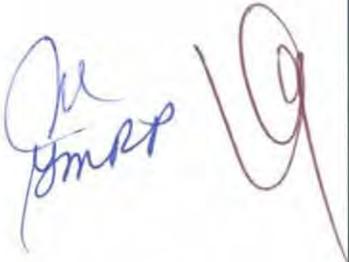
Handwritten signature in red ink.

<u>Responsable</u>	<u>Acción</u>
Director(a) de Servicios Técnicos y Administrativos	<ol style="list-style-type: none">1. Recibe comunicación del usuario informando sobre el equipo defectuoso.2. Comunica por e-mail o por teléfono al Administrador de la red la solicitud del servicio.
Administrador de la red	<ol style="list-style-type: none">3. Visita al usuario para corroborar el problema reportado y tratar de resolverlo.<ol style="list-style-type: none">a) Si lo resuelve registra el caso como completado.b) Si el equipo periferal requiere reparación procede a crear un "ticket" con la compañía Hewlett Packard.
Compañía Hewlett Packard	<ol style="list-style-type: none">4. Visita al usuario para corroborar el problema y reparar el equipo.

Handwritten signature in blue ink.

Handwritten signature in red ink.

	<p>a) Si tiene la(s) pieza repara el equipo y registra el servicio como completado.</p> <p>b) Si no tiene la(s) pieza informa al administrador de la red y mantiene el caso abierto.</p>	
Administrador de la red	5. Informa a la directora (a) de Servicios Técnicos y Administrativos que el problema no se pudo resolver.	
Director (a) de Servicios Técnicos y Administrativos	6. Comunica por e-mail, por teléfono o personalmente al Director de la Oficina de Asuntos Fiscales que el problema no se pudo resolver y pregunta si se puede esperar por el recibo de la(s) pieza o se requiere informar al Coordinador de Emergencias para activar el "Contingency Site".	a) Si se puede esperar por la(s) pieza(s) se informa al Administrador de la red y el caso se mantiene abierto.



	b) Si no se puede esperar se informa al Coordinador de Emergencias para que se active el "Contingency Site".
Coordinar de Emergencias	7. Activa los Comités de Emergencias conforme a los procedimientos establecidos en la Sección 1 de este Plan de Contingencia. 8. Informa a la dirección ejecutiva de la JGS911 que el "Contingency Site" está activado para atender la emergencia.

3.6 Fallas en Los Programas "Software Failures"

El sistema operativo y otros programas que se ejecutan en la red administrativa de la JGS911 son mantenidos primordialmente por los ingenieros de la(s) compañía(s) que manufacturan los productos. Los suplidores del sistema operativo y otros programas instalados en la red son:

<u>Producto</u>	<u>Suplidor</u>	<u>Contacto</u>	<u>Número Telefónico</u>
Exchange 2003	Microsoft/ARJ, Inc./OGP	ARJ, Inc. Sr. Juan González	787-635-7417 787-977-9200 ext.4211,4286



Mail Secure for Exchange	Microsoft/ARJ, Inc./OGP	ARJ, Inc. Sr. Juan González	787-635-7417 787-977-9200 ext.4211,4286
WorkForce (Time and Attendance) Version 4.3	Interboro	ISC Servicio	787-641-7800
WUS "Windows Update Services" 2005	ARJ, Inc.	ARJ, Inc.	787-635-7417
Ghost Symantec	ARJ, Inc./OGP	ARJ, Inc. Sr. Juan González	787-635-7417 787-977-9200 ext.4211,4286
Websense Version 6.2	ARJ, Inc.	TechQuest	
Veritas Backup Version 9.1	ARJ, Inc.	ARJ, Inc.	787-635-7417
Data Peachtree	ARJ, Inc.	ARJ, Inc.	787-635-7417
ISA 2004	ARJ, Inc./OGP	ARJ, Inc. Sr. Juan González	787-635-7417 787-977-9200 ext.4211,4286

La implantación de los cambios provistos por el manufacturero para el sistema operativo y otros productos de Microsoft se instalan automáticamente a través del servicio WUS de Microsoft. En el caso de otras aplicaciones los cambios son instalados por técnicos de la(s) compañía(s) que representan el producto en Puerto Rico. Todos estos cambios se coordinan a través del director(a) de Servicios Técnicos y Administrativos y el Administrador de la Red. Sin la presencia de estos funcionarios ninguna persona puede acceder a la red para realizar algún tipo de instalación o actualización. Si un cambio causa una falla mayor

o afecta seriamente el servicio del CSI, el administrador de la red podrá corregir los mismos ya sea aplicando una solución provista por el manufacturero o restaurando las aplicaciones del sistema a la versión anterior que está sin los cambios. Si esto no fuese posible el director(a) de Servicios Técnicos y Administrativos debe informar al Coordinador de Emergencias para que se active el plan de contingencia conforme a lo establecido en la Sección 1 de este plan.

3.7 Fallas De Las Aplicaciones "Applications Failures"

Varias de nuestras aplicaciones son preprogramados comprados a suplidores externos y tienen servicio de mantenimiento por estas compañías. Algunas son desarrolladas por los usuarios quienes son capaces de darle mantenimiento.

Los suplidores que dan apoyo a los sistemas preprogramados son:

<u>Producto</u>	<u>Suplidor</u>	<u>Contacto</u>	<u>Número Telefónico</u>
Peachtree	ARJ, Inc.	ARJ, Inc.	787-635-7417
MS Office	Microsoft	ARJ, Inc.	787-635-7417
Veritas	ARJ, Inc.	ARJ, Inc.	787-635-7417
WorkForce (Time and Attendance) Version 4.3	Interboro	ISC Servicio	787-641-7800

La programación de aplicaciones es muy similar a la programación del sistema en cuanto a posibles fallas de las versiones nuevas de los programas. Los procedimientos para el control de cambios proveen herramientas para hacer pruebas adecuadas antes de realizar los

OK Group



cambios en forma permanente y eliminar los cambios si se detecta algún problema en los mismos.

Sin embargo, un tipo serio de falla en las aplicaciones es uno donde, a causa de un error de un programa, un usuario u otros obtienen datos incorrectos al grado que las consecuencias para la JGS911 son serias.

En este caso, el personal a cargo de dar apoyo a la aplicación, debe determinar el método a seguir para corregir los datos erróneos. Los resguardos en cinta magnética de los archivos pueden ser o no útiles dependiendo de la cantidad del tiempo transcurrido entre la generación del resguardo y el tiempo en que el error de los datos proliferó. En un caso serio, una programación especial podría requerirse para reparar los datos. En el peor de los casos, las transacciones originales deben ser re-entradas para reconstruir los archivos, después de corregir los programas y eliminar los datos erróneos.

3.8 Desastres Mayores

Un desastre mayor es uno que requiere una activación del "Contingency Site" debido a la incapacidad de operar los sistemas en el CSI por un largo periodo de tiempo. Las razones pueden variar desde una destrucción del Centro de Sistemas de Información o una emergencia menos severa que afecte las operaciones de los servidores y deje intacto el Centro de Sistemas de Información. Refiérase a la Sección 6 para información sobre el tema de Desastres Mayores.

Sección 4 Políticas para Reducir Riesgos

4.1 Protección de la Información disponible en la Red Administrativa

La información almacenada en los servidores de la red administrativa está protegida por una combinación de procedimientos de resguardo y de procedimientos de almacenamiento fuera de las facilidades físicas del CSI de la JGS911. En los resguardos se copia la información del disco a un medio magnético (1/2" cartridges tape – imitation Super DLT Save I – 320 gigabytes comprimido, 160 gigabytes sin comprimir) para que se pueda restaurar la información en caso de que se pierda. El Lugar de Resguardo (Backup Site) protege la información en caso de que los servidores se destruyan por causa de un desastre en el CSI.

Ninguna empresa puede recuperarse de un desastre si sus datos vitales son destruidos y no se mantiene una copia de resguardo en otra localización.

4.1.1 Procedimiento para Resguardo

El procedimiento para hacer una copia de resguardo de los sistemas que se ejecutan en la red administrativa es el siguiente:

- Diariamente se realiza un resguardo de todos los archivos que fueron actualizados durante el día.
- Se resguarda todo el sistema a diario, semanalmente, mensualmente y a fin de año natural.
- Los resguardos diarios se mantienen hasta por tres semanas en el robot modelo HP Storage Work MSL 5000 en el CSI.

Para más información sobre como realizar resguardo de los datos, refiérase al Procedimiento para hacer Copias de Resguardo (Backups) de Todos los Sistemas que se incluye como Anejo D.1 en este plan.

4.1.2 Procedimiento para Almacenar una Copia de Resguardo

Las cintas con copias del resguardo se guardan dentro y fuera de la JGS911. El almacenamiento dentro de la JGS911 consiste de una caja fuerte a prueba de fuego ubicada en la oficina del Sr. Caleb Cedeño ubicada en el Centro de Recepción de Llamadas en el primer piso del edificio. El almacenamiento externo se realiza en las facilidades físicas de "International Safe Deposit". En el Anejo D.2 se detallan en su totalidad las facilidades del "Backup Site" (nombre, localización, etc.).

El procedimiento para almacenar una copia de resguardo en el "International Safe Deposit" (Procedimiento para el Movimiento de Medios Magnéticos del (CSI) a la Bóveda ubicada en las Facilidades Físicas de International Safe Deposit) se incluye como Anejo D.3 en este plan.

4.1.3 Procedimiento de Restauración de Copia de Resguardo

Cualquiera de las personas autorizadas a visitar las facilidades de "International Safe Deposit" puede recoger copias de resguardo de dicho lugar. Las personas autorizadas son las siguientes:

<u>Nombre</u>	<u>Posición</u>
Sr. Caleb Cedeño	Técnico de Grabaciones y Audiovisuales
Sr. Tomas Ortiz	Ayudante Especial I

El Procedimiento para realizar una restauración a los sistemas que se ejecutan en la red administrativa se incluye en este plan como Anejo D.4.

