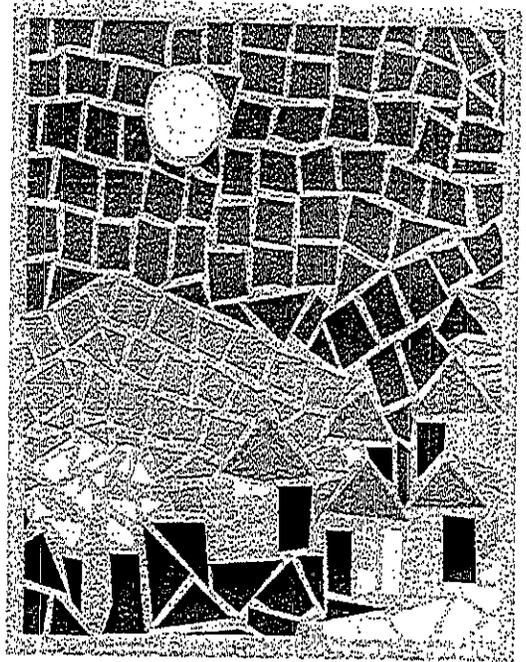


ESTADO LIBRE ASOCIADO
DE PUERTO RICO



**PLAN
DE CONTINGENCIA**

**ÁREA DE SISTEMAS
DE INFORMACIÓN**

**COMUNIDADES
ESPECIALES
PUERTO RICO**



Tabla de Contenido

	Página
I. Propósito.....	2
• Niveles de Acción.....	2 - 3
• Premisas.....	3 - 4
• Activación del Plan.....	4 - 5
II. Implantación	
• Efectividad.....	5
• Adiestramiento.....	5
• Equipo de Emergencia.....	6
• Estación Alterna.....	6
• Medidas de Seguridad.....	6 - 7
III. Previsión de Desastres	
• Desalojo por Emergencia o Fuego.....	7
• Fallas del Sistema Computadorizado.....	7 - 8
• Fallas en Comunicación.....	9
• Personal.....	9
IV. Administración del Plan	
• Actualización.....	10
• Ejercicios y Pruebas.....	10
• Evaluación.....	10 - 11
V. Anejos Incluidos	
• Destrucción Total, Severa y Parcial.	
• Estructura de Llamadas	
• Grupos de Trabajos	
• Planes para el Desalojo del Edificio	
• Definición de Prioridades de las Aplicaciones	
• Lista de Accidentes o Emergencias Cubiertas	
• Notificación de Eventos de Desastres	
• Movimiento de Equipo y Personal al Área de Sistemas de Información Alterno	
• Lista de Prioridad para Restauración	

I. PROPÓSITO:

Este plan tiene como propósito especificar el mayor número de decisiones previsibles que se deben tomar si ocurren eventos de desastre que imposibiliten la operación normal del Área de de Sistemas de Información (ASI), en forma alguna. El plan servirá de guía al personal de la Oficina de Comunidades Especiales (OCE) para enfrentar los eventos de desastre y establecer la manera de recuperar las operaciones de este.

Pretende por otro lado, implantar las guías para lograr el restablecimiento de las operaciones del Área de Sistemas de Información (ASI) y de los usuarios, en un tiempo razonable. Pretende reducir el número de decisiones que deban hacerse bajo la presión de una situación de emergencia. Sin embargo, no es sustituto para el ejercicio de un juicio inteligente, ni tampoco es un grupo de reglas rígidas que deben ser seguidas a cualquier costo.

Además, la Agencia integra este plan con el Plan de Emergencia General diseñado para cumplir con la Oficina de Emergencia del Estado Libre Asociado de Puerto Rico.

Representa una base para toda acción posterior. Como tal, debe ser incluido en todas las sesiones de entrenamiento de todos los empleados de la OCE que puedan ser afectados por un evento de desastre.

A. NIVELES DE ACCIÓN:

1. El Área de Sistemas de Información tiene dos (2) componentes importantes que es necesario distinguir entre el salón de Computadoras y las estaciones de trabajo o áreas de servicio.
2. El salón de computadoras centraliza el procesamiento de datos de todas las estaciones de servicio o áreas de trabajo que se encuentran diseminadas a través de las instalaciones. Las estaciones de trabajo o áreas de servicio constan de un número limitado de periferales de entrada y salida, cuyos datos son procesados en el ASI. Estas estaciones de trabajo o áreas de servicio forman parte de las distintas oficinas de la OCEPR.
3. De ocurrir un evento de desastre que afecte al salón de computadoras, probablemente se verán

afectadas todas las oficinas de la OCEPR. Si el evento de desastre ocurre en una sola oficina, posiblemente las demás oficinas no se verán afectadas. Las operaciones de esa oficina se distribuirán y se intentará regresar a la normalidad en menos de 24 horas.

4. Para efectos de este plan, se han clasificado los niveles de acción de acuerdo con un por ciento estimado de la posible pérdida, falta de operación o desastre que ocurra en el salón de computadoras o en las estaciones de trabajo, consideradas estas últimas en conjunto.
5. Los niveles de acción se han identificado como sigue:

1. Destrucción total:	70% o más
2. Destrucción severa:	40% a 69%
3. Destrucción parcial:	menos de 40%

El **Anejo A** presenta una descripción de cada uno de estos niveles de acción. Dentro de cada uno de estos niveles se incluyen las premisas de las cuales se parte, los objetivos que se persiguen, el método a ser utilizado, la presentación de alternativas, la medición del objetivo y los requisitos que se han establecido para cada nivel de acción.

B. PREMISAS:

El Plan de Contingencia está basado en las siguientes premisas:

1. La posibilidad de que ocurra un evento que cause desastres mayores a un área de servicio o al Salón de Servidores, que no permita que sea operante por un período mínimo de un mes.
2. Debe llevarse a cabo en caso de que ocurra un evento de desastre o en los ejercicios de simulación. El (la) Director(a) declarará un estado de emergencia y llamará al personal responsable, según definido en la lista de Estructura de Llamadas incluida en el **Anejo B**.
3. Una vez se active el plan, las tareas, responsabilidades y canales de autoridad serán puestos en acción y se mantendrán hasta que el incidente sea resuelto y el director del

notifique el mismo.

