



HON. MIGUEL ROMERO
SECRETARIO

8 de octubre de 2010

Sra. Lourdes Díaz Valcárcel
Directora
División de Auditorías
de Tecnologías de Información
Oficina del Contralor de Puerto Rico
San Juan, Puerto Rico

INFORME COMPLEMENTARIO AL PLAN DE ACCIÓN CORRECTIVA (ICP-2), INFORME DE AUDITORÍA TI-09-14

Estimada señora Díaz Valcárcel:

Incluimos para su evaluación el **Informe Complementario al Plan de Acción Correctiva (ICP-2)** correspondiente al **Informe de Auditoría TI-09-14 del 6 de febrero de 2009**, emitido por su Oficina, sobre las operaciones de la Oficina de Cómputos y Sistemas de Información del Departamento del Trabajo y Recursos Humanos.

Para información adicional, puede comunicarse con la Sra. Alba I. Maldonado Colón, Directora Ejecutiva de la Oficina de Auditoría Interna y Fiscalización a los teléfonos 787-754-5398 ó 787-754-5397.

Nos reiteramos en nuestro compromiso de colaborar en los procesos que realiza su Oficina para mejorar la fiscalización y administración de la propiedad y de los fondos públicos.

Cordialmente,

Miguel Romero

Anejos

- c Hon. Carlos J. Torres Torres, Presidente
Comisión Conjunta sobre Informes Especiales del Contralor



OFICINA DEL SECRETARIO



PLAN DE ACCIÓN CORRECTIVA

Informe de Auditoría o especial: TI-09-14 Número de unidad: 5310 Entidad auditada: Departamento del Trabajo y Recursos Humanos

Fecha del informe: 6 de febrero de 2009 Período auditado: 11 de Agosto de 2006 al 10 de Octubre de 2007

Indique: PAC ICP - 2

Funcionario enlace: Alba I. Maldonado Colón Puesto: Directora Ejecutiva, Oficina de Auditoría Interna y Fiscalización Teléfono: 787-754-5398

Funcionario principal o representante autorizado: Hon. Miguel Romero Puesto: Secretario Teléfono: 787-754-2119

CERTIFICO QUE ESTA INFORMACIÓN ES CORRECTA Y COMPLETA

[Firma]
 Fecha: 10/8/2010

Firma del funcionario principal o su representante autorizado

| RECOMENDACIÓN | ACCIÓN CORRECTIVA | RESULTADO |
|---|---|----------------------|
| <p>1.c. Realice las gestiones pertinentes para la preparación de un plan de seguridad para la Oficina de Cómputos y Sistemas de Información (OCSI) y someta el mismo para su consideración y aprobación. [Hallazgo 2-a.]</p> | <p>Sometemos el Plan de Seguridad y Manejo de Emergencias de la OCSI, aprobado por el Director de la OCSI y por el Hon. Secretario del Trabajo. (Anejo A: Plan de Seguridad y Manejo de Emergencias de la Oficina de Cómputos y Sistemas)</p> | <p>Cumplimentada</p> |
| <p>1.d. Desarrolle y someta para su consideración y aprobación las normas y los procedimientos escritos para el manejo de incidentes que establezca, entre otras cosas, una estrategia formal y documentada para el manejo de los incidentes, un equipo de respuesta y documentación de las actividades relacionadas con el manejo de los mismos. [Hallazgo 2-b.]</p> | <p>Sometemos el Plan de Seguridad y Manejo de Emergencias de la OCSI, aprobado por el Director de la OCSI y por el Hon. Secretario del Trabajo. (Anejo A: Plan de Seguridad y Manejo de Emergencias de la Oficina de Cómputos y Sistemas)</p> | <p>Cumplimentada</p> |



PLAN DE ACCIÓN CORRECTIVA

Informe de Auditoría o especial:

TI-09-14 Número de unidad:

5310

Entidad auditada:

Departamento del Trabajo y Recursos Humanos

Fecha del informe:

6 de febrero de 2009

Período auditado:

11 de Agosto de 2006

al

10 de Octubre de 2007

| RECOMENDACIÓN | ACCIÓN CORRECTIVA | RESULTADO |
|--|---|----------------------|
| <p>1.e. Revise la Guía Metodológica para el Plan de Manejo de Emergencias (Guía) para que se incluya la información que se indica en el Hallazgo 4.a. Una vez revisada, someta la misma para su consideración y aprobación.</p> | <p>Sometemos el Plan de Seguridad y Manejo de Emergencias de la OCSI, aprobado por el Director de la OCSI y por el Hon. Secretario del Trabajo. (Anejo A: Plan de Seguridad y Manejo de Emergencias de la Oficina de Cómputos y Sistemas)</p> | <p>Cumplimentada</p> |
| <p>1.g. Mantenga una copia de la Guía y de la documentación de los servidores y de las aplicaciones de un lugar seguro fuera de los predios del Departamento. [Hallazgo 4-c.]</p> | <p>A tenor con la recomendación se mantiene una copia en la facilidad externa de resguardo. Se imprimió y se mantiene una copia adicional de la guía señalada en las facilidades de almacenaje del Departamento del Trabajo y Recursos Humanos en el Edificio del Negociado de Seguridad de Empleo. (Anejo B: Certificación Director, Oficina de Cómputos y Sistemas de Información)</p> | <p>Cumplimentada</p> |
| <p>1.k. Enmiende el formulario Hoja de Solicitud de Accesos a Sistemas para que contenga la información que se indica en el Hallazgo 7-a. Además, someter copia del formulario enmendado.</p> | <p>Sometemos Hoja de Solicitud enmendada. (Anejo C: Copia de la Solicitud de Accesos a Sistemas)</p> | <p>Cumplimentada</p> |



PLAN DE ACCIÓN CORRECTIVA

Informe de Auditoría o especial:

TI-09-14 Número de unidad:

5310 Entidad auditada:

Departamento del Trabajo y Recursos Humanos

Fecha del informe:

6 de febrero de 2009

Período auditado:

11 de Agosto de 2006

al **10 de Octubre de 2007**

| RECOMENDACIÓN | ACCIÓN CORRECTIVA | RESULTADO |
|---|---|--|
| <p>1.h. Efectué las modificaciones necesarias a las pantallas de políticas de control de contraseñas (Account Policy), de auditorías (Audit Policy) y de seguridad (Security Options), de manera que se corrijan las situaciones comentadas. [Hallazgo 6-a.1]</p> <p>1.m. Prepare por escrito las normas y los procedimientos necesarios para la producción y la protección de los respaldos de la información mantenida en los servidores del Departamento, y someta los mismos para su consideración y aprobación. [Hallazgo 8-a.1]</p> | <p>Se implantaron las recomendaciones de la OGP del 2 de septiembre de 2009, éstas cumplen con la recomendación de la OCPR. Véase documentos adjuntos relacionados. (Anejo D: Security Infrastructure Project, Network Discovery Documentation; Infrastructure Anti-Spam Solution for Internet Mail Flow for Gobierno.pr)</p> <p>Sometemos el Plan de Seguridad y Manejo de Emergencias de la OCSI, éste incluye las normas sobre los <i>backups</i>. (Anejo A: Plan de Seguridad y Manejo de Emergencias de la Oficina de Cómputos y Sistemas)</p> | <p>Parcialmente Cumplimentada</p> <p>Cumplimentada</p> |
| <p>1.n Realice las gestiones para identificar un lugar para almacenar los respaldos realizados a la información mantenida en los servidores del Departamento que no este expuesto a las mismas posibles amenazas de desastres naturales que el edificio donde esta localizado el Departamento. [Hallazgo 8-a.2]</p> | <p>El Departamento del Trabajo y Recursos Humanos cuenta con una facilidad en el Edificio del NSE para almacenamiento de cartuchos de back up. Como plan alterno se considera utilizar la facilidad del Call Center de Ponce (2010) para tener un área de almacenamiento remoto Server to Server. Disponible a revisión. (Anejo E: Certificación Director, Oficina de Cómputos y Sistemas de Información)</p> | <p>Cumplimentada</p> |



PLAN DE ACCIÓN CORRECTIVA

Informe de Auditoría o
 especial:

TI-09-14 Número de unidad: **5310** Entidad auditada: **Departamento del Trabajo y Recursos Humanos**

Fecha del informe:

6 de febrero de 2009 al **11 de Agosto de 2006** al **10 de Octubre de 2007**

| RECOMENDACIÓN | ACCIÓN CORRECTIVA | RESULTADO |
|---|--|-----------------------------------|
| <p>1.p. Redacte y someta para su aprobación las normas y los procedimientos necesarios para reglamentar las operaciones que se comentan en el Hallazgo 11.a. Una vez aprobados, se asegure de que se oriente al personal sobre las disposiciones de los mismos.</p> | <p>Próximamente estaremos trabajando en la redacción de las Normas y Procedimientos correspondientes para cumplir con la recomendación. A continuación parte del proceso utilizado:</p> <ul style="list-style-type: none"> • Antes de transferir o dar de baja un equipo computarizado y/o medios de almacenamiento de información se borran todos los programas o documentos. Si la computadora se va a transferir a otro usuario, se borran los documentos del usuario anterior o se transfieren al nuevo usuario con autorización del Director del Programa. • Accesos remotos a través de <i>Virtual Private Network</i> • Clasificación de los archivos de acuerdo con su importancia y con las funciones que realiza la OCSI • Notificación del cese de un usuario en sus funciones, se utiliza el documento <i>DTRH Rev. 03/09</i> donde se indica la fecha de cancelación de los servicios y luego se elimina la cuenta del <i>Active Directory</i>. Si el usuario es trasladado dentro del <i>DTRH</i>, se solicita la información del traslado para registrar los cambios en el <i>Active Directory</i>. • La solicitud, autorización y aprobación de los cambios a programas y archivos en producción tiene que solicitarse mediante la hoja de Solicitud de Servicio debidamente cumplimentada y firmada. • Evaluación de las funciones de los empleados para determinar el riesgo de funciones incompatibles. | <p>Parcialmente Cumplimentada</p> |



PLAN DE ACCIÓN CORRECTIVA

Informe de Auditoría o especial:

TI-09-14 Número de unidad: **5310** Entidad auditada: **Departamento del Trabajo y Recursos Humanos**

Fecha del informe:

6 de febrero de 2009 al **11 de Agosto de 2006** al **10 de Octubre de 2007**

| RECOMENDACIÓN | ACCIÓN CORRECTIVA | RESULTADO |
|--|--|-----------------------------------|
| <p>1.g. Revise el inventario de programas instalados en la Red para que se incluya la cantidad de licencias existentes por programa. Además, realice revisiones periódicas del inventario de programas instalados para mantener actualizado el mismo y verificar que los programas instalados en las microcomputadoras sean únicamente los autorizados por el Departamento. [Hallazgo 14]</p> | <p>Incluimos el inventario de programas instalados en la Red, éste incluye la cantidad de licencias existentes en general. Consideraremos la implantación de un programa para las revisiones periódicas del inventario, y así poder mantener un control de los programas instalados en las microcomputadoras. (Anejo F: Inventario de programas instalados en la Red)</p> | <p>Parcialmente Cumplimentada</p> |
| <p>2. Medidas tomadas para ver que:</p> <p>2. Se realice y se documente el análisis de riesgos, según se establece en la Política Num. TIG-003, Seguridad de los Sistemas de Información de la Carta Circular Num. 77-05, Normas sobre la Adquisición e Implementación de los Sistemas, Equipos y Programas de Información Tecnológica para los Organismos Gubernamentales, aprobada el 8 de diciembre de 2004 por la Directora de la Oficina de Gerencia y Presupuesto (OGP), y que sugieren en las mejores practicas en el campo de la tecnología. [Hallazgo 3]</p> | <p>Al presente el Negociado Servicio de Empleo se encuentra en un proceso de modificación de sus operaciones añadiendo servicios a través del teléfono y próximamente servicios a través del Internet. Al mismo tiempo está siendo modificado el Procedimiento de Pago de Beneficios del tradicional cheque al de tarjeta de debito. Realizar un Análisis de Riesgo en las Operaciones cuando todavía no han sido completadas o integradas todas las actividades aquí detalladas resultaría en un esfuerzo y una inversión económica incompleta.</p> <p>La proyección para la consecución para las siguientes actividades se detalla en la siguiente cronología:</p> <ul style="list-style-type: none"> • Integración del Call Center Central y del PEEG (Programa Expreso Empleados Gubernamentales), completado (21 de septiembre de 2010). | <p>Parcialmente Cumplimentada</p> |



PLAN DE ACCIÓN CORRECTIVA

Informe de Auditoría o
 especial:

TI-09-14 Número de unidad: **5310** Entidad auditada: **Departamento del Trabajo y Recursos Humanos**

Fecha del informe: **6 de febrero de 2009** Período auditado: **11 de Agosto de 2006** al **10 de Octubre de 2007**

| RECOMENDACIÓN | ACCIÓN CORRECTIVA | RESULTADO |
|---------------|--|-----------|
| | <ul style="list-style-type: none"> • Puesto en operación del Call Center alterno Oficina de Ponce. • Inicio adiestramiento profesional al personal, 1 de octubre de 2010. • Puesto en operación del Sistema Virtual Hold o Llamada en Espera, noviembre de 2010. • Puesto en producción de las Certificaciones de Deuda de Contribuciones Seguro por Desempleo, pendiente calendario Oficina del Gobernador y del CIO. • Análisis y Desarrollo de la solución de Desempleo en línea (a través de Internet), inicio de labores en noviembre de 2010, y fecha tentativa de terminación para Junio de 2011. • Puesta en producción del Pago de Beneficio mediante tarjeta de debito. Pendiente aprobación de contrato por la Oficina de la División Legal. Posible inicio de labores: enero de 2011. <p>Como detalla la cronología esto implica una re-ingeniería de todos los medios y procesos operacionales y de sistema, que imposibilitan realizar un análisis objetivo de riesgo de operaciones en este momento</p> | |

PLAN DE ACCIÓN CORRECTIVA

Informe de auditoría: **71-09-14** Número de unidad: **5310** Entidad auditada: **Departamento del Trabajo y Recursos Humanos**

