

**COMPañIA DE FOMENTO INDUSTRIAL DE PUERTO RICO
OFICINA DE DESARROLLO ORGANIZACIONAL Y CAPITAL HUMANO
DIVISIóN DE DESARROLLO ORGANIZACIONAL**

**PLAN DE CONTINGENCIA DE LA
OFICINA DE SISTEMAS DE INFORMACIóN**

MA-OSI-001

**Oficina de Desarrollo Organizacional y Capital Humano
DivisióN de Desarrollo Organizacional**

COMPañIA DE FOMENTO INDUSTRIAL DE PUERTO RICO
SAN JUAN, PUERTO RICO

PLAN DE CONTINGENCIA DE LA
OFICINA DE SISTEMAS DE INFORMACIÓN
MA-OSI-001

INDICE

ARTICULO		PAGINA
I	Introducción	1
II	Objetivos del Plan	1
III	Fase Inicial	1
IV	Personal Designado para Implantación del Plan	3
V	Interpretación de Términos	4
VI	Diferentes Presunciones	5
VII	Notificación del Incidente	7
VIII	Estrategia a Seguir en Caso de Fuego	8
IX	Estrategia en Caso de Emergencia por Agua	9
X	Estrategia en Caso de Fenómenos Naturales y Climatológicos	9
XI	Estrategia en Caso de Sabotaje	10
XII	Estrategia para Restaurar las Operaciones en el Centro de Cómputos Remoto	10
XIII	Aplicaciones Críticas y Requerimientos Mínimos	11
XIV	Vigencia	12
ANEJOS		
A –	Lista de Personal a Contactar en Casos de Emergencia o Desastre Natural - CFI	
A –1	Lista de Personal a Contactar en Casos de Emergencia o Desastre Natural - CCE	

- B – Personal Asignado y sus Alternos
- C – Cadena de Mando de la Oficina de Sistemas de Información
- D – Directorio de Suplidores
- E – Acuerdo Interagencial para el Uso de Centro de Control Remoto de los Sistemas de Información de Ocurred un Incidente o Desastre Natural
- 1 CFI – Requisitos de Hardware Necesarios para Recuperar el Mímodo del Ambiente de Sistemas de Información de CFI
- 2 CCE – Requisitos de Hardware Necesarios para Recuperar el Mímodo del Ambiente de Sistemas de Información de la CCE
- F – Retención y Rotación de Resguardos
- G – Lista de Agencias a Llamar en Caso de Emergencia por Prioridad y Dirección
- H – Procedimiento para Desactivar Sistema Operativo
- I – Extintores Manuales para Fuego
- I-1 Plano Ubicación Extintores
- J – Procedimiento para Activar Sistema Contra Incendio Automático
- K – Procedimiento para Desactivar Sistema Automático Contra Incendios
- L – Hoja para Inventario de Equipo y Áreas Afectadas

OTROS ANEJOS

Normas para el Manejo y Recuperación de los Resguardos

Procedimiento para el Manejo de Emergencias de la Oficina de Sistemas de Información

GOBIERNO DE PUERTO RICO
COMPAÑIA DE FOMENTO INDUSTRIAL DE PUERTO RICO
MANUAL DE SISTEMAS Y PROCEDIMIENTOS OPERACIONALES

ASUNTO: PLAN DE CONTINGENCIA DE LA OFICINA DE SISTEMAS DE INFORMACION

MA-OSI-001

Página 1 de 12

I. INTRODUCCIÓN

El Plan de Contingencia de la Oficina de Sistemas de Información (OSI), tiene el propósito de establecer los pasos a seguir en caso de emergencia donde el Centro de Cómputos se encuentre inoperante por un periodo de tiempo indeterminado para que la información de la Compañía de Fomento Industrial de Puerto Rico (CFI) almacenada en esta oficina pueda estar asegurada. Establece, además, las acciones a seguir cuando la interrupción de las operaciones puedan ocasionar pérdidas considerables o potenciales en la Oficina de Sistemas de Información localizada en las Oficinas de la CFI en Hato Rey, así como a la Oficina Regional en Ponce y la Oficina de Nueva York. El Plan aplicará al Departamento de Desarrollo Económico de Puerto Rico (DDEC), y a la Corporación para el Desarrollo de las Artes, Ciencias e Industria Cinematográfica en Puerto Rico (CINE), los cuales utilizan la infraestructura de la tecnología de la Oficina de Sistemas de Información de la Compañía, mientras éstas permanezcan utilizando el mismo sistema de información tecnológica.

Este Plan establece el compromiso de la Compañía de proveer los recursos necesarios para manejar y minimizar los riesgos de la posible pérdida de información de la OSI. Es de extrema importancia para la Compañía que las operaciones tecnológicas de la OSI se puedan reactivar en el menor tiempo posible. El Plan será utilizado para disminuir la cantidad de situaciones imprevistas o no planificadas en caso de un acontecimiento o emergencia. El Director de la OSI utilizará el Plan para impartir instrucciones de manera que se puedan recuperar las operaciones de los programas y la información almacenada en la oficina en el menor tiempo posible, luego de ocurrido el acontecimiento incidental o de emergencia. El Director de la Oficina de Sistemas de Información de la Compañía será responsable de revisar cada dos (2) años este documento.

Este Plan ha sido creado de acuerdo a las especificaciones de la Oficina de Gerencia y Presupuesto (OGP), indicadas en la Carta Circular 77-05 del 8 de diciembre de 2004, sus enmiendas y el proceso establecido en el Procedimiento para el Manejo de Emergencias de la Oficina de Sistemas de Información o cualquier otro subsiguiente.

II. OBJETIVOS DEL PLAN

El objetivo principal del Plan es restablecer las operaciones total o parcialmente de forma inmediata, después de ocurrir cualquier incidente, acontecimiento o emergencia, tomando en consideración la naturaleza del mismo. Cualquier incidente que deje inoperante, las operaciones de la OSI, conlleva una evaluación del método y la determinación o medida que se llevarán a cabo para realizar la reactivación y el funcionamiento de las operaciones, en el menor tiempo posible.

III. FASE INICIAL

En este Plan se desglosan de manera general los pasos a seguir al momento de declarar una emergencia o un incidente.

A. Se declarará el estado de emergencia al momento de ocurrir un incidente de carácter mayor y se activará al personal que ocupa los puestos que desglosamos a continuación:

1. Personal de la Oficina de Sistemas de Información
 - a. Director de Sistemas de Información
 - b. Oficial de Sistemas de Información Senior
 - c. Oficial de Sistemas de Información (Redes y Correo Electrónico)
 - d. Oficial de Sistemas de Información (Bases de Datos)
 - e. Oficial de Sistemas de Información (Desarrollo de Sistemas)
 - f. Oficial de Sistemas de Información (Servicio y Apoyo al Usuario)
 - g. Personal de Apoyo de OSI
 - h. Técnico de Microcomputadora
 - i. Técnicos de Redes y Correo Electrónico (2)
 - j. Analista y Programador de Sistemas
 - k. Oficial Principal de Servicios Administrativos
2. Otro personal de la Compañía
 - a. Director Ejecutivo
 - b. Oficial Principal de Servicios Administrativos
 - c. Director, Desarrollo Organizacional y Capital Humano
 - d. Gerente, División de Seguridad
 - e. Gerente, División de Servicios
 - f. Gerente, División de Conservación y Planta Física
 - g. Oficial Principal de Mercadeo y Comunicaciones
 - h. Secretario del DDEC
 - i. Secretario Auxiliar del DDEC
 - j. Director Ejecutivo de la Corporación de Cine
3. Personal de la Compañía de Comercio y Exportación
 - a. Director Ejecutivo
 - b. Subdirector Ejecutivo (Véase Anejo A y A-1)

IV. PERSONAL DESIGNADO PARA LA IMPLANTACIÓN DEL PLAN

Las responsabilidades, autoridades y designaciones del personal de restauración y el personal alterno de la OSI se detallan en el Anejo B.

El equipo de trabajo de la OSI ayudará en la recuperación y restablecimiento del sistema, para que el mismo esté en funcionamiento en el menor tiempo posible. El equipo de trabajo tendrá asignada las tareas necesarias por empleado, éstos serán liberados de cualquier otra tarea no relacionada a la declaración del incidente. Este equipo de trabajo actuará en coordinación con el Director de la OSI para organizar los recursos disponibles y recuperación de los servicios lo más pronto posible.

El Director de la OSI o el empleado de más alto rango (siguiendo la Cadena de Mando de OSI, Anejo C), que se encuentre al momento del incidente, será responsable del desalojo de todo el personal de la oficina y notificar al Oficial Principal de Servicios Administrativos. Este proceso se realizará con el recurso humano disponible y adiestrado, incluyendo el uso de personal externo, de ser necesario.

Las responsabilidades de los funcionarios y empleados de la OSI se establecen a continuación:

<u>TÍTULO DEL PUESTO</u>	<u>DESCRIPCIÓN Y TAREA</u>
Coordinador del Plan	El Director de la OSI, por tener la autoridad para tomar las decisiones de impacto presupuestario y, de ser necesario, coordinar que las operaciones internas se pueda realizar en el Centro de Cómputos de la CFI o en el Centro Remoto.
Coordinador de Usuarios y Producciones	El Oficial de Sistemas de Información Senior, o el Oficial de Sistemas de Información a cargo de la Administración de Bases de Datos, será el Coordinador de los Usuarios y Producciones y el contacto directo con aquellos usuarios claves. En caso de que ocurra un incidente, donde sea necesaria una recuperación, este empleado fungirá como oficial de asuntos públicos y será responsable de establecer las prioridades del equipo de recuperación.
Coordinador de Restauración de Facilidades	El Oficial de Sistemas de Información de Servicio y Apoyo al Usuario, será el responsable del inventario de las facilidades y de coordinar las compras necesarias para reestablecer el sistema y las facilidades de manera que se encuentren en condiciones adecuadas para trabajar. Véase Anejo D.
Coordinador Administrativo	El Personal de Apoyo será responsable de realizar las gestiones de las decisiones tomadas por el Coordinador del Plan. Además, realizará cualquier otra gestión que sea asignada.

