TCP-I

ANEJO A

ALBA MALDONADO COLON

From: JOSE A. RIOS
Sent: Monday, February 08, 2010 4:13 PM
To: ALBA MALDONADO COLON

Metodologías DMAIC et DMADV

La metodología DMAIC

- **D Define (Definir)**
  ¿Cuál es el problema?
  Definir las necesidades del cliente y precisar los objetivos a conseguir, cuadrar el proyecto. "Define" es la primera etapa del método. Permite definir el perímetro del proyecto, los considerandos, los recursos, y los plazos necesarios.
- **M Measure performance (Medir)**
  ¿Cuál es la capabilidad del proceso considerado?
  Colectar los datos representativos, medir la prestación, identificar las zonas de progreso. Evaluación de la prestación actual y de su variación (tendencia, ciclo...)
- **A Analyze (Analizar)**
  ¿Cuándo, dónde y cómo se producen los defectos?
  Utilización de las herramientas analíticas y estadísticas para identificar las causas de los problemas. En esta etapa del desarrollo del método, debemos entender los problemas para poder luego formular las soluciones susceptibles de llenar la separación entre la situación actual y los objetivos clientes.
- **I Improve performance (Mejorar)**
  ¿ Cuales son las soluciones de mejoría et cómo ponerlas en práctica para alcanzar los objetivos de performance fijados ?
  Identificación y puesta en práctica de las soluciones para eludir los susodichos problemas. Esta fase especialmente importante puede desarrollarse en ciertos casos precisos en varias etapas. Esto con el fin de tomarse el tiempo de someter a prueba y de validar las soluciones las más adecuadas.
- **C Control performance (Controlar)**
  ¿ Como guiar las claves variables para sostener y mantener la ventaja?
  ¿ Cómo guiar las claves variables para sostener y mantener la ventaja? Seguimiento de las soluciones establecidas. Es importante eludir toda vuelta atrás. Por otra parte, los resultados no siempre son visibles inmediatamente. El esfuerzo debe ser constante incluso cambiado de orientación. Se trata de la fase la más delicada, propia de todos los procesos de progreso continuo. La vuelta atrás representa una amenaza constante. Sostener el esfuerzo pasa necesariamente por la implantación de una cultura generalizada de la medición.

Comentario 1 : Se preferirá el método DMADV para establecer nuevos procesos. Este método bastante similar a DMAIC se compone de las siguientes fases : Define (Definir), Measure (Medir), Analyze (Analizar), Design (Diseñar), Verify (Verificar).
La fase Design : Define en el detalle el proceso con el fin de estar en perfecta concordancia con las expectativas de los clientes.
La fase Verify : Verifica que la performance y la capacidad están conformes a los objetivos y a las expectativas de los clientes.
A notar : Existe también otros métodos y variantes de estas últimas.
Comentario 2 : 6 Sigma no se limita al proceso de producción. Por extensión, esa necesidad de regularidad se revela provechosa en muchos otros dominios de la empresa. Asi 6 Sigma puede ser

desplegada con las precauciones de uso en el seno mismo de empresas de servicios como las compañías de seguros, los bancos, los centros de llamadas...
Comentario 3 : La pertinencia de la colecta de datos, la calidad de la medición y el tacto en el pilotaje del proyecto son puntos clave del buen desarollo del mëtodo. La cooperación de la totalidad del personal tambien es una de las reglas del éxito. La formación sistemática de la totalidad del personal concernado por el proyecto pendiente es en efecto un condición previa.

Resumiendo :

Objetivo : Mejorar al maximo la regularidad de la calidad cliente.
Finalidad : Aumentar significativamente los ingresos.
Financiación de la aplicación : Especialmente elevado, pero proporcional a los resultados esperados cuando el proyecto está llevado correctamente.

6 Sigma

Generalidades

El 6 Sigma significa simplemente una medida de la calidad que se esfuerza por alcanzar la perfección. 6 Sigma es una metodología disciplinada, basada en datos para eliminar los defectos en cualquier proceso.

La representación estadística de 6 Sigma describe cuantitativamente cómo un proceso se está realizando. Para alcanzar el estándar 6 Sigma, un proceso no debe producir más de 3.4 defectos por millón de eventos. Un defecto se define como cualquier cosa fuera de especificaciones del cliente. Un evento es entonces la cantidad total de ocasiones para un defecto. La sigma de proceso se puede calcular fácilmente usando una calculadora.

El objetivo fundamental de la metodología del 6 Sigma es la puesta en práctica de una estrategia basada en mediciones que se centre en la mejora de proceso con la aplicación de proyectos de la mejora de 6 Sigma . Esto se logra con el uso de dos metodologías secundarias de 6 Sigma: DMAIC y DMADV.