Fecha del informe: **6 de febrero de 2009** Período auditado: **11 de Agosto de 2006** al **10 de Octubre de 2007**

| RECOMENDACIÓN | ACCIÓN CORRECTIVA | RESULTADO |
|--|--|-----------------------------------|
| <p>6.b. La Secretaría Auxiliar de Recursos Humanos revise el Plan de Clasificación del departamento para que integren al mismo los puestos que ocupan el personal de la OCSI. [Hallazgo 10-a.1]</p> | <p>Al presente no podríamos realizar un plan inmediato para corregir el que el Centro de Cómputos tenga todo su personal con las clasificaciones correctas hasta que se haga el nuevo Plan de Clasificación y Retribución del Departamento. Contamos con una fecha certera de cuándo se espera implantarlo conforme a lo acordado en el nuevo convenio: 1 de abril de 2012 o antes. Estaríamos en los trámites de iniciar la contratación de la compañía que lo trabajará en lo que resta del año, y a partir de enero de 2011, se recopilen los cuestionarios, se organicen y se determinen las clases y su agrupamiento luego de la implantación del Plan de Reorganización. Esto sería de aplicabilidad a todo el Departamento incluyendo los puestos que ocupa el personal de la OCSI.</p> | <p>Parcialmente Cumplimentada</p> |
| <p>10. La OCSI responda a la alta gerencia del Departamento como una unidad independiente de sus usuarios. [Hallazgo 16]</p> | <p>Como parte de la reorganización del DTRH en el nuevo esquema realizado, la Oficina de Cómputos y Sistemas estará como división independiente y responderá a la Oficina del Secretario del Trabajo. El cambio está sujeto a la aprobación de la Oficina de Gerencia y Presupuesto. (Anejo G: Comunicaciones del Director de la OCSI, y del Secretario Auxiliar de Asuntos Gerenciales del DTRH)</p> | <p>Parcialmente Cumplimentada</p> |

ANEJO A



HON. MIGUEL ROMERO
SECRETARIO

DEPARTAMENTO DEL TRABAJO Y RECURSOS HUMANOS

OFICINA DE CÓMPUTOS Y SISTEMAS

PLAN DE MANEJO DE EMERGENCIAS

El Estado Libre Asociado de Puerto Rico es responsable de manejar cualquier tipo de desastre que nos afecte. La forma más eficiente de lidiar con las posibles amenazas es mediante la efectiva coordinación de las Agencias y sus recursos. La densidad poblacional y la posición geográfica del país lo hacen propenso y vulnerable a desastres tanto naturales como tecnológicos, especialmente a huracanes.

Si bien es cierto que los responsables de dirigir una Agencia o una unidad de procesamiento de sistemas no pueden predecir cuándo ocurrirá una interrupción de su área de informática por causa de un desastre natural, lo cierto es que sí pueden prepararse para responder efectivamente a ese evento.

El *Departamento del Trabajo y Recursos Humanos* (DTRH) tiene como visión primordial prevalecer como el organismo gubernamental líder de la provisión y promoción de servicios en Puerto Rico.

En esta época en que se acrecienta en nuestra Isla la posibilidad de ser impactados por un desastre natural, resulta apremiante para la Agencia y para sus áreas operacionales el prepararse para sus posibles estragos. No se trata de aceptar el impacto de un huracán, terremoto, o inundaciones; si no de reconocer que cualquiera de estos eventos puede llevar a una empresa al cierre de sus operaciones al tener un gran impacto en su infraestructura, en especial cuando hoy día la inmensa mayoría de los negocios dependen de sistemas computarizados para seguir funcionando.

Conscientemente de estas situaciones, es apremiante proteger vidas, nuestras instalaciones, el equipo y otras propiedades. Esto con el propósito de continuar ofreciendo los servicios con la misma calidad después de un desastre y cumplir con nuestras responsabilidades con el pueblo de Puerto Rico.

El Departamento del Trabajo y Recursos Humanos, debe estar siempre preparado para tener la habilidad de poder asegurar la continuidad de sus servicios en el menor tiempo posible.

Esto es vital porque la continuidad de las operaciones de la Agencia puede verse afectada tanto por un desastre natural como por algún evento operacional no planificado. Por eso, hay que estar preparados.



OFICINA DEL SECRETARIO

Los VALORES
CUENTAN



Antes y durante un desastre o emergencia del personal del *Departamento del Trabajo y Recursos Humanos* y en especial de la *Oficina de Cómputos y Sistemas* debe familiarizarse con todas las partes y contenido de este Plan. El Personal en general debe tener conocimiento de este Plan como requisito, debe leerlo por lo menos una vez. El coordinador de la Agencia Estatal para el Manejo de Emergencias para el DTRH mantendrá el expediente de las orientaciones, simulacros y otras actividades que se realicen para divulgar el contenido del Plan. Es necesario tener presente y establecido en todo momento, el orden de sucesión del DTRH en caso de emergencias y desastres. El coordinador asegurará que todas las instalaciones cuenten con y promulguen el contenido del Plan Operacional de Emergencias y Desastres entre el personal y los consumidores de los servicios.

PROPÓSITO DEL PLAN

El Plan Ocupacional de Emergencias de la *Oficina de Cómputos y Sistemas del Departamento del Trabajo y Recurso Humanos* contiene información sobre las acciones a seguir a nivel central para proteger vidas y propiedades en acuerdo con las responsabilidades y programas de servicios existentes. Establece la política y organigrama fundamental (línea de mando) en situaciones de emergencias y desastres. El propósito del Plan Operacional de Emergencias es acelerar el proceso de preparación, respuesta y recuperación ante una emergencia o desastre, a través de la implementación rápida de sus programas, que permita ayudar y fortalecer a las áreas afectadas.

SITUACIONES

El pueblo de Puerto Rico está expuesto a peligros debido a emergencias y desastres. Esos tienen el poder de causar daños a la vida y la propiedad en nuestras comunidades.

Entre los peligros que nos amenazan se encuentran: terremotos, huracanes, inundaciones, deslizamientos, derrames de materiales peligrosos, maremotos, incendios, accidentes aéreos, terrorismo o desorden civil.

PRESUNCIONES

En situaciones de emergencias o desastres se verán afectadas las vidas de miles de familias y muchos hogares de Puerto Rico. El Gobierno Central y los Gobiernos Municipales son los responsables primarios de proveer los recursos para salvaguardar vidas y propiedades.

ORGANIZACIÓN Y ASIGNACIÓN DE RESPONSABILIDADES ANTE UNA EMERGENCIA A NIVEL DE LA ADMINISTRACIÓN

En casos de emergencias o desastres se activará el personal directivo y a todo el técnico de Sistemas de Información, y Seguridad y Salud. Se informará a todos los empleados del DTRH, en la medida que sea posible, sobre la emergencia o el desastre.

En caso de que la emergencia sea de naturaleza tal que se avise y se ofrezca tiempo para preparación (como huracanes, inundaciones, etc.) se procederá con los planes ya establecidos de protección de vidas y propiedades. En casos de emergencias o desastres imprevistos, tales como terremotos, fuego, ataques nucleares, etc., se procederá a socorrer los heridos y al desalojo rápido pero seguro del personal de las facilidades, siguiendo los Planes de Desalojo ya establecidos con anterioridad. Para todos los desastres que ocurran la respuesta del personal de la Administración será de acuerdo a los programas y servicios que esta ofrece y a lo ya establecido en este Plan.

FASES DEL MANEJO DE EMERGENCIAS

Mitigación

La fase de mitigación incluye las actividades que pueden eliminar o reducir las probabilidades de que ocurra una emergencia o desastre, o reducen la vulnerabilidad de la comunicación de manera que disminuya al máximo el impacto adverso de una emergencia o desastre. Durante el primer aviso de cualquier evento que resulte en peligro, para minimizar daños en la estructura del edificio se activará el personal de la Oficina de Planta Física para la instalación de las tormenteras en el edificio. Se corroborará que el sistema contra incendio, extintores, lámparas de emergencias estén funcionando correctamente.

Se probará la planta de emergencia una vez al mes durante la temporada de huracanes y una vez cada dos meses el resto del año. La Oficina de Seguridad y Planta Física deberá certificar que la planta eléctrica cuenta con los niveles de combustible diesel óptimo para periodos de operación indefinidos. Se identificarán las áreas vulnerables en caso de emergencia y se intensificará la vigilancia en las mismas. Los directores, supervisores de cada oficina se encargarán de identificar dos personas de su área para que en el momento de la emergencia sean las que ayuden en la movilización del personal.

Preparación

Activación, programas y sistemas de preparación son las frases o etapas previas a una emergencia o desastre. Se utilizan para apoyar y aumentar la respuesta a la situación de emergencia. La Planificación, capacitación y los ejercicios se encuentran entre las actividades de esta fase.

Las operaciones locales están centradas en la red de comunicaciones la cual es el componente que permite la conexión entre todos los importantes sistemas que dependen de ella, entre ellos, SABEN, Interempleo, Sistema MUNIS, Seguro Choferil, Programa Automatizado de Incentivos Salariales (PAIS), Sistema de Sinot y Sistema de Normas del Trabajo. Al presente nuestra agencia cuenta con 2 sistemas de redes integradas como son la de Net-empleo y la de Gobierno.pr. Estas proveen varios servicios de acceso a la agencia, entre los que se mencionan los sistemas de mensajería electrónica y la red global de informática (Internet).

Esquema General

Introducción

Los planes de contingencia constituyen la herramienta más importante para la preparación proactiva de procesos de trabajo alternativos, a ser utilizados en caso de que ocurra una posible falla por desastres naturales (huracanes, terremotos, etc.), incendios, vandalismos, disturbios civiles (amenaza de colocación de explosivos), falta de electricidad o agua que interrumpa la operación normal de la institución. La implementación de planes de contingencia debe asegurar la continuación de los procesos de la agencia a niveles aceptables de servicio y funcionamiento, con el menor tiempo posible de impacto de la manera menos costosa.

Este plan de contingencia debe ser implementado en todos y cada uno de los procesos vitales de la operación de la organización y considerara los componentes críticos que los soportan. Además deben realizarse para todo aquello cuyo control escapa de las manos de la agencia, principalmente en las interacciones con terceros, como son proveedores (OGP, Évertec, PRT, World Net), usuarios, aliados, socios, clientes, etc. También hay que prepararse para posibles fallas en los servicios que apoyan el funcionamiento de la agencia, como son transporte, energía, agua y telecomunicaciones.

Este plan de contingencia se activará cuando algún componente de cualquier proceso crítico falla. También se le empleará cuando aparentemente fallan los esfuerzos de corrección de algún componente. En este caso el plan de contingencia se implementará antes de que ocurra la falla real, para minimizar los daños.

Luego de la experiencia del 9/11 en los Estados Unidos, la seguridad en los Centros de Cómputos se ha convertido en alta prioridad en los proyectos de la Gerencia de las empresas. Las nuevas leyes establecidas anti terrorismo así como anti fraude empresarial obligan la industria a facilitar lo necesario para la protección de la propiedad física e intelectual de las empresas. Los planes de contingencia se han convertido en eje principal de los ajustes que se ven obligados a efectuar los empresarios.

En Puerto Rico muchos piensan que el tener un plan para casos de emergencia es la solución o el reemplazo de un plan de contingencias. Esto ha resultado en dificultades para aquellos que se han enfrentado a una emergencia real y descubren las muchas áreas no consideradas en su plan de emergencias.

Para que una organización funcione correctamente y alcance los objetivos propuestos por la Dirección son necesarios unos activos o recursos:

1. Humanos
2. Materiales (Hardware, ...)
3. Inmateriales (Software, ...)

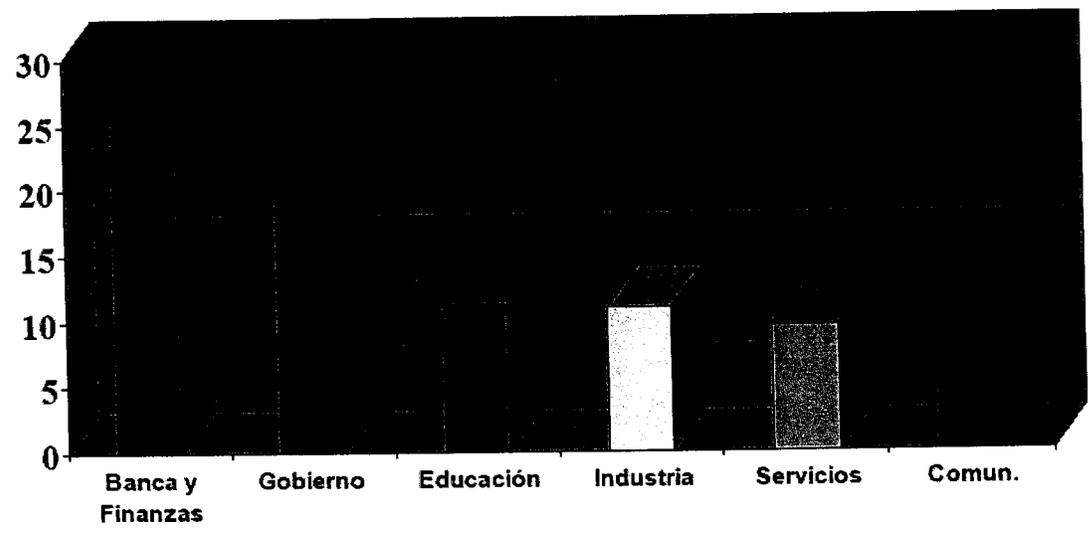
Todos estos recursos se encuentran en un entorno de incertidumbre, que en ocasiones puede provocar interrupciones inesperadas del funcionamiento normal de la actividad.

Hay circunstancias que generan interrupciones que llegan a influir en la capacidad de funcionamiento de los servicios o impiden el desarrollo normal de los mismos.