4. La persona de más alto rango en la escena del evento es responsable por el desalojo de todo el personal en el área, de ser necesario. Esto según definido en el Plan de Desastres en vigor.
5. La cadena de mando normal de la Agencia será utilizada para transmitir órdenes. La lista de teléfonos del personal clave y del Área de Sistemas de Información se mantendrá actualizada.
6. Si la interrupción de las operaciones ocurre por algún desastre que cause pérdidas parciales, se canalizarán todos los esfuerzos para establecer una recuperación operacional del Área de Sistemas de Información en el menor tiempo posible.
7. Se establecerá un área de trabajo alterna para los empleados de oficina o estaciones de trabajo, que estará disponible previa notificación de 24 horas.
8. Se establecerá un Área de Sistemas de Información de cómputos alterno al proceso de aplicaciones y sistemas de proceso en lote ("batch"), que estará disponible previa notificación de 24 horas.
9. El personal de restauración estará activo en la restauración hasta que la misma se termine y el Área de Sistemas de Información pueda reanudar sus operaciones con toda normalidad. Este personal se clasificará en dos (2) grupos de trabajo, según está presentado en el Anejo

C.

C. ACTIVACIÓN DEL PLAN:

Este plan se activará bajo cualquiera de las siguientes circunstancias:

1. Un evento que incapacite parcial o totalmente las instalaciones del Área de Sistemas de Información por un período de 24 horas o más.

2. Un evento que deteriore el procesamiento de los datos de los sistemas, aplicaciones o equipo del Área de Sistemas de Información por circunstancias que estén fuera de los parámetros normales de las operaciones.
3. Este plan cubre los siguientes eventos de desastre:
 - 1) Interrupción de energía eléctrica o aire acondicionado
 - 2) Fuego en las instalaciones del y sus inmediaciones
 - 3) Incidente por agua
 - 4) Fenómenos del tiempo o de la naturaleza
 - 5) Sabotaje

II. IMPLANTACIÓN

La implantación de un plan de contingencia conlleva tiempo. Para poder decir que el mismo está implantado, se debe adiestrar al personal, tener disponible el equipo de emergencia, establecer las áreas de procesamiento alternas, constatar que se conocen los procedimientos y verificar que éstos funcionan.

A. EFECTIVIDAD:

1. El plan de contingencia entrará en vigor al momento de su aprobación por el (la) Coordinador(a) General de la Agencia.
2. El director del Área de Sistemas de Información es responsable de que se establezcan los procedimientos que se detallan en este plan y de que todos los empleados del Área de Sistemas de Información los conozcan.

B. ADIESTRAMIENTO:

1. El (la) Director(a) del Área de Sistemas de Información preparará un itinerario de adiestramientos y ejercicios de prueba para comprobar que el personal conoce las acciones a tomar en caso de que ocurra alguno de los desastres o eventualidades indicadas.

C. EQUIPO DE EMERGENCIA:

1. El equipo de emergencia requerido para ser utilizado en los momentos en que ocurran estas eventualidades o desastres estará disponible y en condiciones útiles. Deberá incluir los siguientes artículos:

- a. Botiquín de primera ayuda *no disponible de*
- b. Cinta adhesiva de seguridad para cristales *NO*
- c. Lámparas portátiles de baterías *solicitarlas*
- d. Detectores automáticos de humo *solicitarlas*
- e. Extintores portátiles para incendios conteniendo las especificaciones descritas en el Manual de Políticas y Procedimientos del Área de Sistemas de Información. *solicitarlas*

D. ESTACIÓN ALTERNA:

1. El Salón de Conferencias ha establecido un área de trabajo que servirá los propósitos de adiestramiento y como estación alterna, en caso de que en alguna oficina de la OCEPR haya ocurrido algún incidente que impida continuar las operaciones del Área de Sistemas de Información en el lugar de origen. *cuál?*
2. Esta estación alterna estará disponible, previa notificación de 24 horas.

E. MEDIDAS DE SEGURIDAD:

1. El Área de Sistemas de Información de Sistemas de Información restringirá el acceso al computador y a la estación alterna. *solicitarlas*
2. Sólo personal autorizado por el (la) Director(a) del Área de Sistemas de Información puede entrar para acceder el computador inclusive al personal de mantenimiento y reparación del equipo.
3. Durante este período serán restringidos los accesos a cintas y documentación.

4. Sólo se tendrá acceso a aquella cinta o documentación que sea necesaria para utilizar. De esta forma se asegurará que ninguna información sea sabotada.

III. PREVISIÓN DE DESASTRES

La previsión de desastres no consiste únicamente en establecer una serie de pasos a seguir para cada uno de los eventos de desastres que puedan ocurrir. Consiste en asumir que los mismos han ocurrido y que hay que actuar sobre las consecuencias que el evento ha causado.

A. DESALOJO POR EMERGENCIA O FUEGO:

1. Los procedimientos de desalojo en casos de emergencia o fuego se especifican en el **Anejo D** y los mismos se discutirán y practicarán con el personal del Área de Sistemas de Información.
2. El plan de desalojo se imprimirá y se fijará en las áreas designadas para cada extintor de fuego.
3. El personal de más alto rango o los líderes de grupo estarán a cargo de desalojar el área y notificar al Departamento de Bomberos y a las áreas u oficinas cercanas al Área de Sistemas de Información.
4. Luego de desalojar el personal en riesgo se comenzará con la comunicación, siguiendo la cadena de mando establecida en la estructura de llamadas que contiene el **Anejo B**.

B. FALLAS DEL SISTEMA COMPUTADORIZADO:

1. El operador de computadoras tratará de restablecer o inicializar los sistemas computadorizados de acuerdo con los procedimientos descritos en el proceso de activar o inactivar los Sistemas Computadorizados del Manual de Políticas y Procedimientos del

Área de Sistemas de Información.