Cuando se declare un estado de emergencia, inmediatamente se activará este plan de acción: las responsabilidades, las tareas del plan y las autoridades se mantendrán activas hasta que la situación haya sido declarada como normalizada por el Director de la OSI o el Oficial de Sistemas de Información a cargo de la emergencia. La restauración del funcionamiento del Centro de Cómputos se considerará terminada cuando esté en óptimas condiciones para continuar los trabajos.

V. INTERPRETACIÓN DE TÉRMINOS

Para propósito de este Plan de Contingencia se utilizará las siguientes interpretaciones:

- A. Acuerdo Interagencial** – Documento firmado por el Director Ejecutivo de la Compañía de Fomento Industrial y el Director Ejecutivo de la Compañía de Comercio y Exportaciones, para autorizar que en caso de una emergencia, donde las labores se vean interrumpidas por un incidente o desastre natural, ambas agencias funcionen como un centro de cómputos alterno, para que puedan continuar sus operaciones diarias a través de un Centro de Cómputo Remoto. (Véase Anejo E)
- B. Autorización** – Es el proceso por el cual se adjudican privilegios específicos a una persona para el uso de recursos en los sistemas de información.
- C. Centro de Cómputos Remoto** – Lugar alterno que se utilizará para establecer parcialmente un Centro de Cómputos, donde puedan ser procesados aquellos sistemas que se hayan definido como críticos en la OSI.
- D. Compañía** – Compañía de Fomento Industrial, PRIDCO por sus siglas en inglés.
- E. Confidencialidad** – Término utilizado para la información que sólo puede ser vista por aquellas personas autorizadas.
- F. Contingencia** – Implica aquellos riesgos que pueden ocurrir y necesitan mayor esfuerzo para efectuar la restauración de las operaciones. Cada estímulo requiere un esfuerzo diferente para la recuperación del sistema. Para propósitos de este Plan, pero sin limitarse, se establecen las siguientes contingencias:
 - 1. interrupción de la energía eléctrica o acondicionador de aire,
 - 2. fuego,
 - 3. inundaciones,
 - 4. fenómenos del tiempo por la naturaleza,
 - 5. sabotaje y
 - 6. vandalismo.

Cuando haya diferentes tipos y niveles de contingencias, también existirán diferentes maneras de restauración.

1. Este Plan cubre:
 - a. restauración parcial de la OSI, operando desde un Centro de Cómputos remoto.
 - b. restauración parcial de la OSI, operando el Centro de Cómputos de la CFI.

G. Incidente – Situaciones de carácter mayor que pueden limitar el uso del Centro de Cómputos; tales como:

1. Un incidente o acontecimiento o suceso que deje inoperante parcial o total las facilidades de la OSI por un período de ocho (8) horas o más.
2. Un incidente, acontecimiento o suceso que deteriore el procesamiento de datos y actividades relacionadas con la OSI, por circunstancias que estén fuera de los parámetros del proceso normal de las operaciones diarias.
3. Un incidente o acontecimiento que resulte en pérdida de data crítica o data media, debido a fenómenos naturales o causado por el hombre, que necesite de restauración por un período de 16 horas o más.

VI. DIFERENTES PRESUNCIONES

A. Primera Presunción

Las facilidades del Cuarto de Máquinas de la OSI han sido totalmente destruidas.

1. Objetivo

Las actividades de OSI deben estar en operaciones desde un centro de cómputos remoto.

2. Medio para Restaurar el Centro de Cómputos

Existen varias alternativas, para atender la primera presunción, algunas de estas son:

Primera Alternativa:

Las actividades continuarán totalmente en el Centro de Cómputos Remoto. La coordinación de este Centro Remoto se realizará siguiendo el Plan de Estrategia para Restaurar Operación en Centro Remoto, según indicado en el Artículo XII, Inciso A, de este Plan.

Segunda Alternativa:

Las actividades continuarán parcialmente en el Centro de Cómputos Remoto. El Director de la OSI removerá de la bóveda los medios de resguardo que se requieran para restablecer las aplicaciones críticas y activará el Plan de Estrategia para Restaurar la Operación en el Centro Remoto, indicado en el Artículo XII, Inciso A.

Tercera Alternativa:

El Director de la OSI restaurará las facilidades alquilando o comprando equipos y programas a los suplidores, según se detallan en el Anejo D.

3. Requisitos Mínimos

Para que este objetivo pueda ser realizado tiene que existir lo siguiente:

- a. Un documento (carta, acuerdo o contrato), entre una agencia externa que opere un Centro de Cómputos Remoto y la Compañía de Fomento Industrial. (Véase Acuerdo Interagencial del Centro de Control Remoto de los Sistemas de Información de Ocurrir un Desastre Natural, Anejo E)
- b. Un programa de retención y resguardo externo de cintas magnéticas identificadas correctamente (Véase Anejo F).
- c. Necesidades inmediatas de: “**Hardware**” y “**Software**”, para el proceso de los sistemas mínimos requeridos, al igual que el personal capacitado, según indicado.

B. Segunda Presunción

Las facilidades de procesamiento de datos de la Compañía han sido severamente dañadas por fuego, agua, vandalismo, sabotaje o falla eléctrica.

1. Objetivo

Lograr que las actividades mínimas de la OSI, estén en operaciones en el Centro de Cómputos Remoto en un período máximo de dos (2) días calendario y las operaciones generales en un período máximo de dos (2) semanas desde el momento del incidente o evento.

2. Medio para Restaurar el Centro de Cómputos

Todas las alternativas para el equipo del objetivo mencionadas en la Primera Presunción, deben ser consideradas.

C. Tercera Presunción

Las facilidades de la OSI han sido temporeraamente inutilizadas por fuego, agua, vandalismo, sabotaje o falla eléctrica. Las operaciones pueden volver a restablecerse en o antes de un (1) día calendario, de acuerdo a lo estimado el personal responsable de administrar el Plan de Contingencia.

1. Objetivo

Las actividades de procesamiento de información de la OSI tienen que estar en operaciones en sus propias facilidades en un periodo de 24 horas.

2. Medio para Restaurar el Centro de Cómputos

Todas las alternativas para el equipo mencionadas en el objetivo de la Primera Presunción deben ser consideradas, así como las siguientes alternativas:

- a. Las actividades del Director de la OSI serán las de verificar los discos de trabajo y restauración de información de los medios de resguardo.
- b. Cuando sólo los equipos hayan sufrido daños, el Director de la OSI coordinará mediante llamada con la compañía que ofrezca el soporte técnico para que repare o reemplace el o los equipos dañados. Las operaciones continuarán después de la reparación o reemplazo de los equipo. Véase Lista de Suplidores, Anejo D.

3. Evaluación del Objetivo

Este objetivo será evaluado en términos de la capacidad operacional del Centro de Cómputos, luego de 12 horas de haber transcurrido el incidente. De lo contrario, las alternativas de equipo mencionadas en el objetivo de la Primera Presunción serán consideradas.

De ser un Centro de Cómputos Remoto, el objetivo será evaluado en términos de la capacidad operacional dentro de un período de tiempo específico que determine el Director de la OSI. Si las aplicaciones críticas especificadas en el Artículo XIII de este Plan son funcionales, el objetivo del Centro de Cómputos Remoto habrá cumplido su objetivo.

Los objetivos mencionados están limitados a las operaciones de la OSI y los requerimientos necesarios para volver a ofrecer servicio a la CFI. Esto no incluye elementos que son orientados al usuario, tampoco incluye aquellos elementos que son funciones de auditoría, como lo es el fraude.

VII. NOTIFICACIÓN DEL INCIDENTE

El Director de la OSI, el Supervisor o el empleado en la escena del incidente tiene las siguientes responsabilidades, en orden de prioridad:

- A. Desalojar, de ser necesario, la oficina y verificar con una lista que todas las personas sean identificadas para asegurarse que han abandonado la oficina.
- B. Contactar al Oficial Principal de Servicios Administrativos en caso de que sea necesario desalojar el edificio. Además, deberá ofrecer información del incidente a las compañías, a los oficiales y civiles que lleguen a la escena para investigar lo sucedido.
- C. Poner en operación la secuencia de llamadas al personal administrativo e indicar en las llamadas, la naturaleza del incidente, el estatus de los empleados y la acción tomada. Este empleado tiene que ser el último en desalojar el área después de verificar, en el grado que sea posible, que todo el personal haya desalojado el área afectada. (Véase Anejo A y A-1)

- D. Asegurarse que el Cuarto de Máquinas esté cerrado. Esta tarea puede ser delegada a un Oficial de Sistema de Información, o cualquier otro empleado de Operaciones que esté presente. Las tareas serán asignadas a dos empleados.
- E. Desalojo de periferales críticos si el tiempo lo permite. El Director de la OSI deberá identificar los periferales críticos a ser removido durante un incidente.
- F. Notificar el incidente a las agencias y autoridades civiles y privadas indicadas. (Véase Anejo G)
- G. Identificarse como el empleado responsable con los oficiales de las compañías que se presenten en la escena, informarle el estatus del incidente y la acción tomada.

VIII. ESTRATEGIA A SEGUIR EN CASO DE FUEGO

- A. En caso de fuego se deben seguir los pasos indicados en los anejos que se indican a continuación:
 - 1. Informar al Director de la OSI sobre cualquier fuego, tan pronto sea detectado. (Véase Anejo J)
 - 2. Si el fuego es en el cuarto de máquinas el operador de turno utilizará el extintor contra incendio manual. Véase ubicación en el plano de la Oficina, Anejo I-1. Si el fuego no es controlable y de ser posible, activará el sistema de “**Sapphire**” manualmente utilizando la palanca roja (Fire Alarm Sapphire), (Véase Anejo I-1), ubicada en la parte derecha de la caja de control del sistema, localizado en la pared derecha al atravesar la puerta del Cuarto de Máquinas. Esto activará o disparará el “**Sapphire**” de inmediato por los cuartos de operadores y máquinas. El empleado deberá desalojar el área de inmediato.

