CONEXIÓN LABORAL
ÁREA LOCAL SUROESTE

AmericanJobCenter
Área Suroeste

Área Local del Suroeste/ALCLS /American Job Center/AJC
Plaza Pitito Carr. # 2 Km. 170.0 Apartado Box 246 San Germán, Puerto Rico 00683
Tel. (787) 787-892-1000 Fax (787) 892-5540 TTY (787)-892-2935 Libre de Cargos 1-800-981-8155

ASUNTO: Procedimiento de respuestas de emergencia y recuperación de la Red y/o Sistema del ALCLS		**NUM. FORM. CL-PROC-024**	**Pág. 1 de 12**
Fecha de Efectividad 1 de abril de 2025	**Revisado _____ Derogado _____**	**Aprobado Por: Roque A. Ramírez Palermo**	

I. INTRODUCCIÓN

Como parte de las medidas de seguridad a llevarse a cabo con los Sistemas de Información (Red y/o Sistema y/o sistema) en Área Local del Suroeste/ALCLS y su Centro de Gestión Única/AJC y su Área de Sistemas de Información/MIS, presenta un procedimiento y/o plan de contingencia a ejecutarse en caso de ataques cibernéticos, desastres naturales, vandalismos, accidentes, acciones premeditadas, entre otros; que pudieran impedir la función de la Red y/o Sistema del ALCLS.

II. BASE LEGAL

Este procedimiento se promulga en virtud de las siguientes leyes, reglamentos, cartas circulares y memorandos que regulan el manejo de los Sistemas de Información gubernamentales en Puerto Rico.

- Ley Federal, WIOA, Ley Pública 113-128 del 22 de julio de 2014.
- Ley del Código Municipal de Puerto Rico, Ley 107 del 14 de agosto de 2020 antes Ley Núm. 81 del 30 de agosto de 1991, Ley de Municipios Autónomos.
- Reglamento 5518 del 27 de noviembre de 1996 de Asuntos Municipales, sobre la implantación de sistemas mecanizados.
- Reglamento 5859 del 17 de septiembre de 1998 emitido por la Oficina del Comisionado de Asuntos Municipales, trata sobre la dispensa del Sistema Computadorizado.
- Carta Circular de la Oficina del Contralor de Puerto Rico OC-98-11 del 18 de mayo de l998 que sugiere normas y controles para el uso de los sistemas computadorizados.
- Carta Circular de la Oficina del Contralor de Puerto Rico OC-06-13 del 28 de noviembre de 2005 que establece la necesidad de advertir al usuario, en la pantalla inicial del sistema, sobre las normas principales para el uso de este.
- Memorando General Núm. 338-04 del 28 de agosto de 2003 que establece la importancia de que las entidades gubernamentales utilicen programas de antivirus y que actualicen los mismos.
- Y todas las leyes estatales y federales aplicadas a la tecnología de información.

III. PROPÓSITO E INSTRUCCIONES ESPECÍFICAS

Este procedimiento describe los controles internos a establecerse en la Custodia, Control de la Propiedad y tecnología (Red y Sistemas) con cargo a los fondos federales administrados por el Área Local del Suroeste/ALCLS /AJC. El Administrador(a) de la Red y/o Sistema junto al Director(a) Ejecutivo(a) son las personas responsables para completar y llevar a cabo este Plan. Este Procedimiento y/o Plan de Contingencia y Prevención, provee una guía para actuar adecuadamente en caso de surgir una situación (causas naturales, accidentales o criminales) que impida el uso de la Red y/o Sistema de ALCLS. Nos brinda unas guías para ayudar a lograr el restablecimiento de las operaciones en la Red y/o Sistema de ALCLS a su normalidad en un tiempo razonable. No obstante, específica posibles situaciones que se deben tomar en consideración, las cuales puedan interrumpir la operación normal del sistema de informática en nuestra agencia. Canaliza el esfuerzo del personal para enfrentar los eventos de desastre y ayudar a restaurar de manera eficiente las funciones y servicios de la Red y/o Sistema, y así poder continuar cumpliendo con la misión de este. Los objetivos incluyen:

- Minimizar la interrupción de servicios
- Planificar un desenlace bajo control y apoyo
- Asignar prioridades a los trabajos
- Asegurar la información, datos y equipo

Como objetivo principal debemos prepararnos adecuadamente para confrontar desastres antes de que ocurran. Es de gran utilidad para casos donde se presenten situaciones de emergencias y se puedan ver afectados los sistemas de la informática. Las estrategias para enfrentar dichas situaciones de desastre, nos permite garantizar menos pérdidas ante cualquier tipo de situación, trabajar con anticipación y capacitar al personal de resguardo para dichas funciones y/o ayuda, logrando que una situación no se transforme en un caos. Entre las estrategias se encuentran:

- Cumplir con las leyes, reglamentos y normas.
- Realizar pruebas periódicas y simulacros para la elaboración de ideas, soluciones estratégicas ante desastres.
- Identificar las necesidades que poseen los sistemas de informática constantemente.
- Utilizar el tiempo mínimo en la recuperación de datos y reestructuración de documentos y/o equipo tras un evento de desastre.
- Analizar el impacto del evento, si es posible con anterioridad, (en caso de huracanes) sobre los sistemas y/o Red.