Handwritten signature in blue ink.

Handwritten signature in red ink.

4.2 Protección de la operación del Centro de Sistemas de Información

4.2.1 Seguridad Física

El acceso al Centro de Sistemas de Información es controlado de la siguiente manera:



Detector de Tarjeta

Las puertas de entrada al CSI solo abren por medio de tarjetas de control de acceso electrónico. Las claves para el control de acceso al CSI y un registro del personal que accede a estas facilidades se mantienen en un sistema de control de acceso que administra el encargado de la seguridad de la JGS911.



Tarjeta de Control de Acceso

Los empleados del Centro entran a sus unidades de trabajo utilizando la clave numérica, la cual es provista por el Encargado de la Seguridad de la JGS911.

El CSI dispone de un sistema eléctrico que permite abrir sus puertas desde el interior de sus facilidades físicas al oprimir un botón. Esta opción se utiliza para permitir entrada y salida de visitantes y personal no autorizado al CSI. El personal del CSI mantiene además un registro de entrada y salida de los visitantes.



Botón de Salida de Emergencia

El riesgo de incendio en el CSI se reduce con:

- Un sistema de detección de incendios FM200
- Extintores de incendio colocados en lugares accesibles dentro del CSI. Véase páginas 3 a la 5 de la sección 3 de este plan.

Al ymep

[Handwritten scribble]

- Normas de **NO FUMAR** dentro de las facilidades del edificio.

El riesgo de daños causados por roturas en la tubería de agua o inundaciones se reduce mediante:

- La ausencia de tuberías de agua en el techo y en el piso del CSI.

El riesgo de daños de un componente eléctrico debido al alto voltaje, bajo voltaje y fluctuaciones eléctricas se reduce con:

- Sistema ininterrumpible de energía eléctrica (UPS Liehbert de 80 KVA.) con dos bancos de baterías para proteger la infraestructura de equipo que apoya la red administrativa en el CSI.



El riesgo de interrupciones al servicio causadas por fallas en suministro de la energía eléctrica comercial, se reduce con:

- Unidad Ininterrumpible de Energía (UPS) con una duración de al menos tres (3) para el equipo ubicado en el CSI.
- Planta de energía eléctrica (SDMO) de 500KV (Vease página 13 de la sección 3)

4.2.2 Seguridad de Acceso a los Servidores que dan apoyo a la Red Administrativa

El acceso a la información contenida en los servidores que dan apoyo a la red administrativa se controla mediante el uso de un procedimiento de cuentas (User name), contraseñas y restricciones de acceso a la información que controla el Director(a) de Servicios Técnicos y Administrativos de la JGS911.

Al ymas

[Handwritten signature]

El acceso a una computadora (PC) lo controla el "User name" del usuario y la contraseña (**password**) secreta que tiene asignada cada uno de los usuarios de la red. El **username** sirve para identificar el usuario a la computadora. El **password** es el código que permite verificar los derechos que puede tener un usuario. Dichos derechos son asignados según las tareas que desempeña el usuario. Solamente la persona que conozca esta contraseña podrá registrarse en el sistema.

Todo usuario del sistema debe mantener en secreto su "password". Cada 180 días todo usuario debe cambiar sus códigos de seguridad. El "software" no permite utilizar el mismo "password", ni los anteriores 5 utilizados por el usuario por restricciones de seguridad. El sistema tiene como mínimo 8 caracteres.

4.2.3 Seguridad del personal Técnico que trabaja en el CSI.

Los siguientes procedimientos proveen seguridad al personal técnico que trabaja en el CSI. :

- Diariamente el personal técnico que comienza a trabajar, debe firmar el Registro de Acceso y proceder a realizar una inspección visual de las facilidades físicas del CSI para determinar si todo está en orden. De existir algo anormal debe proceder a corregirlo, si le es posible, o informarlo inmediatamente al encargado de la seguridad y a la gerencia de la JGS911.
- El personal técnico debe conocer la localización de linternas de baterías. Estas deben estar en lugares accesibles para el caso de que falte la energía eléctrica.

- El personal técnico debe mantener, en todo momento, una lista de números telefónicos de emergencia, un equipo de primeros auxilios y los procedimientos de emergencias.

4.3 Protección de los Records Vitales

Muchos documentos y records magnéticos son vitales para la operación de la JGS911. Algunos procedimientos específicos son implementados para proteger los records vitales, como por ejemplo la entrada del registro de asistencia, los programas de las aplicaciones, las licencias de los programas etc.

Los records vitales que la agencia debe proteger son:

- Mantener registro de los acuerdos de la Junta de Gobierno del Servicio 911.
- Mantener el registro de los casos del Comité de Conciliación bajo el convenio colectivo de la agencia.
- Registro de Asistencia electrónico
- Roster de empleados
 - Expediente Oficial del Empleado
 - Notificación de Nombramiento y Juramento, irregular, transitorio, regular o de confianza.
 - Informes de Cambio Especial.
 - Informe de Cambio.
 - Medidas disciplinarias.
 - Declaración Individual.
 - Licencias de los programas que se utilizan en la red administrativa.
 - Manuales de Procedimientos y Normas Administrativas

Los procedimientos para proteger los records son los siguientes:

- El acceso a los medios magnéticos almacenados en el CSI es controlado por los sistemas de control de acceso al CSI y la



seguridad implantada para acceder a los sistemas por medio de un (User Name) y una contraseña (Password).

Diariamente se realiza un resguardo de todos los archivos que fueron actualizados durante el día en la unidad de almacenamiento HP modelo Storage Work MSL5000 que a su vez tiene una contraseña para permitir el acceso a las cintas de resguardos. En esta unidad se mantiene el resguardo diario hasta por tres semanas.

Semanalmente se almacena en una bóveda a prueba de fuego una copia del resguardo semanal.

Mensualmente se almacena en "International Safe Deposit" una copia del resguardo mensual de los records.

- Se resguarda todo el sistema semanalmente, mensualmente y a fin de año natural.

Para mas información sobre como proteger los records vitales refiérase a los siguientes procedimientos que se incluyen en los Anejo D.3 y D.5 de este plan.

- Procedimiento para el movimiento de Medios de la JGS911 a la Bóveda ubicada en las facilidades físicas de International Safe Deposit.
- Procedimiento para el Control y Custodia de Medios Magnéticos.

4.4 Resguardo de Datos, Equipo, Suministros y Documentación

Toda la información y materiales que han sido identificados como críticos para la recuperación de un desastre se deben guardar en el "Contingency Site" externo al CSI. La localización del "Contingency Site" externo al CSI está identificada en el Anejo D.6

Las copias almacenadas en el "Contingency Site" incluyen:

- Infraestructura de equipo y programación necesaria. (PC, Laptop, sistema operativo, programas de aplicación etc.).

Handwritten signature and initials in blue and red ink.

- Partes críticas de equipo que pudieran dañarse durante el periodo de emergencia.
- Datos necesarios para restaurar los servicios críticos.
- Materiales importantes para ejecutar las operaciones críticas.

Datos y Programas

Todos los datos residentes en la computadora(s), incluyendo los programas de aplicaciones y programas del sistema se resguardan diariamente y semanalmente. El Director(a) de Servicios Técnicos y Administrativos es responsable de cumplir con los procedimientos de resguardo. Las "cartridges" y las aplicaciones consideradas como críticas se deben almacenar periódicamente en el "Contingency Site" externo al CSI.

Equipo

En la sección 5 se describe el "Contingency Site". La planificación de contingencia con relación a periferales especiales y equipo de telecomunicaciones está descrita en la Sección 3. El Director(a) de Servicios Técnicos y Auxiliares es responsable porque se sigan todas las políticas para el resguardo del equipo.

La información relacionada al equipo de repuesto que debe ser mantenido fuera de la JGS911 se incluirá en este Plan tan pronto la JGS911 seleccione el "Contingency Site".

Suministros

Suministros críticos, incluyendo formas especiales y artículos para el Centro de Control de Emergencia (equipo de primeros auxilios), se deben almacenar en el "Contingency Site" seleccionado por la JGS911. El Director(a) de Servicios Técnicos y Auxiliares es responsable de resguardar fuera de la JGS911 los suministros para las operaciones. El Coordinador Alterno de Emergencias es responsable de resguardar los suministros del Centro de Control de Emergencias.

*De
ymrp*



Deben existir suficientes suministros almacenados fuera del CSI como mecanismo de protección contra desastres en el "Contingency Site" primario. De requerirse activar el Plan de Contingencia en el "Contingency Site" que seleccione la JGS911, deben existir suficientes materiales para continuar la operación hasta que se puedan conseguir más materiales de los suplidores.

Las formas y suministros críticos y las cantidades a ser almacenadas en el "Contingency Site" se incluirán en este Plan tan pronto como la JGS911 provea dicha información.

Los procedimientos para el mantenimiento del inventario de los suministros es el siguiente:

- El Director(a) de Servicios Técnicos y Auxiliares es responsable de mantener la cantidad necesaria de suministros en el "Contingency Site" externo. Si se utiliza parte de los suministros, el Director(a) de Servicios Técnicos y Auxiliares debe reemplazarlos inmediatamente.
- Anualmente el Director(a) de Servicios Técnicos y Auxiliares debe realizar un conteo físico del inventario de suministros en resguardo.

Documentación

La documentación crítica para asistir en la recuperación en el evento de un desastre se debe resguardar fuera de la JGS911. Copias de la siguiente documentación debe ser mantenida en un "Contingency Site" externo:

<u>Nombre Del Documento</u>	<u>Copias</u>	<u>Personal Responsable</u>
Plan de Recuperación de Desastre	10	Coordinador Alterno de Emergencias

Handwritten signature

Handwritten scribble

Documentación de Operaciones (Documentación de Equipo, etc.)	2	Director(a) de Servicios Técnicos y Administrativos
Manual de Procedimientos	2	Director(a) de Servicios Técnicos y Administrativos

del manual

4.5 Seguros

A continuación se presentan las cubiertas de seguro que guardan relación con la operación de procesamiento de datos.