En caso que los empleados estén expuestos a un gran riesgo o peligro contra la seguridad, se desalojará de forma inmediata el área, y el Sistema de “**Sapphire**” se activará automáticamente.
 - 3. Identificar por donde deben desalojar los empleados de la OSI y en coordinación con el Oficial Principal de Servicios Administrativos, como se llevará a cabo el desalojo del edificio. El proceso debe ser tan rápido como sea posible, sin arriesgar la seguridad de los empleados. Si hay humo en el área, se deben mover a lugares que no estén afectados, bajando la cabeza cerca del piso. Se contactará al personal designado para casos de emergencia o desastre natural en la OSI, mediante llamadas telefónicas. (Véase Anejo A y A-1)
 - 4. Si la seguridad de los empleados no está en peligro o en riesgo de peligro, se deben desactivar los sistemas operativos de las distintas máquinas usando el procedimiento normal, explicado en el Anejo H. Además, se deben desactivar o desalojar los periferales críticos, los resguardos (**backups**), más recientes de los sistemas operativos y las aplicaciones existentes. De lo contrario, si es necesario e imprescindible desactivar todas las computadoras y sus respectivos discos, utilizará el interruptor de color rojo automático, ubicado en la pared izquierda superior del Cuarto de Máquinas.

IX. ESTRATEGIA EN CASO DE INUNDACIÓN POR AGUA

- A. Esta estrategia indica los pasos a seguir en caso de emergencia por agua:
1. identificar el área afectada;
 2. determinar por dónde entró o entra el agua;
 3. apagar todo el equipo electrónico en el Cuarto de Máquinas;
 4. bajar los interruptores electrónicos del Cuarto de Máquinas utilizando **el interruptor de color rojo**, ubicado en la pared izquierda superior del Cuarto de Máquinas;
 5. desactivar el Sistema Automático Contra Incendio "**Sapphire**", (Véase Anejo K);
 6. sacar del área afectada todo el equipo removible;
 7. informar el incidente utilizando la secuencia de llamadas (Véase Anejo A y A-1);
 8. llamar al servicio de emergencia y hospitales, de ser necesario (Véase Anejo G);
 9. tener a la mano el resguardo de todos los discos y llevarlos a la bóveda; y
 10. llevar a cabo un inventario del equipo y áreas afectadas (Véase Anejo L y L1).

X. ESTRATEGIA EN CASO DE FENÓMENOS NATURALES Y CLIMATOLÓGICOS

- A. El proceso será una combinación de los pasos a seguir, en caso de fuego e inundación por agua. En los casos de daños por agua y viento, se procederá de la siguiente manera:
1. instalar paneles de protección contra huracanes en todas las ventanas de la OSI, si aplica.
 2. interrumpir la energía eléctrica del Cuarto de Máquinas **utilizando el interruptor de color rojo**, ubicado en la pared izquierda superior de dicho cuarto, luego de haber desactivado los sistemas operativos.
 3. cubrir completamente el equipo no removible con carpas plásticas.
 4. dejar abiertas las puertas para que circulen las corrientes de aires, evitando posibles explosiones de ventanas (si aplica).
 5. desactivar el Sistema Automático Contra Incendio "**Sapphire**", (Véase Anejo K).
 6. mover todo equipo que sea removible a un lugar seguro.
 7. tener a la mano doble resguardo y proceder de acuerdo al Manual para el Manejo de Emergencias de la Compañía.

XI. ESTRATEGIA EN CASO DE SABOTAJE

A. Estrategia para el Proceso de Desalojo por Sabotaje

Cuando exista la necesidad de desalojar las facilidades involuntariamente o por la fuerza, se deben seguir las instrucciones que sean recibidas por la persona que esté amenazando con el sabotaje, o el que sea su intermediario. Inmediatamente que la persona se retire de la Compañía, informar lo sucedido, al personal indicado en el Anejo A y A-1. Luego se seguirán los pasos mencionados en el Artículo VII.

En los casos donde no haya necesidad de desalojar a los empleados y el equipo del Cuarto de Máquinas esté libre de peligro, se informará el incidente al Oficial Principal de Servicios Administrativos o su representante, para que realicen las llamadas de rigor a la policía o a cualquier otra agencia o institución que aplique. Véase la estrategia para notificar un incidente que se encuentra en el Artículo VII, de este Plan de Contingencia.

XII. ESTRATEGIA PARA RESTAURAR LAS OPERACIONES EN EL CENTRO DE CÓMPUTOS REMOTO

A. Cuando haya que tomar una decisión para restauración de los servicios, los empleados por instrucciones del Director de la OSI, moverán sus operaciones a un **Centro de Cómputos Remoto**. A continuación, se enumeran las tareas que se llevarán a cabo para reubicar a los empleados mientras permanezca la emergencia:

1. solicitar la activación del Centro Remoto. (Director)
2. reunión del personal de la OSI para la restauración (Anejo B) y determinación de los sistemas a restablecer parcial o totalmente.
3. hacer la coordinación con el personal del Centro de Cómputos Remoto y establecer responsabilidades de trabajo para regresar las operaciones de la OSI, para aquellos sistemas críticos que se requieran.
4. coordinar horario y tiempo de trabajo en el Centro de Cómputos Remoto, de manera que los trabajos de ambos centros puedan continuar sin interrumpir su itinerario.
5. establecer turnos de trabajo.
6. realizar el inventario de equipo, de acuerdo al Anejo L y L1. Coordinar con los servicios auxiliares la reparación o sustitución del equipo que esté fuera de servicio.
7. coordinar la transportación de máquinas, equipo de oficina, periferales y empleados al Centro de Cómputos Remoto.
8. localizar el resguardo "**backups**" de archivos y programas necesarios para continuar la producción en una escala limitada de duración. Si el incidente no afectó físicamente el Cuarto de Máquinas podemos utilizar el "**backup**" más reciente al momento del incidente, de lo contrario utilizaremos el "**backup**", que se encuentra en bóveda. (Estos "**backups**" deben estar acompañados de sus respectivas documentaciones).

9. activar las licencias de los programas a usarse, la aplicación crítica que se van a trabajar y restaurar la información de acuerdo a la aplicación.
10. realizar pruebas de las aplicaciones en el equipo del Centro de Cómputos Remoto.

XIII. APLICACIONES CRÍTICAS Y REQUERIMIENTOS MÍNIMOS

Estas aplicaciones son los programas necesarios para mantener las operaciones de la Compañía.

- A. Las aplicaciones indispensables para que la Compañía realice sus operaciones, se activarán en el Centro de Cómputos Remoto. Estas aplicaciones han sido seleccionadas por prioridad, no obstante, de ser necesario, se pueden incluir otras aplicaciones.
 1. Se mantendrá en una bóveda externa copia de la documentación necesaria de los procesos a seguir para procesar los sistemas y los resguardos “backups” de programas, archivos necesarios para su instalación y reestablecimiento del sistema.
 2. Cuando se reciba un aviso de huracán o cualquier fenómeno atmosférico se procederá de acuerdo al Manual de Manejo de Emergencias de la Compañía.

Los requisitos mínimos de la OSI, en los casos donde se necesite la activación del Centro de Cómputos Remoto, serán los siguientes:

Cinco (5) Servidores con las siguientes Configuraciones:

- Servidor #1 -> **FAS** (Sistema de Finanzas y Contabilidad) y **REOT** (Sistema de Bienes Raíces) **SQL SERVER**
 - Intel DUAL Xeon 2.8Ghz
 - 4 GB RAM
 - 220 GB de espacio de disco en RAID 5
 - 80 GB de espacio de Disco (no necesariamente en RAID)
- Servidor #2 -> **Exchange** (Correo Electrónico de la Compañía)
 - INTEL Xeon 2.8Ghz
 - 2 GB RAM
 - 200 GB de espacio de disco en RAID 5
- Servidor #3 -> **HR-Sense** (Nómina, Desarrollo Organizacional y Capital Humano) Oracle
 - INTEL Xeon 2.8Ghz
 - 2 GB RAM
 - 40 GB de espacio de disco en RAID 5
- Servidor #4 -> **WEBSITES/PROMOCIONES** (Correo Electrónico DDEC y CINE)
 - Intel DUAL Xeon 2.8Ghz

- 4GB RAM
- 100GB de espacio de disco en RAID
- Servidor #5 (opcional) -> **PARQUES** (Planos y fotos propiedades)
 - Intel DUAL Xeon 2.8Ghz
 - 4GB RAM
 - 300GB de espacio de disco en RAID

Véase Anejo E, Acuerdo Interagencial del Centro Control Remoto de los Sistemas de Información de Ocurrencia de un Incidente o un Desastre Natural.

XIV. VIGENCIA

Las disposiciones de este Plan entrarán en vigor inmediatamente que sean aprobadas por el Director Ejecutivo.

RECOMENDADO:


 Grace M. Díaz Pastrana
 Directora
 Desarrollo Organizacional
 y Capital Humano

Fecha: 9/16/10


 Jesús M. López Rodríguez
 Director
 Oficina de Sistemas de
 Información

Fecha: 9/17/10

APROBADO:


 José R. Pérez-Riera
 Director Ejecutivo Designado

Fecha: 26/10/2010

ANEJO A**LISTA DE PERSONAL A CONTACTAR
EN CASOS DE EMERGENCIA O DESASTRE NATURAL**

Compañía de Fomento Industrial

Cuadro: 787-758-4747

Posición	Nombre	Teléfono
Director Ejecutivo Interino	José R. Pérez Riera	939-218-0020
Oficial Principal de Servicios Administrativos	Hernán Rodríguez	787-399-3344
Director Oficina de Sistemas de Información	Jesús M. López	787-402-0304
Oficial de Sistemas de Información	José C. Pérez	787-758-4747-Ext.4396
Oficial de Sistemas de Información	Pedro Soto	787-362-3214
Oficial de Sistemas de Información	José J. González	787-758-4747-Ext. 4207
Oficial de Sistemas de Información	Marlene Ocasio	787-758-4747-Ext. 4621
Técnico de Microcomputadoras	Edwin Quirós	787-758-4747-Ext. 4610
Analista y Programador de Sistemas	Marangely Gómez	787-758-4747-Ext. 4614
Técnico de Redes y Correo Electrónico	María T. Segarra	787-758-4747-Ext.4616
Técnico de Redes y Correo Electrónico	Leslie A. García	787-758-4747-Ext. 4619
Personal de Apoyo	Anabell García	787-758-4747-Ext.4624
Director, Desarrollo Organizacional y Capital Humano	Grace M. Díaz	787-370-9838
Gerente, División de Seguridad	Hernán Rodríguez	787-399-3344
Gerente, División de Servicios	Edward Monefeldt	787-406-3019
Gerente, División de Conservación y Planta Física	Edgardo Lugo	787-403-2499
Oficial Principal de Mercadeo y Comunicaciones	Sandra M. Gutiérrez	787-438-1388
Secretario del DDEC	José R. Pérez	939-218-2567
Secretario Auxiliar del DDEC	Edward Calvesbert	787-758-4747-Ext. 4742
Directora Ejecutiva, Corporación de Cine	Mariella Pérez	787-232-2131