A. Información General

La anticipación a un desastre no consiste únicamente en establecer una serie de pasos a seguir para cada uno de los eventos de estos que puedan afectar la Red y/o Sistema del ALCLS. Consiste en asumir situaciones que puedan ocurrir y determinar acciones a seguir o evitar las consecuencias que esta causa.

1. Tipos de Desastres que pueden afectar Red y/o Sistema de ALCLS

   a. Causas Naturales como: Huracanes, Fuego, Terremotos, Inundaciones, Tormentas, Eléctricas, inserción de animales inesperados, entre otros.
   b. Deterioro de estructuras en oficinas, Cortos circuitos, Inundaciones causadas por tuberías rotas cerca del centro de cómputos y otras áreas, Cambios en temperaturas en el centro de cómputos (humedad excesiva) causados por problemas con el acondicionador de aire, Fallas en la energía eléctrica.
   c. Causados por seres humanos como: Sabotaje al sistema computarizado, a la red, Robo de Equipo, cablería, líneas, a la fibra óptica, Líquidos de limpieza u otros materiales corrosivos que se filtren o exploten.
   d. Errores del usuario como: borrar archivos críticos, utilizar el sistema sin autorización correspondiente, Personal sin experiencia haciendo tareas de Administrador, Utilizar algún "pen drive", disco, etc.) infectado con virus.
   e. Por fallas de equipo o tecnología, en los componentes de la Red y/o Sistema tales como: Servidores, "Hubs", "Power Supply", Disco duro, Corrupción de la Data, Contaminación por algún virus por que el programa de Antivirus no lo detecte.

B. Preparación previa ante un desastre

1. Avisar el personal del Área Local asignado a realizar tareas en la Oficina de Sistemas y Administración de la Red y/o Sistema de ALCLS.

   a. Administrador de la Red y/o Sistema
   b. Técnicos de apoyo
   c. Personal adiestrado
   d. Otro personal asignado según las necesidades y la naturaleza de la emergencia
   e. Personal externo contratado según las necesidades y la naturaleza de la emergencia
   f. Activar el personal asignado a realizar tareas de recuperación
   g. Hay que asegurar que todo el equipo computarizado del Consorcio y de las dependencias localizadas fuera del mismo estén en un área donde no se vean afectado por el desastre.

2. Preparación de Área

   Elementos que se deben tomar en consideración para la ejecución de este Plan son los siguientes:

3. Medidas de Seguridad

   a. Áreas Restringidas:

      - El área donde se encuentra el Sistema esta restringida.
      - Acceso al equipo y el Sistema esta controlado.

- Sólo personal autorizado por el Administrador de la Red y/o Sistema podrá entrar a dichas áreas, accesar y realizar cambios al equipo (operadores, técnicos de comunicaciones, personal de mantenimiento y suplidor de equipo) según sea requerido.

b. Lista de Acceso:

- Se mantienen listas de acceso de todo el personal autorizado a entrar o manejar el Sistema y al área donde este reside, indicando el nivel de autorización a las diferentes secciones del área.

c. Acceso Remoto con Modem

- Con el propósito de salvaguardar la integridad de acceso remoto a las computadoras del centro, se requiere a los usuarios remotos, de haber alguno, un cambio de código de acceso "contraseña" periódicamente, según los requisitos de seguridad lo requieran.

d. Equipo de Emergencia

- El equipo requerido debe estar disponible y en condiciones útiles. Además de tener todo el equipo necesario para procesar el Sistema identificado, se debe considerar incluir como mínimo lo siguiente: Lámparas portátiles de baterías, Detectores automáticos de humo, Extintores portátiles para incendios, Botiquín de primeros auxilios. Además, se debe localizar una planta eléctrica, a utilizarse cuando sea necesario en caso de que la electricidad falte luego de un evento de desastre. Estos equipos deben ser inspeccionados periódicamente por personal competente.

e. Estructura de Llamadas

- El/la director(a) Ejecutivo(a) y el Director de MIS, seleccionarán o identificarán el personal del ALCLS y el orden a ser contactados para la notificación de algún evento de desastre o cualquier emergencia que pueda afectar las operaciones del Sistema.

f. Resguardo de Archivos y Formas

- El mantener un buen sistema de resguardo de datos del Sistema de informática del ALCLS es bien importante y necesario para protegerlos. Una vez esto se determina; el Administrador de la Red y/o Sistema debe identificar el lugar de almacenamiento alterno, fuera del edificio donde se encuentra el Sistema. Este lugar debe ser a prueba de fuego y con las debidas medidas de seguridad.