Seguro de Propiedad

Planta Física

Compañía Aseguradora	MAPFRE
Compañía con la que se Tramitó el seguro	Sr. Edwin I. Rivera Malavé Productor Designado por Hacienda
Número Telefónico	787-273-1808
Fecha de Vencimiento	Julio 07 2008

Cubiertas de seguro relacionadas con el área de equipo y programación. Refiérase al Anejo D.7.

Sección 5 Descripción del "Contingency Site"

5.1 Localización y Contactos:

- Nombre del lugar seleccionado:
- Localización:
- Números Telefónicos:
- Números Telefónicos de Emergencias (Si son diferentes):
- Nombre de las personas contactos:

5.2 Naturaleza Del Acuerdo:

- Naturaleza general del acuerdo, características del lugar para activar el plan de contingencia.

5.3 Configuración de Máquinas y Facilidades

5.3.1 Configuración del equipo ubicado en el "Contingency Site"

5.3.1.1 Equipo

5.3.1.2 Periferales

5.3.1.3 Unidad de Resguardo

5.3.1.4 Impresoras

- Impresoras modelo _____ conectadas al sistema.

5.3.2 Programación del Sistema

5.3.2.1 Sistemas Operativos

*Al
Ymas*

5.3.2.2 Preprogramados o Productos:

<u>Versión</u>	<u>Descripción</u>	<u>Suplidor</u>
----------------	--------------------	-----------------

5.3.3 Facilidades de Telecomunicación**5.3.3.1 Equipo de Telecomunicación**

<u>Equipo</u>	<u>Cantidad</u>	<u>Model</u>
---------------	-----------------	--------------

5.3.4 Facilidades del CSI del "Contingency Site"**5.3.4.1 Aire Acondicionado**

<u>Cantidad</u>	<u>Modelo</u>	<u>Características</u>
-----------------	---------------	------------------------

5.3.4.2 Protección contra fuego**5.3.4.3 Área de Operaciones****5.3.4.4 Otras Facilidades****5.4 Facilidades para acomodar los Comités de Acción de Emergencias****5.4.1 Comité de trabajo de apoyo técnico:**

<u>Posiciones para el Comité de Trabajo</u>	<u>Cantidad</u>
---	-----------------

Modelo de computadoras (PC)

Teléfonos Disponibles:

Líneas para transmisión de voz:

*Ad
Group*

Manuales Técnicos Disponibles:

La cantidad de copias de Manuales Técnicos se distribuye de la siguiente manera:

- Diez (10) copias del Plan de Recuperación de Desastres
- Dos (2) copias de la Documentación de Operaciones (Doc. del equipo, etc.)
- Dos (2) copias del Manual de Operaciones
- Dos (2) copias del Manual de Procedimientos

5.4.2 Características de Seguridad:

5.5 Consideraciones Sobre Itinerarios

5.5.1 Itinerario para realizar pruebas

5.5.2 Restricciones al itinerario de Pruebas

5.5.3 Horas en que los sistemas estarán operando en el "Contingency Site"

*Al
ymp*

Sección 6 Procedimientos para la Restauración en Caso de un Desastre Mayor

Los siguientes Planes de Contingencia, se utilizarán en caso de que ocurra un desastre de gran magnitud en el Centro de Sistemas de Información (CSI). Esto significa que ocurra una pérdida de información del sistema, de tal manera que requiera que se actúe de inmediato para mover todas las operaciones a un Lugar de Contingencia, ("Contingency Site").

6.1 Los Comités de Acción de Emergencias y sus Responsabilidades

Los siguientes Comités de Acción de Emergencias han sido diseñados para utilizarse, en caso de una emergencia en que ocurra un desastre mayor. El propósito, las responsabilidades y los miembros que componen estos comités se describirán mas adelante. El Coordinador de Emergencias o el Comité de Planificación, dependiendo el tipo de emergencia, son los encargados de activar los distintos Comités de Acción de Emergencias. Los comités a su vez deben informar al Coordinador de Emergencias o al Coordinador Externo, según sea el caso. Los Comités de Acción de Emergencias son varios, a saber: Operaciones, Aplicaciones, Equipo Computadorizado, Facilidades Físicas y Ambiente, y Administrativo. El uso de los Comités de Acción de Emergencias y las responsabilidades generales de los líderes se discuten en la sección 1.6. Los líderes y miembros designados de los Comités de Acción de Emergencias son identificados en el Anejo A.3.

*Al
y
m...*



6.1.1 Comité de Operaciones

Propósito

El propósito del Comité de Operaciones es lograr el restablecimiento de los servicios del Centro de Sistemas de Información, en caso de un desastre. Hacia este fin deben asegurar que se restaure y se continúe con el itinerario de procesamiento en el "Backup Site" designado por el Plan de Contingencia, hasta que las operaciones vuelvan a su normalidad en el Centro de Sistemas de Información de la JGS911 o en unas nuevas facilidades físicas.

Responsabilidades

1. Periódicamente revisar y evaluar, que los procedimientos para los resguardos, almacenamiento de datos fuera de la JGS911 y procesos para la restauración estén en forma apropiada y completa. Corroborar que los resguardos incluyan los programas, datos y documentación necesaria en las operaciones del CSI.
2. En caso de un desastre, buscar en "International Safe Deposit" la copia más reciente de resguardo, incluyendo cartuchos magnéticos, materiales y documentación.
3. Participar en la iniciación de las operaciones en el "Backup Site" y mantenerse activo durante las operaciones de contingencia. Mantener comunicación con los otros comités para conocer sobre los niveles de servicio y las dificultades confrontadas durante el período de contingencia. Reunirse con los usuarios para preparar un itinerario revisado de procesamiento, a la luz de la emergencia y mantener informado al Coordinador de Emergencias sobre el estado o condición de los trabajos.

*Q
ympp*



4. Coordinar con los usuarios sobre cómo suministrar las requisiciones de tareas durante la emergencia y sobre la distribución de los resultados.
5. Si las operaciones del Plan de Contingencia continúan por un período de tiempo largo, asegurar que los balances de los materiales necesarios para las operaciones sean adecuados y se mantengan durante las operaciones del Plan de Contingencia.

Miembros del Comité

- Ing. Gladys M. Rodríguez Pérez
- Caleb Cedeño Ruiz
- Carmen Santiago Cruz
- Consultores

6.1.2 Comité de Aplicaciones

Propósito

El propósito del Comité de Aplicaciones es asegurar el funcionamiento apropiado de las aplicaciones que administra el Centro de Sistemas de Información durante el período de emergencia. Para ello coordina con los usuarios acerca de cómo las operaciones deben ser realizadas durante el período de contingencia.

Responsabilidades

1. El Comité de Aplicaciones debe participar en la preparación y las pruebas del Plan de Contingencia. Si se identifican problemas con relación a una aplicación, el Comité de Aplicaciones debe preparar y documentar soluciones para los mismos. La documentación de las aplicaciones y los Planes de Contingencia deben ser almacenados en el "Backup Site" fuera de la Junta.

ymar



2. En caso de un desastre este comité es responsable de localizar la documentación de las aplicaciones y los Planes de Contingencia para la restauración de las operaciones.
3. Coordinar con los usuarios para determinar el trabajo que se estaba realizando al momento del desastre. Cuando las operaciones se hayan restaurado en el "Backup Site", el Comité de Aplicaciones debe entonces ayudar a recuperar cualquier trabajo que haya estado en ejecución y se haya perdido durante la emergencia.
4. Una vez el trabajo haya sido recuperado, coordinar con los usuarios sobre cualquier tipo de cambio que sea necesario realizar para interactuar con sus aplicaciones y proveer apoyo a los usuarios.

Miembros del Comité

- Ing. Gladys M. Rodríguez Pérez
- Cristino Morán Serrano
- Judith Encarnación Figueroa
- Luis Flores Valle
- Caleb Cedeño Ruiz
- Consultores

6.1.3 Comité de Equipo Computadorizado

Propósito

El Comité de Equipo Computadorizado es responsable de la reparación o reemplazo del equipo de computadoras, de su instalación y prueba, y de toda la planificación relacionada a la contingencia del equipo.

Nota: La reparación del equipo se llevará a cabo en el lugar original en donde está ubicado el equipo, en el lugar especificado para reemplazar el equipo o en un lugar designado por los Planes de Contingencia. A menos que se

Handwritten signature in blue ink.

Handwritten signature in red ink.

haya establecido un comité aparte, entonces el Comité de Equipo Computadorizado sería también responsable de las telecomunicaciones.

Responsabilidad

1. Participa en la evaluación y selección del lugar a seleccionar para casos de contingencias, también participa en las pruebas y en todos los asuntos relacionados con la planificación de equipo para el Plan de Contingencia.
2. En el evento de un desastre, evalúa la magnitud del daño, las fallas del equipo y las telecomunicaciones.
3. Coordina con los suplidores, en caso de ser necesario hacer un reemplazo de piezas o reparación al equipo. Coordinar acuerdos para adelantar la entrega de equipo de manera que no se afecten por mucho tiempo las facilidades de telecomunicaciones o equipo de computadora.
4. Coordina con los departamentos de Administración, Seguros y otros; asuntos relacionados con resguardo de equipo, reclamaciones de seguros y el financiamiento para el equipo que se reemplazará.
5. Instalar y probar todo el equipo reemplazado y/o nuevo, y las líneas de datos. Supervisa para resolver cualquier problema o falla que surja.