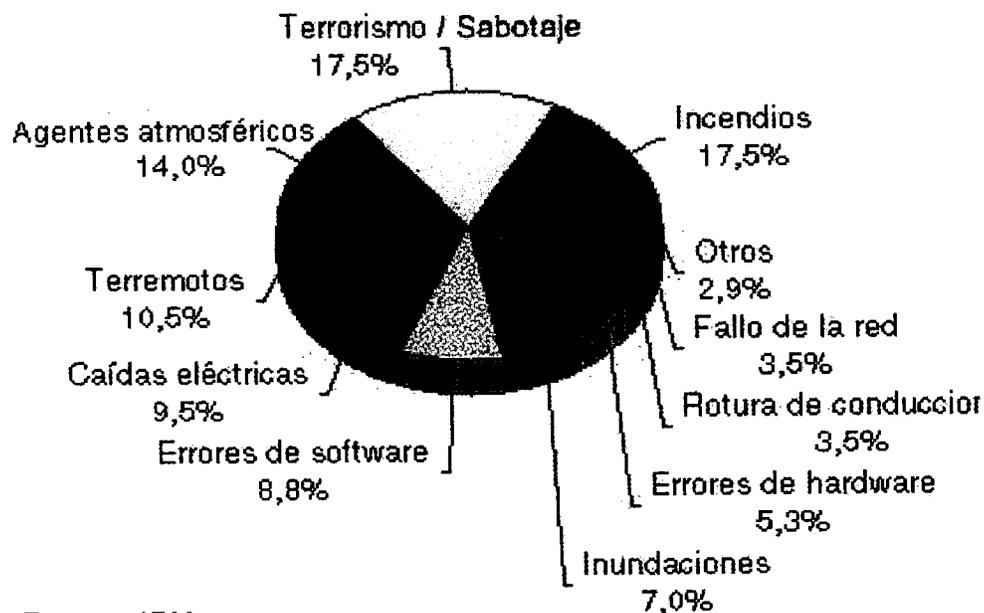
Para prever las consecuencias de estas situaciones hemos establecido estrategias de respuesta ante contingencias que aseguren la continuidad y reanudación de los servicios críticos.

A tales efectos la Oficina de Cómputos y Sistemas decidió desarrollar un estudio de necesidades para sus Centros de Cómputos en el Edificio Prudencio Rivera Martínez así como su Plan de contingencias.

Interrupciones distribuidas por sectores



Causas que interrumpen la actividad informática



Fuente: IBM

El Plan de Contingencias de la *Oficina de Cómputos y Sistemas* implica un análisis de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos de cómputos y la información contenida en los diversos medios de almacenamiento, por lo que en este Manual haremos un análisis de los riesgos, cómo reducir su posibilidad de ocurrencia y los procedimientos a seguir en caso que se presentara el problema. Pese a todas nuestras medidas de seguridad puede ocurrir un desastre, por tanto es necesario que el Plan de Contingencias incluya un Plan de Recuperación de Desastres, el cual tendrá como objetivo, restaurar el Servicio de Cómputos en forma rápida, eficiente y con el menor costo y pérdidas posibles.

Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo posible.

Plan de contingencia y seguridad de la información

Proceso para la implementación de planes de contingencia

Para la Correcta implementación de planes de contingencia de una institución se deben seguir los siguientes pasos:

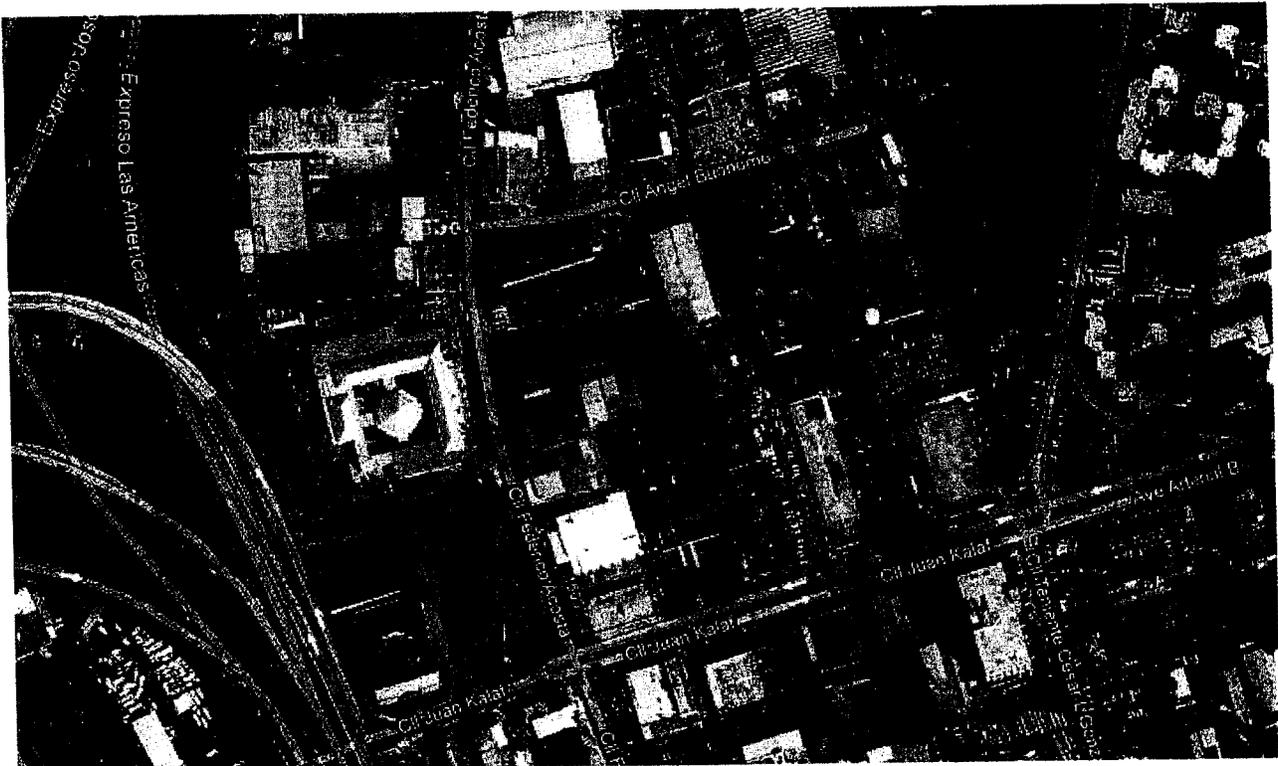
1. Organización del equipo de planes de contingencia

El equipo de planes de contingencia debe incluir no solo recursos del área de Sistemas, sino tantas personas de las áreas funcionales como sea posible. En el grupo hemos seleccionado personas que tengan una visión amplia del funcionamiento global de la *Oficina de Cómputos y Sistemas*, de sus procesos y no de partes aisladas, ya que los planes de contingencia se enfocan ante todo a los procesos y no a los componentes que los soportan. Si bien la premisa básica es la protección de la Integridad del personal, en caso de que el siniestro lo permita (por estar en un inicio o estar en una área cercana, etc.), deberá de existir dos equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y otro para el salvamento de los recursos Informáticos, de acuerdo a los lineamientos o calcificación de prioridades.

El comité asignado al Plan de Manejo de Emergencias está compuesto por:

1. **Sr. José A. Ríos Rivera** -Coordinador
 - Certificado manejo de extintores, primeros auxilios y CPR
 - Instructor búsqueda y rescate sociedad Espeleológica de PR
2. **Sr. Ely J. Padilla Pérez** -Coordinador Alterno
 - Certificado primeros auxilios y CPR
3. **Sra. Ivonne Rivera Agosto** -Coordinadora Asuntos Transferencia Operaciones
4. **Sr. Juan N. Miranda** -Coordinador Asuntos Transferencia Operaciones
5. **Sr. Víctor Medina** -Coordinador Asuntos Transferencia Operaciones
6. **Sra. Myrna Figueroa** -Coordinadora Asuntos Transferencia Operaciones
7. **Daniel Díaz Cabrera**-Búsqueda y Rescate
8. **Sr. Luis Pena Cortes** -Manejo de extintores de incendio
 - Certificado CERT por la OIC. Estatal para el Manejo de Emergencias
9. **Vacante** -Manejo de extintores de incendio

El comité ha definido la métodos de trabajo, cronogramas y responsables de las diferentes actividades, control de avance y ejecución, etc. Es decir, se ha tornado como un proyecto complejo y de suma importancia para la agencia. De esta manera se garantiza que todos las demás personas componentes del equipo y de la agencia apoyen directamente al proceso de planes de contingencia.



2. Análisis de los procesos

Se han identificado los procesos críticos de la *Oficina de Cómputos y Sistemas*, que son aquellos sobre los que se ejecutan las operaciones de sistemas propias de la agencia, y que en caso de ser afectados podrían elevar al colapso total de la misma.

3. Análisis de los activos

Al presente todas las operaciones de aplicaciones de "mainframe" se manejan externamente mediante un "outsourcing" con la compañía Evertec. Aquí se incluyen las operaciones SABEN (Seguro por Desempleo), SINOT, y Contribuciones. Se han ubicado todos los procesos críticos contra todas las aplicaciones de mantenimiento externo, de esta manera será muy fácil la identificación de los activos que más procesos críticos soportan y los procesos que más elementos de posible falla contienen.

La agencia tiene en contrato los servicios del Disaster Recovery Center de la compañía Evertec ubicado en el Centro Industrial 3 Monjitas. De activarse las operaciones de dicho centro el DTRH contaría con la continuidad de los siguientes servicios de Misión Crítica.

Seguro por Desempleo

- A. Corridas diarias.
- B. Impresión de cheques, órdenes de pago, determinaciones monetarias y Reportes.
- C. Resguardo de datos y Recuperación de Desastres.
- D. Conciliación bancaria.
- E. Intercambio de Información con el Gobierno Federal
- F. Mantenimiento de Aplicaciones.

2. Contribuciones

- A. Corridas diarias
- B. Impresión de reportes, informes y planillas patronales.
- C. Resguardo de datos y Recuperación de Desastres.
- D. Conciliación bancaria.
- E. Mantenimiento de aplicaciones.

3. SINOT

- A. Corridas diarias
- B. Impresión de reportes, informes y planillas patronales.
- C. Resguardo de datos y Recuperación de Desastres.
- D. Conciliación bancaria.
- E. Mantenimiento de aplicaciones.

4. Modelo de Costos

- A. Corridas diarias
- B. Impresión de reportes e informes.
- C. Resguardo de datos y Recuperación de Desastres.
- D. Mantenimiento de aplicaciones.

A los efectos, forma parte de este Plan copia del Business Continuity Plan elaborado por la compañía Evertec para el DTRH y aprobado por el Director de la Oficina de Cómputos y Sistemas.

Para asegurar que se consideraran todas las posibles eventualidades, se ha de elaborar una lista de todos los riesgos conocidos, para lo cual se deberá realizar un análisis de riesgos.

4. Análisis de riesgos

El análisis de riesgos supone más que el hecho de calcular la posibilidad de que ocurran cosas negativas. Se ha de poder obtener una evaluación económica del impacto de estos sucesos negativos. Este valor se podrá utilizar para contrastar el costo de la protección de la Información en análisis, versus el costo de volverla a producir (reproducir).

La evaluación de riesgos y presentación de respuestas debe prepararse de forma personalizada para cada organización.

La evaluación de riesgos supone imaginarse lo que puede ir mal y a continuación estimar el costo que supondría. Se ha de tener en cuenta la probabilidad de que suceda cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado.

El análisis de riesgos supone responder a preguntas del tipo:

- ¿Qué puede ir mal?
 - Falta de Agua o Electricidad en el edificio
 - Vandalismo por empleados internos o por conflictos obrero patronales
 - Pérdida de datos por Virus
 - Incendio accidental o malicioso
 - Hurto de equipo

- Hurto de cheques de producción
- ¿Con que frecuencia puede ocurrir?
 - Durante temporada de huracanes
 - Durante conflictos obrero patronales
 - Durante conflicto civil
- ¿Cuales serian sus consecuencias?
 - Perdida de materiales
 - Incapacidad para generar pagos de beneficios de Desempleo, SINOT y Chóferes
 - Incapacidad para realizar cobros de Contribuciones patronales
 - Incapacidad para realizar pagos de nomina interna
 - Incapacidad para radicar reportes o comunicaciones al Gobierno Federal

En lo fundamental la evaluación de riesgos que se ha de llevar a cabo ha de contestar, con la mayor fiabilidad posible, a las siguientes preguntas:

- ¿Que se intenta proteger?
 - Vida y propiedad
 - Equipos y estructuras de comunicaciones
 - Equipos de generación de electricidad y enfriamiento
 - Documentos, datos e información pública y confidencial
- ¿Cuál es su valor para uno o para la organización?
 - Equipos y estructuras son recuperables
 - Vida y continuidad de operaciones (no contabilizable)
- ¿Frente a qué se intenta proteger?
 - La gran amenaza para las organizaciones de hoy no son los empleados insatisfechos o los hackers maliciosos: muchas veces son las empresas o gerentes de tecnología mal informados.

La falta de seguridad en el tejido mismo de la compañía es, con frecuencia, una receta catastrófica. Con múltiples puntos de entrada y consecuencias como sabotaje, robos de datos y virus, se deben aplicar medidas de seguridad en múltiples niveles y puntos, y de diferentes maneras.

No hay ningún lugar en donde los datos o comunicaciones corporativas sean más vulnerables que en la línea frontal de una organización: los computadores de escritorios y portátiles de los empleados.
- ¿Cuál es la probabilidad de un ataque?
 - Los conflictos obrero patronales suelen tomar un carácter político ajeno a la gestión pública.
 - Empleados insatisfechos o consultores podrían alterar borrar o neutralizar defensas de seguridad de sistemas, datos o introducir virus sobre los sistemas de la agencia.

Cómo se realiza una evaluación de riesgos.

El o los responsables de la *Oficina de Cómputos y Sistemas* se sentarán con los responsables de las áreas usuarias y realizarán el siguiente conjunto de puntualizaciones:

¿A qué riesgos en la seguridad informática se enfrenta la Institución?