  De esta manera, se asegurará que los archivos de datos del Sistema estén disponibles en caso de necesitarlos para recuperar mismos.

- Cada información o data que se ha resguardado debe indicar el Nombre de ALCLS, el servidor o servidores, el tipo de resguardo *"Backup"*, y la fecha. Este resguardo se debe documentar, para tener un registro de la data resguardada y donde está almacenadas.

g. Edificio Alterno o Provisional:

- En caso de que la planta física del ALCLS haya sufrido problemas durante un desastre que le impida el funcionamiento del Sistema, pero el equipo y el Sistema se encuentran en condiciones funcionales, se debe mudar el equipo junto con el Sistema a algún edificio alterno o provisional con las facilidades necesarias. Este edificio alterno se identificará previamente haciendo los arreglos pertinentes para solicitar su uso cuando sea necesario. Toda la información o data debe estar provista o almacenada en la *"Nube de Microsoft"*, ya que de esa forma en cualquier lugar alterno se pueda acceder sin necesidad de mudar tantos equipos.

h. Procedimiento de recuperación

- Se debe identificar claramente el proceso a seguir para recuperar los datos de ALCLS. Se debe revisar periódicamente y modificar para que se ajuste a las necesidades existentes en cada momento.

i. Adiestramientos y Simulacros

- El Administrador de la Red y/o Sistema preparará un itinerario de adiestramiento y ejercicios de prueba para verificar que el personal conozca las acciones a tomar en caso de que ocurra algún tipo de desastre o eventualidad.

j. Resguardo del Plan

- Es sumamente importante guardar copia de la última versión del Plan de Contingencia para la Red y/o Sistema Sistemas de Información, con el *"Backup"*.

k. Designación de áreas críticas

- La designación de áreas críticas pretende establecer los parámetros necesarios para declarar una emergencia en los servicios de la Red y/o Sistema de ALCLS, los cuales requieran la activación de este plan. Las áreas críticas son: Área de servidores en la oficina administración de la red y/o sistema principal/MIS y secundario, sistema de internet.

l. Posibles escenarios

- Problemas en el hardware
- La destrucción o daño por causas fortuitas, naturales o de otra índole o incapacidad de poner en funcionamiento cualquiera de los servidores.
- La destrucción o daño del disco duro o procesador por causas fortuitas, naturales o de otra índole o incapacidad de poner en funcionamiento cualquiera de estas partes en los servidores.
- La destrucción o daño por causas fortuitas, naturales o de otra índole del cableado y/o equipo de comunicación o incapacidad de poner en funcionamiento la mencionada estructura.

m. Problemas de programación o lógica

- El daño, destrucción o imposibilidad de utilizar los archivos, programa de base, y otros por causas naturales, energía o virus informáticos en los servidores.

4. Análisis del impacto del desastre

a. Prioridades:

- Evitar pérdidas de vida
- Satisfacer las necesidades básicas
- Reanudar las operaciones lo antes posible
- Identificar áreas afectadas lo antes posible

b. Definición de los niveles mínimos de servicio

- Se considerará como niveles mínimos de servicio lo siguiente: acceso a los archivos, comunicación con las dependencias.

c. Identificación de las alternativas de solución.

- Reemplazo de servidor por uno de los alternos, energía, seguridad, si las condiciones de ambiente, energía, seguridad y/o comunicaciones así lo requieren.
- Además de: implementar procesos manuales, contratar servicios de ser necesarios con terceros, diferir la tarea crítica por un tiempo determinado u otra medida que permita continuar las operaciones.

IV. Activación del Procedimiento o Plan de surgir alguna situación

El Plan de Respuestas a Emergencias se activará bajo cualquiera de las siguientes circunstancias:

1. Esperar las instrucciones de oficiales gubernamentales y de la agencia, ALCLS, indicando la probabilidad de que la aproximación de un desastre para la isla es inminente.

2. Evento de Desastre: Un evento que incapacite parcial o totalmente las instalaciones del sistema del ALCLS por un periodo mayor a 4 horas.

3. Deterioro de Operaciones: Un evento que deteriore el procesamiento de los datos del Sistema o equipo del ALCLS por circunstancias que estén fuera de los parámetros normales de las operaciones.

   El Director(a) Ejecutivo(a) y el Administrador de MIS declararán un estado de emergencia y notificarán a las áreas correspondientes, las tareas, responsabilidades y se mantendrán hasta que el incidente sea resuelto y notifique que todo está en orden.

V. Procesos activados:

Los siguientes procesos efectuarán a la mayor brevedad posible:

1. 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 Sistema en el menor tiempo posible.