**LISTA DE PERSONAL A CONTACTAR
EN CASOS DE EMERGENCIA O DESASTRE NATURAL**

Compañía de Comercio y Exportación

Cuadro: 787-294-0101

Posición	Nombre	Teléfono
Director Ejecutivo (base PRIDCO)	José R. Pérez Riera	787 758-4747-Ext. 2166
Subdirector Ejecutivo	Rafael Marín Pagán	787 294-0101-Ext. 2013
Director de Sistemas de Información	Francisco López Ortiz	787 294-0101-Ext. 2045
Gerente de Sistemas de Información	Carlos Soltero	787 294-0101-Ext. 2047
Especialista de Bases de Datos	Raúl Dávila	787 294-0101-Ext. 2048
Técnico de Servicios al Usuario	Miguel Negrón	787 294-0101-Ext. 2051
Técnico de Servicios al Usuario	José Delgado	787 294-0101-Ext.2053
Técnico de Servicios al Usuario	Marisol Polanco	787 294-0101-Ext. 2052
Programador	Manuel Adorno	787 294-0101-Ext. 2050
Asistente Administrativo Senior	Diana Gómez	787 294-0101 ext. 2046
Directora, Recursos Humanos y Relaciones Laborales	Jannette González Guzmán	787 294-0101 ext. 2067
Gerentes de Servicios Generales	Luis R. Pérez	787 294-0101-Ext. 2077

ANEJO B

PERSONAL ASIGNADO Y SUS ALTERNOS

Coordinador	Persona Asignada	Persona Alterna
Coordinador Plan de Contingencia	Jesús M. López Rodríguez	José D. Martínez Montes
Coordinador de Usuarios y Producción de la RED	Pedro Soto Meléndez	Jesús M. López Rodríguez
Coordinador de Restauración de Facilidades	José González Vélez	Pedro Soto Meléndez
Coordinador de Usuarios y Producción de Aplicaciones	Jesús M. López Rodríguez	Marlene Ocasio Santana José C. Pérez Curry
Coordinar Transportación y Compras	Anabell García Marrero	Marangely Gómez Hernández
Realizar llamadas	Anabell García Marrero	Marangely Gómez Hernández
Coordinador Administrativo	Hernán Rodríguez Schmidt	Edward Monefeldt Vélez

CADENA DE MANDO DE LA OFICINA DE SISTEMAS DE INFORMACIÓN

A continuación los nombres de empleados que responderán en ausencia de los Oficiales y/o Director de la Oficina de Sistemas de Información. Está compuesto en orden de mando.

Oficina del Director – Jesús M. López Rodríguez

- José D. Martínez Montes
- Pedro Soto Meléndez
- José González Vélez
- Marlene Ocasio Santana
- José C. Pérez Curry

Redes y Correo Electrónico – Jesús M. López Rodríguez

- Pedro Soto Meléndez
- José González Vélez
- Marlene Ocasio Santana
- José C. Pérez Curry

Bases de Datos – Pedro Soto Meléndez

- Jesús M. López Rodríguez
- José González Vélez
- Marlene Ocasio Santana
- José C. Pérez Curry

Desarrollo de Sistemas – Jesús M. López Rodríguez

- Marlene Ocasio Santana
- José C. Pérez Curry

Servicio y Apoyo al Usuario – José González Vélez

- Pedro Soto Meléndez
- Jesús M. López Rodríguez
- Marlene Ocasio Santana
- José C. Pérez Curry

ANEJO D

DIRECTORIO DE SUPLIDORES

Compañía	Dirección	Teléfono	Persona de Contacto
Dell		1-800-805-7545	Camila Terrazas
Nustream	Ave. de la Constitución #316 San Juan, PR 00901	787 724-4842 787 2204748	Juan M. Rodríguez Alexandria Castro Edwin Candelario
Data Access	Ave. Ponce de León 316, Suite 100 San Juan, PR 00901	787 977-8025	Edgardo de la Torre
Clary Corp. of PR	PO Box 9752 San Juan, PR 00908	787 764-2833	Germán Busó
Avant Technologies	PO Box 9359 Caguas, PR 00726-9359	787 746-9191	Ada Vega

Descripción del acondicionador de aire del Centro de Cómputos:

Marca: Liebert
Modelo: System 3
Volts: 200-230
Capacidad: 5 toneladas

Este servicio debe ser solicitado a través del Ing. Edgardo Lugo Arrufat, Gerente de la División de Conservación de Planta Física de PRIDCO.

ACUERDO INTERAGENCIAL PARA EL USO DE CENTRO DE
CONTROL REMOTO DE LOS SISTEMAS DE
INFORMACION DE OCURRIR UN INCIDENTE
O DESASTRE NATURAL

2008-000430

-----COMPARECEN-----

-----DE LA PRIMERA PARTE: La COMPAÑIA DE FOMENTO INDUSTRIAL DE PUERTO RICO (en adelante denominada como "CFI"), corporación pública del Estado Libre Asociado de Puerto Rico, con personalidad jurídica propia creada bajo la Ley Número 188 del 11 de mayo de 1942, según enmendada, seguro social patronal número 660-29-2871, representada en este acto por su Director Ejecutivo, Lodo. Boris Jaskille, quien es mayor de edad, soltero y vecino de San Juan, Puerto Rico.-----

-----DE LA SEGUNDA PARTE: La Compañía de Comercio y Exportación de Puerto Rico (en adelante denominada como "CCE"), una corporación pública del Gobierno del Estado Libre Asociado de Puerto Rico creada en virtud de la Ley Núm. 323 de 28 de diciembre de 2003, según enmendada, seguro social patronal número 660-63-9355, representada por el Sr. Juan Manuel Román Castro, Director Ejecutivo Designado, quien es mayor de edad, casado y vecino de San Juan, Puerto Rico.-----

-----EXPONEN-----

-----Para cumplir con la Ley 151 del 22 de junio de 2004, conocida como "Ley de Gobierno Electrónico", la cual le impone a las agencias y entidades del Gobierno del Estado Libre Asociado de Puerto Rico el crear un andamiaje que garantice controles efectivos con relación a la seguridad de los sistemas de información que sustentan las operaciones y activos gubernamentales. Así como para también cumplir con la Política Núm. TIG-003 establecida por la Oficina de Gerencia y Presupuesto, que establece que las agencias del Gobierno de Puerto Rico mantendrán un Plan de Contingencia donde incluirán las medidas necesarias a considerarse en caso de una emergencia o desastre natural que incapacite parcial o totalmente las facilidades de las áreas de Sistemas de Información y realizarán acuerdos con otras agencias para establecer un centro de cómputos remoto, desde donde puedan ser procesados aquellos sistemas que se hayan definido como críticos en el Plan de Mecanización de las Agencias.-----

-----Las Oficinas de Sistemas de Información de la CFI y de CCE, (en adelante, ambas conjuntamente denominadas las Agencias), han acordado que de surgir algún incidente que obstaculice las operaciones de uno de sus respectivos Centros de Cómputos, la Agencia con el Centro de Cómputos funcional servirá de centro alterno para el procesamiento de los sistemas críticos de la Agencia cuyo Centro de Cómputos esté afectado. A la Agencia que provea a la otra el uso de las facilidades de su Centro de Cómputos se le conocerá como Centro Alterno.

-----CLAUSULAS Y CONDICIONES-----

-----PRIMERO: Ambas Agencias definieron los sistemas críticos a ser procesados y las especificaciones mínimas de equipo para su procesamiento. Las mismas se incluyen en los anejos 1 y 2, los cuales se incorporan y se hacen formar parte del presente acuerdo interagencial.-----

-----SEGUNDO: Después de haber terminado la emergencia se reunirán los Coordinadores, Directores Ejecutivos y los Administradores de las Agencias, según establecidos en el Plan de Contingencia, para activar los planes previamente definidos.-----

-----TERCERO: El Centro Alterno pondrá a la disposición de la Agencia afectada el equipo necesario para que pueda reestablecer las operaciones según especificado en sus respectivos planes de contingencia.-----

-----CUARTO: El Centro Alterno coordinará turnos de trabajo que no interrumpa con los trabajos de su Agencia.-----

-----QUINTO: La Agencia afectada es responsable de la localización de los resguardos de programas, archivos y documentaciones de la bóveda y de la transportación de equipo, personal y materiales al Centro Alterno.-----

-----SEXTO: El uso de equipo y tiempo de proceso en el Centro Alterno será libre de costo para la Agencia que lo utilice.-----

-----SEPTIMO: Las Agencias realizarán pruebas periódicas para verificar, y de ser necesario, actualizar los procedimientos de las operaciones.-----

-----OCTAVO: Las partes podrán dar por terminado este Contrato sin necesidad de mostrar causa alguna, mediante notificación por escrito a la otra parte con seis (6) meses de anticipación a la fecha de terminación.-----

-----NOVENO: El desempeño negligente de sus obligaciones o el abandono de éstas por alguna de las partes, se considerará como una violación de este Acuerdo y será causa suficiente para que la otra parte lo dé por terminado sin necesidad de notificación previa.-----

-----DECIMO: Conforme a lo dispuesto en el Artículo 3.3 (c) (d) de la Ley de Ética Gubernamental, según enmendada, cada una de las partes comparecientes certifica que los funcionarios autorizados a contratar a nombre de la CCE y de la CFI o algún miembro de su unidad familiar, no tuvo, ni ha tenido, durante los últimos cuatro (4) años antes de ocupar sus cargos, directa o indirectamente, interés pecuniario en la entidad o negocios del Acuerdo.-----