2. Se notificará al (a la) Director(a) del Área de Sistemas de Información sobre las fallas que ocurran, quien a su vez mantendrá informada al (a la) Coordinador(a) General de estas eventualidades.
3. En ausencia del (de la) Director(a) del Área de Sistemas de Información, su ayudante principal, los líderes de grupo o cualquier otro empleado, será responsable de notificar la incidencia, esto en el orden de responsabilidades que se establezca y se notifique.
4. Los sistemas o aplicaciones se ejecutarán de acuerdo con la prioridad establecida en el **Anejo E**.
5. Si el evento se debe a fallas eléctricas en el área de la Capital, el Viejo San Juan, Puerta de Tierra o Miramar, el sistema se apagará.
6. Todos los sistemas se asegurarán, de manera que cuando regrese la energía eléctrica el equipo se activará junto a sus aplicaciones y sistemas, de acuerdo con la prioridad establecida para estos.
7. Se establecerá una coordinación adecuada con las demás áreas de trabajo de forma que si la falla eléctrica ocurre en una de las áreas u oficinas de trabajo, se comunicarán con el (la) Director(a) del Área de Sistemas de Información para verificar la disponibilidad de un área alterna o de emergencia en lo que se establece la electricidad en el área afectada.
8. Si la falla del sistema se debe a deficiencias del aire acondicionado del Área de Sistemas de Información, el equipo se deberá apagar antes de que ocurran daños severos al sistema o equipo y notificar a las áreas afectadas antes de apagar los equipos.
9. Se deberán utilizar unidades de aire acondicionado temporeras o abanicos que mantengan baja la temperatura del Área de Sistemas de Información para que no se afecte el equipo.

C. FALLAS EN LA COMUNICACIÓN:

1. La comunicación entre el LAN y la Oficina de Gerencia y Presupuesto (OGP) y el computador central y las áreas de trabajo localizadas se lleva a cabo a través de una antena externa y líneas de comunicación CAT 5e que van por conductos entre los pisos. Sólo el (la) Director(a) del Área de Sistemas de Información o su ayudante principal están autorizados a intervenir en las fallas causadas por avería.
2. Los procedimientos de recuperación por fallas en la línea de comunicación tienen prioridad de primer orden.

D. PERSONAL:

1. Cuando problemas de cualquier índole retrasen al operador del Área de Sistemas de Información en su hora de entrada, el director u otra persona a cargo en la cadena de mando se cerciorarán de que las aplicaciones de mayor prioridad se ejecuten primero.
2. Las prioridades de los sistemas se presentan en el **Anejo E**.
3. Una lista de los accidentes o emergencias relacionadas se incluye en el **Anejo F** y una copia de ésta se fijará en el Tablón de Edictos del Área de Sistemas de Información.
4. Cualquier accidente en el trabajo se debe referir al hospital más cercano.
5. Todos los teléfonos de emergencia se encuentran en los procedimientos para notificación de Eventos de Desastres que se incluyen en el **Anejo G**.

IV. ADMINISTRACIÓN DEL PLAN:

El (la) Director(a) del Área de Sistemas de Información tendrá a su cargo la administración total del Plan de Contingencia y será responsable de que el mismo esté actualizado. Será a su vez responsable de que se lleven a cabo los simulacros de prueba necesarios. *Condición.*

A. ACTUALIZACIÓN:

Para garantizar que el Plan de Contingencia se mantenga actualizado, se le incorporarán cambios a medida que estos sean necesarios.

1. No se dependerá de revisiones periódicas.
2. El (la) Director(a) del Área de Sistemas de Información será responsable de que el plan esté al día.
3. El monitor interno revisará el Plan de Contingencia por lo menos dos (2) veces al año y verificar que la información contenida esté actualizada.

B. EJERCICIOS Y PRUEBAS:

1. El equipo de emergencia será verificado dos (2) veces al año para asegurar su buen funcionamiento.
2. De tener alguna falla, la misma se corregirá inmediatamente.
3. El (la) Director(a) del Área de Sistemas de Información programará ejercicios de simulación y pruebas para adiestrar a los empleados sobre las funciones que deberán ejecutar y para evaluar el nivel de eficacia en la ejecución de los procedimientos.

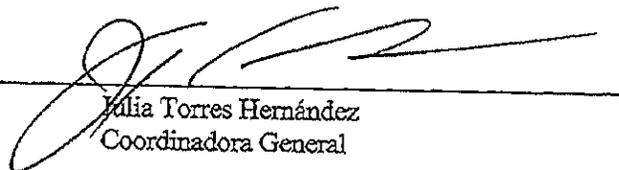
C. EVALUACIÓN:

1. Con el propósito de obtener el mejor nivel de eficiencia en la ejecución del Plan de Contingencia se evaluarán las fallas cometidas en los ejercicios de simulación.

2. Después de cada simulacro o emergencia, el (la) Director(a) convocará al personal del Área de Sistemas de Información a una reunión con el propósito de evaluar la ejecución del plan y sugerir modificaciones, de ser necesarias.

V. VIGENCIA

Este procedimiento estará en vigor desde el 15 de febrero de 2007.



Julia Torres Hernández
Coordinadora General



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

15 de febrero de 2007

A todo el personal del
Área de Sistemas de Información

Director Interino
Área de Sistemas de Información

PLAN DE CONTINGENCIA

Adjunto copia del Plan de Contingencia del Área de Sistemas de Información. Favor de firmar y anotar la fecha en que recibió su copia. Es importante recalcar que este documento debe ser leído en su totalidad para que así estén al tanto de los procedimientos que se llevan a cabo de surgir algún acontecimiento. De tener alguna duda favor de comunicarla de inmediato.

<u>Nombre del Empleado</u>	<u>Firma</u>	<u>Fecha</u>
1. _____	_____	_____
2. _____	_____	_____
3. _____	_____	_____
4. _____	_____	_____
5. _____	_____	_____
6. _____	_____	_____
7. _____	_____	_____

ANEJO A

DESTRUCCIÓN TOTAL

PREMISA:

Las instalaciones del salón de computadoras o las estaciones de trabajo consideradas en conjunto han sido destruidas totalmente, o en un por ciento mayor del 70%.