2. En caso de fuego o terremoto 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.

3. Se implantará un proceso de restauración y se activará inmediatamente.

VI. Procedimientos para efectuar durante el desastre

Una vez se haya decretado la llegada del desastre, se deben efectuar los siguientes procesos:

1. Localización y protección de los equipos en el consorcio:

   a. Se debe evaluar la localización de los equipos utilizados en el ALCLS para los trabajos del sistema y evitar posibles daños ante el paso de un huracán o desastres naturales.

   b. Se debe relocalizar el equipo que esté más propenso a sufrir daños realizando lo siguiente:

      - Apagar y desconectar el equipo electrónico de los interruptores eléctricos.
      - Identificar correctamente la cablearía que va desde el sistema central hasta los terminales, impresoras y otros prefiérales, antes de moverlos de su sitio.
      - Colocar el equipo en un lugar elevado; se requiere sumo cuidado en el manejo de este equipo.
      - Alejar el equipo de ventanas o puertas que puedan afectarse con el suceso.
      - Asegurar ventanas y puertas cercanas al equipo.
      - Cubrir el equipo con bolsas plásticas u otro material protector.

2. Protección para material de trabajo:

    a. Se debe organizar y proteger todo el material de oficina, documentos, equipo y herramientas importantes para el procesamiento de la Red y/o Sistema de ALCLS como prevención al paso de un huracán o cualquier desastre natural.

    b. Resguardo de datos:

        - Se debe realizar un resguardo adicional al resguardo diario de los últimos datos de la Red y/o Sistema de ALCLS, para poder usarlos tan pronto termine el evento de desastre. Debe guardarse en el lugar seleccionado para resguardo y debe identificarse apropiadamente. De no ser posible por la avenencia del evento, el Administrador de Sistemas de Información deberá guardarlo en otro lugar que sea seguro y protegido contra el desastre.

        - Se deberán guardar digitalmente todos aquellos documentos necesarios (informes, etc.) para actualizar la data, en caso de que la cinta resguardada no se pueda utilizar o no tenga los datos más recientes.

    c. Desalojo del lugar:

        - De ser necesario el desalojo del lugar, el personal debe desalojar el área y notificar a las áreas pertinentes y desalojar el personal en riesgo.

    d. Actividades durante el evento:

        - Permanecer en un lugar seguro e informado a través de radio, en especial lugares posiblemente afectados por el desastre. Seguir las instrucciones de las autoridades oficiales designadas en el evento.

VII. Procedimiento después del desastre

De surgir algún tipo de desastre natural que impida la continuidad del procesamiento diario de datos por medio de Red y/o Sistema de ALCLS, y de existir urgencia para la utilización y procesamiento de estos datos luego de ocurrido el desastre, el ALCLS debe ejercer las siguientes tareas:

1. Acceso al Sistema:

    a. Durante el período de restauración, el acceso al Sistema se restringirá a usuarios autorizados solamente para el manejo de documentación y programación útil. De esta forma nos aseguramos de que ninguna información sea saboteada durante la activación del Sistema de Informática.

    b. Además, se requerirá la más estrecha vigilancia en las puertas de entrada y salida, para así salvaguardar y minimizar pérdidas de propiedad de ALCLS.

2. Verificar y Relocalizar el equipo:

   a. Verificar el equipo y relocalizar en áreas disponibles el equipo que funciona para que el personal pueda continuar con su agenda de trabajo.
   b. El encargado de la red y/o sistema de ALCLS tratará de restablecer o inicializar el sistema de acuerdo con los procedimientos descritos a continuación:

      - Verificar que el ambiente sea seguro para el operador y el equipo a la red y/o sistema, que la carga eléctrica del ALCLS sea adecuada para minimizar daños al equipo y ver físicamente los daños ocasionados durante la emergencia, que esté todo correctamente conectado y que pueda subir el sistema normalmente y poder entrar. Si al conectarlo y prenderlo no funciona debidamente, se deben comenzar la restauración de la red y/o sistema de ALCLS.

3. Evaluación de daños:

   a. Luego del desastre, se debe realizar una evaluación de posibles daños a los equipos cuidadosamente. En dicho inventario se debe especificar el tipo falla (si es de hardware o software).

   b. El equipo que se encuentre defectuoso se debe informar rápidamente para contratar suplidores, esto con la autorización del PDL la para reparación o cambio.

4. Trámite con compañía de seguros:

   a. Si el desastre ocurrido ha causado daño al equipo, se debe tramitar la reclamación con la compañía de seguros, primeramente, la reclamación correspondiente antes de comprar.

5. Restauración de la Red y/o Sistema de ALCLS:

   a. Los pasos por seguir para que el Sistema funcione dependerán de la condición de este o de la planta física donde este localizado. Por ejemplo:

      - Fallas en Planta Física Solamente

      Si el único problema en el edificio de ALCLS donde se encuentra localizado el sistema de informática, es causa de problemas eléctricos, pero el equipo y el sistema se encuentran en condiciones funcionales, se debe utilizar la planta eléctrica previamente localizada y reservada para estos casos en lo que se restablece la electricidad en dicha área.

      De haber surgido problemas en la planta física del ALCLS que impida el funcionamiento del sistema de informática, pero el equipo y el sistema se encuentran en condiciones funcionales, se podría mudar este equipo y el sistema a un edificio alterno con las facilidades necesarias para operar el Sistema.