Miembros del Comité

- Ing. Gladys M. Rodríguez Pérez
- Caleb Cedeño Ruiz
- Consultores

6.1.4 Comité de Facilidades Físicas y Ambiente

Propósito

El propósito del Comité de Facilidades Físicas y Ambiente es el de restaurar o reemplazar el Centro de Sistemas de Información de

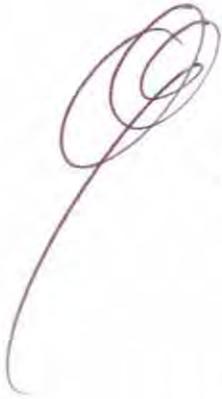


la JGS911 y otras facilidades de procesamiento de datos que hayan pasado por un desastre.

Responsabilidades

1. Mantener documentadas las configuraciones actuales de las facilidades físicas y de ambiente del Centro de Sistemas de Información ya sea, como un anejo para el Plan o como parte de apoyo a la documentación también resguardada en un lugar fuera de la Junta. Las configuraciones deben incluir plano del espacio provisto, lista de todas las facilidades, tal como el aire acondicionado, la distribución de energía eléctrica, "power conditioning", etc. También incluir las especificaciones de los números de los modelos, las capacidades y los requerimientos eléctricos.
2. En el evento de un desastre, investigar y estimar los daños y la restauración de las facilidades. Si la facilidad se puede utilizar, proceder a organizar las reparaciones inmediatamente.
3. Si las facilidades de procesamiento de datos son destruidas y no se pueden utilizar, proceder a localizar un reemplazo para dichas facilidades y asegurar que las mismas se puedan utilizar por un período de tiempo suficientemente razonable, en el caso de que no se conviertan en permanentes. Este comité debe tener presente que las facilidades no incluyen como requisito único los pies cuadrados que ocupa un edificio, sino también, la cabling, el piso falso, el aire acondicionado y la energía eléctrica para poder funcionar.
4. Coordinar con los proveedores de las facilidades para proveer lo que se necesite de emergencia como el equipo, la

*Al
y mmp*



instalación y los permisos. Se debe, en lo posible, negociar los Planes de Contingencia por adelantado.

5. Coordinar con los departamentos de Compras, Finanzas, Seguros, Legal y otros, los acuerdos para la compra de nuevo equipo, contratación de espacio y "buildout", reclamos de seguro y el financiamiento de nuevas facilidades.

Miembros del Comité

- Ing. Gladys M. Rodríguez Pérez
- Neysha I. Figueroa Rios
- Luis Flores Valle
- José L. Belmont Santaliz
- Consultores

6.1.5 Comité Administrativo

Propósito

El Comité Administrativo es responsable de todas las actividades durante el proceso de restauración en caso de un desastre, que no sean manejados por otros Comités de Acción de Emergencias. Estas actividades podrían incluir arreglos de transportación, adelanto de gastos, viajes y otras funciones administrativas.

Responsabilidades

1. Desarrollo y revisión de los procedimientos administrativos del Plan.
2. Participar en las pruebas del Plan con el propósito de realizar efectivamente las funciones administrativas necesarias y evaluar los procedimientos y otros requerimientos.
3. Dirigir y supervisar todas las actividades administrativas para transportación, hospedaje, viaje, adelanto de gastos,

etc. y llevar la contabilidad de cada subsidiario. Realizar contratos y aprobaciones administrativas, así como otras tareas relacionadas con otros departamentos.

4. Realizar funciones administrativas y clericales cuando sean necesarias durante la restauración en un desastre.

Miembros del Comité

- Yolanda Cruz Vázquez
- Cristino Morán Serrano
- Judith Encarnación Figueroa
- Luis Flores Valle
- Ing. Gladys M. Rodríguez Pérez
- Caleb Cedeño Ruiz
- Carmen Santiago Cruz
- Consultores

6.2 Notificación a los Miembros del Comité de Planificación

Un aspecto crítico de la restauración en un desastre es la reacción rápida del Comité de Planificación. Esto requiere de una notificación inmediata al personal apropiado, para que así el Plan de restauración en caso de desastre pueda ser iniciado tan pronto sea posible.

El Coordinador de Emergencias debe establecer y mantener una Lista de Notificación de Emergencia (ver el Anejo A.2) y asegurar que todo el personal clave la tenga disponible junto con los teléfonos de las siguientes organizaciones de emergencia: Administración del edificio (Arrivea Inc.), el Departamento de Bomberos y el Departamento de la Policía. En caso de un desastre, se seguirá el procedimiento de notificación que aquí se presenta a continuación:

Guías

1. Si un desastre ocurre mientras el CSI está operando, se debe iniciar el proceso de notificación tan pronto sea posible. Al personal del CSI se le requerirá memorizar los números de teléfono de emergencia del Departamento de la Policía,

Handwritten signature

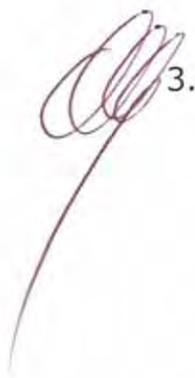
Handwritten signature

Departamento de Bomberos y del Área de Administración del Edificio Arrivea, Inc.. Si el personal del CSI no está realizando sus deberes, el guardia de seguridad del edificio debe iniciar la notificación del desastre siguiendo los procedimientos apropiados.

2. El Coordinador de Emergencias figura como el primero de la Lista de Notificación, con todos los posibles números de teléfonos donde se puede localizar en caso de que no esté en su trabajo o en su hogar. Si al Coordinador de Emergencias no se le ha podido contactar, el Coordinador de Emergencias Alterno u otras personas autorizadas se deben llamar hasta que un miembro del Comité de Planificación sea notificado.
3. El primer miembro notificado del Comité de Planificación es responsable de notificar al resto de los miembros del comité e iniciar la acción. La acción inicial será reunir el equipo de los miembros del Comité de Planificación en el Centro de Sistemas de Información o en el lugar de ubicación del Centro de Control de Emergencia en la JGS911 o en un lugar externo. (Backup meeting)

Nota: Recuerde, que el tiempo es determinante, en una situación por causa de un desastre.

*Al
Ymmp*



6.3 Procedimientos Iniciales del Comité de Planificación

Una vez el Comité de Planificación ha sido notificado, ellos deben proceder a realizar de inmediato una investigación de la situación e iniciar conforme al Plan, las acciones pertinentes.

Guías

1. El primer miembro del Comité de Planificación que fue notificado es responsable de notificar a los otros miembros del Comité de Planificación e iniciar la acción. La acción inicial debe ser reunir al comité en el Centro de Sistemas de Información o en las facilidades seleccionadas por la JGS911 para ubicar el Centro de Control de Emergencia.
2. Si el Coordinador de Emergencias, todavía no ha sido contactado, el sustituto a éste o las personas autorizadas que están listadas luego del Coordinador de Emergencias, asumirán la responsabilidad completa del Coordinador de Emergencias, hasta que él o ella llegue y sea completamente informado. El Coordinador de Emergencias o la persona autorizada, procederá a implementar los Planes de Contingencia.
3. En primer lugar debe realizar una investigación de la situación directamente en la escena de los hechos, si es posible. Si no, debe basar su investigación en la información suministrada por las diferentes fuentes de los hechos.
4. Basado en la investigación de la situación el Comité de Planificación, debe determinar la severidad del problema y decidir la acción a tomar.
5. Si el Comité de Planificación juzga la emergencia como un gran desastre, procede de la siguiente forma:
 - a. Activa el Centro de Control de Emergencias
 - b. Notifica a los Comités de Acción de Emergencias

Al
ymat

- c. Notifica a la Alta Gerencia
 - d. Notifica a Internacional Safe Deposit ("Backup Site" de medios magnéticos) fuera de la JGS911.
 - e. Notifica al lugar de contingencia seleccionado por la JGS911
- Estos pasos constituyen la activación de los Planes de Contingencia para un desastre mayor. Otros procedimientos para la ejecución de estas tareas se proveen en las siguientes páginas.
6. Si la emergencia no es considerada como un desastre mayor el comité debe implementar los Planes de Contingencia apropiados para la emergencia. En estos casos deben ser notificados los Comités de Acción de Emergencias pertinentes para que tomen la acción correspondiente.

De ymap



Nota: Recuerde, que el tiempo es determinante, en una situación en la que se deba restaurar por causa de desastre.

6.4 Activación del Centro de Control de Emergencias

En el evento de un desastre mayor la JGS911 debe establecer, un Centro de Control de Emergencias centralizado, a través del cual todas las comunicaciones y actividades pueden ser dirigidas por el Coordinador de Emergencias.

Localización del Centro de Control de Emergencias

- La localización principal y alterna del Centro de Control de Emergencias será determinada por la JGS911 y se incluirá en el Plan cuando se provea la información.
- Si los lugares designados no son accesibles, el Coordinador Alterno es responsable de conseguir otra localización.

Guías

1. El Coordinador de Emergencias Alterno es responsable de mantener el Centro de Control de Emergencias disponible. El Centro de Control de Emergencias deberá estar equipado con mesas, sillas, teléfonos, pizarras y otros materiales y suministros de emergencias que se deben guardar en un lugar seguro, si posible fuera de la JGS911.
2. Cuando el Coordinador de Emergencias ha declarado una emergencia mayor, el Coordinador Alterno procederá a tomar todos los pasos necesarios para activar el Centro de Control de Emergencias.
3. El primer paso será la activación del lugar seleccionado como Centro de Control de Emergencias previamente identificado. El coordinador de emergencia debe requerir las llaves de acceso y disponer de los nombres, direcciones y números de teléfonos que son necesarios para tener acceso al lugar.
4. Si es necesario, se ordenarán teléfonos a la compañía de teléfonos



para que sean instalados de emergencia y los materiales serán obtenidos de los resguardos u otras fuentes para equipar apropiadamente el Centro de Control de Emergencias.

5. Si el Centro de Control de Emergencias es diferente al que se designó originalmente, se debe notificar a todas las Organizaciones y al Personal de Emergencias los números de teléfonos de dicho centro.