-----UNDECIMO: Las Agencias aseguran que han cumplido con todos los procedimientos para poder contratar y para llevar a cabo lo aquí descrito y que no existe ninguna ley, reglamentación o regla que las Agencias necesiten cumplir que prohíba otorgar este Acuerdo.-----

-----DUODECIMO: El presente constituye el único acuerdo entre las partes sobre el asunto descrito anteriormente y suspende o deja sin efecto cualquier otro acuerdo anterior, negociaciones, entendidos y otros asuntos, escritos o verbales, con respecto a lo acordado en este Acuerdo. Este Acuerdo no podrá ser modificado, cambiado o enmendado, excepto a que se haga por escrito, con la firma autorizada de representantes autorizados de cada parte.-----

-----DECIMOTERCERO: CONFLICTO DE INTERESES. Cada una de las partes reconoce que, en el descargo de sus funciones profesionales tienen un deber de lealtad completa hacia la otra parte, lo que incluye el no tener intereses adversos al otro organismo gubernamental. Estos intereses adversos incluyen la representación de clientes que tengan o pudieran tener intereses encontrados con las partes. Esta decir, además, incluye la obligación continua de divulgar a las partes, todas las circunstancias de sus relaciones con clientes y terceras personas y cualquier interés que pudiere influir en CCE y CFI al momento de otorgar este Acuerdo o durante su vigencia.-----

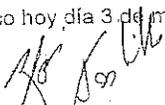
La otra parte representa intereses encontrados cuando, en beneficio de un cliente, es su deber promover aquello o que debe oponerse en cumplimiento de sus obligaciones para con otro cliente anterior, actual o potencial. Representa intereses en conflicto, además, cuando su conducta es descrita como tal en las normas éticas reconocidas a su tipo de entidad, o en las leyes y reglamentos del Estado Libre Asociado de Puerto Rico.-----

Ambas partes reconocen el poder de fiscalización del principal ejecutivo de la otra parte con relación al cumplimiento de las prohibiciones aquí contenidas. De entender el principal ejecutivo de una parte que existe o han surgido intereses adversos para con la otra parte, le notificará por escrito sus hallazgos y su intención de resolver el contrato en el término de treinta (30) días. Dentro de dicho término, la parte notificada podrá solicitar una reunión al principal ejecutivo de la parte que notifica para exponer sus argumentos a dicha determinación de conflicto, la cual será concedida en todo caso. De no solicitarse dicha reunión en el término mencionado, o de no solucionarse satisfactoriamente la controversia durante la reunión concedida, este acuerdo quedará resuelto.

---DECIMOCUARTO: Ninguna prestación o contraprestación objeto de este Acuerdo podrá exigirse hasta tanto el mismo se haya presentado para registro en la Oficina del Contrator a tenor con lo dispuesto en la Ley Núm. 18 de 30 de octubre de 1975, según enmendada.

---DECIMOQUINTO: Este Acuerdo no conlleva desembolso por parte de ninguna de las Agencias y tendrá una vigencia de cinco (5) años a partir de su otorgamiento.

--Y PARA QUE ASI CONSTE, las partes suscriben este Acuerdo en la Ciudad de San Juan, Puerto Rico hoy día 3 de marzo de 2008.


Ldo. Boris Jaskille
Director Ejecutivo
Compañía de Fomento Industrial


Sr. Juan M. Román Castro
Director Ejecutivo Designado
Compañía de Comercio y Exportación

REQUISITOS DE HARDWARE NECESARIOS PARA RECUPERAR EL MÍNIMO DEL AMBIENTE DE SISTEMAS DE INFORMACIÓN DE CFI

Cinco (5) Servidores con las siguientes Configuraciones:

- Servidor #1 -> **FAS** (Sistemas de Finanzas y Contabilidad) y **REOT** (Sistema de Bienes Raíces) **SQL SERVER**
 - Intel DUAL Xeon 2.8Ghz
 - 4 GB RAM
 - 220 GB de espacio de Disco en RAID 5
 - 80 GB de espacio de Disco (no necesariamente en RAID)

- Servidor #2 -> **Lotus Notes** (Correo Electrónico de PRIDCO)
 - INTEL Xeon 2.8Ghz
 - 2 GB RAM
 - 200 GB de espacio de Disco en RAID 5

- Servidor #3 -> **HR-SENSE** (Nómina, Recursos Humanos/Oracle)
 - INTEL Xeon 2.8Ghz
 - 2 GB RAM
 - 40 GB de espacio de Disco en RAID 5

- Servidor #4 -> **EXCHANGE** (Correo Electrónico DDEC y Cine)
 - Intel DUAL Xeon 2.8Ghz
 - 4GB RAM
 - 100GB de espacio de Disco en RAID

- Servidor #5 (opcional) -> **PARQUES** (Planos y fotos propiedades)
 - Intel DUAL Xeon 2.8Ghz
 - 4GB RAM
 - 300GB de espacio de Disco en RAID

Equipo adicional disponible:

- Tape Drive SDLT 320 con conexión SCSI

Facilidades necesarias:

El Director Ejecutivo de la Compañía de Comercio y Exportación de Puerto Rico (CCE), a través de la Directora de la Oficina de Sistemas de Información, nos indica que se habilitarán dos (2) salones del sexto (6to) piso del edificio principal de CCE con:

- Veinte (20) áreas de trabajo con facilidades de:
 - Teléfono
 - Internet (del usuario tener autorización)
- Facilidades de fotocopiar
- Facilidades de impresión
- Facilidades de fax



REQUISITOS DE HARDWARE NECESARIOS PARA RECUPERAR EL MÍNIMO DEL AMBIENTE DE SISTEMAS DE INFORMACIÓN DE LA CCE

Seis (6) Servidores con las siguientes configuraciones:

- Servidor #1 -> **EXCHANGE**
 - Intel DUAL Xeon 3Ghz
 - 4 GB RAM
 - 220 GB de espacio de Disco en RAID 5
 - 80 GB de espacio de Disco (no necesariamente en RAID)

- Servidor #2 -> **FILE SERVER**
 - INTEL Xeon 3Ghz
 - 2 GB RAM
 - 220 GB de espacio de Disco en RAID 5

- Servidor #3 -> **HR-SENSE**
 - INTEL Xeon 3Ghz
 - 2 GB RAM
 - 40 GB de espacio de Disco en RAID 5

- Servidor #4 -> **VMWARE 1**
 - Intel DUAL Xeon 3Ghz
 - 4GB RAM
 - 300GB de espacio de Disco en RAID 5 (preferiblemente RAID 10)

- Servidor #5 -> **VMWARE 2**
 - Intel DUAL Xeon 3Ghz
 - 4GB RAM
 - 300GB de espacio de Disco en RAID 5 (preferiblemente RAID 10)

- Servidor #6 -> **TIVOLI**
 - PowerPC Processor 2Ghz
 - 2GB RAM
 - 300GB de espacio de Disco (no necesariamente en RAID)
 - Acceso a TAPE DRIVE ULTRIUM LTO2

Equipo adicional disponible:

- Tape Drive ULTRIUM LTO 2 con conexión SCSI o FIBER (la conexión tiene que ser compatible con las especificaciones del Servidor #5 en la lista anterior)

Facilidades necesarias:

El Director Ejecutivo de la Compañía de Fomento Industrial (CFI), a través del Director de la Oficina de Sistemas de Información, nos indica que se habitará el Teatrito del cuarto piso del edificio principal de CFI con:

- Veinte (20) áreas de trabajo con facilidades de:
 - Teléfono
 - Internet (del usuario tener autorización)
- Facilidades de fotocopiar
- Facilidades de impresión
- Facilidades de fax



Estado Libre Asociado de Puerto Rico
Commonwealth of Puerto Rico
OFICINA DEL CONTRALOR
Office of the Comptroller
San Juan, Puerto Rico

30992008000430050805

CERTIFICACIÓN
CERTIFICATION

SOBRE OTORGAMIENTO DE CONTRATO, ESCRITURA O DOCUMENTO RELACIONADO
REGARDING THE EXECUTION OF CONTRACTS, DEEDS AND OTHER RELATED DOCUMENT

Código de Entidad 3099
Entity Code

Número de Contrato: 2008-000430
Contract Number

Fecha de Otorgamiento (dd/mm/aa) 03/03/08
Date of execution (dd/mm/yy)

Cuantía Total \$0.00
Total amount

Cuentas: N/A
Accounts

Código del Tipo de Contrato 26-ACUERDOS NO FINANCIEROS
Contract Type Code

Exento 10-No conllevan un desembolso de fondos
Exempt

Orden (Aprobación o dispensa de algún organismo del Gobierno) _____
Authorization or waiver from another government entity

Vigencia desde (dd/mm/aa) 03/03/08 hasta (dd/mm/aa) 02/03/13
Effective date from (dd/mm/yy) to (dd/mm/yy)

Seguro Social Personal o Patronal 660-29-2871
Social Security Number

Contratista(s) COMPAÑIA DE FOMENTO INDUSTRIAL DE PR
Contractor

Representante(s) de la(s) Entidad(es) Gubernamental(es) JUAN M. ROMAN CASTRO
Government Representative(s)

se somete la presente certificación en un cumplimiento con la Carta Circular promulgada por el Contralor de Puerto Rico y en cumplimiento con el Reglamento Núm. 33 Sobre Registro de Contratos, Escrituras y Documentos Relacionados y Envío de Copias a la Oficina del Contralor. Esta debe ser remitida a la Oficina del Contralor.

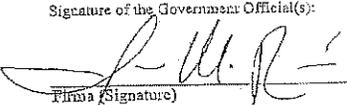
this certification is submitted in compliance with the instructions issued by the Comptroller of Puerto Rico and in accordance with Regulation No. 33, regarding the Registration of Contracts, Deeds and Other Related Documents and the Mailing of such Copies to the Comptroller's Office by the government entity.