Esto con la debida solicitud y autorización del PDL. Si el problema no es tan grave se puede funcionar u operar en la unidad móvil provisionalmente en lo que se restablece el sistema en las facilidades físicas. ALCLS es el responsable de la mudanza del equipo. Se requiere que el personal a cargo de la mudanza identifique correctamente y con sumo cuidado en el manejo de este equipo.

- Fallas en Comunicación

La comunicación entre el equipo de computadoras y las áreas de trabajo (los usuarios) se lleva a cabo a través de las líneas de cable distribuidas a través del techo y red y/o sistemas del edificio, y los "hubs" localizados en los paneles de comunicación. Sólo el administrador de la red y/o sistema o personas designadas estarán autorizados a intervenir en las fallas causadas por averías de cables de comunicación.

- Sistema o Equipo no está Funcional:

De haberse averiado los equipos que no puedan ser útiles, se debe recurrir a obtener los "Backups", de resguardo.

- Uso de la Red y/o Sistema de ALCLS Alterno:

Una vez restaurados los datos y creado la contraseña, se podrá utilizar el Sistema alterno.

- Resguardo (*Backup*) de los datos generados en la Facilidad Alterna:

Luego de que el ALCLS haya finalizado la utilización de la red y/o sistema en las instalaciones alternas, se procederá a hacer un resguardo (*backup*) diario de los datos generados.

- Restauración de los datos generados para la actualización

Una vez finalizado el procesamiento en las instalaciones alternas y el sistema se encuentre operando, se deberán restaurar los datos generados en el mismo.

- Otras opciones de restauración son: *restauración incremental*, se guardan todos los datos que han cambiado desde el *"Backup"*, *restauración diferencial*, se guardan todos los datos de último *"Backup"*, *restauración selectiva*, se guardan los datos seleccionados por el operador, *restauración-"Hosting"*, se guardan los datos en un servidor privado.

VIII. Pruebas de Respuestas a Emergencias

Estas pruebas al manejo de sistemas de informática deberán probarse, como mínimo, cada 6 meses. Esto debe incluir:

1. Verificación del equipo a usarse en caso de desastre en la instalación
2. Utilización de los archivos que están siendo resguardados,
3. Activación del grupo de trabajo.
4. Esto ayudará a lo siguiente:

    - Verificar que el personal asignado en caso de desastre conozca las acciones a tomar en caso de que ocurra alguno de los desastres o eventualidades indicadas.
    - Mantener a empleados designados para ayudar y adiestrarlos en los procedimientos que se deben seguir y adiestrar al empleado nuevo.
    - Asegurarse que procedimiento no ha sufrido cambios desde que se creó inicialmente.
    - Asegurar la eficacia en el procesamiento de los datos de la red y/o sistema de ALCLS en casos de emergencia.
    - Velar que la instalación del local alterno seleccionado está capacitada para trabajar los datos del ALCLS en caso de desastre.

Con el propósito de obtener el mejor nivel de eficiencia en la ejecución de este procedimiento y/o plan de contingencia para el manejo de sistema de informática para la restauración de la red y/o sistema de ALCLS, se deberán evaluarán los incidentes ocurridos.

El propósito es mejorar los procedimientos a seguirse en el ejercicio de recuperación. Se debe medir el tiempo que tomó poner en operación el sistema, ya sea en el ALCLS o la instalación del local alterno. Se deben anotar todos los contratiempos ocurridos que impidieron que el procedimiento o plan se ejecutara de forma eficiente.

Se deben para anotar los resultados de cada ensayo o adiestramiento. Después de cada ensayo, el Director(a) Ejecutivo(a) o el Director(a) de Sistema de Información convocará a todo el personal con el propósito de evaluar la información recopilada durante el ensayo y sugerir modificaciones que puedan mejorar la ejecución del procedimiento o Plan.

IX. Administración del procedimiento o plan

El Director(a) Ejecutivo(a) o persona designada del ALCLS tendrá a cargo la administración de este procedimiento o Plan. Además, será responsable y velará de que esté actualizado, se lleven a cabo los adiestramientos y se lleven a cabo los ensayo o simulacros de prueba necesarios.

X. Actualización:

Para garantizar que el procedimiento o plan del sistema de informática se mantenga actualizado, se le incorporarán cambios a medida que éstos surjan. El Director(a) Ejecutivo(a) o persona designada será responsable de que el Plan se mantenga al día. Este deberá ser revisado por lo menos cada 6 meses para mantener la información actualizada.

XI. Ejercicios y pruebas:

El Director(a) Ejecutivo(a) o persona asignada programará los ejercicios de simulación. Además, programará la ejecución de pruebas para adiestrar a los empleados sobre las funciones que deberán llevar a cabo, según el adiestramiento identificado. Esto le permitirá evaluar el nivel de eficacia en la ejecución de los procedimientos.