OBJETIVO:

Establecer un Área de Sistemas de Información Alterna para poder llevar a cabo las operaciones del Área de Sistemas de Información en tiempo no menor de una (1) semana y no mayor de cuatro (4).

MÉTODO:

Existen varias alternativas que dependerán de la condición de destrucción en que se encuentra el equipo y los sistemas.

➤ Alternativa 1

Las actividades del Área de Sistemas de Información se reanudarán en un lugar de resguardo alterno o secundario, operando a un máximo de 12 horas. El movimiento de equipo y personal a este Área de Sistemas de Información alterno se detalla en el **Anejo H**.

➤ Alternativa 2

Las actividades del Área de Sistemas de Información se llevarán a cabo parcialmente en el Área de Sistemas de Información de resguardo.

➤ Alternativa 3

El Área de Sistemas de Información restaurará las facilidades arreglando o comprando el equipo que se haya dañado de acuerdo con el **Anejo I**.

➤ Alternativa 4

Las actividades de procesamiento de datos se contratarán con compañías privadas.

➤ Alternativa 5

Los trabajos se realizarán manualmente y luego se actualizarán en los sistemas computadorizados; cuando éstos se encuentren operando.

MEDICIÓN:

Este objetivo será medido a base del tiempo que tome poner en operación el Área de Sistemas de Información.

REQUISITOS:

Para que este objetivo pueda llevarse a cabo es necesario tener lo siguiente:

- Considerar un contrato entre la OCEPR y otra institución para usar las facilidades de procesamiento electrónico de datos como Área de Sistemas de Información de resguardo tendría que ser considerado en dos partes (área Administrativa y Ejecutiva).
- Procedimientos de retención y resguardo externo de cintas magnéticas debidamente identificadas para activar el Área de Sistemas de Información de resguardo.
- Diseñar y utilizar un plan de desarrollo de nuevas instalaciones debidamente estructurado para ponerse en acción de ser necesario.

DESTRUCCIÓN SEVERA

PREMISA:

Las instalaciones del salón de computadoras o las estaciones de trabajo consideradas en conjunto han sido destruidas severamente o en un por ciento entre el 40% y el 69%.

OBJETIVO:

Las actividades del Área de Sistemas de Información deben estar funcionando en el Área de Sistemas de Información Alternativo, dentro de un período mayor de una (1) semana, pero menor de cuatro (4) semanas.

MÉTODO:

Todas las alternativas presentadas en el objetivo de destrucción total deben ser consideradas, además de la siguiente:

1. **Alternativa 1**

El Área de Sistemas de Información extraerá del plan de retención de archivos de reserva, las cintas o discos de resguardo localizados en la bóveda que se requieran para implantar las aplicaciones más importantes.

MEDICIÓN:

Este objetivo será medido en términos del tiempo requerido para poner en funcionamiento al Área de Sistemas de Información alterno. El objetivo del Área de Sistemas de Información alterno se habrá cumplido cuando las aplicaciones más importantes estén operando.

DESTRUCCIÓN PARCIAL

PREMISA:

Las instalaciones del salón de computadoras o las estaciones de trabajo consideradas en conjunto han sido destruidas parcialmente o menos de un 40%. En el caso de destrucción parcial, una de las dos computadoras del salón de computadoras no se ha afectado y está operando.

OBJETIVO:

Las actividades del Área de Sistemas de Información se llevarán a cabo en sus propias instalaciones a un ritmo operacional limitado por un período menor de una (1) semana mientras se restauran los daños ocurridos.

MÉTODO:

Todas las alternativas presentadas en el objetivo de destrucción total o severa deben ser consideradas, además de las siguientes:

➤ **Alternativa 1**

Las actividades del Área de Sistemas de Información estarán orientadas a verificar los discos de trabajo

y restauración de cintas y discos.

➤ **Alternativa 2**

Esta alternativa parte de la premisa de que sólo el equipo sufrió daños. Se notificará al manufacturero o representante de servicio para que reparen el equipo. Las operaciones continuarán durante el proceso de reparación pero de forma limitada.

MEDICIÓN:

Este objetivo será medido a base del tiempo que tome poner en operaciones el Área de Sistemas de Información.

ANEJO B

ESTRUCTURA DE LLAMADAS

I. Eventos de Emergencia

Fuego

- Bomberos..... 343-2330

Disturbios

- Policía..... 343-2020
- Emergencias Médicas.....
- Centro Médico 754-3535
- Hospital Industrial..... 754-2525
- Auxilio Mutuo..... 758-2000
- Emergencias Médicas 343-2222
- Ashford Community Hospital 721-2160
- Hosp. Municipal de San Juan 766-2222
- Centro de Envenenamiento..... 754-8536
- CDT Hoare.....
- Defensa Civil..... 863-1502

II. Dirección

- Coordinador(a) General
- Subcoordinador(a)
- Administrador(a)

ANEJO C
GRUPOS DE TRABAJO

GRUPO A

Líder de Grupo --Director(a) de Área de Sistemas de Información

El **Grupo A** será responsable por la operación eficiente del Área de Sistemas de Información (ASI), esto incluye la instalación de todas las aplicaciones necesarias en los servidores durante la ejecución del plan. Se harán responsables por verificar que el equipo opere a capacidad dentro de las circunstancias establecidas y velarán por la seguridad de éste si es el caso.

GRUPO B

Líder de Grupo --Técnico de Sistemas de Información (Programadores, etc.)

El **Grupo B** se hará responsable de las aplicaciones a ser instaladas para continuar con las aplicaciones del Área de Sistemas de Información de las circunstancias establecidas. Ayudarán en la recuperación del sistema operativo y las aplicaciones, para continuar con las operaciones de la OCEPR dentro de las circunstancias establecidas. Orientarán a los usuarios para que éstos trabajen rápido y eficientemente. De esta forma todos los usuarios afectados podrán utilizar el sistema para continuar con sus trabajos.

Tanto el grupo A y B son responsables de cubrir y proteger los equipos del ASI, concentradores y "switches" y cuartos de comunicación por piso.