Los suscribientes certificamos haber otorgado hoy el contrato descrito en este documento.
The undersigned, certify having that the contract described in this document was executed on this date.

En (ciudad) SAN JUAN, PR, Puerto Rico, hoy (dd/mm/aa) 03/03/08
Puerto Rico, today (dd/mm/yy)

Firma(s) Contratista(s):
Signature of the Contractor(s):

SS: 660-29-2871
Firma (Signature)
COMPAÑIA DE FOMENTO INDUSTRIAL DE PR
Letra de molde (print)

Firma(s) Funcionario(s) Gubernamental(es):
Signature of the Government Official(s):

Firma (Signature)
JUAN M. ROMAN CASTRO
Letra de molde (print)

RETENCION Y ROTACION DE RESGUARDOS

En este anejo presentamos el movimiento de los diferentes tipos de resguardos de información y su vida útil.

RESGUARDO DIARIO:

El resguardo diario guarda todos los archivos que se actualizaron o modificaron durante el día. La retención de estos es de una semana.

RESGUARDO SEMANAL

Este consiste de todos los directorios con sus respectivos archivos del disco del sistema, mejor conocido como **RESGUARDO GENERAL**. La retención de este resguardo es de cuatro semanas. Dichos resguardos se efectúan los primeros días de cada semana del mes.

Anejo: Manual de Normas para el Manejo y Recuperación de los Resguardos "Backups" (SIF-NO-132) aprobado el 30 de enero de 2006.

LISTA DE AGENCIAS A LLAMAR EN CASO DE EMERGENCIA POR PRIORIDAD Y DIRECCION

Agencia	Dirección	Teléfono	Persona de Contacto
Cuerpo de Bomberos de Puerto Rico	Pda. 8 Fernández Juncos San Juan, Puerto Rico 00908	787 725-3444	Sra. Carmen Rodríguez
Fire Control Corporation	Avenida JT Piñero 1044 Caparra Terrace, P.O. Box 3318 Hato Rey, PR 00919	787 793-6060	Sr. Roberto Cruz Sr. Hilario Jorge
Policía Precinto Parada 15 Santurce	Calle Cera 902, Pda. 15 Santurce, PR	787 724-5996 787 343-2020	Oficial de Retén
Emergencias Médicas	Centro Médico / ASEM PO Box 2129 San Juan, PR 00922-2129	787 777-3535	Dr. Ernesto Torres
	Div. Operaciones Especiales Ave. Muñoz Rivera 506 Hato Rey, PR 00918	787 754-1007	Teniente Carlos Méndez
	San Juan Health Centre 150 Ave. de Diego San Juan, PR	787 725-0202	Emergencias
	Hospital Pavía Calle Profesor Augusto Rodríguez #1462 Pda. 22 Santurce, PR	787 727-6060	Dr. Charlie Gómez
	Hospital San Jorge 258Calle San Jorge Santurce, PR 00912	787 727-1000	Dra. Carmen Lebrón
Servicios Administrativos PRIDCO	1er. Piso	787-399-3344	Sr. Hernán Rodríguez
División de Seguridad PRIDCO	1er. Piso	787 406-3019	Sr. Hernán Rodríguez
		787 370-2401	Sr. Eddie Iñesta
División Conservación de Planta Física	1er. piso	787 403-2499	Ing. Edgardo Lugo
Compañía de Comercio y Exportación de PR	3er. piso	787 294-0101 939 639-9128	Sr. Francisco López, Director Sistemas de Información

PROCEDIMIENTO PARA DESACTIVAR SISTEMA OPERATIVO

Los Sistemas Operativos Microsoft Windows 2000 Server, Windows 2003 Server, Windows XP y Windows 2000 se desactivarán según se indica a continuación:

- Entrar al sistema con user y password autorizados
- Oprimir "Start"
- Escoger "Shut Down"
- Verificar que la selección sea "Shut Down"
- Oprimir "OK"
- Una vez el sistema operativo este completamente desactivado, apagar monitor, el CPU si procede, apagar baterías si alguna.

Sistemas Operativos LINUX

- Entrar al sistema con user y password autorizados
- Escribir Shut down -H now
- Una vez el sistema operativo este completamente desactivado, apagar monitor, el CPU si procede, apagar baterías si alguna.

EXTINTORES MANUALES PARA FUEGO

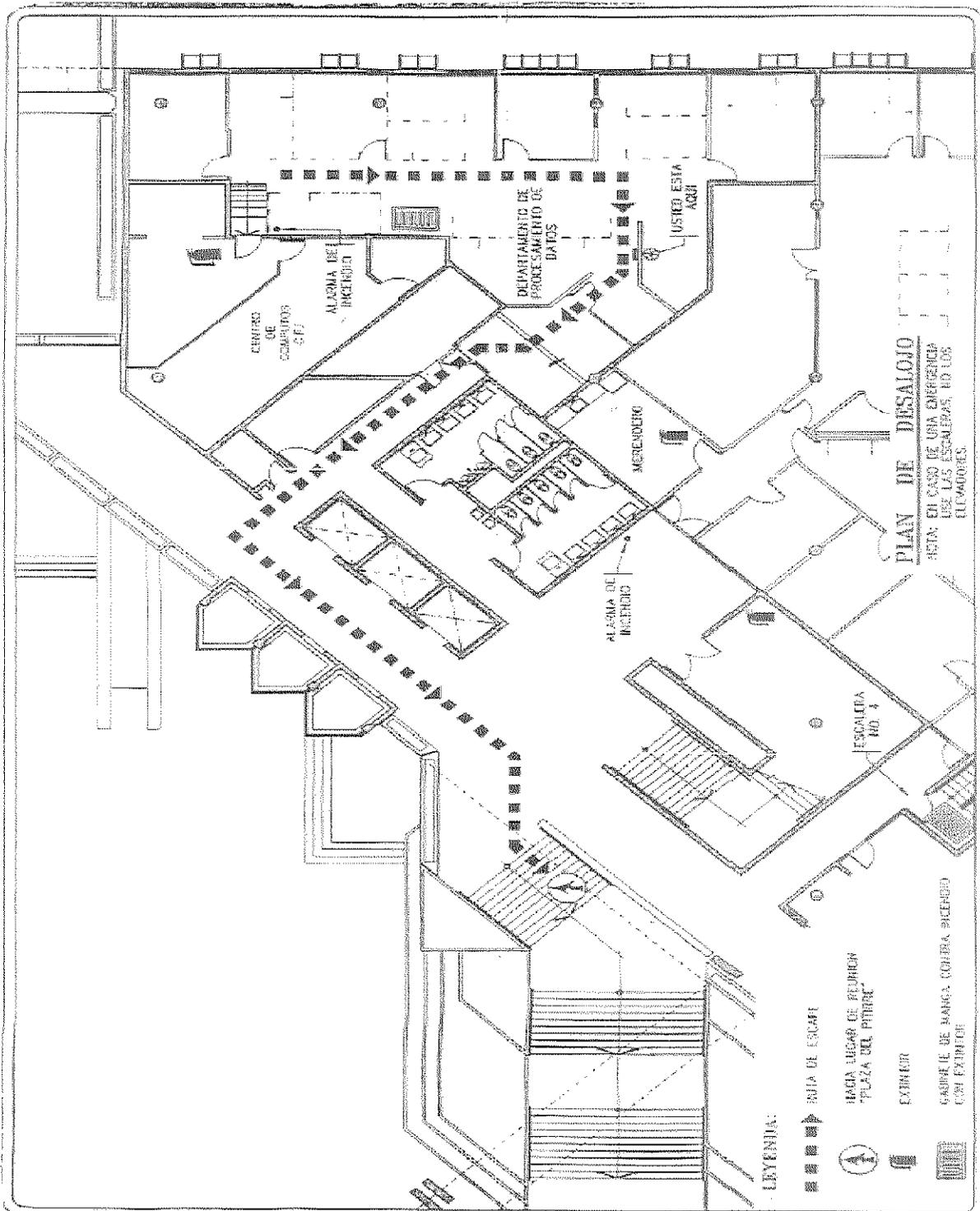
La Oficina de Sistemas de Información de la Compañía cuenta con un (1) gabinete de manga contra incendio, dos (2) extintores manuales distribuidos a través de la Oficina, (uno en el gabinete de la manga contra incendio y el otro en el cuarto de máquinas al lado izquierdo de la puerta de entrada) y un sistema "Sapphire" para fuego en el cuarto de máquinas.

Extintores Manuales:

Lugar	Cantidad	Capacidad
Cuarto de Máquinas	1	16 lbs.
Gabinete de manga contra incendio	1	16 lbs.

Anejo: Plano Ubicación Extintores

PLANO UBICACION EXTINTORES



**PROCEDIMIENTO PARA ACTIVAR
SISTEMA CONTRA INCENDIO AUTOMATICO**

la Oficina de Sistemas de Información cuenta con un Sistema Contra Incendios Automático, el cual nos garantiza y protege los equipos en las siguientes aéreas.

- Cuarto de Operaciones
- Cuarto de Máquinas (Servidores)

Pasos a Seguir:

1. Prender el Panel de Control (caja roja) ANSULAUTOPULSE® que se encuentra en la pared izquierda en el cuarto de máquinas (Servidores) "AC POWER".
2. Colocar el interruptor en posición **Normal**. Este se encuentra en la parte de abajo de la caja roja del panel de control ANSULAUTOPULSE®, en la pared izquierda en el cuarto de máquinas (Servidores).

Nota: De tener alguna falla abrir el panel rojo y darle a System Reset. Esto devuelve todo la configuración original.

**PROCEDIMIENTO PARA DESACTIVAR
SISTEMA AUTOMATICO CONTRA INCENDIOS**

Situaciones a considerar al desactivar el Sistema Automático Contra Incendios en la Oficina de Sistemas de Información.

Paso a Seguir

1. Colocar el interruptor en posición "Disconnet". Este se encuentra en la parte de abajo de la caja roja, panel de control ANSULAUTOPULSE®, en la pared izquierda en el cuarto de máquinas (Servidores).

Nota: Este proceso solamente desactiva la botella color roja del "Sapphire", por lo que el resto del equipo continuará con sus funciones tales como: el monitoreo de los sensores de incendio y alarma de incendio.