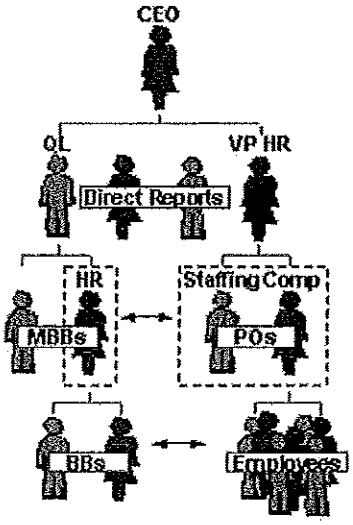
El proceso DMAIC (por las siglas en ingles de defina, mida, analice, mejore, controle) es un sistema de mejora para los procesos existentes que quedan por debajo de la especificación y que buscan una mejora incremental.

El proceso DMADV (por las siglas en ingles de defina, mida, analice, diseñe, verifique) es un sistema de mejora usado para desarrollar nuevos procesos o productos a nivel de calidad 6 Sigma. Puede también ser empleado si un proceso actual requiere más que una mejora incremental.

Ambos procesos son puestos en practica por Cintas Verdes, Cintas Negras y Maestros Cinta Negra del proceso 6 Sigma. Estos son expertos entrenados en los aspectos del proceso 6 Sigma.

Papeles y Responsabilidades

El 6 sigma es una metodología de la calidad que puede producir una ventaja significativa a los negocios y a las organizaciones. Una estructura organizacional comun en una compañía iniciada en esta metodología es como la que sigue:



Lider/Administrador de Calidad (QL/QM) – su responsabilidad es representar las necesidades del cliente y mejorar la eficacia operacional de la organización. La función de la calidad se separa típicamente de la fabricación o de las funciones de proceso transaccionales para mantener imparcialidad. El encargado de calidad se sienta en el personal de CEO/Presidentes, y tiene autoridad igual a el resto de los informes directos.

Los Cinta Negras Principales (MBB) – los cintas negra principales se asignan típicamente a un área o a una función específica de un negocio o de una organización. Puede ser un área funcional tal como recursos humanos o legal. El trabajo de MBB con los propietarios del proceso es asegurarse de que los objetivos y las blancos de la calidad estén fijados, los planes se determinen, se sigue el progreso, y se proporciona la educación.

El propietario de proceso (PO) – son los individuos responsables para un proceso específico. Por ejemplo, en el departamento jurídico hay generalmente una persona encargada que es el propietario de proceso. Dependiendo de la talla de las actividades de negocios y de base, se puede tener propietarios de proceso en niveles más bajos de la estructura de la organización.

Los cinta negra (BB) – es el corazón y el alma de la iniciativa de la calidad de 6 sigma. Su propósito principal es conducir proyectos de la calidad y trabajar a tiempo completo hasta que son completados.

Los cinta verde (GB) – los empleados entrenados en 6 sigma que pasan una porción de su tiempo en proyectos, pero mantienen su papel y responsabilidades regulares del trabajo. Dependiendo de su carga de trabajo, pueden pasar dondequiera de 10% a 50% de su tiempo en su proyecto. Como el programa se desarrolle, los empleados comenzarán a incluir la metodología de 6 sigma en sus actividades diarias.

Recompensas y reconocimiento

Todos sabemos que la asignación de los papeles no es bastante para comenzar y para mantener un programa acertado de calidad. Las recompensas y el reconocimiento deben ser parte de la ecuación.

Cintas Verdes – dependiendo de la talla del proyecto y de las ventajas que resultan, los vales, el efectivo y las opciones comunes son todos los factores de la motivación. Pero no hay que subestimar la potencia de la motivación del las felicitaciones públicas delante de los compañeros muchas veces aún más eficaces que una cantidad monetaria. Dependiendo del progreso del programa, se puede atar su sueldo a los resultados del proyecto.

Cintas Negras y Cintas Negras Principales – su estructura del sueldo y de la prima se debe relacionar al número de proyectos y a la ventaja de esos proyectos.

Propietarios de proceso – aquí está uno de los papeles dominantes que necesita ser definido correctamente. La remuneración del propietario de proceso (sueldo y prima) se debe atar directamente a los esfuerzos de calidad dentro de la organización.

Lider de Calidad – el funcionamiento es la base para la remuneración (sueldo y prima). Las capacidades de la dirección son críticas a esta posición, no solamente los aspectos cuantitativos (ahorros, proyectos, entrenamiento, los etc.) deben medirse, sino también sus cualidades. La dificultad se presenta en definir y claramente identificar los comportamientos requeridos.