ANEJO D

PLANOS PARA EL DESALOJO DEL EDIFICIO

1. Plano del sótano
2. Plano del primer piso
3. Plano del segundo piso
4. Plano del tercer piso
5. Plano del cuarto piso
6. Plano del quinto piso

ANEJO E

DEFINICIÓN DE PRIORIDADES DE LAS APLICACIONES

- **PRIORIDAD # 1**

Extremadamente crítica para la institución. Estas aplicaciones son absolutamente esenciales para la continuidad de las operaciones en la OCEPR. Las mismas deben procesarse con el menor retraso posible.

- **PRIORIDAD # 2**

Estas aplicaciones son esenciales al desarrollo de operaciones de la OCEPR. Ajustes pueden llevarse a cabo para el proceso de las mismas, permitiendo un pequeño retraso en su proceso.

- **PRIORIDAD # 3**

Estos procesos son llevados a cabo en el control de las operaciones de la OCEPR. Las aplicaciones se procesan a medida que el tiempo esté disponible.

- **PRIORIDAD # 4**

Estas aplicaciones serán restablecidas en la etapa final del proceso de recuperación, encaminándose nuevamente hacia el proceso normal de las aplicaciones.

ANEJO F

LISTA DE ACCIDENTES O EMERGENCIAS CUBIERTAS

ESTRATEGIA A SEGUIR EN CASO DE FUEGO:

Esta estrategia detalla los pasos a seguir en caso de fuego:

1. El personal de turno activará de forma manual el extintor de incendios. Si el fuego no es controlable, el empleado deberá desalojar el área.
2. Informar el fuego al (a la) Director(a) del Área de Sistemas de Información tan pronto éste se detecte. El director pondrá en efecto la operación de llamadas de la cadena de mando que se presenta en el Anejo B.
3. Habrá un coordinador en cada piso para dirigir el proceso de desalojo del edificio. El proceso debe ser tan rápido como sea posible, sin arriesgar la seguridad del personal.
4. Si hay humo en el área, las personas deberán moverse a áreas que no estén afectadas y bajar la cabeza tan cerca del piso como les sea posible.
5. Desconectar la energía eléctrica del computador y sus periferales accionando el interruptor que se encuentra en el Panel de Control del Área de Sistemas de Información.
6. Si la seguridad del personal no está en peligro, se debe apagar la máquina usando el procedimiento normal, según se explica en el Manual de Normas y Procedimientos del Área de Sistemas de Información.

ESTRATEGIA A SEGUIR EN CASO DE INUNDACIÓN:

Esta estrategia detallará los pasos a seguir en caso de inundación ocasionada por filtración, tubería pluvial dañada o cualquier otra emergencia causada por efecto del agua.

1. Identificar el área afectada.
2. Informar la inundación al director del Área de Sistemas de Información, tan pronto ésta se detecte.
3. Determinar la fuente de origen del agua.
4. Apagar todo el equipo electrónico accionando el interruptor que se encuentra en el Panel de Control del Área de Sistemas de Información.
5. Sacar todo el equipo removible del área afectada.
6. Reportar el incidente.

7. Sacar el agua con aspiradoras o asegurarse de que el personal designado realice adecuadamente esta labor.
8. Llamar al equipo de emergencia, de ser necesario.
9. Recoger todos los discos y cintas para llevarlos a la bóveda.

ESTRATEGIA A SEGUIR EN CASO DE FENÓMENOS NATURALES Y CLIMATOLÓGICOS:

Esta estrategia será una combinación de los procedimientos para fuego y agua. Presume daños por agua y viento. En los casos en que los fenómenos son predecibles, existe un tiempo de preparación antes de la llegada del evento que deberá utilizarse para tomar todas las medidas de prevención. A continuación se enumeran algunas de éstas:

ANTES DEL FENÓMENO:

1. Instalar paneles de protección contra huracanes en todas las ventanas de cristal del Salón de Computadoras. Estos paneles de protección estarán preparados con antelación a la temporada de huracanes.
2. Desconectar la energía eléctrica del computador y sus periferales, activando el interruptor que se encuentra en el Panel de Control del Área de Sistemas de Información.
3. Cubrir el equipo con bolsas plásticas o toldos plásticos para evitar que se moje.
4. Mudar todo equipo removible a un área designada como segura.
5. Recoger todos los discos y cintas. Llevarlos a la bóveda.

LUEGO DEL FENÓMENO:

1. Reportar el incidente.
2. Sacar el agua con aspiradoras.
3. Llamar al equipo de emergencia de ser necesario.

ANEJO G

NOTIFICACIÓN DE EVENTOS DE DESASTRE

El (la) Director(a) del Área de Sistemas de Información o el empleado de mayor rango en la escena del incidente o desastre tendrá a su cargo las siguientes responsabilidades:

1. Velar por la seguridad del personal del Área de Sistemas de Información. Asegurarse de notificar a todas las personas presentes en el lugar de los hechos y de que la ocurrencia del evento de desastre sea informada a las compañías y a las entidades gubernamentales requeridas.
2. Notificar la ocurrencia del evento de desastre a las autoridades requeridas a través de sus números de emergencia:

Fuego

- Bomberos..... 343-2330

Disturbios

- Policía..... 343-2020

Emergencia Médica

- Centro Médico..... 754-3535
- Hospital Industrial
- Auxilio Mutuo 758-2000
- Emergencias Médicas 343-2222
- Ashford Community Hospital 721-2160
- Hospital Municipal de San Juan 766-2222
- Centro Inf. de Envenenamiento 754-8536
- Estación Enfermería 723-4801

Electricidad

- Autoridad de Energía Eléctrica..... 289-3434

Desastres Naturales

- Defensa Civil..... 724-0124

3. El bibliotecario o el (la) custodio de las cintas deberá asegurarse de que el gabinete de cintas magnéticas

de resguardo esté cerrado.