6.5 Notificación a los Comités de Acción de Emergencias y a la Alta Gerencia

En el evento de una emergencia mayor, los Comités de Acción de Emergencias y la Alta Gerencia de la JGS911 serán también notificados de la situación. La Alta Gerencia necesita conocer acerca de la emergencia y el estado actual del personal, propiedad, etc. Los Comités de Acción de Emergencias deben llevar a cabo muchas funciones especializadas en una situación de restauración después de un desastre, y serán llamados en caso de emergencia.

Guías

1. Determinar cuál comité de los Comités de Acción de Emergencias debe ser activado y si la presencia de algún personal de la alta gerencia se necesita para dar apoyo a las actividades de emergencia o a los procedimientos de contingencia.
2. El Coordinador de Emergencias debe notificar lo sucedido a la alta gerencia. El Coordinador de Emergencias o cualquier miembro del Comité de Planificación pueden notificar a los Comités de Acción de Emergencias.
3. El Anejo E.1 contiene la "Lista de Notificación en Orden Jerárquico a los Miembros de la Alta Gerencia", con sus nombres, direcciones, números de teléfonos y posiciones de cada uno de los

miembros, para que puedan ser notificados. El Coordinador de Emergencias debe informar brevemente de lo ocurrido, el estado actual, el Plan de Acción, la localización y los números de teléfonos del Centro de Control de Emergencia.

4. Para la activación de los Comités de Acción de Emergencias, los líderes de cada comité deben ser llamados de la "Lista de los Comités de Acción de Emergencias", que se encuentra en el Anejo A.3. Se les debe informar brevemente de lo que ha pasado, el estado actual, el Plan de Contingencia, la localización y los números de teléfonos del Centro de Control de Emergencias. Cada líder debe tener en su hogar un Plan de restauración en caso de desastre, para que pueda prepararse e iniciar una acción apropiada con su equipo de trabajo. El o ella es responsable de reunir a los miembros de su comité y actuar de acuerdo a sus Planes de Contingencia (contenidos en la sección 6.8 - **Procedimientos Específicos para las Contingencias en el Centro de Sistemas de Información**).

Al ymt



6.6 Notificación a "International Safe Deposit" y a las Localizaciones Externas a Utilizar para Implementar los Planes de Contingencia

La activación del Plan de Contingencia requiere la notificación de la emergencia a "International Safe Deposit" y al "Contingency Site". Para que se pueda realizar la recuperación, el Plan de Contingencia requiere el que se obtengan los resguardos en medios magnéticos (cartuchos). También se debe recuperar la documentación de los sistemas y los materiales necesarios para establecer las operaciones en el "Contingency Site". Los Comités de Acción de Emergencias deben realizar estas tareas de acuerdo

a los procedimientos de la sección 6.8. Sin embargo, para agilizar el proceso inicial de restauración, el Comité de Planificación notificará a "International Safe Deposit" y al "Contingency Site", de que un desastre ha ocurrido y que el Plan de Contingencia ha sido activado. El Anejo D.2 contiene los nombres, direcciones, contactos y números telefónicos de "International Safe Deposit" y del "Contingency Site".

Guías

1. El lugar designado ha sido provisto con procedimientos escritos. Estos procedimientos están incluidos en la sección 6.8.
2. Se notifica a "International Safe Deposit" que una emergencia ha sucedido y sobre los medios magnéticos que serán requeridos para la recuperación de las operaciones. Los procedimientos de contingencia deben identificar qué materiales como cartuchos, discos magnéticos, etc. serán removidos del lugar de almacenamiento. Los procedimientos también especifican precisamente qué se hará con los materiales. El Anejo D.2 contiene el nombre, dirección, contactos y números telefónicos del lugar designado.
3. Notificar al "Contingency Site" que un desastre ha ocurrido lo cual requiere que se active el Plan de Contingencia. Los procedimientos de contingencia deben especificar los pasos que el "Contingency Site" debe implantar antes de que lleguen los miembros de los Comités de Acción de Emergencias. El Anejo D.6 contiene los nombres, direcciones, contactos y números telefónicos de los lugares designados.

*De
Gman*



6.7 Resumen de Guías

Esta sección provee un resumen general de las operaciones de contingencia. Los procedimientos de las tareas específicas se encuentran en las secciones 6.8 y 6.9.

Resumen de las Guías

1. El Comité de Operaciones o los miembros designados tendrán que visitar las facilidades de "International Safe Deposit" (bóveda) y recuperar los medios magnéticos requeridos por el Plan de Contingencia. Debido a que la notificación se hizo con anticipación por el Comité de Planificación, los medios magnéticos deben estar listos para entrega a su llegada. El Comité de Operaciones verificará los medios magnéticos y realizará cualquier ajuste que sea necesario en el Centro de Control de Emergencias.
2. Los otros comités activados se reunirán en el Centro de Control de Emergencias para que se les informe de lo ocurrido, discutirán cualquier problema que se haya identificado y coordinarán según el Plan de Contingencia a que corresponda la solución de (los) problemas. Si es necesario el Comité Administrativo hará los arreglos pertinentes para la transportación de los comités que tengan que ir al "Contingency Site".
3. El Comité de Aplicaciones procederá a identificar el trabajo que necesita ser recuperado y cuál es la mejor forma de hacerlo. Los miembros del comité se presentarán en el "Contingency Site" para ayudar en la recuperación de las aplicaciones y del trabajo en progreso. Además, serán responsables de notificar a los usuarios y coordinar los procedimientos de enlace que sean necesarios.
4. El Comité de Operaciones se dirigirá de inmediato al "Contingency Site" para comenzar a subir el sistema y los datos para iniciar las operaciones. Una vez recuperado el sistema, las operaciones se

Al
Ymmp



mantendrán en el "Contingency Site" por el tiempo que sea requerido. Si las operaciones externas se extendieran por mucho tiempo se recomienda que el Coordinador Externo de Emergencia se haga cargo de atender las relaciones con los usuarios.

5. Si el equipo ha sido dañado, destruido o gravemente afectado, el Comité de Equipo Computadorizado procederá a tomar las medidas de contingencia apropiadas para reparar o reemplazar el equipo que se haya averiado.
6. Si las facilidades físicas y/o de ambiente han sido dañadas, destruidas o gravemente afectadas, el Comité de Facilidades Físicas y Ambiente procederá a tomar las medidas de contingencia apropiadas para reemplazar o reparar las mismas.
7. El Comité Administrativo apoyará las operaciones del Centro de Control de Emergencias y de los Comités de Acción de Emergencias cuando sea requerido.
8. El Coordinador de Emergencias continuará dando servicio al Centro de Control de Emergencia tanto como sea necesario, y coordinará las operaciones hasta que vuelvan a la normalidad.

*Al
Smith*



6.8 Procedimientos Específicos para Contingencias Durante las Operaciones de Procesamiento de Datos

Esta sección contiene procedimientos específicos para la implementación del Plan de Contingencia destinados al área de operaciones. Los siguientes procedimientos están clasificados por el número de la sección y por materia.

Procedimientos Incluidos en esta Sección:

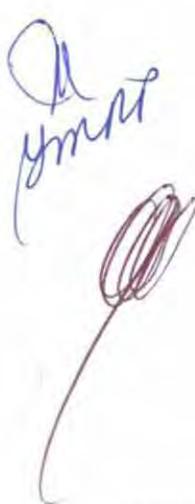
- 6.8.1 Procedimientos Iniciales a Implantar en el "Contingency Site"
- 6.8.2 Procedimiento de Coordinación Administrativa por parte del Comité Administrativo
- 6.8.3 Procedimientos para la Recogida de Materiales de Resguardo por parte del Comité de Operaciones
- 6.8.4 Procedimiento de Reunión y Coordinación de Todos los Comités de Emergencia
- 6.8.5 Procedimiento para la Recuperación por parte del Comité de Operaciones
- 6.8.6 Procedimiento para Recuperación de Trabajos en Progreso por Parte del Comité de Aplicaciones
- 6.8.7 Procedimiento para la Coordinación de los Usuarios por Parte del Comité de Aplicaciones



6.8.1 Procedimientos Iniciales a Implantar en el "Contingency Site"

Se preparará un Lugar de Contingencia conocido como el "Contingency Site", con los equipos necesarios como computadoras, impresoras, máquina para enviar facsímiles, equipo telefónico etc., para poder llevar a cabo las operaciones diarias que se realizan en la JGS911.

Procedimientos Iniciales a Implantar en el "Contingency Site"



<u>Responsabilidad</u>	<u>Acción</u>
Coordinador de Emergencias de la JGS911	1. Notifica al "Contingency Site" que ha ocurrido una emergencia.
Persona Autorizada del "Contingency Site"	2. Procede a realizar los pasos iniciales, para que cuando el personal de la JGS911 llegue, todo esté preparado. Estos pasos incluyen: a. Los preparativos para que los requerimiento técnicos del sistema se puedan llevar a cabo sin problemas.

Notas:

1. En la tabla siguiente, se presenta el nombre de la aplicación, el "Family name" y el espacio requerido para la distribución de espacio en disco por aplicación. En adición, se presenta el nombre del archivo, "Family Name" y el espacio requerido para la distribución de los archivos de datos.