CEO – Si el CEO está completamente a bordo con la iniciativa de la calidad, no tendrá ningún problema el cotejar su remuneración en base a sus reportes de calidad.

Entrenamiento en 6 Sigma

Poner las 6 sigma en ejecución dentro de una organización es similar a poner cualquier otra iniciativa en ejecución empresarial. La determinación del contenido y del marco, desarrollar los materiales, y rodarlos hacia la compañía es solamente mitad del trabajo necesario. La otra mitad está tratando de cambiar la cultura.

El entrenamiento es uno de los factores más importantes a el cual contribuye y ayuda a modificar y formar una cultura 6 sigma.

Gerencia Mayor

La gerencia mayor, también conocida como ' gerencia de Nivel C ' (CEO, CIO, CFO), es los individuos que fijan, comunican y conducen los objetivos del negocio. Son también los individuos que se requieren incorporar objetivos de 6 sigma en sus planes operacionales. Los ejemplos de objetivos pueden incluir:

ð El porcentaje de empleados entrenados por cierta fecha

ð Reducción del porcentaje en los defectos para todos los procesos

ð Ahorros proyectados del año

El entrenamiento para la gerencia mayor debe incluir una descripción del programa y ventajas financieras de la puesta en práctica, ejemplos del mundo real, una aplicación específica a la industria, y el entrenamiento y las herramientas requeridos para asegurar la puesta en práctica acertada. Dependiendo de disponibilidad del tiempo de la gerencia mayor y de su deseo de aprender los detalles, el entrenamiento de cintas negras también se recomuienda.

Encargados Funcionales / De proceso

Los encargados funcionales y de proceso son el nivel de la gerencia que señala directamente a la gerencia mayor. Dependiendo de la talla de la organización, puede ser que incluyan a encargados funcionales de áreas tales como recursos humanos, finanzas y entrenamiento, y los encargados de proceso de áreas tales como ensamblaje, la producción y la llamada se centran.

El entrenamiento para los encargados funcionales y de proceso es más detallado que lo proporcionada a la gerencia mayor. Los asuntos incluirían el concepto de 6 sigma, la metodología, las herramientas y los requisitos de asegurar la puesta en práctica acertada dentro de la organización.

Lideres de Calidad

Ayudan a los encargados funcionales y de proceso y conducen la visión de la 6 sigma dentro de sus áreas específicas. Llevan registro de los ahorros del negocio, aseguran que las metas del entrenamiento se satisfagan, revisan los estados de los proyectos en las fechas limite, comparten las mejores prácticas, y aseguran el uso apropiado de herramientas y de metodologías.

El entrenamiento para los lideres de calidad incluye la información detallada sobre el concepto, la metodología y las herramientas, así como estadística detallado y el uso de la herramienta del análisis computarizado. Dependiendo del instructor, la duración es generalmente entre tres y cuatro semanas.

Lideres de Proyecto

Ponen la metodología y las herramientas en ejecución dentro del negocio. Mantienen líneas del tiempo y el presupuesto, determinan uso apropiado de las herramientas, realizan análisis, y actúan como punto central de contacto para los proyectos específicos de la mejora de procesos.

El entrenamiento para los lideres de proyecto incluye la información detallada sobre el concepto, la metodología y las herramientas. Dependiendo del instructor, la duración es generalmente entre dos y cuatro semanas.

Empleados

Los empleados, también conocidos como cintas verdes, pueden también tomar los cursos de aprendizaje desarrollados específicamente para los lideres de proyecto de medio tiempo. El entrenamiento es similar, pero más corto en la duración porque pone menos detalle en las herramientas complejas y la estadística que se proporciona.

Los procesos DMAIC y DMADV

Para la integración de la metodología 6 Sigma se cuenta con dos tipos de métodos. Ambos son similares, incluso las iniciales son parecidas, pero cada uno de estos procesos es aplicable en ciertas situaciones.

Primero miremos las metodologías de DMAIC y de DMADV y hablemos de sus semejanzas. DMAIC y DMADV son ambos:

- Metodologías de 6 sigma que conducen los defecntos a menos de 3,4 por millón de oportunidades.
- Soluciones basadas en datos. La intuición no tiene ningún lugar en 6 sigma, solamente hechos.
- Puesto en ejecución por Cintas Verdes, cintas negras y cintas negras principales.
- Maneras de ayudar alcanzar la línea de fondo en los negocios.
- Puesto en ejecución con la ayuda de un propietario del proceso.