- a. Esta tarea podrá ser delegada al operador del computador u otra persona.
 - b. Es recomendable que esta tarea se asigne a, por lo menos dos, (2) personas.
4. Poner en operación la secuencia de llamadas en la cadena de mando que comienza con una llamada del empleado que se encuentra en el Área de Sistemas de Información.
- a. En caso de que no se consiga a la persona de turno o a la persona representante del (de la) Coordinador(a) General.
 - b. El empleado a cargo en el momento del Área de Sistemas de Información informará la naturaleza del incidente, el estatus del personal y la acción tomada.
 - c. De ser necesario desalojar el área, el empleado que informó el incidente será la última persona en abandonar el área, después de verificar, en el grado que sea posible, que el resto del personal haya salido.
5. El empleado de más alto rango de la unidad afectada, o en su ausencia, el empleado que informó el incidente, deberá permanecer en las inmediaciones de la escena hasta que se persone allí un funcionario de la OCEPR de más alta jerarquía que asuma la responsabilidad de coordinar los trabajos para enfrentar los daños.
6. El empleado del Área de Sistemas de Información le informará la naturaleza del incidente, la situación del personal y las acciones tomadas.

ANEJO H

MOVIMIENTO DE EQUIPO Y PERSONA A CENTRO DE CÓMPUTOS ALTERNO

En los casos en que la ocurrencia de un desastre requiera que se establezca un centro de cómputos alterno en el Área de Sistemas de Información, cambiará su lugar de actividades normales al área que se haya determinado o en el centro de cómputos alterno. A continuación, se enumeran las tareas que se deben llevar a cabo para el movimiento:

1. Reunión del personal de restauración para coordinar los pasos a seguir de acuerdo al **Anejo I**.
2. Arreglos para transportación de máquinas, equipo de oficina, periferales y personal al Área de Sistemas de Información Alterno.
3. Prueba de las aplicaciones críticas en el equipo del Área de Sistemas de Información alterno de acuerdo al **Anejo E**.
4. Instalación de la programación necesaria para continuar la producción en una escala limitada de duración.
5. Establecer un itinerario de horarios para que las distintas aplicaciones puedan ejecutarse.



Gobierno de Puerto Rico
Oficina del Coordinador General
Para el Financiamiento Socioeconómico y la Autogestión

Normas sobre el uso de los Sistemas Electrónicos de la OFSA

Yo, _____, hoy ___ de _____ de _____, certifico que cumpliré con las medidas de seguridad implantadas por el Área de Sistemas de Información que se expresan a continuación y que:

Introducción:

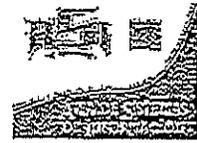
La Oficina del (la) Coordinador (a) General para el Financiamiento Socioeconómico y la Autogestión de Puerto Rico (OFSA) cuenta con acceso a computadoras, redes, servicios electrónicos internos y a la red Internet. De la única forma en que usted puede utilizar esta computadora y los servicios asociados es entendiendo y aceptando las siguientes condiciones.

Titularidad y Derechos

- Esta computadora, los servicios asociados tanto internos como externos, el sistema de correspondencia electrónica (e-mail), el acceso al Internet y los documentos y programas que existen en la misma, son propiedad de la OFSA y sólo podrán utilizarse para propósitos lícitos, prudentes, responsables y dentro de las funciones o poderes de esta Oficina.
- Toda información, dato, obra literaria o de arte, escrito, documento, programa, acción, privilegio, patente, derecho de autor o cualquier otro derecho que surja, se cree o modifique mediante el uso de una de las computadoras de la OFSA, será propiedad de la Oficina, aunque la información, dato, obra literaria o de arte, escrito, documento, programa, acción, privilegio, patente, derecho de autor o cualquier otro derecho haya surgido mediante el esfuerzo personal del usuario.
- La información contenida en esta computadora, los servicios asociados tanto internos como externos, los mensajes de correspondencia electrónica (e-mails), información de la Intranet o el Internet y los documentos y programas existentes, no podrán reproducirse o utilizarse para fines ajenos a las funciones y poderes de la OFSA.

Seguridad

- El uso de un código de acceso "password", no impedirá que se audite el sistema y no significa que el usuario albergue expectativa de intimidad alguna con relación a la información almacenada en la computadora que tenga asignada o en cualquier otra. Las contraseñas deben mantenerse en estricta confidencialidad y administrarse conforme a las medidas de seguridad adoptadas por la OFSA.



- La OFSA se reserva el derecho de auditar, vigilar y fiscalizar los sistemas de correspondencia electrónica y todos los servicios computarizados para garantizar que su propiedad se utilice para los propósitos y gestiones relacionadas con el trabajo. Estas auditorías se realizarán periódicamente o al azar, o cuando exista una investigación sobre una situación en particular.

Por estas circunstancias, el personal de la OFSA no tiene derecho a la intimidad con relación a cualquier información, documento o mensaje creado, recibido o enviado a través del sistema de "e-mail".

- Para evitar poner en peligro la confidencialidad de la información de la OFSA, se prohíbe el envío fuera de la Oficina de documentos electrónicos o mensajes por medio del "e-mail" que contengan información confidencial.
- Todos los archivos que se creen en las computadoras deben guardarse en el "Server" dentro del directorio asignado a cada usuario con el propósito de que puedan protegerse mediante los mecanismos de resguardo "backup" existentes.
- Deberá apagar "Shut Down" una vez finalizada las labores del día.

Políticas Antidiscriminación

- Existe una prohibición absoluta y cero tolerancias a la utilización de la computadora o del sistema de correspondencia electrónica para enviar, recibir o crear mensajes o documentos de contenido discriminatorio por razón de raza, género, credo, ideas políticas u origen social o nacional, o que puedan ser catalogados como hostigamiento sexual.
- Está prohibido el manejo o transmisión de material obsceno, profano u ofensivo a través del sistema de computadoras o del sistema de comunicación electrónica de la OFSA. Esto incluye a modo de ejemplo, acceso a material pornográfico, bromas de cualquier forma o cualquier comentario o chistes que pueda violar la política de discriminación de la OFSA o su política de hostigamiento sexual.
- Se prohíbe que se utilicen protectores de monitores "screen savers" con fotos de personas, artistas, modelos, deportistas, fotos de calendario o cualquier otra imagen que pueda resultar poco seria, ofensiva u obsceno.
- Se prohíbe la divulgación por cualquier medio de cualquier tipo de opiniones personales específicas con relación a raza, origen nacional, sexo, orientación sexual, edad, ideas o creencias religiosas o políticas, así como opiniones sobre personas con impedimento físico o mental.