Nombre de la Aplicación a Restaurar:

Peachtree Accounting 2005

Distribución de Espacio en Disco por Aplicación

Folder se encuentra en Servidor E911BDC en la partición D "Data"

- a. Folder "PeachTree2005" Espacio 4.96GB
- b. Folder "PeachTree8.1" Espacio 1.44GB
- c. Folder "PeachTree_Backup" Espacio 9.03GB

Archivos de Datos "Personal que acceden"

- a. Folder "PeachTree2005"
 1. Neysha Figueroa Ríos, Directora de Servicios Generales "Ayudante Especial I"
 2. Glenda Ojeda, Agente Comprador I
 3. Angelina Estrada, Agente Comprador II
 4. Yesenia Rivera, Oficinista II
 5. Cristino Morán, Director Asuntos Fiscales
 6. Maribel de León, Auxiliar Fiscal I
 7. Yarilys Feliciano, Auxiliar Fiscal I
 8. Isamar Ocasio, Auxiliar Fiscal I
 9. Daisy Morales, Auxiliar Fiscal II
 10. Vivian González, Contadora
 11. Gladys Rodríguez, Directora de Servicios Técnicos y Auxiliares
- b. Folder "PeachTree8.1"
 1. Vivian González, Contadora
 2. Maribel de León, Auxiliar Fiscal I
- c. Folder "PeachTree_Backup"
 1. Cristino Morán, Director Asuntos Fiscales
 2. Daisy Morales, Auxiliar Fiscal II
 3. Vivian González, Contadora

6.8.2 Procedimiento de Coordinación Administrativa por parte del Comité Administrativo

Responsabilidad	Acción
Comité Administrativo	<ol style="list-style-type: none"><li data-bbox="878 426 1458 758">1. Si el "Contingency Site" está localizado a una distancia razonablemente lejos del Área Metropolitana, se deben hacer arreglos para acomodar el equipo de trabajo en algún hotel u hospedaje, según sea requerido.<li data-bbox="878 758 1458 1310">2. Una vez el Coordinador de Emergencias ha declarado la emergencia se activa el Comité Administrativo para que éste maneje aspectos administrativos, tales como, compra de suministros, pagos de dietas, peaje, hospedaje, etc. <i>Nota: Los desembolsos y gastos de los arreglos serán manejados directamente por las Oficinas de Servicios Generales y Asuntos Fiscales de la JGS911.</i><li data-bbox="878 1310 1458 1646">3. Ayuda en el empaque y transportación de materiales al "Contingency Site". Ayuda con alguna otra actividad asignada por el Coordinador de Emergencias o por los líderes de los Comités, incluyendo tomar minutas en las reuniones de emergencia.

Handwritten signature in blue ink: JMS

Handwritten signature in red ink: [Signature]

6.8.3 Procedimiento Para la Recogida de Materiales de Resguardo por Parte del Comité de Operaciones

Este procedimiento se aplicará cuando ocurra una emergencia y se necesite buscar los materiales almacenados en el lugar de resguardo (Backup Site). El lugar de resguardo para la JGS911 es "International Safe Deposit". A continuación se presentan los pasos a seguir para este procedimiento:

Responsabilidad	Acción
<p>Líder del Comité de Operaciones</p>	<p>1. Si la emergencia ha ocurrido en horas laborables:</p> <p>a. Coordina con uno o dos miembros del Comité de Operaciones para que en un solo viaje puedan recoger los materiales necesarios de resguardo.</p> <p>Nota: El líder del comité debe tener conocimiento de los materiales que hay en el "Backup Site", por lo tanto puede requerir el tipo de transportación necesaria.</p>
<p>Miembros Autorizados</p>	<p>b. Recogen los materiales apropiados que requiera la emergencia. Por ejemplo:</p> <ol style="list-style-type: none"> 1) Archivos vitales 2) Cartuchos magnéticos 3) Formularios 4) Discos Magnéticos 5) Otros <p>c. Proceden a presentarse a las oficinas de "International Safe Deposit" con las tarjetas de identificación y la llave que dicha compañía les ha proveído para buscar los materiales de resguardo.</p>
	<p>d. Llenan una hoja de "Servicio de</p>

Handwritten signature in blue ink.

Handwritten scribble in blue ink.

Handwritten signature in blue ink, possibly "J. Ympt", and a red scribble below it.

	<p>Emergencia" para certificar la visita y el "Record de Cartuchos Removidos" y la firman.</p> <p>e. Dividen los materiales de acuerdo a su destino, hacia el Centro de Control de Emergencias o al "Contingency Site" antes de removerlos a los vehículos.</p> <p>1) En el "Contingency Site" algunos de los Materiales que deben haber son los siguientes:</p> <ul style="list-style-type: none">a. Cartuchos magnéticosb. Materiales para el procesamiento de datos.c. Una copia de toda la documentación. <p>2) Los materiales para el Centro de Control de Emergencias serían por ejemplo:</p> <ul style="list-style-type: none">a. Equipo periferal que requiere la infraestructura de equipo y programación que se va a utilizar en la emergencia.b. Documentación <p>f. Proceden a llevar los materiales de resguardo al Centro de Control de</p>
--	--

Handwritten signature in blue ink.

Internacional Safe Deposit, se debe notificar a Internacional Safe Deposit.

- 4. Todo "backup" que sea guardado en la bóveda debe estar debidamente identificado, porque de no ser así, la "Internacional Safe Deposit" lo podría eliminar para evitar que se le entregue a otra compañía y/o utilizar de un modo contraindicado.

6.8.4 Procedimiento de Reunión y Coordinación de todos los Comités de Acción de Emergencia

Este procedimiento enfoca la reunión inicial de los Comités de Emergencia con el Coordinador de Emergencia y otros miembros del Comité de Planificación.

Al grupo

Responsabilidad	Acción
Coordinador de Emergencia	1. Una vez todos los Comités de Emergencia hayan sido organizados en el Centro de Control de Emergencia, informa a dichos comités sobre lo que ha ocurrido y notifica a los mismos la evaluación del Comité de Planificación sobre el estado.
Comités de Emergencia	2. Pregunta a todos los Comités de Emergencia si estos conocen alguna otra información o circunstancias que necesiten ser consideradas. 3. Discuten todos los aspectos básicos de la situación y discuten estudios de problemas debido al itinerario de procesamiento o cualquier otro asunto pertinente, antes de llevar a cabo sus funciones particulares. Nota: Es importante que todos los Comités de Emergencia entiendan todos los asuntos claves, ya que esto resultará en una mejor coordinación.
Coordinador de Emergencia	4. Antes de cualquier Comité retirarse, repasa con cada uno de los líderes de los siguientes grupos las labores que cada comité debe realizar.

Al ymt

	<ul style="list-style-type: none">• Comité Administrativo (Este comité es responsable de, entre otras cosas, realizar los arreglos para los comités que se trasladarán al Lugar de Contingencia "Contingency Site")• Comité de Operaciones (Trabaja conjuntamente con el Comité de Aplicaciones para recuperar los trabajos en proceso y comenzar a trabajar en la recuperación de las operaciones en el "Contingency Site")• Comité de Aplicaciones (Trabaja conjuntamente con el Comité de Operaciones para coordinar con los usuarios principales. Una vez esto sea completado, algunos o todos los miembros del comité se trasladarán al "Contingency Site")• Comité de Facilidades (Este comité es responsable de reparar el CSI según sea requerido)• Comité de Equipo (Este comité es responsable de reparar el equipo computadorizado según sea requerido)
--	--

[Handwritten signature]

6.8.5 Procedimiento para la Recuperación por parte del Comité de Operaciones

Responsabilidad	Acción
Comité de Operaciones y en Comité de Aplicaciones	<p>1. Identifican el estado de los archivos producción y de los trabajos en progreso antes de trasladarse al lugar de Contingencia.</p> <p>a. Si durante la situación de emergencia se pierden datos o trabajos ya procesados, se reúnen con el Personal del Área de Operaciones, un grupo de usuarios y personal a cargo de los sistemas para evaluar las posibles soluciones a la situación.</p> <p>Nota: No todos los detalles se deben discutir en esta reunión debido a la limitación de tiempo.</p>
Comité de Operaciones	<p>2. Se traslada al "Contingency Site" una vez se hayan resuelto los asuntos relacionados a la pérdida de datos y de trabajos en proceso al momento de la emergencia.</p> <p>3. Organiza todos los materiales de resguardo (medios magnéticos, documentación, aplicaciones, equipo, etc.) tan pronto como llegue al "Site".</p> <p>Nota: Los materiales se deben mantener en un área específica designada por el personal del "Site".</p> <p>4. Se familiariza con las facilidades del "Site", la operación de las computadoras y los procedimientos de seguridad.</p>
Líder del Comité de Operaciones	5. Informa a los miembros del comité sobre la importancia de mantener

Al grupo

(Handwritten scribble)

	<p>todas las labores realizadas en una bitácora adicional a las creadas durante las operaciones normales del CSI. Debe asegurarse de que los empleados entienden la importancia de incluir toda la información necesaria en la bitácora adicional.</p>
Comité de Operaciones	<p>6. Instalará las aplicaciones y los datos en la(s) máquina(s) del "Site" tan pronto como el personal del lugar instale y prepare el equipo. En la sección 6.8.1 se detalla el espacio en disco requerido por cada aplicación.</p> <ul style="list-style-type: none">a. Ejecuta el comando Restore.b. Solo se instalarán:<ul style="list-style-type: none">1) El sistema operativo2) Las aplicaciones críticas3) Datos relacionados a las aplicaciones críticas <p>7. Realiza pruebas cortas a las aplicaciones para corroborar que están operando correctamente.</p> <p>8. Solicita al Comité de Aplicaciones información sobre como realizar las labores de recuperación de trabajos perdidos (trabajos en proceso no completados o no resguardados).</p>
Comité de Aplicaciones	<p>a. Si se pierden datos entrados al computador después del último resguardo, se reúne con los usuarios principales para determinar como resolver la situación. En algunos casos se podrán buscar los documentos de donde se obtuvo la información para que sea entrada al computador y procesada nuevamente.</p> <p>Nota: A todo el personal que se le puede solicitar que participe en el proceso de entrada de datos de ser necesario.</p>
Comité de Operaciones	<p>9. Coordina con el Comité de</p>