Aquí es donde las semejanzas acaban. Cada proceso tiene un fin diferente:

DMAÍC	**Defina** **Mida** **Analice** **Mejore** **Controle**	• Defina las metas del proyecto y las variables (internas y externas) del cliente • Mida el proceso para determinar funcionamiento actual • Analice y determine la raíz de los defectos • Mejore el proceso eliminando defectos • Controle el funcionamiento de proceso futuro

La metodología de DMAIC, en vez de la metodología de DMADV, debe ser utilizada cuando un producto o un proceso está en existencia en una compañía pero no está resolviendo la especificación del cliente ni se está realizando adecuadamente.

DMADV	**Defina** **Mida** **Analice** **Diseñe** **Verifique**	• Defina las metas del proyecto y las variables (internas y externas) del cliente • Mida y determine las necesidades y las especificaciones de cliente • Analice las opciones de proceso para resolver las necesidades del cliente • Diseñe (detallado) el proceso para resolver las necesidades del cliente

		• Verifique el funcionamiento y la capacidad del diseño de resolver las necesidades del cliente

La metodología de DMADV, en vez de la metodología de DMAIC, debe ser utilizada cuando:

- Un producto o un proceso no está en existencia en su compañía y una necesita ser desarrollado
- El producto o el proceso existente existe y se ha optimizado (con o DMAIC o no) y todavía no resuelve el nivel de la especificación del cliente o del nivel 6 sigma.

ANEJO B

DEPARTAMENTO DEL TRABAJO Y RECURSOS HUMANOS

OFICINA DE CÓMPUTOS Y SISTEMAS

GUÍA METODOLOGICA PARA 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.

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.

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.

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 ayudad y fortaleces a las familias 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. 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 par apoyar y aumentar la respuesta a la situación de emergencia. La Planificación, capacitación y los ejercicios se encuentran entre las actividades de esta fase.

LOCALIZACIÓN DE LA ADMINISTRACIÓN

La Oficina de Cómputos y Sistemas (Centro de Cómputos) está ubicada en el sexto piso de las Oficinas Centrales del Departamento del Trabajo y Recursos Humanos en el Edificio Prudencio Rivera Martínez. Avenida Muñoz Rivera 505 Hato Rey P.R.

El Departamento del Trabajo y Recursos Humanos cuenta con una de las redes de sistemas más amplias y robustas en capacidad y en continuo crecimiento. Nuestro sistema abarca comunicación, interna e interagencial con mecanismos que garantizan la seguridad del contenido de la data de nuestros sistemas. 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, 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 mensajeria electrónica y la red global de informática (Internet).

La Oficina de Cómputos y Sistemas cuenta con un total de 24 empleados en 4 áreas operacionales. De este total 20 laboran en el horario de 7:30am a 4:00pm y 4 laboran de 8:00am a 4:30pm.

Nuestras facilidades constan de unos 10,285 pies cuadrados, distribuidos en las áreas de Comunicaciones, Programación y Sistemas, Servidores, Recibo y Tramite.

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, ect.), 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 105 procesos de la agencia a niveles aceptables de servicio y funcionamiento, con el menor tiempo posible de impacto y de la manera menos costosa.

Los planes de contingencia deben ser implementados en todos y cada uno de los procesos vitales de la operación de la organización y deben considerar 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, 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.

Los planes de contingencia se activan cuando algún componente de cualquier proceso crítico falla. También se los emplea cuando aparentemente fallan los esfuerzos de corrección de algún componente. En este caso los planes de contingencia se implementan 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, ...)

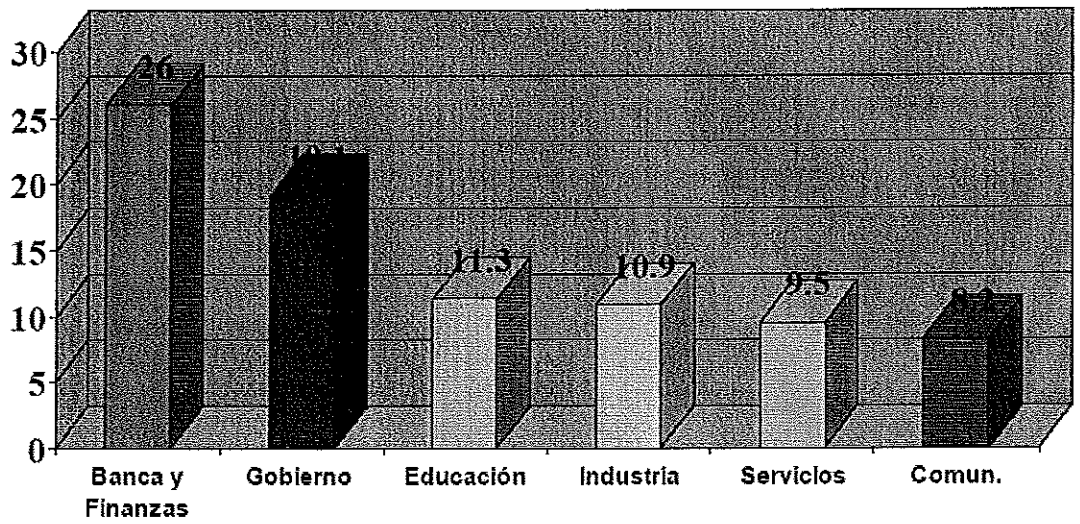
Todos estos recursos se encuentran en un entorno de incertidumbre, que en ocasiones puede provocar interrupciones inesperadas del funcionamiento normal de la actividad.