Correo Electrónico

- No se podrá crear archivos o enviarlos mediante el correo electrónico que excedan la capacidad de la cuota del usuario en el servidor.

Disposiciones Misceláneas

- Las políticas antes mencionadas sobre el uso del correo electrónico y sus auditorías serán igual aplicación para los otros recursos de la Intranet e Internet tales como el "WWW", "FTP", "Chat", etc.
- Es responsabilidad de los usuarios el cumplir con las normas de cuotas de espacio en los servidores.
- Las políticas de Internet serán revisadas periódicamente en caso de que surjan nuevas necesidades, únicas y particulares de la OFSA. Se incorporan y se hacen formar parte de estas advertencias todos los documentos, memorandos, instrucciones, manuales o políticas que se notifiquen de tiempo en tiempo y que sea pertinentes al uso de las computadoras de OFSA.

La Política Pública

- La política pública protegida por la Ley de Ética Gubernamental (LEG) recoge una disposición constitucional que en términos generales prohíbe la utilización de propiedad o fondos públicos para fines privados. De esa manera el uso de fondos públicos debe tener el propósito de promover el bienestar o interés de la comunidad en general y no intereses individuales o políticos-partidistas. Véase Constitución del ELAPR, Art. VI, Sec. 9; Art. 6 (A) (1), 6 (F) REG.
- La política pública protegida por la Oficina de Ética Gubernamental (OEG) pretende asegurar que las actuaciones de los (as) funcionarios(as) y empleados(as) públicos(as) sean llevadas a cabo dentro de los más altos estándares de moralidad y rectitud. Se aspira que a las actuaciones de los(as) Servidores(as) Públicos(as) no afecten adversamente la confianza del público en la integridad y honestidad de las instituciones gubernamentales. Véase Art. VI, Sec. 9, Constitución del ELAPR; Art. 11, 011 (b) Ley de Municipios Autónomos, Art. 3-2 (a), 3-2 (c) LEG; Art. 6 (A)(1)(6); 6(D); 6 (E); 8 (A) REG.
- La OEG puede presentar una querrela administrativa, según las disposiciones de la Ley de Procedimiento Administrativo Uniforme (Ley Núm. 170 de 12 de agosto de 1988,



según enmendada). Además, la Oficina puede referir al Departamento de Justicia aquellos casos en los que se trate de una violación a la Ley que constituya delito.

- La mayoría de las disposiciones de la Ley de Ética Gubernamental son tipificadas como delito. Esto quiere decir que se podría procesar por la vía criminal y el (la) infractor (a) se expone a las penas dispuestas por Ley.
- Toda persona que viole intencionalmente las prohibiciones sobre el uso de la propiedad y fondos públicos, la aceptación o solicitud de regalos y la norma de confidencialidad incurrirá en delito grave. De probarse la violación con pena de reclusión de un año o con una multa de \$2,000, o ambas penas a discreción del tribunal. Además, la persona convicta no tendrá beneficio de sentencia suspendida.
- El Director Ejecutivo de la Oficina de Ética Gubernamental podrá imponer multas administrativas hasta \$20,000 por cada violación. Esto tendría lugar luego de celebrarse un proceso administrativo en la Oficina de Ética Gubernamental.
- También podrá recomendar a la autoridad nominadora una amonestación escrita, suspensión de empleo y sueldo, destitución o despido.

Prohibiciones

- No divulgaré mi número de usuario (USERNAME) asignado, ni mi contraseña (PASSWORD) y toda la información de todo tipo confidencial que contenga la computadora que me fuera asignada.
- No dejaré información o aplicaciones sensibles en la pantalla, ni abandonare mi escritorio dejando la computadora asignada expuesta, sin hacer "logoff" o "Lock Computer".
- No utilizare aplicaciones que no estén autorizadas por el (la) Director(a) del Área de Sistema de Información ni juegos en la computadora asignada, ni copiare aplicaciones que tienen derecho de autor.
- No usare ninguna aplicación ni equipo de computadoras sin haber recibido la autorización del (de la) Director(a) de Sistemas de Información y la orientación o adiestramiento sobre su uso.
- No insertaré en la computadora que me fue asignada ningún disquete, disco compacto "CD", "DVD", "Memory Stick" o cualquier equipo para almacenar información que no haya sido examinado previamente con una aplicación de antivirus. Para ello se debe seguir el procedimiento de seguridad previamente establecido.



- No crearé archivos de datos sin asignarle nombre de inmediato o guardar dicho activo.
- No ingeriré alimentos, ni bebidas mientras esté utilizando la computadora, discos ópticos o disquetes.
- No me llevaré el equipo que me fuera asignado, ni ningún otro, sin la debida autorización del (de la) Director(a) del Área de Sistema de Información y de ser autorizado, completaré una autorización escrita provista por el (la) Director(a) del Área de Sistema de Información conteniendo las razones para su uso, la fecha en que se recibe y la fecha en que será devuelto.
- Notificaré al (a la) Director(a) del Área de Sistema de Información sobre cualquier falla, daño o violación al uso, ocurrida al equipo que me fuera asignado, en un periodo de veinticuatro (24) horas máximo.
- Utilizaré el equipo de computadora asignado para propósito de trabajos relacionados a mis responsabilidades en la Agencia, *exclusivamente*.
- No haré uso indebido del Internet, ni accederé a portales que no hayan sido previamente autorizados por el (la) Director(a) del Área de Sistema de Información y de hacerlo me responsabilizo por las sanciones disciplinarias que me sean impuestas por el (la) Director(a) del Área de Recursos Humanos o su representante autorizado. Además, no supliré información de carácter confidencial a partidos políticos u otra entidad, ni grabaré y produciré mensajes con fines exclusivamente político partidista.
- No usaré los sistemas de computadoras y comunicaciones de la Oficina para propósito personal, de recreo, para manejo de un negocio o asunto privado o para el envío y recepción de mensajes en cadena, para tener acceso a compras, juegos, concursos, encuestas, páginas de entretenimiento o cualquier otro asunto o servicio no oficial o ajeno a las funciones que me fueran asignadas.
- No haré envío fuera de la Oficina, de documentos electrónicos o mensajes por medio del correo electrónico "E-mail" que contengan información confidencial.
- No haré uso de computadoras portátiles, Laptop, o cualquier otro equipo electrónico personal, para realizar trabajos en la Oficina, sin previa autorización del (la) Coordinador(a) de la OFSA.
- No haré envío o recibo de mensajes de correo electrónico del personal de la Oficina y otras personas ajenas al mismo, en los cuales se divulguen, comenten o expresen hechos, opiniones u otra situación o asuntos internos de la Oficina, que puedan poner en entredicho la reputación y la imagen de ésta.
- No realizaré tareas de instalación de equipo, programas "software" ni de reparación en la computadora que me fuera asignada.