INSTRUCCIONES

Hoja para Inventario de Equipo y Áreas Afectados

I. PROPÓSITO

Se utiliza para llevar un control del equipo defectuoso de las áreas de trabajo, afectadas.

II. TRÁMITE

El Oficial Principal, Director o Gerente del área afectada completará el formulario y lo enviará al Director de la Oficina de Sistemas de Información. El Director de la Oficina de Sistemas de Información coordinará con su personal las evaluaciones y acción a seguir para restaurar los servicios de las áreas de trabajo afectadas.

III. DISTRIBUCIÓN

Original – Oficina de Sistemas de Información

Copia – Oficina afectada

IV. IMPRESIÓN

Material: Papel Blanco

Impresión: Medio Electrónico

Tamaño: 8 ½ x 11

**COMPAÑIA DE FOMENTO INDUSTRIAL DE PUERTO RICO
OFICINA DE DESARROLLO ORGANIZACIONAL Y PLANIFICACION INTERNA
DIVISION DE ANALISIS Y DOCUMENTACION DE SISTEMAS**

**NORMAS PARA EL MANEJO Y RECUPERACION DE LOS RESGUARDOS
"BACKUPS"**

(SIF-NO-132)

30 de enero de 2006

NORMAS PARA EL MANEJO Y RECUPERACIÓN DE LOS RESGUARDOS "BACKUPS"

I. PROPOSITO

Establecer los mecanismos necesarios para el manejo y recuperación de los resguardos "Backups".

II. NORMAS

- A. Para asegurar una administración ordenada y continua de los "backups" de los datos, aplicaciones y "softwares" utilizados en la Compañía se seguirán las disposiciones contenidas en la Sección A de estas Normas.
- B. Para asegurar la integridad de los "backups" realizados con el propósito de probar y revisar las cintas almacenadas en las diferentes localidades (Rack de cintas, Bóveda Local o Bóveda Externa) se llevará a cabo el proceso descrito en la Sección B, una vez por mes o cuando sea requerido por los usuarios de la Compañía.

III. DEFINICIÓN DE TERMINOS

- A. "Backups" – se entenderá como resguardos.
- B. Compañía – se referirá a la Compañía de Fomento Industrial de Puerto Rico.
- B. OSI – Oficina de Sistemas de Información.
- C. Resguardos – se referirá a las cintas, discos compactos (CD) y otros medios utilizados para almacenar información electrónica.

IV. GUIAS

A. Manejo de los "Backups"

A.1 – Forma de etiquetar las cintas magnéticas

Las cintas magnéticas serán identificadas con un número de control secuencial de acuerdo a los datos resguardados.

A.2 – Registro de Control de los "Backups"

Los Registros de Control contendrán todas las secuencias de los medios de "backups" incluyendo la siguiente información:

A.2ª - Registro Interno

- Número de cinta : Identificación de la secuencia de la cinta
- Fecha : Fecha en la cual se realizó el "backup"
- Comentarios : Algún suceso o evento relacionado al "backup"
- Hora de inicio : Hora de comienzo del "backup"
- Inicial oficial : Iniciales de la persona que efectuó el "backup"
- Fecha salida : Fecha en que el "backup" es enviado a una bóveda externa
- Fecha entrada : Fecha en que el "backup" regresa a la Compañía

A.2b – Registro Externo

- Nombre y firma empleado : Firma del empleado que atiende al funcionario
- Fecha del depósito : Fecha en que es almacenado en la bóveda externa
- Cantidad de cintas : Número de cintas entregadas
- Fecha del "backup" : Fecha en que fue realizado el "backup"
- Número de la cinta : Número secuencial del "backup"
- Archivos y/o servidores : Contenido de la cinta

Estos resguardos irán acompañados de un "log" impreso por el sistema, utilizado para hacer los resguardos conteniendo todo lo relacionado a la cinta.

El sistema utilizado para los "backups" tendrá integrado un inventario completo de todos los resguardos por fechas y contenido de los mismos.

Las personas responsables de manejar el registro de control serán los Técnicos de Redes y Correo Electrónico y el Gerente del Área de Operaciones de la Compañía.

El proceso de resguardar los datos de la Compañía será efectuado todos los días laborables del año.

A.3 – Almacenaje de los "Backups"

El almacenaje de los "backups" estarán guardados en las siguientes localidades:

Un armario con cerradura para cintas identificado con el número de secuencia y contenido de aplicaciones.

- Una bóveda local para guardar los medios que serán enviados a la bóveda de una institución fuera de la Compañía.
- Los "backups" históricos y mensuales estarán en la bóveda externa para asegurar los mismos.

La persona responsable de entregar y buscar los "backups" a la institución externa será el Gerente del Área de Operaciones.

B. Recuperación de los "Backups"

1. Se seleccionará al menos un soporte del backup semanal y uno mensual de entre todas las cintas de los "backups" realizados.
2. Se elegirán para recuperar al menos dos archivos de estos "backups" lo que deben de estar en distintos lugares de la cinta.
3. Utilizando la documentación "log" de recuperación del "backup", se bajarán los archivos a una localidad temporera para ser examinado.
4. Al finalizar el procedimiento se completará un registro de control con la siguiente información:
 - Fecha de prueba
 - Equipo
 - Archivos recuperados
 - Se recuperó correctamente "sí o no"
 - Problemas encontrados
 - Oficial de OSI

Este registro de control será iniciado por el Técnico a cargo de Operaciones.

El sistema utilizado para recuperar los archivos contará con su propio "log" electrónico, el cual mantendrá un historial de todas las cintas y catálogos de las mismas. En los manuales provistos por el programa de hacer los "backup", se encontrarán todas las instrucciones para hacer las restauraciones de los archivos. El Técnico se referirá a dichos manuales, en caso de ser necesario.

RECOMENDACIÓN PARA LA APROBACIÓN:


Lcdo. José L. Ramírez
Subdirector Ejecutivo Senior

Fecha: 13 febrero/06

APROBADO:


Lcdo. Jorge Silva Puras
Director Ejecutivo

Fecha: 17/02/06



FOMENTO

ESTADO LIBRE ASOCIADO DE PUERTO RICO
Compañía de Fomento Industrial

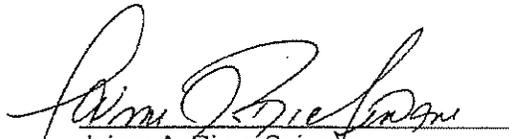
CERTIFICACIÓN

Yo, Jaime A. Riera Seivane, Secretario Corporativo, Interino, de la Compañía de Fomento Industrial de Puerto Rico, CERTIFICO que:

"La Junta de Directores de la Compañía de Fomento Industrial de Puerto Rico, en su reunión del 8 de marzo de 2006, aprobó las *Normas para el Manejo y Recuperación de los Resguardos ("Backups")* (SIF-NO-132). Estas Normas establecen los mecanismos necesarios para el manejo y recuperación de los "backups" de los datos, aplicaciones y "softwares" utilizados en la Compañía de Fomento Industrial."

En San Juan, Puerto Rico, a 16 de marzo de 2006.




Jaime A. Riera Seivane

Affidávit Núm.: 387

Jurada y suscrita ante mí por Jaime A. Riera Seivane, mayor de edad, casado, abogado y vecino de San Juan, Puerto Rico, en su carácter de Secretario Corporativo Interino de la Compañía de Fomento Industrial, a quien doy fe de conocer personalmente.

En San Juan, Puerto Rico, a 16 de marzo de 2006.




Notario Público

COMPAÑIA DE FOMENTO INDUSTRIAL DE PUERTO RICO
OFICINA DE DESARROLLO ORGANIZACIONAL Y PLANIFICACION INTERNA
DIVISION DE ANALISIS Y DOCUMENTACION DE SISTEMAS

**PROCEDIMIENTO PARA EL MANEJO DE EMERGENCIAS DE LA
OFICINA DE SISTEMAS DE INFORMACION
MA-ADM-146**

EQUIPO DE TRABAJO

José Reyes Rivera- Gerente
Ricardo Santiago- Especialista en Sistemas y Procedimientos Administrativos

COMPAÑÍA DE FOMENTO INDUSTRIAL DE PUERTO RICO
MANUAL DE SISTEMAS Y PROCEDIMIENTOS OPERACIONALES

Asunto: PROCEDIMIENTO PARA EL MANEJO DE EMERGENCIAS DE LA OFICINA DE SISTEMAS DE INFORMACION	Procedimiento Núm. MA-ADM-146	Página 1 de 8
--	----------------------------------	---------------

I. PROPÓSITO

Establecer un Plan de Recuperación de Desastres adecuado y que permita al personal de la Oficina de Sistemas de Información recuperarse efectivamente de un desastre en un tiempo mínimo.

II. BASE LEGAL

Este Procedimiento se promulga en virtud de las disposiciones contenidas en:

- A. Ley Núm. 188 del 11 de mayo de 1942, según enmendada, la cual crea la Compañía de Fomento Industrial de Puerto Rico;
- B. La Ley Núm. 203, del 29 de diciembre de 1997, Ley que enmienda la Ley Núm. 188 del 11 de mayo de 1942;
- C. Reglamento Interno (By-Laws) de la Compañía de Fomento Industrial de Puerto Rico aprobado el 7 de enero de 1958, según enmendado;
- D. Carta Circular Núm. 96-01 del Comité del Gobernador sobre Sistemas de Información.

III. DEFINICIÓN DE TÉRMINOS

- A. Aplicaciones de Producción – Todo programa creado por los programadores de la Compañía.
- B. Centro – Oficina de Sistemas de Información de la Compañía.
- C. Centro de Cómputos – Área localizada en la Oficina de Sistemas de Información donde se encuentran los equipos de procesamiento y almacenamiento de datos.
- D. Centro de Cómputos Alternos – Área provisional donde se localizará el Centro.
- E. Centro de Cómputo Interno – Área provisional dentro de la Compañía donde se verificarán las operaciones del Centro.
- F. Centro de Cómputo Externo – Área provisional en la Oficina de Nueva York en el caso que se afecte el Centro de Cómputos de la Compañía por un daño mayor.
- G. Compañía – Compañía de Fomento Industrial de Puerto Rico.
- H. Equipos Periféricos – Todos aquellos equipos que van conectados a un computador (Ej. Monitor, Mouse, etc.)