- Al fuego. Que puede destruir los equipos y archivos.
 - Se activara el DRC de Evertec para restablecer las aplicaciones de SABEN, Contribuciones, Modelo de Costo y SINOT.
 - Se implementara una activación remota de servicios de Internet y Mensajería Electrónica desde las facilidades de contingencia en Ponce.
 - Se solicitara la activación de servicios de Internet y Mensajería Electrónica a través de la OGP como instancia secundaria.
- A un robo común. Llevándose los equipos y archivos
 - Se dará parte a las autoridades pertinentes.
 - Se hará inventario de perdidas identificando su valor monetario y su valor funcional operacional.
 - Se activara el DRC de Evertec para restablecer las aplicaciones de SABEN, Contribuciones, Modelo de Costo y SINOT.
 - Se implementara una activación remota de servicios de Internet y Mensajería Electrónica desde las facilidades de contingencia en Ponce.
- Al vandalismo. Que dañen los equipos y archivos.
 - Se dará parte a las autoridades pertinentes.
 - Se hará inventario de perdidas identificando su valor monetario y su valor funcional operacional.
 - Se activara el DRC de Evertec para restablecer las aplicaciones de SABEN, Contribuciones, Modelo de Costo y SINOT.
 - Se implementara una activación remota de servicios de Internet y Mensajería Electrónica desde las facilidades de contingencia en Ponce.
- A fallas en los equipos, que dañen los archivos.
 - Se utilizarían los servicios de recuperación de documentos y archivos internos, de no ser recuperables se utilizarían los servicios externos de compañías especializadas en estos servicios como On Track <http://www.ontrackdatarecovery.com/> .
- A equivocaciones, que dañen los archivos
 - Se utilizarían los servicios de recuperación de documentos y archivos internos, de no ser recuperables se utilizarían los servicios externos de compañías especializadas en estos servicios como On Track <http://www.ontrackdatarecovery.com/> .
- A la acción de virus, que dañen los equipos y archivos
 - En segundo lugar, se pueden bloquear ciertos puertos para minimizar el riesgo de contraer virus y otras violaciones de seguridad mientras se le permite acceso a Internet a los usuarios.
 - Se bloquearan por os usuarios no autorizados utilizan un programa de pirateo llamado *Ethereal (shareware)*, que sirve para 'olfatear' el tráfico que viaja a través de la red. Así obtienen nombres de usuarios y contraseñas, que después usan para lograr acceso a datos confidenciales.
 - Ninguna lista servirá para prevenir por completo la aparición de nuevos caballos troyanos o infecciones de virus. Como último recurso, se duplicaran periódicamente los datos de sus

servidores y PC. Aunque la duplicación centralizada de bases de datos generalmente solo incluye computadores de escritorio fijos, los usuarios de equipos portátiles deberán siempre tener alguna estrategia de duplicación personal.

- Se activaran los servicios de apoyo de la OGP con Microsoft y con la compañía Trinexus.
 - Se realizara auditoria de sistemas en conjunto con la Unidad de Auditoría Interna y se pondrá bajo custodia todos los archivos y equipos envueltos en la actividad.
 - En algunos casos, no existen parches antivirus para contrarrestar las nuevas mutaciones. Entonces, lo que sucede es que estas mutaciones se infiltran en algún computador y contagian rápidamente a toda la compañía
 - La mejor defensa contra estos virus continúa siendo la aplicación de actualizaciones continuas de software antivirus. Pero, en el peor de los casos, cuando no hay ningún antivirus disponible, se recomienda la implementación de un plan de respuesta rápido para minimizar el contagio y los daños:
 - Primero, se determinará si el virus es una epidemia (más de 10 computadoras en 10 minutos).
 - Segundo, compile los hechos iniciales: ¿Cómo se está pasando el virus? ¿Qué puerto está usando el virus para propagarse a otros dispositivos? ¿Dónde se reportó el primer contagio del virus? ¿El virus está modificando archivos locales?
 - Tercero, minimice los contagios bloqueando el puerto TCP que el virus está usando para propagarse. Una vez más, los "embedded" firewall ofrecen una solución práctica y de administración fácil para estos casos.
- A terremotos, que destruyen el equipo y los archivos.
 - Se activara el DRC de Evertec para restablecer las aplicaciones de SABEN, Contribuciones, Modelo de Costo y SINOT.
 - Se implementará una activación remota de servicios de Internet y Mensajería Electrónica desde las facilidades de contingencia en Ponce.
 - Se solicitará la activación de servicios de Internet y Mensajería Electrónica a través de la OGP como instancia secundaria.
 - A accesos no autorizados, filtrándose datos no autorizados.
 - Se dará parte a las autoridades pertinentes.
 - Se hará inventario de perdidas identificando su valor monetario y su valor funcional operacional.
 - En caso de robo de dispositivos físicos, los archivos confidenciales en los computadores portátiles o asistentes digitales se pueden penetrar con sólo descifrar el código de ingreso al sistema operativo Windows.
 - Use seguridad local en Windows 2000 y XP, y controle las políticas de contraseñas, así como las políticas de auditoría para el computador.
 - Además de desactivar los archivos compartidos en Microsoft NetBIOS, la mejor defensa contra el descifrado de las contraseñas es asegurar que éstas sean robustas, a partir de los siguientes lineamientos:
 - Deberán tener de 8 a 16 caracteres de longitud
 - Deberán ser una mezcla de caracteres alfabéticos y no alfabéticos
 - No deberán contener espacios en blanco, signos de igual o de exclamación
 - No se deberán derivar de una sola palabra del diccionario
 - No se deberán derivar de su nombre o de los nombres de ningún pariente o mascota
 - No se deberán derivar de su número de teléfono, número de identificación o fecha de nacimiento.
 - Para archivos extremadamente confidenciales, utilice software de encriptación comercial, para codificar archivos o discos duros completos en computadores portátiles o asistentes digitales.
 - Se realizara auditoria de sistemas en conjunto con la Unidad de Auditoría Interna y se pondrá bajo custodia todos los archivos y equipos envueltos en la actividad.

- Al robo de datos, difundiendo los datos sin cobrarlos.
 - Se deben usar contraseñas robustas para protegerse contra ataques, pero también se deben tomar algunas medidas adicionales, recomendadas por el experto en seguridad y escritor Gary Bahadur:
 - Aplique medidas físicas de seguridad para prevenir robos de computadoras portátiles, tales como candados con cadenas y alarmas para la detección de movimientos.
 - Para archivos extremadamente confidenciales, utilice software de encriptación comercial, para codificar archivos o discos duros completos en computadores portátiles o asistentes digitales
 - Se realizara auditoria de sistemas en conjunto con la Unidad de Auditoría Interna y se pondrá bajo custodia todos los archivos y equipos envueltos en la actividad.
- Al fraude, desviando fondos merced a la computadora
 - Se dará parte a las autoridades pertinentes.
 - Se hará inventario de perdidas identificando su valor monetario y su valor funcional operacional.
 - Se realizara auditoria de sistemas en conjunto con la Unidad de Auditoría Interna y se pondrá bajo custodia todos los archivos y equipos envueltos en la actividad.

Esta lista de riesgos que se puede enfrentar en la seguridad, es bastante corta. La Institución deberá profundizar en el tema para poder tomar todas las medidas del caso.

Luego de elaborar esta lista, el personal de la *Oficina de Cómputos y Sistemas* deberá estar listo para responder a los efectos que estos riesgos tendrán para la Agencia.

¿Qué probabilidad hay de que tenga efecto alguno de los riesgos mencionados?

- **Al fuego**, que puede destruir los equipos y los archivos
- A un **robo común**. Llevándose los equipos y archivos
- Al **vandalismo**, que dañen los equipos y archivos
- A **fallas en los equipos**, que dañen los archivos
- A **equivocaciones** que dañen los archivos
- A la acción de **virus** que dañen los archivos.
- A **terremotos** que destruyen los equipos y archivos
- Al **robo de datos** difundiendo los datos
- Al **fraude**, desviando fondos merced a la computadora.

Para cada riesgo, se debe **determinar la probabilidad del factor de riesgo**. Como ejemplo se mencionan algunos factores de riesgo:

- Factor de riesgo bajo
- Factor de riesgo muy bajo
- Factor de riesgo alto
- Factor de riesgo muy alto
- Factor de riesgo medio

5. Análisis de impacto y probabilidad de falla

Si bien todos los procesos de la Agencia analizados son críticos para la institución, y por ende todas las aplicaciones que los soportan son importantes, para la recuperación ordenada de los servicios se debe establecer una valoración de impacto y probabilidad de falla, con el objetivo de priorizar la elaboración de planes de contingencia para aquellos de mayor criticidad.

Para determinar el impacto de falla de un determinado sistema, activo o aplicación se deben considerar varios criterios:

CRITERIO DE PARTICIPACIÓN:

- Si la(s) aplicación(es) participan en un solo proceso crítico, entonces el impacto es BAJO.
- Si el activo participa en dos procesos críticos, entonces el impacto es MEDIO.
- Si el activo participa en más de 2 procesos críticos a la vez, entonces el impacto es ALTO.

CRITERIO ECONÓMICO:

- Si se produce una falla en la(s) aplicación(es), la pérdida económica es mínima, entonces el impacto es BAJO.
- Si se produce una falla en la(s) aplicación(es), la pérdida económica es menor al 10% del ingreso mensual de la agencia-cliente, entonces el impacto es MEDIO.
- Si se produce una falla en la(s) aplicación(es), la pérdida económica es mayor al 10% del ingreso mensual de la agencia-cliente, entonces el impacto es ALTO.

CRITERIO DE TIEMPO

- Si se produce una falla en la(s) aplicación(es), el tiempo de recuperación del proceso es de unas pocas horas, entonces el impacto es MÍNIMO.
- Si se produce una falla en la(s) aplicación(es), el tiempo de recuperación del proceso es de unos pocos días, entonces el impacto es MEDIO.
- Si se produce una falla en la(s) aplicación(es), el tiempo de recuperación del proceso es de más de cinco días, entonces el impacto es ALTO.

CRITERIO SOCIAL:

- Si se produce una falla en la(s) aplicación(es) se puede afectar medianamente a cientos de personas, entonces el impacto es MÍNIMO.
- Si se produce una falla en la(s) aplicación(es) se puede afectar medianamente a miles de personas o considerablemente a cientos de personas, entonces el impacto es MEDIO.
- Si se produce una falla en la(s) aplicación(es) se puede afectar considerablemente a miles de personas, entonces el impacto es ALTO.

Una vez analizados estos criterios el impacto final de la(s) aplicación(es) se determina de la siguiente manera:

- Si el resultado de todos los criterios es impacto bajo, entonces el impacto final del activo es BAJO.
- Si el resultado de al menos uno de los criterios es alto, entonces el impacto final del activo es

- ALTO.
- Cualquier otro resultado nos da un impacto final del activo MEDIO.

Desarrollo del plan de contingencia

Sistemas de Información. La agencia deberá tener una relación de los Sistemas de Información con las que cuenta, tanto las realizadas por el Centro de Cómputos como los hechos por las áreas usuarias. Debiendo identificar toda información sistematizada o no, que sea necesaria para la buena marcha Institucional.

La relación de Sistemas de Información deberá detallar los siguientes datos:

- Nombre del Sistema
- Lenguaje o Paquete con el que fue creado el Sistema. Programas que lo conforman (tanto programas fuentes como programas objetos, rutinas, macros, etc.).
- La Dirección (Gerencia, Departamento, etc.) que genera la información base (el «dueño» del Sistema).
- Las unidades o departamentos (internos/externos) que usan la información del Sistema.
- El volumen de los archivos que trabaja el Sistema.
- El volumen de transacciones diarias, semanales y mensuales que maneja el sistema.
- El equipamiento necesario para un manejo óptimo del Sistema.
- La (s) fecha(s) en las que la información es necesitada con carácter de urgencia.
- El nivel de importancia estratégica que tiene la información de este Sistema para la Institución (medido en horas o días que la Institución puede funcionar adecuadamente, sin disponer de la información del Sistema). Equipamiento mínimo necesario para que el Sistema pueda seguir funcionando (considerar su utilización en tres turnos de trabajo, para que el equipamiento sea el mínimo posible).
- Actividades a realizar para volver a contar con el Sistema de Información (actividades de "Restore").

Con toda esta información se deberá realizar una lista priorizada (un ranking) de los Sistemas de Información necesarios para que la Institución pueda recuperar su operatividad perdida en el desastre (contingencia).

Relación de aplicaciones y sistemas:

1. SABEN
2. Contribuciones + Portal de Patronos
3. CybelDOL
4. SINOT

5. Chóferes On Line
6. Exchange Server (Correo Electrónico)
7. ISA Server (Servicio Internet)
8. Pagina Web del DTRH
9. PRIFAS/RHUM
10. MUNIS
11. Normas del Trabajo
12. Sistema de Seguimiento Asuntos Legales
13. Estadísticas
 - a. Índice de Precios
 - b. Coste de Vida
 - c. Net-Empleo

b) Equipos de Cómputos Hay que tener en cuenta:

Inventario actualizado de los equipos de manejo de información (computadoras, lectoras de microfichas, impresoras, etc.), especificando su contenido (software que usa, principales archivos que contiene), su ubicación y nivel de uso Institucional.

- Pólizas de Seguros Comerciales. Como parte de la protección de los Activos Institucionales, pero haciendo la salvedad en el contrato, que en casos de siniestros, la restitución del Computador siniestrado se podrá hacer por otro de mayor potencia (por actualización tecnológica), siempre y cuando este dentro de los montos asegurados.

Esta información puede ser provista por la Oficina de Servicios Administrativos, persona de contacto José Torres Llompart.

- Señalizar y/o etiquetar de las Computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. En caso de emergencias por ejemplo etiquetar (colocar un sticker) de color rojo a los Servidores, color amarillo a las PC's con Información importante o estratégica y color verde a las PC's de contenidos normales.
- Tener siempre actualizada una relación de PC's requeridas como mínimo para cada Sistema permanente de la agencia (que por sus funciones constituyen el eje central de los Servicios Informativos de la Institución), las funciones que realizara y su posible uso en dos o tres turnos de trabajo, para cubrir las funciones básicas y prioritarias de cada uno de estos Sistemas.

Obtención y almacenamiento de los Respaldos de Información (BACKUPS).

Se deberá establecer los procedimientos para la obtención de copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los Sistemas o aplicativos de la agencia. Para lo cual se debe contar con:

L. Backups del Sistema Operativo (en caso de tener varios Sistemas Operativos o versiones, se contará con una copia de cada uno de ellos).

2) Según establecido en el Manual del Administrador se tomará "Backup" diaria de los servidores (Exchange, Developer, WEB), el proceso de Archive en los servidores de Informix, se tomará además un resguardo de la base de datos de Informix (DOL 1, DOL2, DOL3, DOL4, DOL5).

El personal de Operaciones deberá correr el programa ó "script" **FULLBACKUP .DOL, RESTORE.DOL** en caso de que se tenga que restaurar la información de algún servidor, **INFORMIX.BACKUP** para el resguardo de la base de datos. Todos estos procesos deberán ser registrados en una bitácora.

3) Backups del Software Base (Paquetes y/o Lenguajes de Programación con los cuales han sido desarrollados o interactúan nuestros Aplicativos Institucionales). Se mantendrán generaciones diarias de resguardo del sistema operativo, aplicaciones, utilitarios y bases de datos. La generación que se produzca los viernes deberá ser enviada los lunes en la mañana a la bóveda del Centro de Recuperación de Desastre de la firma Evertec en la Zona Industrial 3 Monjitas, firma contratada para tales efectos.