Al
ymr

Q

Al grupo

	<p>c. Si se pierden datos o trabajos, durante la emergencia, revisan detalladamente cada aplicación para determinar como recuperarán los datos o trabajos perdidos.</p> <p>3. Se trasladan al "Contingency Site" una vez se hayan decidido los procesos a seguir para recuperar los documentos y trabajos perdidos.</p>
Coordinador Externo	<p>4. Si el proceso de recuperación es complicado, prepara el itinerario para que los tres grupos participen en las labores de recuperación de trabajos. Para ello se requerirá, según amerite la situación: turnos rotativos, la entrada de datos, corrección de archivos de datos, corrida de trabajos especiales y/o procesar nuevamente las aplicaciones.</p> <p>a. Si no hay personal suficiente para trabajar en todas las aplicaciones simultáneamente, establece prioridad a las labores según sea su impacto y las asigna al personal disponible.</p> <p>b. Si la información contenida en los documentos perdidos no se puede recuperar, se debe llegar a una decisión sobre qué hacer para reponer dicha información.</p> <p>c. Si se pierden datos o trabajos, durante la emergencia, revisan detalladamente cada aplicación para determinar como</p>

[Handwritten signature]

	recuperarán los datos o trabajos perdidos.
Líder del Comité de Aplicaciones	1. Notifica la situación de emergencia a los usuarios principales y los cita a una reunión en el Centro de Control de Emergencias.
Comité de Aplicaciones, de Operaciones y Usuarios	2. Identifican los trabajos (documentos fuente, archivos y trabajos en proceso) que se crearon después del último resguardo y que se perdieron durante la situación de Emergencia. a. Si durante la situación de emergencia se pierden documentos importantes, revisa el Plan de Archivos Vitales para determinar el procedimiento a seguir para recuperar los documentos perdidos o la información contenida en los mismos. b. Si la información contenida en los documentos perdidos no se puede recuperar, se debe llegar a una decisión sobre qué hacer para reponer dicha información. c. Si se pierden datos o trabajos, durante la emergencia, revisan detalladamente cada aplicación para determinar como recuperarán los datos o trabajos perdidos.
Coordinador Externo	3. Se trasladan al "Contingency Site" una vez se hayan decidido los procesos a seguir para recuperar los documentos y trabajos perdidos. 4. Si el proceso de recuperación es complicado, prepara el itinerario

*Al
pmp*

(Handwritten signature)

Al grupo

	<p>para que los tres grupos participen en las labores de recuperación de trabajos. Para ello se requerirá, según amerite la situación: turnos rotativos, la entrada de datos, corrección de archivos de datos, corrida de trabajos especiales y/o procesar nuevamente las aplicaciones.</p> <p>a. Si no hay personal suficiente para trabajar en todas las aplicaciones simultáneamente, establece prioridad a las labores según sea su impacto y las asigna al personal disponible.</p>
--	--

6.8.7 Procedimiento de Coordinación de los Usuarios por parte del Comité de Aplicaciones

Es responsabilidad del Comité de Aplicaciones asegurar que las aplicaciones del sistema funcionen apropiadamente para los usuarios, que el trabajo perdido pueda ser recuperado, y que los usuarios entiendan acerca de cómo las operaciones deben ser realizadas durante el periodo de contingencia.

Responsabilidad	Acción
Comité de Aplicaciones	<p>1. Determina el estado de los archivos de producción y del trabajo en proceso. (Refiérase a la sección 6.8.6 para más información). Este proceso se coordinará conjuntamente con el Comité de Operaciones.</p> <p>2. Dependiendo el día y la hora del itinerario mensual establecido, solicitará a los usuarios principales que se presenten al Centro de Control de Emergencias para que participen en el proceso de determinar el estado de las aplicaciones.</p>
Líder del Comité de Aplicaciones	<p>3. Informa a los usuarios principales</p>

[Handwritten scribble]



	<p>del estado inicial de la situación, luego divide a los empleados en grupos por aplicaciones del sistema o subsistema, preferiblemente incluyendo en cada grupo una variedad de usuarios, programadores y operadores.</p> <p>4. Cuando los asuntos de la recuperación de trabajos perdidos hayan sido discutidos, coordina un itinerario de trabajo con los usuarios principales y el Líder del Comité de Operaciones. Discute cuidadosamente el impacto del trabajo en proceso de manera que los usuarios principales entiendan claramente la situación y puedan dar instrucciones apropiadas a sus subordinados. Los usuarios de las áreas deben entender que sus planes de trabajo interinos son hasta que los sistemas computadorizados estén totalmente recuperados.</p>
Comité de Aplicaciones	<p>5. Una vez el proceso de recuperación se haya completado coordina con los usuarios principales para asegurarse que ellos puedan interactuar con sus aplicaciones y determinar si aun existen restricciones con la operación de las aplicaciones. Si la cantidad de computadoras no son suficientes para manejar el volumen de trabajo, los usuarios necesitarán trabajar en turnos para tomar ventaja de las horas nocturnas. Sin embargo, el líder del Comité de Operaciones debe participar en el desarrollo del itinerario para evitar conflictos de procesamiento. Si se encuentra con problemas inesperados, trabaja rápidamente para encontrar sus soluciones.</p>



6.9 Procedimientos Específicos de Contingencia para los Usuarios

Esta sección contiene procedimientos específicos para establecer el enlace entre los usuarios y la operación de sus aplicaciones. Los procedimientos que se presentan a continuación están clasificados por materia.

Procedimientos Incluidos en esta Sección:

- 6.9.1 Procedimiento para la Coordinación de las Operaciones de los Usuarios por parte del Coordinador Externo**
- 6.9.2 Operación de la Aplicación de Manejo de la Nómina.**

Nota: La operación de cada una de las aplicaciones se incluirán en el Plan tan pronto el Centro de Sistemas de Información lo provea.

*Al
YMP*

6.9.1 Procedimiento para Coordinación de las Operaciones de los Usuarios por parte del Coordinador Externo

Funciones, Políticas y Datos

1. La posición del Coordinador Externo será imprescindible en situaciones donde un gran número de empleados tenga que laborar en el "Contingency Site".

En situaciones de emergencia de gran magnitud, el Coordinador Externo será la persona a cargo de dirigir las labores del "Site". Si la situación es de menor magnitud, el Líder del Comité de Operaciones será la persona con mayor autoridad.

Responsabilidad	Acción
Coordinador Externo y Comité de Operaciones	<ol style="list-style-type: none"> 1. Se familiariza con las facilidades del "Contingency Site" y analiza si son apropiadas para la situación actual. <ol style="list-style-type: none"> a. Si el espacio no es suficiente para acomodar el personal esperado, realiza las gestiones necesarias para obtener facilidades adicionales. 2. Revisa los procedimientos e itinerarios de recuperación para asegurarse de que satisfacen las necesidades y prioridades de la JGS911 en el caso de una emergencia. <ol style="list-style-type: none"> a. Si identifica algún factor que pueda afectar significativamente las operaciones: <ol style="list-style-type: none"> 1) Discute la situación con el Coordinador de Emergencias 2) Informará la situación a la Alta Gerencia. 3. Asiste a los diferentes grupos durante las operaciones de recuperación y de procesamiento de datos. 4. Prepara el itinerario de los turnos de trabajo.
Coordinador de Emergencias	
Coordinador Externo o Líder del Comité de Operaciones	

	<p>5. Brinda apoyo moral y orientación al personal.</p> <p>6. Mantiene comunicación continua con el Coordinador de Emergencias para mantenerlo informado de todo lo que ocurre, en cuanto al progreso de las operaciones, decisiones tomadas, gastos extraordinarios y asuntos administrativos.</p>
--	---

6.9.2 Operación de la Aplicación de Manejo de la Nómina.

Este procedimiento fue aprobado por la Junta de Gobierno del Servicio 911 el 19 de julio de 2007. El mismo aparece en los siguientes S.O.P..

Primero: S.O.P F-100 Manual de Procedimientos Operacionales – (F) Fiscalización Area de Pagaduría, Contabilidad y Presupuesto (Páginas 23 a la 27)

Segundo: S.O.P. F-300 Manual de Procedimiento Operacionales (F) Fiscalización Área de Nómina (Páginas 62 a la 80).

En el Anejo E.4 de esta sección se incluye estos procedimientos.

6.10 Procedimiento para el Reemplazo del Centro de Sistemas de Información

Si el Centro de Sistemas de Información de la JGS911 es destruido, se deben tomar acciones inmediatas para establecer un nuevo Centro de Sistemas de Información. Se debe buscar una localización con espacio adecuado, se debe construir o modificar un cuarto para las computadoras, que incluye los requisitos básicos de ambiente como: aires acondicionados, equipo para la distribución de energía, piso falso, cablería, etc.

*Al
página*



Procedimiento

1. Los Comités de Equipo y Facilidades deben tener identificado dentro de sus Planes de Contingencia, lugares para un potencial reemplazo de las facilidades y el equipo del Centro de Sistemas de Información. Estos planes deben incluir acuerdos escritos entre suplidores.
2. Si el equipo o las facilidades son salvadas, los Comités de Equipo y Facilidades investigan qué se puede utilizar o ser reparado y qué necesita ser reemplazado e inician el traslado del equipo y/o las actividades de reparación que sean necesitadas.
3. Los Comités de Equipo y Facilidades ordenarán los nuevos equipos y/o facilidades que requieran ser sustituidos de emergencia. Los asuntos de seguros, financieros y legales se deben atender durante este proceso.
4. Cuando el nuevo Centro de Sistemas de Información esté construido y el equipo se haya recibido, los Comités de Facilidades y de Equipo coordinarán para obtener los permisos necesarios, realizar los trabajos para hacer la instalación, proveer los servicios de energía eléctrica que requiere el equipo, tirar el cableado para las comunicaciones y todas aquellas tareas necesarias para asegurar que el nuevo Centro de Sistemas de Información está preparado para operar apropiadamente.
5. Los Comités de Facilidades y de Equipo realizarán pruebas para verificar la funcionalidad del nuevo Centro de Sistemas de Información. Cuando encuentren que está listo coordinarán con el Comité de Operaciones para transferir las operaciones del "Contingency Site" hacia el nuevo Centro de Sistemas de Información.
6. Los procedimientos estarán completados cuando todos los problemas encontrados con las operaciones en el nuevo Centro de

*Al
gmpp*

[Handwritten scribble]

Sistemas de Información se hayan resuelto y las operaciones estén normalizadas.