- No haré movimiento de equipos así como de sus periferales sin que haya sido coordinado y autorizado por el (la) Director (a) del Área de Sistemas de Información de la Agencia.
- Al finalizar el día me comprometo a retirar mis claves de acceso de los terminales o computadoras y apagar todos los equipos electrónicos que me fueran asignados.
- No podrá utilizar programas o recursos para los cuales no exista licencia o autorización de uso válida a nombre de la OFSA.
- No podrá terminantemente copiar programas de la OSFA para instalarlos en otras computadoras, sin la autorización por escrito del (la) Coordinador (a) ó del Director (a) de Sistema de Información.
- No podrá instalar programas en las computadoras de la OSFA sin la autorización por escrito del (la) Coordinador (a) General ó el (la) Director (a) de Sistema de Información.
- No podrá modificar los privilegios de acceso a las redes internas o externas para obtener acceso no autorizado a dichos recursos.
- No podrá modificar de los parámetros o configuración de las computadoras de la OSFA para darle la capacidad de recibir llamadas telefónicas o cualquier otro tipo de acceso o conexión remota que permita intrusiones no autorizadas a la red de la OFSA.
- Se prohíbe leer, revisar o interceptar cualquier tipo de comunicación electrónica de la OFSA o de cualquier otra persona o entidad, sin el consentimiento expreso del remitente y del destinatario de la comunicación.
- Se prohíbe el uso de programas de charlas "Chats", "Messengers", "Facebook", "Tweeter" y etc a menos que sean autorizados por escrito por el Coordinador General ó el Director de Sistemas de Información.
- No está permitido almacenar fotos, músicas y videos personales en los "Servers" y PC de la OSFA.
- Se prohíbe codificar, asignar contraseñas o modificar de alguna manera la información, mensajes de correo electrónico o archivos propiedad de la OSFA con el propósito de impedir que alguien pueda leerlos, entenderlos o utilizarlos, o con el propósito de falsear o alterar el nombre del usuario, la fecha de creación o modificación u otra información que se utilice regularmente para identificar la información, mensajes o archivo, si no se obtiene previamente el consentimiento por escrito del Coordinador General. En el caso de que por razones de seguridad se permita codificar, asignar contraseñas o modificar alguna información a fines de evitar que otras personas puedan leerla, la OFSA estará facturada para decodificar la misma o restituirla a su condición original, y el usuario será responsable de proveer todos los datos para lograr acceso a la información y archivo.



Aceptación y Procedimientos Disciplinarios

- Se tomarán las medidas disciplinarias, civiles o criminales que correspondan contra los usuarios que violen estas políticas o abusen del acceso al Internet, según sea el caso.
- La OFSA se reserva el derecho de radicar acusaciones criminales por las actuaciones que constituyen delito federal o estatal aunque no estén expresamente prohibidas por estas condiciones de uso de los equipos de computadoras.
- Entiendo las normas citadas y acepto que se ha divulgado toda información relacionada al uso de esta computadora. Además, el personal cualificado de la OFSA está disponible para aclarar las dudas que puedan surgir en cuanto al cumplimiento de estas condiciones de uso.
- Acepto que es mi obligación como usuario, conocer y seguir todas las políticas o instrucciones de la OFSA en cuanto a las medidas de seguridad del uso del equipo de computadoras y de las redes disponibles, particularmente las *Normas Adoptadas para la Utilización del Internet*.
- El hecho de que una conducta o actuación relacionada con las computadoras, redes, sistemas y recursos electrónicos de la OFSA no esté contemplada en estas advertencias y condiciones de uso de las computadoras, no impide que el usuario pueda ser sancionado, si a juicio del (la) Coordinador General se trata de una conducta o actuación imprudente o irresponsable en relación a los referidos equipos y recursos electrónicos. A los fines de estas advertencias y condiciones de uso, una conducta o cualquier actuación imprudente o irresponsable significa cualquier acción directa o indirecta que ponga en riesgo la seguridad, integridad y confiabilidad de los equipos, las redes, la información, los programas y los sistemas de la OFSA. Uso imprudente o irresponsable significa, además, cualquier actuación o conducta directa o indirecta que pueda ocasionar daño físico, mental, moral, problemas interpersonales o un menoscabo de la reputación de los usuarios, personas ajenas a la OFSA o el (la) Coordinador(a) General.
- Acepto que es mi obligación al Coordinador (a) General; al (a) Director (a) de Sistema de Información y a mi supervisor inmediato o a la persona delegada a esos fines, cualquier situación, incidente o problema de seguridad, acceso indebido o violación voluntaria o involuntaria de estas normas, que surja en el uso de las computadoras.

Al aceptar utilizar la (s) computadora (s) usted reconoce haber leído y entendido dicho Reglamento de Normas sobre el Uso de los Sistemas Electrónicos.

Firma: _____

Fecha del ___ de _____ de 2011