4) Backups del Software Aplicativo (Considerando tanto los programas fuentes, como los programas objetos correspondientes, y cualquier otro software o procedimiento que también trabaje con la data, para producir los resultados con los cuales trabaja el usuario final). Se debe considerar también las copias de los listados fuentes de los programas definitivos, para casos de problemas.

5) Backups de los Datos (Bases de Datos, Índices, tablas de validación, passwords, y todo archivo necesario para la correcta ejecución del Software Aplicativo de nuestra agencia).

6) Backups del Hardware. Se puede implementar baja dos modalidades'

PROCEDIMIENTO

1.- Objetivo

Este procedimiento está basado en estrategias, personas, procedimientos y recursos, los cuales se integran para la creación de procesos que permitan el resguardo de sistema operativo, archivos y base de datos informix contenidos en los servidores UNIX DOL1, DOL2, DOL3 y DOL4 en caso de fallas potenciales.

2.- Información General

El resguardo para los servidores arriba mencionados se divide entre dos categorías:

a- Resguardo de base de datos INFORMIX

El resguardo de base de datos INFORMIX contiene solo la información necesaria para restaurar la base de datos con la información que tenía al momento de hacer el resguardo. Es responsabilidad del administrador de la base de datos restaurar la misma en caso de alguna falla.

b- Resguardo de archivos del sistema operativo

Este resguardo contiene archivos de directorios importantes para la recuperación del servidor. Para cada servidor se identificó los directorios que son incluidos en este resguardo. Entre los directorios identificados se encuentran los que contienen archivos relacionados a las aplicaciones que utilizan de plataforma al servidor. Ejemplo: Directorios relacionados con MUNIS en DOL3. Es responsabilidad del administrador de cada aplicación restaurar la misma luego de alguna falla.

El resguardo de archivos del sistema operativo se realiza de manera automática cinco backups a la semana para los servidores que no contienen INFORMIX y cada miércoles para los servidores que contienen INFORMIX. El resguardo de INFORMIX se realiza de manera automática cinco veces a la semana en los servidores que corresponda. A continuación se describe ambos procedimientos.

L. Proceso de Resguardo Archivos de Sistema Operativo

Se compone de un script que se describe a continuación:

- **File backup-** Se encuentra bajo el directorio /AdminTools/Abakup/bin. Este realiza un resguardo de los archivos contenidos en los directorios especificados a continuación:

| Dol1 | Dol2 | Dol3 | Dol4 |
|---------|-----------|--------|-------|
| /etc | /etc | /etc | /etc |
| /home | /home | /home | /home |
| /opt | /lib | /munis | /opt |
| /saben | /oi_image | /opt | /usr |
| /pc_nfs | s | /usr | /var |
| _oi | /oidb | /var | |
| /oidb | /pc_nfs_o | | |
| /oi_ima | i | | |
| ge | /usr | | |
| /wang | /var | | |

Un archivo log llamado FILEBackup.log es creado con el resultado de su operación, este se encuentra en el directorio /AdminTools/Abackup/log.

| Nombre Script | Localización | Archivo Log |
|-------------------|-----------------------------|---|
| fileBackup | /AdminTools/Aback up/bin | /AdminTools/Abackup/log/ FileBackup.log /AdminTools/Abackup/log/ BackError.log |

5.0 Horarios

A continuación un resumen de los horarios establecidos para efectuar los resguardos descritos arriba:

DOL1:

| Proceso | Tipo | Script name | Frecuencia | Unidad | Hora |
|--|------------|------------------------------------|------------|-------------|-------|
| Resguardo Archivos de Sistema Operativo | Automático | filebackup | Miércoles | 0m - 4mm | 10:00 |
| Resguardo Base de Datos Informix | Automático | /usr/22nformix/bin/dbbackup.s h | L-V | 0m - 4mm | 1:00 |

DOL2:

| Proceso | Tipo | Script name | Frecuencia | Unidad | Hora |
|--|------------|-------------|------------|-------------|------|
| Resguardo Archivos de Sistema Operativo | Automático | filebackup | L-V | 0m - 4mm | 1:00 |

0

DOL3:

| Proceso | Tipo | Script name | Frecuencia | Unidad | Hora |
|--|------------|-------------|------------|-------------|------|
| Resguardo Archivos de Sistema Operativo | Automático | filebackup | L-V | 0m - 4mm | 1:00 |

DOL4:

| Proceso | Tipo | Script name | Frecuencia | Unidad | Hora |
|--|------------|-------------------------------|------------|-------------|-------|
| Resguardo Archivos de Sistema Operativo | Automático | filebackup | Miercoles | 0m - 4mm | 10:00 |
| Resguardo Base de Datos Informix | Automático | /usr/informix/bin/dbbackup.sh | L-V | 0m - 4mm | 1:00 |

4.- Verificación de Falla del Resguardo

A continuación se explica cómo revisar notificaciones para ambos resguardos:

a. Resguardos de base de datos Informix

El operador debe revisar el resultado del resguardo verificando el correo electrónico del usuario root en el servidor. Para hacerlo debe seguir las siguientes instrucciones:

1. Haga "click" al botón Start de su máquina Windows
2. En el menú que aparece, haga "click" sobre la palabra Run como se muestra en la Figura 1

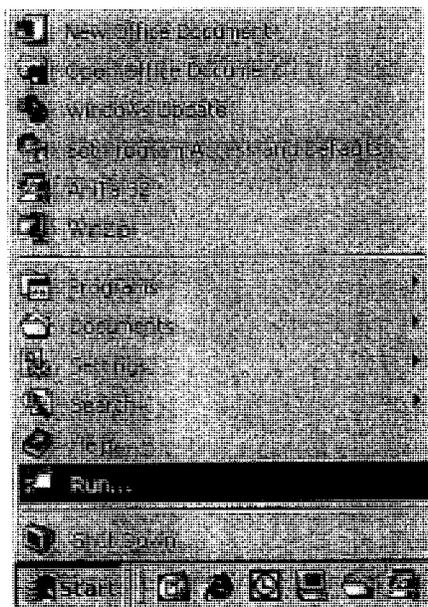


Figura 1.

3. Escriba el siguiente comando en la pantalla de "Run" que aparecerá: `telnet ipaddress`. Cambia la palabra `ipaddress` por el "IP address" del servidor para el cual estas verificando el resultado de resguardo. Vea Figura 2

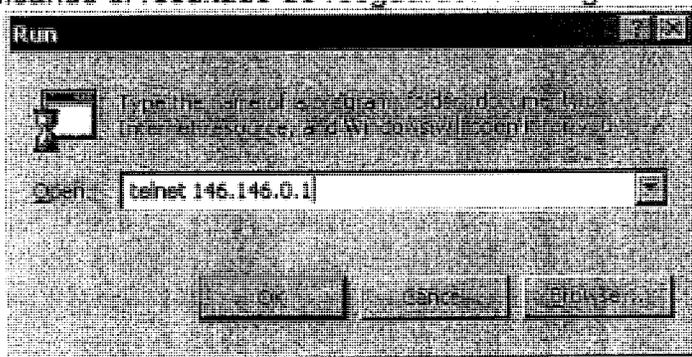
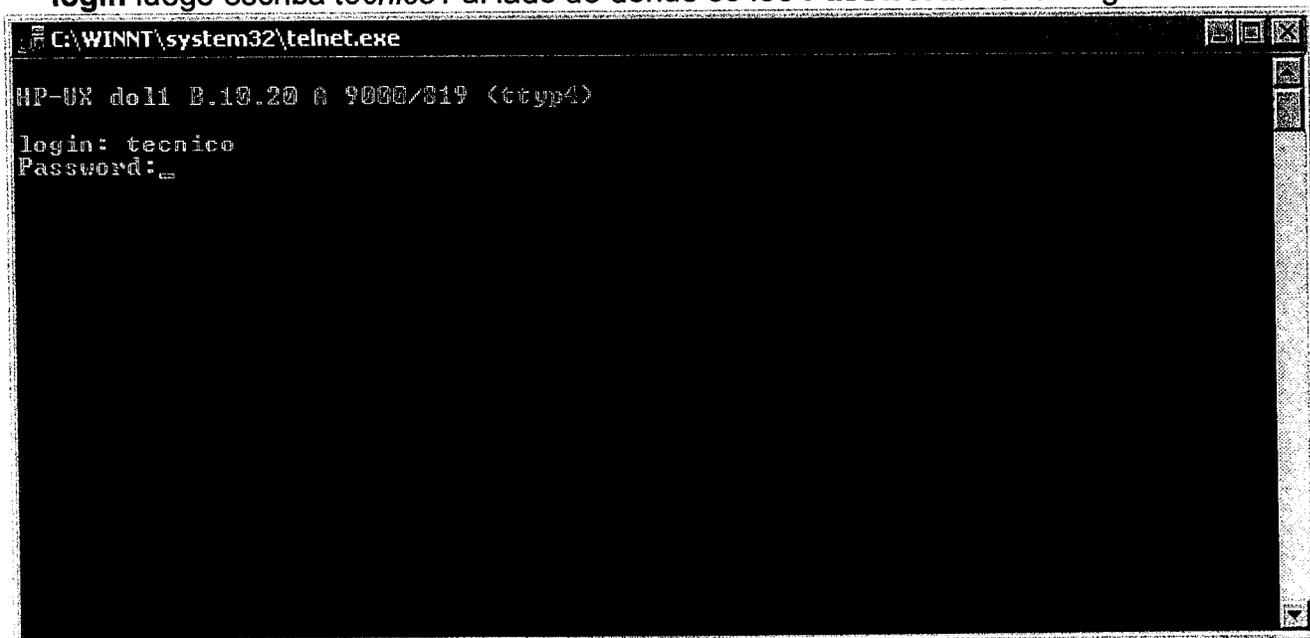


Figura 2

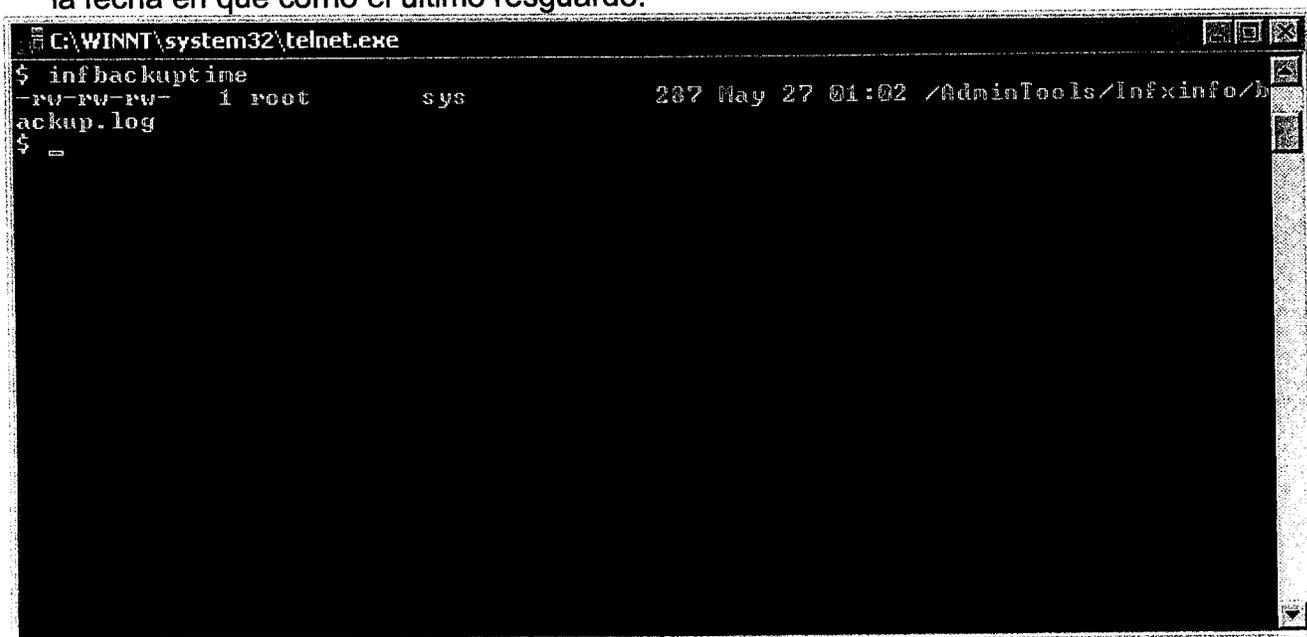
4. En la pantalla de "telnet" que aparecerá escribe *técnico* al lado de donde se lee **login** luego escriba *tecnico1* al lado de donde se lee **Password**. Véase Figura 3



```
C:\WINNT\system32\telnet.exe
HP-UX doll B.10.20 A 9000/S19 (tty4)
login: tecnico
Password: _
```

Figura 3.

5. Luego de completado estos pasos deberías estar en una pantalla parecida a la presentada en la Figura 4. En ella debes escribir *infbackuptime* para determinar la fecha en que corrió el último resguardo.



```
C:\WINNT\system32\telnet.exe
$ infbackuptime
-rw-rw-rw- 1 root      sys      287 May 27 01:02 /AdminTools/Infxinfo/b
ackup.log
$ _
```

Figura 4.

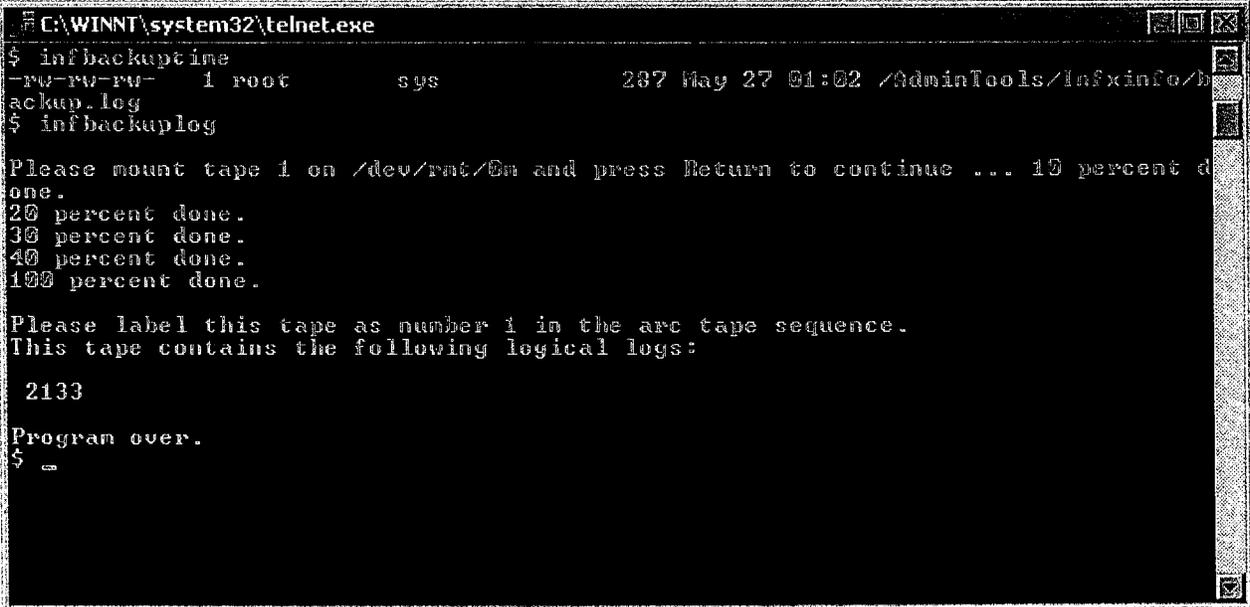
6. El día y la hora en que se ejecuto el último resguardo se muestran en la columna seis, siete y ocho del resultado de este comando. En la Figura 4 se muestra un

resguardo que se ejecuto en Mayo 27 a la 1:02 am (se muestra la hora en formato militar).