6.11 Procedimiento para Retornar a las Operaciones Normales

Los siguientes procedimientos tienen como propósito servir de guía para el retorno a las operaciones normales en el Centro de Sistemas de Información después de ocurrir una situación de emergencia.

Guía

1. Cuando las operaciones en el CSI vuelvan a la normalidad será responsabilidad del Coordinador de Emergencias informar a los usuarios y a la gerencia de dicho evento de manera que los Comités de Acción de Emergencias puedan hacer los ajustes necesarios para administrar el cambio.
2. Al transferir las operaciones nuevamente al Centro de Sistemas de Información. El Comité de Operaciones es responsable de proteger las aplicaciones y la información. También de traer al Centro de Sistemas de Información todos los materiales y equipo que le pertenezcan a la JGS911.
3. El Coordinador de Emergencias y el Comité de Planificación deben mantenerse alertas a cualquier situación inesperada que surja en el Centro de Sistemas de Información. Además solicitarán al Comité de Operaciones que transfieran los materiales y las cintas de resguardo al "Backup Site".
4. Un memorando oficial debe ser enviado a todos los empleados para informarles que la emergencia ha sido corregida y que las operaciones ya se normalizaron o pronto volverán a la normalidad. El Centro de Control de Emergencias debe ser desactivado.
5. La operación final del Plan de Contingencia será una reunión entre



el Comité de Planificación y los Comités de Acción de Emergencias. En dicha reunión se discutirán las actividades de recuperación llevadas a cabo. El Coordinador de Emergencias se encargará de que se documenten todos los sucesos, problemas, soluciones, etc. discutidos en la reunión. Una vez esté completa la documentación, los Comités de Acción de Emergencias y el Comité de Planificación se pueden desactivar. Durante la próxima revisión del Plan, el Coordinador de Emergencias se asegurará de que cualquier lección aprendida durante el período de emergencia sea incorporada al Plan.

Al grupo

Sección 7 Prueba y Mantenimiento Del Plan de Contingencia

El Plan de Contingencia no puede ser considerado completo y final hasta que se haya realizado la prueba de aceptación. Esta prueba verifica que todas las facetas del Plan hayan sido implantadas y evaluadas como correctas y suficientes. Después de una aceptación inicial del Plan, se debe ir probando el mismo periódicamente para asegurar una continua validez de su contenido. El Plan también debe ser revisado regularmente y actualizado cuando sea necesario. Esta sección atiende estos asuntos proveyendo políticas y procedimientos para probar el Plan. También provee para las revisiones periódicas y la actualización del Plan.

7.1 Políticas y Procedimientos para Pruebas

Para probar el Plan, la JGS911 debe establecer las siguientes políticas y procedimientos:

Políticas

El Plan de Contingencia debe ser probado desde su fase inicial de desarrollo y antes de su publicación final. El Plan puede ser probado para aspectos organizacionales y procedimientos, así como para evaluar su habilidad técnica para permitir el procesamiento de aplicaciones en el lugar externo seleccionado por la JGS911 ("Contingency Site"). Además, puede ser probado para que el Comité de Emergencias pueda estar familiarizado con el Plan de Contingencia. El Coordinador de Emergencias debe ser responsable de conducir una prueba al terminar la revisión anual del Plan. Los resultados de la prueba deben ser revisados y aprobados por el Director(a) de la Oficina de Servicios Técnicos y Auxiliares y el Comité de Planificación.

Procedimiento para Realizar Pruebas al Plan de Contingencia

Responsabilidad	Acción
Coordinador de Emergencias	<p>1. De acuerdo con las Políticas y Procedimientos de Revisión y Actualización del Plan, diseña y establece un itinerario de eventos para la ejecución de procesos en el "Contingency Site" y notifica a los miembros del Comité de Planificación sobre la prueba anual para evaluar diferentes elementos del Plan. La prueba puede variar de año en año.</p> <p>Nota:</p> <ul style="list-style-type: none">• No obstante, la prueba debe dar énfasis a probar todos los procedimientos principales que envuelven a los comités de trabajo y debe probar la habilidad del proceso en el "Contingency Site" <p>2. Organiza una serie de diferentes pruebas durante el año, o sea cada prueba será de una porción diferente del Plan.</p> <p>Notas:</p> <ul style="list-style-type: none">• Sin embargo, al menos una vez al año el Plan debe ser probado en su totalidad.• Las pruebas deben ser consideradas como ejercicios de repaso y adiestramiento así como pruebas sobre la funcionalidad del Plan. No obstante, siempre habrá algunas características del Plan las cuales deben ser probadas en su totalidad. Esto significa que las

Qu
Ymup

Q

	<p>pruebas deben ser observadas, medidas y llevar un registro de todos los sucesos y fallas. El Coordinador de Emergencias Alterno debe servir como moderador de las pruebas. Durante el progreso de la prueba, si se encuentra algún problema, se debe buscar una solución al mismo inmediatamente.</p> <ul style="list-style-type: none">• Al menos en las pruebas de la aceptación inicial (primer año) y los años posteriores, TODAS las aplicaciones críticas deben ser probadas en el "Contingency Site" para verificar que no haya problemas técnicos que impidan ofrecer servicios a través del "Contingency Site". Durante los años subsiguientes, las pruebas de las aplicaciones críticas deben escalonarse para reducir la complejidad de las pruebas y el tiempo requerido.• Las pruebas podrían extenderse sobre un período de tiempo razonable. Preferiblemente menos de dos semanas de manera que no tengan impacto en otras actividades de trabajo. No obstante, las pruebas deben ser completadas para la fecha especificada en la política de pruebas.
--	--

Al
primer

	<ul style="list-style-type: none">• Después de las pruebas, se documentan los resultados, incluyendo cualquier cambio recomendado en el Plan.
Director(a) de Servicios Técnicos y Administrativos y Comité de Planificación	3. Revisan y aprueban los resultados de la prueba. Nota: Si hay cambios al Plan de Contingencia como resultado del proceso de pruebas, estos deben ser incorporados junto con los cambios del proceso de revisión semi-anual (Ver la sección 7.2)

7.2 Políticas y Procedimientos de Revisión y Actualización

La efectividad del Plan de Contingencia se afecta por los cambios al ambiente bajo el cual el Plan fue creado. Algunos factores principales que pueden afectar el Plan son: nuevo equipo, cambio en los sistemas, cambios en la organización y personal del CSI, y nuevas aplicaciones.

Las siguientes políticas y procedimientos deben ser desarrollados para asegurar que el Plan es revisado y actualizado de forma confiable y periódicamente.

Política

Dos veces al año el Plan de Contingencia debe ser revisado por el Coordinador de Emergencias y aprobado por el Director(a) de Servicios Técnicos y Auxiliares y el Comité de Planificación.

Procedimiento para Revisar y Actualizar el Plan de Contingencia

Responsabilidad	Acción
Coordinador de Emergencias	<ol style="list-style-type: none">1. Asigna un comité de trabajo de dos o más personas para revisar y actualizar el Plan de Contingencia dos veces al año.2. Cuando el comité de trabajo designado haya completado su revisión para la actualización, revisa y aprueba el Plan revisado.3. Entrega el Plan revisado al Director(a) de Servicios Técnicos y Auxiliares y al Comité de Planificación en la fecha requerida por la Política de revisión, para una aprobación final. Nota: El Plan revisado podría ser utilizado para las pruebas anuales. La actualización del Plan es la mayor prioridad que deben tener las pruebas. No obstante, las pruebas mismas podrían también identificar cambios a realizar en el Plan. Además, luego de la pruebas, se debe distribuir el Plan actualizado.4. Instruye al Coordinador Alterno para que distribuya las revisiones al Plan. Nota: Por consideraciones de costo, las revisiones deben ser distribuidas como actualizaciones de la versión anterior.5. Revisa y actualiza frecuentemente el Plan de Contingencia. Nota: No obstante, esto debe requerir la aprobación de la JGS911 debido al impacto que esta acción puede tener en otros proyectos.

Al
ymrp

Estado Libre Asociado de Puerto Rico

Junta de Gobierno Servicio 9-1-1

**Plan para la Recuperación de Desastres para el Componente Administrativo de la
Junta de Gobierno del Servicio 9-1-1**

Título: Plan para la recuperación de desastres (DRP, por sus siglas en inglés) para el Componente Administrativo de la Junta de Gobierno del Servicio 9-1-1

Revisión: 0

Unidad: Oficina de Sistemas de Información

Fecha de Efectividad: 1 de junio de 2008

Fecha de Revisión: _____ de _____ de _____

Recomendado por:

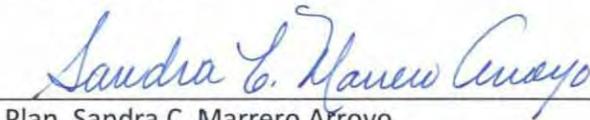


Ing. Gladys M. Rodríguez Pérez, MBA
Directora
Sistemas y Procedimientos

6-may-08

Fecha

Visto bueno por:



Plan. Sandra C. Marrero Afroyo
Directora Ejecutiva

14-Mayo-08

Fecha

Aprobado por:



Lcdo. Pedro Toledo Dávila
Presidente
Junta de Gobierno Servicio 9-1-1

30/mayo/08

Fecha



DISASTER RECOVERY PLAN

ANEJOS



ANEJOS

SECCION 1

SECCION 1
ANEJO A.1

Números Telefónicos de Servicios de Emergencia