En el campo de sistemas computadorizados de información se implantaron procedimientos para la protección de los equipos, la reconstrucción de archivos y equipos, y el restablecimiento de las operaciones en el menor tiempo posible, en una forma organizada y correcta. Se deben efectuar los siguientes procedimientos de prueba, ensayo, simulacro y actualización de información para este procedimiento plan de Contingencia. En la actualidad el ALCLS consta con servicios de restauración de data en caso de un desastre o accidente; Vitalización de Servidores – ALCLS tiene un servidor virtualizado con tres servidores. También se hace "Backup", en unos servidores privados.

XIII. VIGENCIA

Si cualquier palabra, inciso artículo, sección o parte del presente procedimiento fuese declarada inconstitucional o nula por un tribunal, tal decisión no afectará, menoscabará, invalidará las estantes disposiciones y partes de este procedimiento. La nulidad o invalidez de cualquier palabra, inciso, oración, artículo, sección o parte del reglamento por determinación judicial no se entenderá que afecta o perjudicará en sentido alguno su aplicación a validez en cualquier otro caso.

Este procedimiento podrá enmendarse en cualquier momento que así lo creyere conveniente el Área Local de Conexión Laboral del Suroeste/ALCLS/AJC, de acuerdo con lo estipulado en la Ley WIOA, su Reglamentación Federal y Ley del Código Municipal de Puerto Rico, Ley 107 del 14 de agosto de 2020 antes Ley de Municipios Autónomos, en beneficio del interés público. Este procedimiento comenzará a regir inmediatamente después de su aprobación.

Aprobado en San Germán, Puerto Rico, hoy 27 de marzo de 2025.

Aprobado por:

Sr. Roque A. Ramírez Palermo
Presidente Junta Local/WDB

Agnes Mojica Comas
Secretaria Junta de Directores/WDB

Anejo A

ÁREAS RESTRINGIDAS SISTEMA RED Y/O SISTEMA DE ALCLS

EDIFICIO	DESCRIPCIÓN AREA
Oficina Central – 2do piso	Servidor internet, panel distribución, concentradores y almacén.
Oficina Central – 2do piso	Servidor primario y secundario, panel distribución, concentradores y área de reparaciones.

NIVEL DE AUTORIZACION

Grupo	Componentes	Funciones
A	Gerencia	Decisiones Generales
B	Sistema de Información	Coordinación – Informa al Grupo A
C	Encargada de Propiedad	Restauración de Centro-Equipo

PERSONAL AUTORIZADO ACCESAR AREA SISTEMA RED Y/O SISTEMA DE ALCLS

Nombre	Puesto	Nivel de Autorización
Elliot Class Torres	Director Ejecutivo	A
Carmen Ríos Seda	Ayudante Director Ejecutivo	A
Griselda Rivera Perez	Ayudante Director Ejecutivo	A
Norma I. López Padilla	Directora de Finanzas	A
Iris J. Ruiz Bermúdez	Directora de Recursos Humanos	A
Herbert Ortiz Rodríguez	Director MIS	A y B
Jan-Karl Michael Vélez	Técnico de Computadoras	B
Richard Rivera Torres	Supervisor Cómputos	B
Myrna Figueroa Lugo	Encargada de la Propiedad	C

Anejo B

Procedimiento de Resguardo de Sistema

Los procedimientos para hacer el backup de Sistema se explican a continuación.

1. Servidor: Central2

   a. Hacer 2 clicks sobre el icono Verita Backup exec 9.1 for Windows Servers.
   b. Seleccionar Pestaña de Backup ó hacer click en la flecha al lado de Backup y seleccionar New Backup Job.
   c. Seleccionar Backup.
   d. Hacer click sobre Selections:
      - En Selection list description: (Escribir breve descripción del Backup).
      - Hacer click sobre la pestaña de "View by Resourse":
        - En central2, seleccionar:
          - System State
          - Shadow Copy Components
        - Hacer click sobre "Microsoft Windows Network":
          - Hacer click sobre ALCLS (Ver documento adjunto Backup todos-excepto Archivo, muestra los equipos y los directorios a hacer Backup).
        - En Destination, seleccionar "Device and Media"
        - En Settings (Ver documento adjunto Backup todos-excepto Archivo, este muestra los Settings apropiados).
        - En Schedule:
          - Run According to Schedule
          - Recurring Week Days, OK. (Ver documento adjunto "Backup", todos-excepto Archivo donde muestra Schedule). Nota: El "Backup", se realizará de acuerdo al itinerario establecido.

2. Servidor: Archivo
   a. Seguir los pasos indicados para el Servidor: central2, excepto que en documento adjunto: Backup Job Properties: Backup Servidor Archivo – Archivos y System State, está impreso los pasos para configurar el Backup.