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.

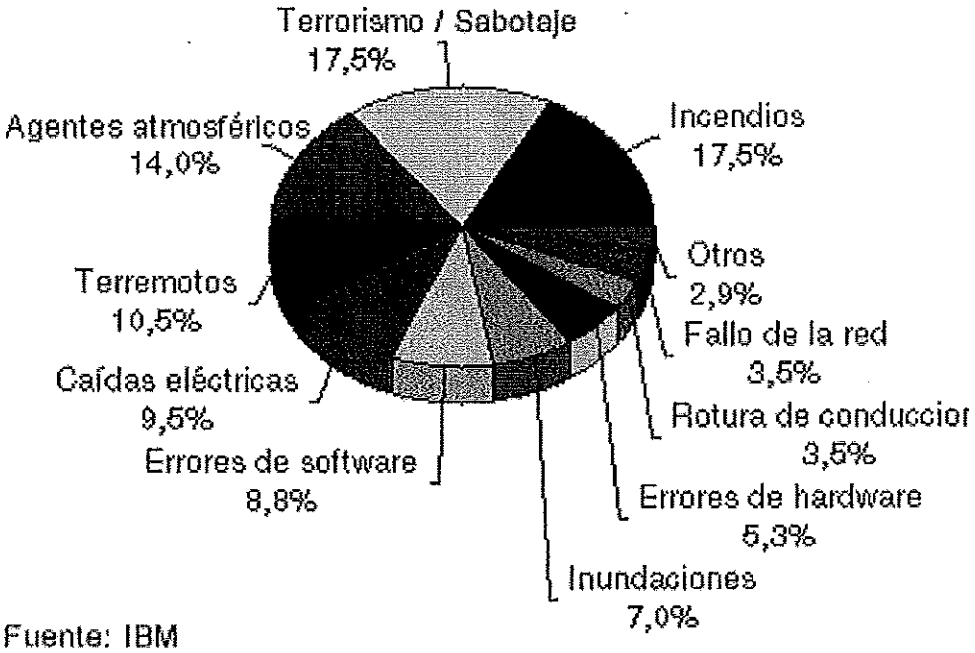
Para prever las consecuencias de estas situaciones es necesario establecer estrategias de respuesta ante contingencias que aseguren la continuidad y reanudación de los servicios críticos.

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



El Plan de Contingencias del Centro de Cómputos implica un análisis de los posibles r iesgos a l os Cu ales p ueden estar ex puestos nuestros eq uipos d e cómputo 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 Cómputo en f orma rápida, eficiente y con el m enor 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 del Centro, 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 0 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
2. **Sr. Ely J. Padilla Pérez** -Coordinador Alterno
3. **Sra. Ivonne Rivera Agosto** -Coordinadora Asuntos Transferencia Operaciones
4. **Sra. Juan N. Miranda** -Coordinadora Asuntos Transferencia Operaciones
5. **Luís R. Lopez** -Búsqueda y Rescate
6. **Sr. Luis Pena Cortes** -Manejo de extintores de incendio
7. **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 corno un proyecto complejo y de suma importancia para la agencia. De esta m anera se garantiza que todos las dem ás personas componentes de l equipo y de la agencia apoyen directamente al proceso de planes de contingencia.

2. Análisis de los procesos

Se han identificado los procesos críticos del Centro, que son aquellos sobre los que se ejecutan las operaciones de sistemas propias de la agencia, y que en caso de ser afectados podrían llevar 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. Aqui 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 mas procesos críticos soportan y los procesos que más elementos de posible falla contienen.