7. Para verificar el resultado de este resguardo, escribe el siguiente comando: `infbackuplog`.
8. En la Figura 5 se muestra el resultado de este comando que muestra un resguardo que culminó de forma exitosa. Se presenta que el 100% del resguardo fue completado.

Como leer los mensajes de email para el usuario root

La frase **100 percent done** debe aparecer en el resultado. Si ves un mensaje parecido pero no igual, sin el mensaje de **100 percent done** o si no devuelve ningún resultado notifica inmediatamente a tu DBA o al administrador del sistema.



```
C:\WINNT\system32\telnet.exe
$ infbackuptime
-rw-rw-rw- 1 root      sys      287 May 27 01:02 /AdminTools/Infxinfo/b
ackup.log
$ infbackuplog

Please mount tape 1 on /dev/rmt/0m and press Return to continue ... 10 percent d
one.
20 percent done.
30 percent done.
40 percent done.
100 percent done.

Please label this tape as number 1 in the arc tape sequence.
This tape contains the following logical logs:

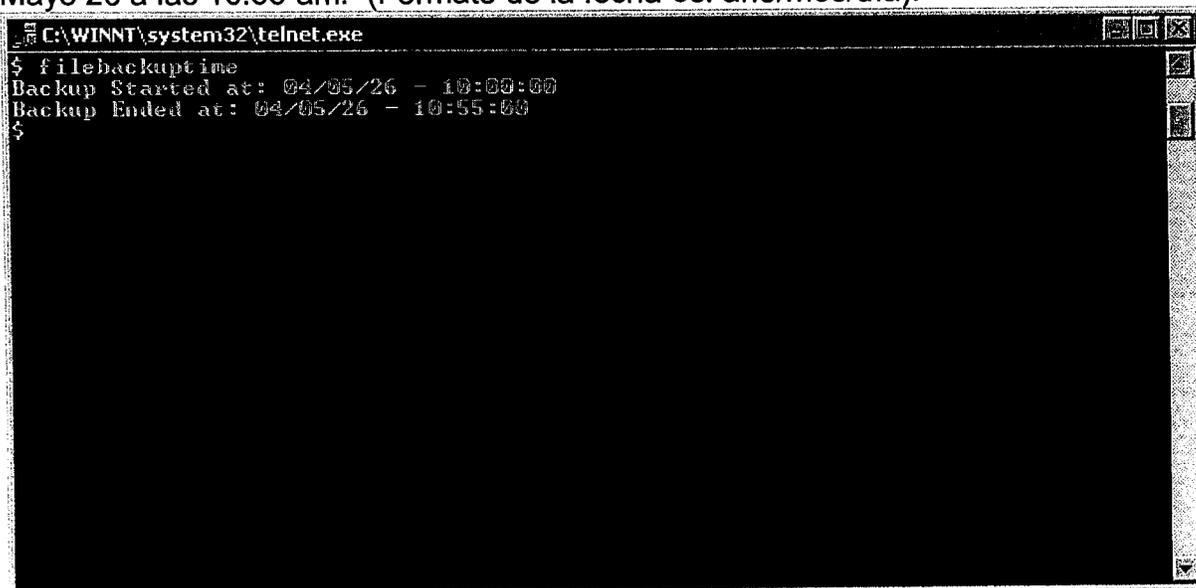
2133

Program over.
$ _
```

Figura 5

b. Verificación de resguardos de Sistema Operativo

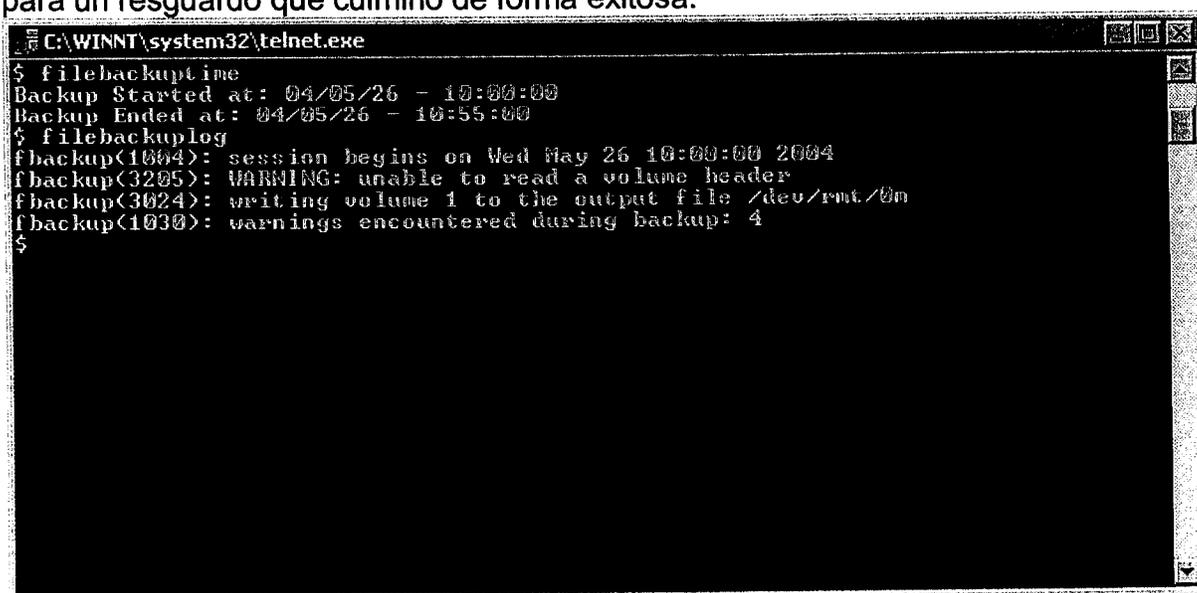
Para verificar los resguardos del sistema operativo debes seguir los pasos del 1 al 4 presentados en la sección 4-a. Luego escribe el siguiente comando: **filebackuptime**. Este comando te mostrara la hora en que comenzó y termino el último resguardo de archivos en el sistema operativo que se ejecuto. En la Figura 6 se muestra un ejemplo del resultado de este comando. En esta se muestra un resguardo que comenzó en Mayo 26 a las 10:00 am y termino en Mayo 26 a las 10:55 am. (Formato de la fecha es: ano/mes/día).



```
C:\WINNT\system32\telnet.exe
$ filebackuptime
Backup Started at: 04/05/26 - 10:00:00
Backup Ended at: 04/05/26 - 10:55:00
$
```

Figura 6

El resultado de los resguardos se puede verificar con el comando **filebackuplog**. La Figura 7 muestra un ejemplo del resultado de este comando para un resguardo que culmino de forma exitosa.



```
C:\WINNT\system32\telnet.exe
$ filebackuptime
Backup Started at: 04/05/26 - 10:00:00
Backup Ended at: 04/05/26 - 10:55:00
$ filebackuplog
fbackup(1004): session begins on Wed May 26 10:00:00 2004
fbackup(3205): WARNING: unable to read a volume header
fbackup(3024): writing volume 1 to the output file /dev/rmt/0m
fbackup(1030): warnings encountered during backup: 4
$
```

Figura 7

5.- Resguardos de los Backups (Vault)

5.1 Tiempo de retención

Se está manteniendo los Backup en la bóveda por un tiempo de 30 días.

5.2 Frecuencia

El operador deberá trasladar las cintas y cartridge para un lugar seguro todos los lunes.

6. Etiquetas para la identificación de cintas

7. Responsabilidades

Operadores

- Responsable del cambio diario de las cintas y los cartridges antes de la ejecución del Backup.
- Responsable de verificar los resguardos antes de removerlos de los servidores.
- Responsable de limpiar el dispositivo de hacer resguardos periódicamente o cuando el dispositivo así lo indique.
- Responsable de descartar cartuchos que han excedido su uso limite
- Responsable de notificar si se produce algún problema con las cintas y cartridges.
- Responsable de etiquetar los cartuchos.
- Responsable de trasladar las cintas y cartridge a la bóveda todos los lunes.
- Responsable de trasladar a la oficina las cintas y cartridge que se rehusaran para la ejecución de los Backups.

Administrador de UNIX

- Responsable modificar el proceso de resguardos automáticos debido a errores encontrados o cambios que ocurran.
- Responsable de efectuar los resguardos manuales cuando el resguardo automático falle o no complete correctamente.

8. Reporte de Grupos de Trabajo

| Nombre | Teléfono Oficina | Teléfono Celular | Grupo |
|---------------|------------------|------------------|----------------------|
| Víctor Medina | (787) 754-2154 | | Operador de Sistemas |

APENDICE A

Errores Comunes

fbackup(1102): WARNING: file number ##### was not backed up /
fbackup(3005): WARNING: file number ##### was NOT backed up.

Un error parecido a los que se muestran en la siguiente figura pueden ocurrir. Esto es un error que no afecta el resultado final del resguardo. Este error significa que los archivos mencionados fueron eliminados luego de que el proceso de resguardo los marcara para incluirlos en el proceso y antes de que lograra resguardarlos.

```
fbackup(1004): session begins on Tue Jun 1 01:00:01 2004
fbackup(3203): volume 1 has been used 39 time(s)
fbackup(3024): writing volume 1 to the output file /dev/rmt/0m
fbackup(1102): WARNING: unable to stat file /var/spool/mqueue/dfBAA03998
fbackup(3005): WARNING: file number 29739 was NOT backed up
fbackup(1102): WARNING: unable to stat file /var/spool/mqueue/qfBAA03998
fbackup(3005): WARNING: file number 29758 was NOT backed up
fbackup(1030): warnings encountered during backup: 4
```

fbackup(3047): could not open output file /dev/rmt/0m

Este error significa que la cinta para resguardo no estuvo disponible ya sea porque no había cinta disponible en el "drive" o porque la cinta estuviera defectuosa o el "drive" está sucio. El resguardo no fue ejecutado para este día.

```
fbackup(1004): session begins on Thu May 27 01:00:01 2004
fbackup(3047): could not open output file /dev/rmt/0m
fbackup(3019): would you like to enter a new output file?
fbackup(3004): writer aborting
fbackup(1002): Backup did not complete : Reader or Writer process exit
```

Modalidad Externa. Mediante contrato con Evertec se nos brinda la seguridad de poder procesar nuestra información, y ser puestos a nuestra disposición, al ocurrir una contingencia y mientras se busca una solución definitiva al siniestro producido. Este contrato tiene al tanto las consideraciones de equipamiento como de ambientes y facilidades de trabajo que cada institución se compromete a brindar, y debe de ser actualizado cada vez que se efectúen cambios importantes de sistemas que afecten a cualquiera de las aplicaciones de "mainframe" de la agencia.

Modalidad Interna. Como contamos con más de un local para continuidad de, en ambos debemos tener señalados los equipos, que por sus características técnicas y capacidades, son susceptibles de ser usados como equipos de emergencia del otro local, debiéndose poner por escrito (igual que en el caso externo), todas las actividades a realizar y los compromisos asumidos.

En ambos casos se deberá probar al menos una vez al año y asegurar que los procesos de restauración de Información posibiliten el funcionamiento adecuado de los Sistemas. En algunos casos puede ser necesario volver a recompilar nuestro software aplicativo bajo plataformas diferentes a la original, por lo que es imprescindible contar con los programas fuentes, al mismo grado de actualización que los programas objeto.

Una vez identificados los procesos y la(s) aplicación(es) y prioritarios, entonces se debe empezar con el desarrollo de los planes de contingencia.

Los elementos de nuestro plan de contingencia son los siguientes:

a) Objetivos del plan

Una vez establecido el orden prioritario de las aplicaciones a los objetivos del plan deben indicar claramente a que proceso crítico y que falla de la(s) aplicación(es) se espera superar. Incluyendo los resultados deseados, como son niveles de servicio, calidad de producto, y los posibles riesgos comprometidos en el uso del plan, es decir cómo puede afectar a la agencia.

b) Identificación de alternativas

Se deben buscar alternativas creativas, que logren el efecto de mitigar el impacto en caso de que la falla considerada se produzca. Se recomienda revisar el plan actual de emergencia y recuperación de desastres que la agencia pueda tener, seguramente existan convergencias entre los criterios usados en dichos planes y los ahora necesarios por el Centro de Cómputos.

Las alternativas pueden ser tan simples como identificar un proveedor que pueda cambiar un equipo crítico, o hasta incluir lineamientos de una serie de pasos manuales para cubrir actividades normalmente automatizadas.

Disponer de buenas alternativas requiere el análisis de muchas posibilidades. Cualquier alternativa, por disparatada que parezca, merece ser considerada. Algunas sugerencias generales a considerar son:

- Planificar la necesidad de personal adicional para atender los problemas que ocurran.
- Recurrir al procesamiento manual si fallan los sistemas automatizados. Instalación de generadores de energía eléctrica a cada una de las bases de datos y disponer de una reserva de combustible para la planta eléctrica.
- Almacenar suministros críticos para la operación, con la antelación del caso.

- Poner en moratoria las vacaciones del personal esencial.

Todas las alternativas encontradas han sido documentadas claramente para que puedan ser evaluadas.

c) Responsabilidades, roles y autoridades

Como expusimos anteriormente se han identificado claramente quien hará que, cuando se esté operando en modalidad de contingencia. De la misma manera se han definido quienes toman las decisiones de implementar, cambiar y descontinuar las operaciones contingentes.