Historial de Resguardo

La siguiente tabla contiene un historial de la frecuencia con que cada archivo ha sido resguardado. Esto indicará cual es la información más reciente disponible en el lugar de almacenamiento seleccionado, en caso de surgir un desastre. Los códigos usados en la tabla son los siguientes: **Tipo Backup** A = **Archivo,** F = **Full**, S = **System State**, O = **Otro,** FR = **Frecuencia de Resguardo**, **donde** D = **Diario**, S = **Semanal**, M = **Mensual**, A = **Anual**, O = **Otro**

Nombre Empleado	Tipo Bakup	Lugar Almacenamiento		FR	Hora/Set	Fecha de Resguardo
		Consorcio	Archivo			
		Consorcio	Archivo			
		Consorcio	Archivo			
		Consorcio	Archivo			
		Consorcio	Archivo			

Anejo C

Procedimiento de Restauración de Datos

Los procedimientos para hacer la restauración de datos del Sistema se explican a continuación.

1. Servidor: Central2
   a. Insertar la cinta ("Tape") en la unidad externa rotulada Tape Backup-IBM.
   b. Hacer 2 click sobre el icono Verita Backup exec 9.1 for Windows Servers.
   c. Seleccionar Pestaña de Device:
      - En central2:
        - En Stand Alone Drives "Dell1", hacer "right click" y seleccionar Inventory, Run Now.
        - Luego, en Stand Alone Drives "Dell1", hacer "right click" y seleccionar Catalog.
        - Seleccionar la Pestaña de Restore hacer click en la flecha al lado de Restore y seleccionar New Restore Job…
        - Hacer click en OK al mensaje que muestra en pantalla.
        - Seleccionar Pestaña de "View by Media".
        - Seleccionar el "Media" de acuerdo a la fecha deseada. Luego, seleccionar la data deseada.
        - En Destination: Se puede seleccionar "File Red y/o Sistema Irection" – Si se desea que la data se restaure en otro lugar.
        - En Settings, en General: Seleccionar en "Restoring existing files":
          - Restore over existing files – si se desea restaurar la data de la cinta sobre la data que existe en el disco.
          - Overwrite the file on the disk only if it is older – Reescribir la data en el disco solo si ésta (data del disco) es más vieja que la que se copia de la cinta. Nota: Dependiendo de la situación, es la opción para seleccionar.
        - En Advanced:
          - When restoring registry information:
            - Merge the existing hardware configuration and registry services with the data to be restored y/o Sistema.
            - Overwrite the existing hardware configuration and registry services with the data to be restored y/o Sistema.

Nota: Dependiendo de la situación, es la opción por seleccionar. Cuando termina el proceso de Restore el sistema genera un informe indicando el status. Si nos interesa recuperar algún dato es tan simple como ir a la pestana "DISPOSITIVOS" y sobre nuestra unidad de copia dar con el botón derecho a 'Inventariar" para que Backup Exec se dé cuenta de la cinta que tiene, una vez hecho eso, en el mismo sitio botón derecho y "Catalogar", para que Backup Exec vea el contenido que tiene la cinta y nos lo muestre y así ya podamos "RESTAURAR" los datos que nos interesen a donde nos interese.

Anejo D

Orden de Notificación y Responsabilidades

En caso de un desastre o emergencia que pueda o haya afectado el Sistema Red y/o Sistema de ALCLS, la persona a notificar el mismo, deberá poner en operación la secuencia de llamadas en la cadena del mando (ver lista de números al final de este Anejo). Llamar al empleado que se encuentra en el Área de Sistemas de Información de ALCLS.

1. Llamará al Administrador de Sistemas Red y/o Sistema de ALCLS (MIS)
2. De no conseguirlo, llamará al Supervisor de Cómputos (MIS)
3. De no conseguirlo, se llamará al director(a) Ejecutiva
4. De no conseguirlo, se llamará a la directora(a) de Recursos Humanos
5. De no conseguirlo, se llamará al Encargado(a) de Propiedad
6. De no conseguirlo, se llamará al Administrador (a) de Documentos Públicos

La persona que notifique el evento deberá informar la naturaleza del incidente, el status del personal y la acción tomada. De ser necesario desalojar el área. El empleado que informó el incidente será la última persona que abandonará el área, después de verificar *(hasta donde sea posible)* que el resto del personal haya salido.

El empleado de más alto rango en el área afectada, o en su ausencia, el empleado que informó el incidente deberá permanecer en las inmediaciones de la escena hasta que se presente allí un Director o personal autorizado de ALCLS de más alta jerarquía, para que asuma la responsabilidad de coordinar los trabajos. Se le informará la naturaleza del incidente, la situación del personal y las acciones tomadas al Director(a) Ejecutivo(a) o personal autorizado.

El Director(a) de Finanzas o el empleado de mayor rango en la escena del incidente o desastre tendrán a su cargo las siguientes responsabilidades:

1. Velar por la seguridad del personal de ALCLS.

2. Asegurarse de notificar a todas las personas presentes en el lugar de los hechos y a todas las demás personas que deban notificarse.