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 c osta de l a p rotección de l a l nformación en análisis, v ersus el c osto 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?
- ¿Con que frecuencia puede ocurrir?
- ¿Cuales serian sus consecuencias?
- ¿Que credibilidad tienen las respuestas a las tres primeras preguntas?

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?
- ¿Cuál es su valor para uno o para la organización?
- ¿Frente a qué se intenta proteger?
- ¿Cuál es la probabilidad de un ataque?

A continuación se muestra un ejemplo de 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.
- 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 equipos y archivos
- A terremotos, que destruyen el equipo y los archivos.

- A accesos no autorizados, filtrándose datos no autorizados.
- Al robo de datos, difundiéndole los datos sin cobrarlos.
- Al fraude, desviando fondos merced a la computadora

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 Institución estará listo para responder a los efectos que estos riesgos tendrán para su Institución.

¿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 dañen
- A **terremotos** que destruyen los equipos y archivos
- Al **robo de datos** difundiéndose 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 analizados son críticos para la institución, y por ende todas las aplicaciones que los soportan son importantes, 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 activo se deben considerar varios criterios:

CRITERIO DE PARTICIPACIÓN:

- Si el 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.

CRITERÍO 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.

Los datos de probabilidad e impacto de falla de todos los activos deben incluirse en cada proceso, facilitando así la priorización de los mismos.

Se han diseñado planes de contingencia por lo menos para todos los procesos críticos que contengan activos con alta probabilidad de falla, priorizando los que tengan aplicación(es) con niveles altos de impacto.

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 10 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 deber de 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).

b) Equipos de Cómputos Aparte de las Normas de Seguridad que de Seguridad que se verán en los capítulos siguientes, 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.

- Señalización o etiquetado de los Computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. 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:

1) 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'

Modalidad Externa. Mediante convenio con otra Institución o agencia que tenga equipos similares o mayores y que brinden 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 tipo de convenios debe tener 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 instituciones o agencias.

Modalidad Interna. Si tenemos mas de un local, 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 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

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 como 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 este 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 funcionara 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 c onforme al m emorando de definición d e r oles (17 d e febrero d e 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), numero de "beeper" (si tiene) y dirección de correo electrónico. Esto garantizara

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 panes involucradas en el Comité de Manejo de Emergencias del Centro de Cómputos 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.

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 situaci6n 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 individuas 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 opor1unidades de la gente que podría querer dañar los datos o el sistema.
Existen diferentes formas de implementarlo:

- **Forma Institucional.-** El acceso al Área de Sistemas se identifica en el área de Recepción Institucional, asignándole un color específico: rojo por ejemplo.
- **Solo en el Área.-** Asignando un puesto de vigilancia en el ingreso al Área de Sistemas.

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.).

Restricciones que pueden ser aplicadas:

- Determinación de los períodos de tiempo para tos 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.

Control de acceso a la Información

Algunos usuarios o extraños (personal no autorizado) pueden encontrar alguna forma mediante la cual, logren el acceso al sistema o la base de dat os y descubrir informaci6n clasificada o datos no autorizados.

Se deberá considerar la existencia de:

Programas de Control. Deben existir programas protegidos que mantengan y controlen a l os u suarios y s us der echos de ac ceso, y a s ea por g rupos o individualmente.

El uso de tal programa puede conferir al usuario algunos de los privilegios que corresponden al controlador de dichos programas. La transferencia de privilegios es adecuada si el programa actúa como filtro de la información.

Palabra de Acceso (Password). Es una palabra especial o código que debe 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.

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

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

En todo proceso corporativo es recomendable que el responsable de cada área asigne y actualice en forma periódica el password a los usuarios.

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.

Esto es, el Jefe Inmediato superior tendrá en un sobre lacrado, los passwords de su personal, debiendo utilizar un cuaderno de control, cuando exista la necesidad de romper el sobre lacrado (anotando techa, hora, motivo, etc.), así como un procedimiento de cambio de passwords periódicos y por dichas eventualidades.

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 acuerda 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 informaci6n pero no la eliminación de datos.

Borrado. Permite la eliminaci6n 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 es preferible que esta función sea de responsabilidad del Centro de Cómputo.

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.

Destrucción

Sin adecuadas medidas de seguridad las empresas pueden estar a merced no sólo de la destrucción de la información sino también de la destrucción de su equipo informático.

La destrucción del equipa puede darse par una serie de desastres cama san: incendias, inundaciones, sismos, a posibles fallas eléctricas, etc.