- I. Equipo de Estimado de Daños – Funcionarios o encargados para verificar daños dentro de la Oficina de Sistemas de Información.
- J. Equipos de Recuperación de Operaciones – Se referirá al equipo creado por la Oficina de Sistemas de Información para el manejo de emergencias dentro de su oficina.
- K. Equipo de Recuperación Gerencial – Se referirá al equipo creado por el Director(a) Ejecutivo(a) para el manejo de emergencias en la Oficina de Sistemas de Información.
- L. "Hardware" – Es el equipo eléctrico, electrónico y mecánico que es parte integral de un sistema computadorizado. El "hardware" necesita instrucciones del "software" para llevar a cabo sus tareas.
- M. Red de Comunicaciones (Network) – Conjunto de equipos electrónicos interconectados mediante cables o equipos inalámbricos y otros dispositivos de telecomunicaciones.
- N. Servidor – Computadora que provee las facilidades de almacenamiento de archivos, instrucciones y ejecución de aplicaciones críticas.
- O. "Software" – Serie de aplicaciones que le ordenan al "hardware" cómo llevar a cabo las tareas. Incluye aplicaciones diseñadas para ayudar a los usuarios en el desempeño de sus tareas.

IV. UNIDADES PARTICIPANTES

- A. Oficina de Sistemas de Información
- B. Área de Desarrollo de Infraestructura

V. NORMAS

- A. La Oficina de Sistemas de Información será la responsable de mantener, identificar y documentar los equipos de trabajo crítico, especialmente, el equipo gerencial que controlaría las operaciones críticas en caso de emergencia.
- B. La Oficina de Sistemas de Información tendrá que hacer simulacros de emergencias semestralmente.
- C. Los equipos se dividirán en cuatro, a saber:
 - a. Equipo Gerencial de Recuperación
 - b. Equipo de Valorización y Daños
 - c. Equipo de Recuperación de Operaciones en facilidades alternas
 - d. Equipo de Establecimiento de facilidades primarias
- D. La Oficina de Sistemas de Información identificará las aplicaciones críticas que se procesen en el Centro de Cómputos. Además, identificará y documentará las funciones críticas.

- E. La Oficina de Sistemas de Información creará dos equipos dentro de su oficina que se llamarán Equipo de Computación Central y Equipo Electrónico de Computación y de Comunicaciones con los Centros de Cómputos Alternos, Externos e Internos.
- F. La Oficina de Sistemas de Información mantendrá un inventario de aplicaciones y componentes del Sistema Operativo, éstos deben identificar y documentar todas las aplicaciones críticas y componentes del Sistema Operativo necesarios para ejecutar las aplicaciones críticas.
- G. La Oficina de Sistemas de Información deberá mantener en un lugar seguro un inventario de:
 - a. Papel
 - b. Cinta de Backup
 - c. Cheques y formas especiales
 - d. Doce (12) computadoras portátiles
 - e. Hub/switches necesarios para crear un Net Work
- H. La Oficina de Sistemas de Información debe identificar un lugar seguro con espacio necesario para:
 - a. el equipo electrónico de computación.
 - b. personal operacional de apoyo que trabajan en las operaciones y para materiales de operación de recuperación.

VI. RESPONSABILIDADES

- A. La Oficina de Sistemas de Información será responsable de:
 - 1. Evaluar las vulnerabilidades de la organización dentro y fuera del Área de Sistemas de Información, puntos de referencia existentes y capacidades planeadas comparado con las mejores prácticas;
 - 2. Revisar planes de respuestas a emergencias;
 - 3. Dar prioridad a planes de acción basados en efectividad, eficiencia y sustentabilidad;
 - 4. Implantar planes de recuperación apropiados para cada función crítica;
 - 5. Planificar pruebas para adaptación y práctica sobre un plan establecido; y
 - 6. Desarrollar planes alternos para minimizar las consecuencias a las operaciones de apoyo a las áreas de servicios a las industrias antes y después del incidente.
- B. Área de Desarrollo de Infraestructura será responsable de:
 - 1. Coordinar con la Oficina de Sistemas de Información las personas que van a pertenecer al equipo de recuperación;
 - 2. Proveerle los servicios necesarios de espacio, corriente eléctrica, mesas y sillas para comenzar con el proceso de recuperación y

3. Darle un inventario de la propiedad dañada a la Oficina de Sistemas de Información.

VII. FORMULARIOS UTILIZADOS

- | | |
|---------|--|
| SIF-032 | Lista de Cotejo de Sistemas para Recuperación de Desastre y Simulacros |
| SIF-033 | Tabla Descripción de Daños |

VIII. DOCUMENTOS RELACIONADOS

- | | |
|-------------|---|
| MPE-DCI-210 | Plan Operacional de Emergencias |
| MPE-DCI-211 | Procedimiento a Seguir en Caso de Huracán o Temporal |
| MPE-DCI-212 | Procedimiento Situaciones de Emergencias provocadas por Terremotos |
| MPE-DCI-213 | Procedimiento a Seguir en Caso de Incendio |
| MPE-DCI-214 | Procedimiento Amenaza de Bomba en el Edificio de Fomento |
| MPE-DCI-215 | Procedimiento para Desalojar el Edificio |
| MPE-DCI-216 | Procedimiento Rutas de Desalojo del Edificio en Casos de Emergencias |
| MPE-DCI-218 | Procedimiento Atención de los Industriales como Consecuencia de Desastres Naturales |

IX. PROCESO

A. Identificación del Personal Crítico y Equipos de Trabajo

Director, Oficina de
Sistemas de Información

1. Solicitará al Director(a) Ejecutivo(a) que nombre un Equipo Gerencial de Recuperación.

Estos equipos deberán tener integrantes de las siguientes Áreas: Finanzas, Promoción, Desarrollo de Infraestructura, Recursos Humanos, y Relaciones Laborales y de las Oficinas de Promoción, Sistemas de Información, Asesoría Legal General; y la División de Riesgos y Seguros.

2. Creará el Equipo de Estimado de Daños, Equipo de Recuperación de facilidades alternas y Equipo de Establecimiento de Facilidades Alternas.

B. Funciones de los Equipos Designados para la Recuperación de la Oficina de Sistemas de Información

Equipo Gerencial
de Recuperación

1. Recibirá notificación del desastre.
2. Recibirá los informes de daños SIF-033 "Tabla de Descripción de Daños" enviados por las diferentes oficinas de la Compañía.
3. Determinará si declarará un desastre.
4. Coordinará la activación de las facilidades alternas.
5. Coordinará todas sus actividades relacionadas con:
 - a. Compañías de Seguro
 - b. Movimiento de Personal y materiales críticos
 - c. Adquisición de máquinas de materiales críticos para continuar con las operaciones
 - d. Asuntos Legales

- e. Asuntos de Recursos Humanos
- f. Asuntos relacionados con la Unión.

Equipo de Estimado de Daños

6. Revisará e informará al Equipo Gerencial de Recuperación la severidad de los daños y el tiempo aproximado para restablecer operaciones normales relacionadas a los Sistemas de Información en la Compañía.

Equipo de Recuperación Operaciones en Facilidades Alternas

7. Activará el Centro Cómputos en las de facilidades alternas.
8. Buscará materiales, programas y data necesaria para las operaciones.
9. Realizará las operaciones del Centro de Cómputos necesarias para procesar todas las aplicaciones críticas de la Compañía.
10. Enviará informe al equipo de recuperación gerencial sobre la situación de la estructura operacional de la Oficina de Sistemas de Información.

Equipo de Establecimiento de Facilidades Primarias

11. Establecerá facilidades primarias del Centro de Cómputos.
12. Se reportará al equipo recuperación gerencial.

C. Identificación de Aplicaciones Críticas que se Procesan en la Oficina de Sistemas de Información

Director, Oficina de Sistemas de Información

1. Identificará y documentará todas las aplicaciones críticas que utilizará la Compañía.
2. Completará un inventario de cada una de las aplicaciones que identifique como críticas para la Compañía.

D. Identificación y Documentación de Funciones Críticas

Director, Oficina de Sistemas de Información

1. Identificará y documentará todas las funciones críticas de la Oficina de Sistemas de Información. Estas funciones incluirán las siguientes tareas:

- a. activación y desactivación del equipo electrónico de computación.
- b. activación y desactivación de los equipos y líneas de comunicaciones.
- c. restauración de los programas y archivos de las aplicaciones críticas con la frecuencia necesaria.
- d. mantener el resguardo (backup) de datos.
- e. facilidades internas y externas para almacenar los resguardos.
- f. puntos de control y cuadro de información.
- g. generación de informes y preparación de lista de distribución de informes.

E. Pruebas del Plan de Recuperación de Desastres

- | | |
|---|---|
| Director, Oficina de Sistemas de Información | 1. Hará un simulacro semestralmente, activando todos los equipos de apoyo de recuperación. |
| Equipo de Establecimientos de Facilidades Primarios | 2. Mejorará el plan basándose en los problemas encontrados. |
| Auditor | 3. Completará el Formulario SIF-032 "Lista de Cotejo de Sistemas para Recuperación Desastres y Simulacros". |
| | 4. Revisará todas las áreas de las pruebas y deberá rendir un informe. |

X. CLÁUSULA DEROGATORIA

Mediante la implantación de este Procedimiento se deroga todo proceso en conflicto con las disposiciones contenidas en este Procedimiento.

XI. FECHA DE EFECTIVIDAD

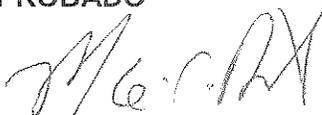
Las disposiciones contenidas en este Procedimiento entrarán en vigor una vez aprobado por la Directora Ejecutiva.

RECOMENDADO


Lcdo. José L. Ramírez
Subdirector Ejecutivo Senior

Fecha: 6 de abril de 2005

APROBADO


Lcda. Marie A. Robert
Directora Ejecutiva Designada

Fecha: 7 Abril 05.