También hemos desarrollado para uso interno una lista de responsables a la persona que más conoce del proceso en cuestión, quien puede dar el soporte necesario (incluye personal asesor externo), en caso de que el plan de contingencia no funcionará como se espera, y se lo deba cambiar sobre la marcha.

Todos los involucrados están al tanto de su responsabilidad y que la han aceptado conforme al memorando de definición de roles (17 de febrero de 2000).

d) Duración del plan.

El plan tendrá un tiempo determinado de duración, en el que el proceso pueda continuar operando en modo de contingencia. Esto se definirá dependiendo de la cantidad de recursos que se considerará para su ejecución lo que impactará en el presupuesto del plan.

La duración del plan dependerá del tiempo que tome arreglar definitivamente el problema y debe estar alineado con los objetivos propuestos en la primera parte del plan.

e) Procedimientos para comunicar la activación del plan de contingencia a los involucrados.

Se cuenta con 2 directorios con la información necesaria del personal que labora en estas facilidades y la de los consultores externos que laboran dentro de nuestras facilidades en el desarrollo o mantenimiento de las aplicaciones. Dada la posibilidad de interrupciones en las telecomunicaciones, se debe prever formas alternativas de comunicación, que puedan garantizar que todo el personal de la organización sepa de la activación del plan.

Por esta razón este directorio incluye números de teléfono, números de teléfono celular (si tiene) y dirección de correo electrónico. Esto garantizará la reacción inmediata de los involucrados y generar las expectativas adecuadas de niveles de servicio y funcionamiento a las demás personas

f) Capacitación al equipo de implementación del plan.

Las personas involucradas en el Comité de Manejo de Emergencias de la Oficina de Cómputos y Sistemas están capacitadas en los procedimientos y practicas nuevas contempladas en el plan de contingencia y deben ser instruidas sobre el ejercicio de sus respectivos roles y responsabilidades asignadas. Muchos de los miembros del comité cuentan con experiencia militar, manejo de extintores de incendio (certificados), en primeros auxilios (certificados) o en búsqueda y rescate (certificados).

Nos hemos asegurado que todos los involucrados conozcan el plan y sus detalles, y que tengan a la mano la documentación del caso, para suplir cualquier olvido involuntario.

g) Pruebas del plan.

La prueba de plan de contingencia es necesaria para validar la efectividad, posibilidad y capacidad de la alternativa elegida. Las pruebas de integración completa constituye la mejor forma de validar la capacidad del plan para sustentar las operaciones. Las pruebas a escala completa tienen, por lo general, un costo muy alto y, debido a ello, se acostumbra probar solo componentes claves.

Anualmente realizamos una prueba de recuperación de desastres y se documenta la misma en las facilidades del DRC de Evertec.

Aun cuando el procedimiento de recuperación establecido sea aprobado y aceptado como correcto, deberá establecerse periodos para simulacros de emergencia. De esta manera se podrá comprobar la confiabilidad de los procesos claves en una situación real de emergencia.

SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información y por consiguiente de los equipos informáticos, es una cuestión que llega a afectar, incluso, a la vida privada de la persona humana, de ahí que resulte obvio el interés creciente que día a día se evidencia sobre este aspecto de la nueva sociedad informática.

Ladrones, manipuladores, saboteadores, espías, etc. reconocen que el Centro de Cómputos de una institución es su nervio central, que normalmente tiene información confidencial y que, a menuda, es vulnerable a cualquier ataque.

La seguridad de la información tiene dos aspectos. El primero consiste en negar el acceso a los datos a aquellas personas que no tienen derecho a ellos, al cual también se le puede llamar protección de la privacidad, si se trata de datos personales, y mantenimiento de la seguridad en el caso de datos institucionales.

Un segundo aspecto de la protección es garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio de acceso, las cuales tienen la responsabilidad de proteger los datos que se les ha confiado.

En general, la protección de los datos requiere ejercer un control sobre la lectura, escritura y empleo de esa información. Para obtener mayor eficiencia en la protección se debe tener siempre presente la protección de los datos, el mantenimiento de la privacidad y la seguridad del secreto.

El secreto se logra cuando no existe acceso a todos los datos sin autorización. La privacidad adecuada puede lograrse cuando los datos que puedan obtenerse no pueden enlazarse a individuos específicos o no pueden utilizarse para imputar hechas acerca de ellas.

Por otro lado, es importante incorporar dispositivos de seguridad durante el diseño del sistema en vez de añadirlas después. Los diseñadores de sistemas deben entender que las medidas de seguridad han llegado a ser criterios de diseño tan importantes como otras posibilidades funcionales, así como el incremento de costos que significa agregar funciones, después de desarrollado un Sistema de Información.

Acceso no Autorizado

Sin adecuadas medidas de seguridad se puede producir accesos no autorizados a:

- Área de Sistemas.
- Computadoras personajes y/o Terminales de la red.
- Información Confidencial.

Control de Acceso al Área de Sistemas

La libertad de acceso al área de sistemas puede crear un significativo problema de seguridad. El acceso normal debe ser dado solamente a la gente que regularmente trabaja en esta área. Cualquier otra persona, de otro modo puede tener acceso únicamente bajo control. Mantener la seguridad física de su área de sistema es su primera línea de defensa. Para ello deberá tomar en consideración el valor de sus datos, el costo de protección, el impacto que su pérdida podría tener en su organización y la motivación, competencia y oportunidades de la gente que podría querer dañar los datos o el sistema.

Palabra de Acceso (Password). Es una palabra especial o código que habrá de teclearse al sistema de computadora antes que se realice un proceso. Constituye un procedimiento de seguridad que protege los programas y datos contra los usuarios no autorizados.

La identificación de un individuo debe ser muy difícil de imitar y copiar. Aunque su nombre pueda ser único, es fácil que cualquiera que observe a quienes tienen acceso al sistema lo copie, por lo que no es una clave adecuada.

Una vez que se obtiene una clave de acceso al sistema, esta se utiliza para entrar al sistema de la base de datos desde el sistema operativo. La responsabilidad del manejo de la clave corresponde tanto al que acceso como al sistema operativo.

A fin de proteger el proceso de obtención de una clave del sistema, cuando el usuario realiza la entrada (en inglés LOGIN), solicita una clave de acceso con el nombre del usuario, la cual consiste de unas cuantas letras elegidas por el usuario.

Un intruso puede intentar descubrirla de dos maneras: una, observando el ingreso de la clave y otra, utilizando un método de ensayo y error para introducir posibles claves de acceso y lograr entrar. También existen aplicaciones para quebrar claves de accesos que deben ser consideradas como método de violación a la seguridad interna del *Departamento del Trabajo y Recursos Humanos*.

El sistema de computación debe cerrarse después que un individuo no autorizado falle tres veces al intentar ingresar una clave de acceso.

Las claves de acceso no deben ser largas puesto que son más difíciles de recordar.

Todos los procesos se actualizan en forma periódica el password a los usuarios cada 30 o 90 días según la aplicación.

No se puede depender de que la ausencia de un operador o responsable de un computador trabe la operatividad normal de una agencia, por lo que puede ser necesario el establecimiento de un procedimiento de tener un duplicado de los passwords asignados, bajo un esquema de niveles jerárquicos, en sobre lacrado. Todas las claves de acceso se ubican en sobre sellado en la bóveda de seguridad de la *Oficina de Cómputos y Sistemas*.

Niveles de Acceso. Los programas de control de acceso deberán identificar a los usuarios autorizados a usar determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidas a la lectura o modificación en sus diferentes formas.

De acuerdo a ello se tienen los siguientes niveles de acceso a la información:

- Nivel de consulta de la información no restringida o reservada
- Nivel de mantenimiento de la información no restringida o reservada
- Nivel de consulta de la información incluyendo la restringida o reservada.
- Nivel de mantenimiento de la información incluyendo la restringida

a) Nivel de consulta de la información

El privilegio de lectura está disponible para cualquier usuario y sólo se requiere un conocimiento de la estructura de los datos, o del sistema de otro usuario para lograr el acceso.

La autorización de lectura permite pero no se modifica la base de datos.

b) Nivel de mantenimiento de la información

El concepto de mantenimiento de la información consiste en:

Ingreso. Permite insertar datos nuevos pero no se modifica los ya existentes

Actualización. Permite modificar la información pero no la eliminación de datos.

Borrado. Permite la eliminación de datos.

Un usuario puede tener asignados todos, ninguno o una combinación de los tipos de autorización anteriores. Además de las formas de autorización de acceso de datos antes mencionados, es posible autorizar al usuario para que modifique el esquema de la base de datos, pero esta función es responsabilidad de la *Oficina de Cómputos y Sistemas*.

Cada palabra clave debe tener asignado uno de los niveles de acceso a la información mencionados anteriormente.

La forma fundamental de autoridad es la que se le da al administrador de la base de datos, que entre otras cosas puede autorizar nuevos usuarios, reestructurar la base de datos, etc. Esta forma de autorización es análoga a la que se provee a un "súper usuario" o al operador para un sistema operativo.

La *Oficina de Cómputos y Sistemas* mantiene un control de acceso electrónico y biométrico a todas las áreas de trabajo internas incluyendo a su vez las áreas de comunicaciones del Call Center y sus áreas administrativas en el PEEG.

Acceso Limitado a los Terminales

Los terminales que son dejados sin protección pueden ser mal usados. Cualquier terminal que puede ser utilizado como acceso a los datos de un Sistema controlado, debe ser encerrado en un área segura o guardado, de tal manera que no sean usados, excepto por aquellos que tengan autorización para ello.

Igualmente, se deberá considerar la mejor manera de identificar a los operadores de terminales del Sistema, y el uso de contraseñas, cuando un terminal no sea usado pasado un tiempo predeterminado (5- 10 Min.).

A modelo de seguridad tenemos implementado el sistema Top Secret para el control de acceso a aplicaciones de "mainframe" según se detalla.

| PROCESOS DE SEGURIDAD | BENEFICIOS |
|--|---|
| Identifica usuarios que desean acceder a un sistema seguro (SABEN; SINOT, Contribuciones). Identificación | Permite asociar a un identificación único con cada usuario potencial del sistema cuando entra al sistema |
| Verifica que cada usuario sea quien dice ser. Autenticación | Provee un nivel adicional de identificación, como contraseña para verificar que el usuario tiene el identificador correcto para acceder al sistema. |
| Permite solo a usuarios autorizados a acceder a los recursos protegidos | Le provee al usuario un nivel apropiado de autorización para cada recurso protegido. |
| Permite de una manera conveniente y centralizada para administrar seguridad | Permite seleccionar la clase de estructura de seguridad que se ajuste a la instalación. |
| Registra los accesos a los recursos protegidos | Provee otro nivel de contabilidad para determinar quien usa el recurso. |
| Documenta cualquier violación inmediata o por periodos predefinidos (informes) | Permite ver las violaciones cuando se deseen en el formato que desee. |
| Lista los recursos claves protegidos y el nivel de protección para cada uno | Permite ver como cada recurso ha sido protegido. |
| Minimiza el acceso a los recursos no definidos | Todo recurso no definido está protegido. |

Esto garantiza que se mantenga solo la actividad real de seguridad de los empleados que prestan funciones para SABEN, SINOT y Contribuciones.

El sistema permite determinar ¿quién acceso al sistema? ¿Cuándo entro? ¿Qué transacciones uso y por cuánto tiempo? Son estos los principales campos de acción a consultar en casos de investigación de fraudes. Esto beneficiara grandemente a la Unidad de Investigaciones y Fraude del N.S.E. y a la Oficina de Auditoría Interna.

El sistema de seguridad permitirá solo 3 intentos para entrar al sistema, de lo contrario bloqueara su clave de acceso, al igual que después de un tiempo predefinido sin utilizarse el terminal / microcomputadora, pedirá clave nuevamente para continuar.

Bajo este nuevo enfoque, el ambiente de producción del Departamento del Trabajo se encuentra bajo una estructura robusta y segura en los últimos niveles de tecnología existentes bajo la estructura de "mainframe".

Restricciones aplicadas:

- Determinación de los períodos de tiempo para los usuarios o las terminales.
- Designación del usuario por terminal o del terminal por usuario.
- Limitación del uso de programas para usuario o terminales.
- Límite de tentativas para la verificación del usuario.
- Tiempo de validez de las señas.

Facilidades especiales:

La *Oficina de Cómputos y Sistemas* cuenta con 8 extintores de incendios y se recomienda la adquisición de otras adicionales categorías C (Fuego eléctrico).

El área ocupada por la oficina de Comunicaciones cuenta con 4 unidades externas de aire acondicionado en adición de la unidad central del edificio. Esta área suele ser usada como Centro de Operaciones de Emergencia en Sistemas durante emergencias ambientales siempre que las condiciones así lo permitan. En adición cuenta con provisión de energía eléctrica a través de la planta eléctrica.

Se solicitó la adquisición de un botiquín de primeros auxilios, linternas y provisión extra de agua y baterías durante la principal temporada de huracanes.

DETECCION DE INCENDIO

Olor ha quemado

Cuando se detecte olor a quemado **no fuerte**, la persona que lo detecte, notificará al supervisor más cercano y a la Administración. La Administración notificará a los supervisores de los demás pisos para tratar de conseguir la fuente del olor. Debido a que el edificio es cerrado, si no se detecta la fuente del olor a quemado en los primeros diez minutos, el (la) Administrador (a) deberá ponderar el desalojar las facilidades, preventivamente.

Cuando se detecte olor a quemado **fuerte**, la persona que lo detecte, notificará al supervisor más cercano y a la oficina de Seguridad y Planta Física. La oficina de Seguridad y Planta Física notificará a los supervisores de los demás pisos y se procederá a desalojar las facilidades preventivamente. La oficina de administración notificará al personal de mantenimiento del edificio para que localicen la fuente.

Humo

Cuando se observe **humo tenue**, la persona que lo detecte, notificará al supervisor más cercano y a la oficina de administración. El supervisor localizará a fuente del mismo. De poder controlarlo procederá a extinguirlo e informará a la oficina de Seguridad y Planta Física. De no poder detectar la fuente del humo o no poder controlar la misma, el supervisor informará a la oficina de Seguridad y Planta Física y esta tomará la decisión de desalojar el edificio.

Cuando se observe **humo espeso** la persona que lo detecte, desalojará el área inmediata alertando a los compañeros más cercanos y activará la alarma de incendio.