Cuando se pierden datos y no hay disponibles copias de seguridad, se han de volver a crear los datos o trabajar sin ellos. De hecho, se puede comprobar cómo una gran parte del espacio en disco esta ocupado por archivos, que es útil tener a mano pero que no son importantes para el funcionamiento normal. Un ejemplo típico son las copias de la correspondencia en forma de archivos del procesador de textos. Estos archivos se guardan muchas veces como referencia o, por si hubiera que enviar cartas parecidas en un futuro. Sin embargo, probablemente también existe copia en papel de estas cartas. Si se borran los archivos, puede ser molesto, pero las consecuencias en la organización pueden ser mínimas.

Los archivos de contabilidad suponen una situación diferente, ya que volver a crearlos puede necesitar de mucho tiempo y costo. Muchas organizaciones basan en estos archivos la toma de decisiones diaria. Sin los datos al día, el funcionamiento se vería seriamente dañado. Para evitar daños mayores al ser destruida la información, debe hacerse **backups** de la información vital para la empresa y almacenarse en lugares adecuadamente preparados para ese fin y de preferencia aparte del local donde se encuentran los equipos que usualmente lo manejan.

Revelación o Infidencia

La revelación o infidencia es otra forma que utilizan los malos empleados para su propio beneficio. La información, que es de carácter confidencial, es vendida a personas ajenas a la institución. Para tratar de evitar este tipo de problemas se debe tener en cuenta lo siguiente:

Control del uso de información en paquetes abiertos o cintas y otros datos residuales

La información puede ser conocida por personas no autorizadas, cuando se deja en paquetes abiertos o cintas que otras personas pueden usar. Se deben tomar medidas para deshacerse del almacenaje secundario de información importante o negar el uso de esta a aquellas personas que pueden usar mal los datos residuales de estas.

Mantener datos sensitivos fuera del trayecto de la basura

El material de papel en la plataforma de la descarga de la basura puede ser una fuente altamente sensitiva de recompensa para aquellos que esperan el recogido de la basura. Los datos sensitivos deben ser aparados de este procedimiento para tener una mayor seguridad de protección de la información, cuando estos son descartados o eliminados, debiendo recurrirse a destructores o picadoras de papel.

Preparar procedimientos de control para la distribución de información

Una manera de controlar la distribución y posible diversificación de información, es mantener un rastro de copias múltiples indicando confidencialidad o usando numeración como "Pág. 1 de 9". Desafortunadamente, es muy común ver grandes volúmenes de informaciones sensitivas tiradas alrededor de las oficinas y relativamente disponibles a gran número de personas.

Modificaciones

Los usuarios deben ser concientizados de la variedad de formas en que los datos pueden perderse a deteriorarse. Una campaña educativa de este tipo puede iniciarse con una reunión especial de los empleados, profundizarse con una serie de seminarios y reforzarse con carteles y circulares relacionados al tema.

Las empresas deben tener muy en cuenta los siguientes puntos para la protección de sus datos de una posible contingencia.

1. Hacer de la copia de seguridad una política, no una opción
2. Hacer que la copia de seguridad resulte deseable
3. Facilitar la ejecución de la copia de seguridad (equipos adecuados, disponibilidad, suministros).
4. Hacer la copia de seguridad obligatoria
5. Asegurarse de que las usuarias cumplen la política de copia de seguridad (Política de Auditoria a las Copias de Seguridad).

PROTECCIÓN ESPECIAL DE LA INFORMACIÓN

Una de las funciones muy importantes de los responsables de comunicaciones es mantener controlado el uso de los datos de la compañía y los sistemas de transmisión.

Además de c ontrolar el u so del s istema por e mpleados autorizados, de ben también considerarse los problemas relativos a empleados que pueden tener acceso al computador, pero que no estc1n autorizados a usar programas o acceder a los ficheros de bases de datos, así como los problemas con individuos ajenos a la agencia.

Un sistema de información puede ser causa de violación de su seguridad, debido a varios factores:

- La naturaleza de la organización y de sus operaciones.
- Los tipos de aplicaciones y de bases de datos en el sistema de proceso de datos.
- La pasibilidad de beneficia económica para las delincuentes.

- El tamaño de la población de usuarios del sistema
- El tipo de sistema y las posibilidades disponibles para los usuarios

Las amenazas potenciales contra un sistema de proceso de datos y las perdidas que pueden producirse, son razones suficientes para la estimación de riesgos contra la seguridad.

La protección de información reservada en un canal de comunicación, es esencial. Uno de los principales métodos para ofrecer protección es hacer que la información del mensaje sea infrangible por medio de técnicas criptográficas, sin intentar ocultar la existencia del mensaje.

Encriptación

Definición.- Es una técnica mediante la cual se transforman los datos de forma que no proporcionen información al ser interceptados, puesto que tal como están almacenados o transmitidos son completamente ininteligibles.