3. Informar la ocurrencia del evento del desastre a las compañías y a las entidades gubernamentales requeridas a través de sus números de emergencia.

4. Asegurarse que el proceso de prevención del Sistema se haya ejecutado según detallado en el Plan de Respuestas a Emergencias y que las cintas con los últimos datos del Sistema hayan resguardado en un sitio seguro.

Anejo E

Itinerario de Simulacros

I. **Información General:**

Clase de Ejercicio: _____

Oficina/Departamento: _____

Lugar donde se originó: _____

Fecha: _____ Hora: _____

II. **Pasos a seguir:**

1. La Gerencia:

Acción Tomada	Si	No	N/A
Activó el Plan de Respuesta de Emergencia y Recuperación. (Líder Área)			
Notificó a las organizaciones de servicio y emergencia.			
Inició la restauración de utilidades generales y de seguridad			

2. Sistemas/Finanzas:

Acción Tomada	Si	No	N/A
Notificaron a los funcionarios que participan en el Plan de Respuesta de Emergencia y Recuperación.			
Notificó a los miembros de los grupos que ocurrió un desastre o emergencia.			
Notificó y activó a ALCLS			
Comunicación entre agencias (InfoSystems, OGP, OCAM, Phoenix).			
Se utilizaron formatos alternos en las áreas afectadas para recopilar información.			
Acción Tomada	**Si**	**No**	**N/A**
Se establecieron procesos alternos - áreas afectadas			
Se mantuvo la privacidad y confidencialidad de la información.			
Tiempo adecuado en la producción de tareas. Tiempo aproximado:			
Creó respaldos del Sistema Operativo y archivos de producción.			
Relocalizar respaldos de bóvedas externas a la Oficina o Departamento.			
Identificar y relocalizar los equipos e inventario.			
Verificó daños y estado general de los Sistemas (documentar).			
Identificar las necesidades para la restauración.			
Notificó y activó los servicios de recuperación.			

3. Sistemas/Finanzas:

Acción Tomada	Si	No	N/A
Analizar opciones de recuperación y notificar los servicios de recuperación que se pueden utilizar.			
Notificar a suplidores, de equipo y otros productos de la emergencia y posibles necesidades.			
Documentó respuestas de Suplidores y la prontitud en ofrecer lo solicitado.			
Reconstruyó medio ambiente de trabajo.			
Se restauró el Sistema Operativo y programas.			
Se restauró los datos, archivos de producción y aplicaciones críticas.			

4. Personal:

Acción Tomada	Si	No	N/A
El Supervisor del departamento afectado respondió adecuadamente.			
El personal de las áreas afectadas respondió adecuadamente.			

5. Otras observaciones:

Acción Tomada	Si	No	N/A
Existió control en la comunicación entre los departamentos.			
Existió control del personal.			
Se identificó algún personal para proveer el control. Nombre:			
Uso adecuado del teléfono.			

6. Agencias externas en este simulacro:

Acción Tomada	Si	No	N/A
Intervino alguna agencia externa en este simulacro. Nombre Agencia: _____ Personal Agencia: _____			
Personal de la agencia estuvo físicamente. Tiempo que estuvieron en el Municipio:			
Personal de la agencia ayudó vía teléfono. Tiempo que ayudaron:			

7. Hora en que terminó el simulacro/evento: _____

8. Tiempo de duración del simulacro/evento: _____

9. OBSERVACIONES GENERALES:

_____
_____
_____
_____
_____
_____

10. RECOMENDACIONES:

_____
_____
_____
_____
_____
_____
_____

_____ _____ _____

Fecha **Hora** **Evaluador**

Anejo F

Lista de Cotejo

La siguiente lista le ayudará a cotejar si ha tomado en consideración todos los elementos necesarios para la preparación de un Plan de Respuestas a Emergencias. Debe indicar con " √ " si tomó o no en consideración cada elemento, y debe presentar el Anejo correspondientes como evidencia:

Asunto	Sí	No	N/A	Sección de Referencia	Documento Para Entregar
Medidas de preparación					
Medidas de seguridad					
Áreas restringidas					
Lista de Acceso					
Acceso remoto con módem					
Equipo de emergencia					
Agencia Estatal para el Manejo de Emergencias					
Estructura de llamadas					
Información del municipio					
Edificio Alterno a Proveer las Facilidades en Caso de Desastre					
Inventario de equipo, programas y aplicaciones requeridas para correr el Sistema en el ALCLS					
Diagrama de la estructura del equipo en ALCLS					
Resguardo de archivos					
Inventario de equipo, programas y aplicaciones en la facilidad alterna					
Convenio					
Costos relacionados al procesamiento de datos en la facilidad alterna					
Edificio alterno					
Procedimiento de recuperación					
Personal encargado de la restauración del Sistema					
Personal a utilizar las facilidades alternas					
Itinerario de adiestramiento					
Itinerario de pruebas (simulacros)					
Lugar de resguardo del Plan de Respuestas a Emergencias					