Fuego

De producirse un **fuego y éste se detectado en su inicio**, se procederá a tratar de apagarse con los extintores disponibles y/o mangueras contra incendios. De ser necesarios se activará la alarma de incendio.

Cuando un empleado detecte un **fuego ya iniciado**, éste dará la voz de alerta de inmediato y se activará la alarma de incendio. De ser un **fuego pequeño**, se tratará de apagar con el equipo disponible y de ser un **fuego de mayor** proporción, se abandonarán las facilidades inmediatamente.

DESALOJO DEL PERSONAL:

Todas las áreas de operación de la *Oficina de Cómputos y Sistemas* están rotuladas en áreas visibles con el plano de desalojo de las facilidades por las 2 rutas de escape por las escaleras. En adición se ha identificado el personal con impedimentos o dificultades especiales para traslado. No se ha identificado ningún empleado con problemas crónicos de visión y solo una con problemas de audición o que dependan de equipo de movilización especial o de prótesis que requieran de asistencia especial para traslado.

Una vez se activen las alarmas o el Director decida desalojar las facilidades, los Supervisores verificarán que el personal desaloje las facilidades inmediatamente. El último supervisor en llegar a la puerta de salida de su área preguntará en voz alta si queda alguien, verificará el baño y abandonará el edificio. Esto se hará en orden, caminando y utilizando las escaleras. **EN TODO MOMENTO SE EVITARÁN LOS ASCENSORES.**

Una vez fuera del edificio el personal se moverá a las áreas asignadas. Los supervisores allí harán un inventario de personal y verificarán que todo su personal este en el área. Para la identificación positiva del personal en caso de desalojo de emergencia cada supervisor entregará el registro de asistencia al coordinador alterno y una vez completado el desalojo se procederá a un conteo de emergencia. Es responsabilidad del personal una vez que llegue al área buscar su grupo de trabajo y reportarse a su supervisor.

AMENAZA O HALLAZGO DE ARTEFACTOS EXPLOSIVOS O BOMBAS

Procedimientos:

Cualquier empleado puede ser notificado de que en su área han puesto artefactos explosivos o bombas. Esta notificación puede venir mediante comunicación escrita o de alguna llamada directa. El empleado va a proceder de la siguiente manera:

1. Copiar el texto exacto de la amenaza, si es vía telefónica
2. Hora y número del teléfono por el cual se recibe la llamada.
3. Detalles sobre la persona que hace la llamada:
 - Sexo
 - Edad
 - Tono de voz (ronca, disfrazada, etc.)
 - Acento (nacionalidad)
 - Animosidad (llorando, alegre, etc.)
 - Ruidos de fondo
 - Indicar el nombre de posible sospechoso, si le es familiar
4. Tratar de mantener la conversación:
¿Dónde está? ¿Cómo es? ¿Por qué?

Es importante que estas llamadas sean tratadas como importantes y verdaderas emergencias y se responda a ellas de acuerdo a las mismas. Notifique de inmediato al Coordinador de Emergencias y al Director de Informática.

El Oficial a cargo del Plan de Emergencia, seguirá el siguiente procedimiento, cuando implante el Plan de emergencia:

1. Notificará a la Administración sobre la situación al respecto
2. Si la llamada es sobre una amenaza de bomba, inmediatamente notifique al cuartel de la policía local para que se persone al lugar.
3. Notifique a todos los componentes del equipo de búsqueda (directores de Oficinas) dentro de la dependencia, quienes participarán en la búsqueda o registros.
4. En vías de mantener un control sobre esta situación se va a proceder de la siguiente manera: ¿dónde deben buscar?
 - Lugar donde se indicó que estaba la bomba, según la amenaza.
 - Áreas de fácil acceso al público
 - Alrededor del edificio, entrada principal, área de visitantes, baños sanitarios, pasillos, etc.
 - Áreas susceptibles a sabotaje
 - Sub-estaciones eléctricas, plantas, acondicionadores de aires, Oficina de Sistemas de Información.
 - Áreas controladas de importancia:
 - Oficinas Administradores, Directores
 - Si se decide desalojar, los primeros en salir son aquellas personas que están más cerca del artefacto sospechoso o bomba. Se utiliza el Plan de Evacuación a menos que la localización del artefacto obligue a cambiar el desalojo.
 - El hallazgo de un artefacto explosivo o sospechoso, requiere la presencia de los Técnicos de explosivos, quienes serán notificados por la Policía.
 - La orden de que todo está bajo control, será luego de haber completado el Plan de Emergencia y haber transcurrido un tiempo razonable, de haber terminado la búsqueda y registros de todas las oficinas sin hallazgo alguno de posible artefacto explosivo, o luego de haber sido removido el artefacto encontrado por el personal técnico de explosivos.

Precauciones

La vida humana es lo primero que debemos asegurar. Es importante utilizar el sentido común. El tipo y tamaño del artefacto, depende de la imaginación del que lo construye. Todos los sitios tienen que ser registrados y todo lo que se encuentra en las áreas que no pertenece a ellas debe ser tratado como artefacto sospechoso.

Acción que se tomará cuando sean encontrados artefactos sospechosos:

- No tocar ni mover los objetos.
- Tener mucho cuidado para asegurar que el objeto no sea movido de ninguna forma.
- Desalojar todas las personas cuando se les ordene, a un sitio seguro y lo más lejos posible del área de peligro.
- Notificar al coordinador de emergencias sobre la descripción y localización del artefacto. Estos a su vez notificarán a las autoridades pertinentes (División de Explosivos.)
- Mantener la seguridad en toda el área no permitiendo entrar personas no autorizadas.
- Cortar la luz eléctrica en el área de peligro (de ser posible).
- Abrir puertas y ventanas en el área, para reducir la explosión y daños de fragmentación secundaria (de ser posible).
- Hacer preparativos necesarios para combatir el fuego en caso de que haya una explosión (ubique los extintores en posición).
- Mantener custodia del área donde fue encontrado el artefacto hasta que los técnicos e investigadores lleguen y le releven.

Departamento de Bomberos y Policía de Puerto Rico

Tan pronto se personen a la escena de la emergencia, el Comandante de los Bomberos o la Unidad especial de la Policía, evaluarán todos los hechos concernientes y determinarán la magnitud de la emergencia. El que reciba la llamada deberá estar disponible para ofrecer al Departamento de Bomberos, a la Policía y a sus investigadores, toda la información que conoce, de la persona que hizo la llamada y del artefacto si este es encontrado. Hasta que la orden de

MEDIDAS PARA LA PRESERVACIÓN DE DOCUMENTOS ESENCIALES

Uno de los aspectos más difíciles de un programa de preservación de documentos es el seleccionar los documentos esenciales para proveer la información que será requerida por cualquier dependencia durante una emergencia. La selección apropiada de estos documentos, es posible solamente si el criterio de selección ha sido establecido primero y estrictamente aplicado a todos los casos. La clasificación de los documentos esenciales en tres en una base funcional, es también aplicable a los documentos de los gobiernos estatal y municipal. Esas tres categorías son:

Primera Categoría- Documentos que contienen información esencial para conducir operaciones de supervivencia durante el desastre, que incluye planes operacionales de diversos servicios de emergencias.

Segunda Categoría- Documentos que contienen información esencial en la fase de recobro para restablecer las estructuras organizacionales y funciones básicas

y responsabilidades del gobierno incluyendo, por ejemplo, documentos relacionados con la salud pública, protección de vida, propiedad, etc.

Tercera Categoría- Documentos que contienen información esencial en la fase de recobro para restablecer los derechos básicos de los individuos y cuerpos corporativos, incluyendo derechos legales, de propiedad y otros.

A continuación presentamos algunas medidas para conservar los documentos en situaciones de emergencias:

1. Tener los documentos en una estructura física resistente a ráfagas de vientos fuertes, movimientos sísmicos, fuegos y lluvias torrenciales.
2. Asegurar con paneles o planchas de metales las puertas y ventanas.
3. Cubrir con material plástico los archivos y cajas de documentos.
4. Bajo ninguna circunstancias colocar cajas de documentos a no menos de 6 pulgadas del nivel del piso.
5. El área debe mantenerse libre de polvo, humedad, sabandijas, entre otros.
6. No se debe ingerir alimentos en el área.
7. Extintores contra incendios y alarmas de fuego deben ser instaladas.
8. La ventilación y temperatura apropiada es necesaria para evitar el desarrollo y crecimiento de hongos.
9. Controlar el acceso a los documentos.

Cuando la orden de desalojar sea dada, la persona a cargo, el asistente, supervisores y equipos de búsqueda, pueden establecer un puesto de comando en su área donde podrán dar y recibir instrucciones y órdenes.

DEBERES Y RESPONSABILIDADES DEL (DE LA) COORDINADOR (A) DE MANEJO DE EMERGENCIAS

- Preparará y mantendrá actualizado el Plan de manejo de Emergencias.
- Suplirá todos los anejos que le sean requeridos para actualizar el Plan Estatal.
- Supervisará a los coordinadores Alternos.
- Se asegurará que se active el Plan de Contingencia.
- Orientará a todo el personal de la Administración en coordinación con el Coordinador Interagencial sobre los conocimientos básicos relacionados con las distintas emergencias, como enfrentarlas y cómo reaccionar correctamente a las mismas, tanto en el trabajo como en el hogar.
- Asistirá a todas las actividades y reuniones que el Coordinador Interagencial del *Departamento del Trabajo y Recursos Humanos* le delegue.
- Trabaja turnos rotativos cuando el Coordinador Interagencial requiera su presencia en el Comité de Operaciones de Emergencias de la Agencia Estatal para el Manejo de emergencias o el Centro de Mando cuando haya una activación por una emergencia o desastre.
- Participará en los ejercicios llevados a cabo por la Agencia Estatal para el Manejo de emergencias.
- Coordinará y canalizará todas las gestiones necesarias a través del Coordinador Interagencial.
- Rendirá un informe al Coordinador Interagencial de la labor realizada durante la emergencia.
- Se asegurará que su equipo de comunicación esté en buenas condiciones y se reportará diariamente con el Coordinador Interagencial indicando que está en referencia.
- Nombrará grupos de apoyo para emergencias y le asignará las responsabilidades específicas a cada uno.
- Adiestrará a estos grupos de emergencia utilizando los cursos y adiestramientos de manejo de emergencias que ofrece la Agencia Estatal para el Manejo de Emergencias y otras Agencias y servirá como recurso.
- Realizará simulacros donde sus planes o procedimientos de emergencias se practiquen por lo menos dos veces al año.
- Estos deberes estarán sujetos a revisión de acuerdo a las situaciones que puedan surgir.

DEBERES Y RESPONSABILIDADES DEL (DE LA) COORDINADOR(A) DE MITIGACIÓN

- Coordinar, preparar planes y actividades de mitigación
- Colaborar en el establecimiento de prioridades para proyectos de mitigación.
- Participar en la evaluación de daños ocasionados por emergencias o desastres.
- Participar en el proceso de identificación de actividades o medidas de mitigación cuyo propósito sea reducir daños futuros y/o salvar vidas.
- Elaborar o coordinar la preparación de propuestas para la obtención de fondos para el desarrollo de proyectos de mitigación.
- Asistir a reuniones, seminarios, adiestramientos y talleres relacionados a las actividades de mitigación.
- Asistir a todas las actividades y reuniones que el Coordinador de Manejo de Emergencias de la Administración le delegue.

DEBERES Y RESPONSABILIDADES DEL (DE LA) COORDINADOR (A) ALTERNO (A).

- Se reportará y estará bajo las ordenes y directrices del (de la) coordinador (a) de Asuntos para el manejo de Emergencias para la Administración.
- Ayudará al (a la) Coordinador (a) en todos las áreas que le sean solicitadas y asignadas por dicho (a) Coordinador (a).
- Ayudará a mantener funcionando los Sistemas de Comunicación para uso inmediato.
- Ayudará a identificar grupos o voluntarios de emergencia para que el (la) Coordinador (a) los nombre y asigne tareas específicas.
- Coordinará los adiestramientos a empleados y grupos utilizando cursos y adiestramientos de Manejo de Emergencias que ofrece la agencia estatal para el Manejo de Emergencias.
- Actuará como recurso en los adiestramientos según le sea requerido por el (la) Coordinador (a).
- Ayudará a organizar a los reservistas (grupos de ayuda en emergencias).
- Cooperará con el (la) Coordinador (a) para orientar al personal de la Administración sobre conocimientos básicos relacionados con las emergencias.
- Asistirá a aquellas actividades y reuniones que le sean requeridas por el (la) Coordinador (a) o que éste (a) deleguen él /ella como alterno (a).
- Participará en los ejercicios llevados a cabo por la Agencias Estatal para el Manejo de Emergencias, cuando así le sea requerido por el (la) Coordinador (a)
- Rendirá informes periódicos al (a la) Coordinador (a) sobre todas las actividades que realice.
- Notificará cambios en su dirección, teléfono de oficina y residencial. Estará disponible en todo momento.
- Estará presto a representar a la Administración cuando debido a situaciones imprevistas el (la) Coordinador (a) así lo decida.

DEPARTAMENTO DEL TRABAJO Y RECURSOS HUMANOS
Oficina de Operaciones y Apoyo Técnico

PLAN DE CONTINGENCIA 2010

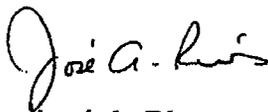
Introducción

Propósito

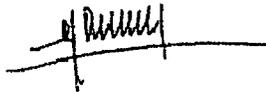
Proveer una guía disponible al personal de la Oficina de Cómputos y Sistemas acerca de la seguridad, localización de los equipos y pasos a seguir en caso ocurrir un desastre. Canalizar el esfuerzo de todo el personal para cumplir con la misión de la agencia, las funciones y política pública que nos dirigen.

A. Grupos de Recuperación

| Grupo | Componentes | Función | Personal |
|--------------|--------------------|----------------------------------|-----------------|
| A | Gerencia | Decisiones Gerenciales | José A. Ríos |
| B | Sistemas/Finanzas | Coordinación-Reportar al Grupo A | Ivonne Rivera |
| C | Sistemas | Restauración del Centro Primario | Luis Pena |
| D | Sistemas | Activación del Centro Alterno | Ely J. Padilla |
| E | Sistemas | Operacional del Centro Alterno | Juan N. Miranda |



José A. Ríos
Director, OCSI



Miguel Romero
Secretario del Trabajo

16/ sept / 2010