Cada carácter es un registro reemplazado por otro carácter, así por ejemplo

La palabra SMITH se almacena como @LAZ#

En este caso, toda S es reemplazada por el símbolo @, etc., de este modo si alguien obtiene los datos no los entenderá, a menos que el lector sepa cómo descifrar la información.

La mayor aplicación de escribir los datos usando criptografía, se aprecia en la protección de los mismos cuando se transmiten a través de las líneas de comunicación.

Elementos de la Criptografía

Los mensajes que deben ponerse en clave se conocen como **texto en claro** y, a la operación en que los símbolos básicos se transponen o sustituyen para transformar los datos, se denomina **puesta en cifra.** La salida de procesos de puesta en clave se conoce como **texto cifrado** o criptograma, que luego es transmitida.

La persona que intenta accesar a la información puede escuchar y copiar cuidadosamente el texto cifrado completo. Sin embargo, a diferencia del receptor asignado, dicha persona no conoce la clave y por lo tanto, no puede descifrar con facilidad dicho texto (Ver Figura NO. 1).

En algunas ocasiones el intruso no solo escucha la comunicación que se hace a través del canal (intruso pasivo), si no también puede registrar los mensajes y repetirlos posteriormente, incluir sus propios mensajes, o bien, modificar los mensajes originales antes de que lleguen al receptor (caso de un intruso activo).

El hecho de quebrar el cifrado se conoce como criptoanálisis y, el de inventar cifras, criptografía y desbaratarlas, como cristología.

Características de las Transformaciones Criptográficas

- El tamaño de la clave debe ser muy grande para dificultar los intentos de descubrirla.
- Las características del lenguaje (frecuencia de letras, pares de tetras, etc.) deben quedar enmascaradas y alteradas.
- La transformación debe ser muy compleja para evitar el análisis matemático.
- Las transformaciones, por ejemplo, la substitución poligráfica de un carácter por un grupo de caracteres, aumentan la longitud del mensaje cifrado sobre la del original.
- En las situaciones simples no hay propagación de errores, ya que se aplican sobre cada carácter independientemente, a diferencia de los cifrados por bloques que se propagan a lo largo del bloque o texto cifrado subsiguiente.
- La longitud de la clave es impor1ante para dificultar el criptoanálisis. Las claves cor1as del mensaje deben aplicarse repetidas veces en el proceso del cifrado. Las claves más largas que el mensaje, elegidas aleatoriamente y que se utilizan solo una vez son mas seguras.
- De acuerdo al tipo de transformación, estos sólo pueden funcionar cuando los dispositivos de cifrado/descifrado están sincronizados en el tiempo, por cuya pérdida se puede impedir el descifrado correcto.

Aplicaciones de la Criptografía

La aplicación de un tipo de transformaciones de cifrada en un sistema de teleproceso o de archivo, depende de las características de una aplicaci6n en particular y de los aspectos técnicas del sistema. Aunque la finalidad del cifrada es dar seguridad a los datos almacenadas a en tr8nsita, sus efectos sobre utilidad de una aplicación también son importantes.

Las características de una aplicación que determinan la elección del método de cifrado son:

- El valor de la información a proteger.
- El tipo de lenguaje utilizado (lenguaje natural o de programación).
- Dimensiones y dinámica de la aplicación (volumen de mensajes o registros que deben transmitirse o almacenarse, las velocidades y tiempos de respuesta exigidos).

Facilidades especiales:

La Oficina de Cómputos y Sistemas cuenta uno o más 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 adicción cuenta con línea telefónica directa (756-1082) y provisión de energía eléctrica a través de la planta eléctrica.

Se solicito 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 a 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 le 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 m antenimiento 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 empelado 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 piano 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 h a identificado ningún empleado con problemas crónicos de visión o 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 se 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 preparaciones necesarias 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 f uncional, es también ap licable 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 publica, 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 m antenerse libre de polvo, h umedad, 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.

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 como reaccionar correctamente a las mismas, tanto en el trabajo como en el hogar.
- Asistirá a todas las actividades y reuniones que el Coordinador Ineragencial del Departamento del Trabajo y Recursos Humanos le delegue.
- Trabajará turnos rotativos cuando el Coordinador Interagencial requiera su presencia en el Comité de Operaciones de Emergencias de la Agencias 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 par a 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 especificas.
- 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 2008

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 publica 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	Luís Pena
D	Sistemas	Activación del Centro Alterno	Ely J. Padilla
E	Sistemas	Operacional del Centro Alterno	Vidian Lebrón