ANEXO A

GUIA PARA EL DESARROLLO DE UN PLAN DE CONTINGENCIA

ANEXO A: GUIA PARA EL DESARROLLO DE UN PLAN DE CONTINGENCIAS

A.1. INTRODUCCION

Este anexo presenta una guía para el desarrollo de un plan de contingencias, en adelante llamado simplemente Plan, adaptado a nuestro medio y además dá algunas recomendaciones sobre Seguridad General en el centro PED.

Los términos contingencia y desastre pueden verse en su caracter general, sin embargo es el interés de esta presentación enmarcarlo dentro del ámbito del procesamiento electrónico de datos.

Según el diccionario de la Real Academia Española de Lenguas se define "contingencia" como la "posibilidad de que una cosa suceda o no suceda. Riesgo, peligro, evento." y "Desastre" como "Una desgracia grande, un suceso infeliz y lamentable."

Según la Comisión Nacional de Emergencia, un desastre (en general) es una "situación crítica originada por la naturaleza o el hombre, que consiste en el desequilibrio entre oferta y demanda de los servicios básicos de un asentamiento humano devenido por pérdidas materiales y humanas y que le pone en necesidad de recibir asistencia externa".

Se define un desastre en PED como un "evento seguro de ocurrir que puede causar un desbaratamiento o ruptura en las capacidades de los servicios de información por un tiempo suficientemente largo como para afectar las operaciones de la organización".

Un plan de contingencias es hecho para garantizar la operación de la organización, en el flujo de información vital, bajo la acción de eventos que tienen poca probabilidad de ocurrir.

"Los procedimientos para recobrarse de un desastre son hechos para los eventos de más seria ocurrencia. Los eventos de menos magnitud pueden ser manejados en un nivel apropiado, con un subconjunto de procedimientos de recuperación."

Al referirse a la necesidad de Plan para recobrarse del desastre, se indica que "Las medidas de seguridad son empleadas para prevenir o detectar omisiones, modificaciones o destrucción de datos, o la pérdida

de los medios de procesamiento de datos. Los planes para recobrarse del desastre son diseñados para reducir las consecuencias de la pérdida de cualquier recurso o capacidad del centro PED hasta un nivel aceptable."

El propósito de un plan de contingencia es "contar con procedimientos para el manejo de emergencias en casos de catástrofes y amenazas mayores para proteger personal, minimizar el daño a operaciones y equipo de procesamiento de datos, así como reducir la magnitud de la interrupción en el servicio".

Puede concluirse de lo anterior que el aspecto clave es proteger el personal y la información vital para la organización. Esta protección conduce a realizar un análisis de los riesgos a que está sometida dicha información y la forma de minimizar el efecto de esos riesgos. Esto mismo lleva a desarrollar los mecanismos necesarios que permitan identificar los elementos involucrados y mitigar los efectos del desastre o salir de él lo más exitosamente posible.

La elaboración de un plan de contingencias es una tarea que requiere de la participación del personal del área de informática como conocedores del ambiente de PED y sus características, de los usuarios como dueños de los sistema y de la alta administración como agentes de apoyo en las decisiones a tomar. Puede determinarse un conjunto de elementos comunes que hay que considerar dentro de un plan de contingencias; sin embargo el plan en cada organización se desarrolla de manera específica y responde a sus necesidades particulares.

Un Plan de contingencias contiene las previsiones que tomamos para afrontar un riesgo, peligro o evento que de alguna manera pueda afectar, particularmente la capacidad de procesamiento de datos y el ofrecimiento oportuno de la información que es vital para las operaciones de la organización.

El desarrollo de un plan de este tipo es costoso, involucra tiempo y una total disposición de la administración tanto del área PED como del resto de la organización. Es justificable desde el punto de vista del costo en que se incurre si sucede una contingencia que afecte significativamente las operaciones vitales y no se está preparado para hacerle frente a esa situación.

Los aspectos principales que deben considerarse en un plan de este tipo son:

- Análisis de los riesgos a que están expuestos los Centros PED.

- Análisis de aplicaciones, donde se determina el nivel de criticidad de las mismas, se identifica el grado de vulnerabilidad, el nivel de sistematización y el impacto del no procesamiento.

- Requerimiento de personal, equipos, materiales y otros recursos, convenios de soporte, para la operación en condiciones anormales.

- Procedimientos a seguir durante la contingencia; estrategias específicas de acción en los diferentes casos.

- Procedimientos a seguir después de la contingencia.

- Entrenamiento, capacitación y pruebas del plan.

Es necesario considerar la importancia de un plan de este tipo en las instituciones que dependen en gran parte del área informática y dirigir los esfuerzos para lograr que se inicie el proyecto de elaboración y puesta en marcha de un plan de contingencia.

A.2 SEGURIDAD GENERAL

Este apartado presenta algunas consideraciones importantes sobre la seguridad general en el centro PED.

Cuando se habla de una contingencia en un centro PED, se debe fundamentalmente a la falta de prevención o la poca o mala planeación.

Es necesario en primer lugar hacer un análisis de los riesgos a que está expuesto el centro PED y la probabilidad de ocurrencia.

Esta información puede ser tomada de datos históricos o de estimaciones cualitativas generadas por el grupo encargado de hacer el análisis de riesgos. Los resultados del análisis pueden diferir grandemente de una institución a otra.

Es importante identificar los riesgos cuyas causas son factores humanos, fuentes naturales o fallas internas, y el cómo mitigar sus efectos.

A.2.1 FACTORES DE RIESGO

Hemos dividido los centros PED en diez áreas específicas vulnerables a la ocurrencia de riesgos asociados a diferentes factores, los que de seguido enumeramos.

A.2.1.01 EDIFICIO

- Materiales de construcción de mala calidad.

-.Centro de cómputo situado en el primer piso o en el último o cerca de la calle, cocinas, laboratorios o parqueos.

-.Agua, tanques de almacenamiento o drenajes cercanos a centro PED, edificaciones situadas en zonas de inundación, carencia de detectores de agua y cobertores plásticos para el equipo

- Localización Geográfica.

- En áreas urbanas potencialmente conflictivas.

- Cerca de compañías peligrosas (por política o por la naturaleza de sus productos o actividades).

- Cerca de sitios de Radar.

- Autopistas muy transitadas.

- Cercana a vías Ferroviarias.

- Dentro del perímetro de rutas de vuelo.

A.2.1.2 AMBIENTE DEL CENTRO DE PROCESAMIENTO

- Aire acondicionado

- Inadecuado sistema o mantenimiento

- Energía eléctrica

- Falta de UPS o planta propia

- Inadecuado mantenimiento del equipo

- Mala distribución de la energía

- Inadecuado señalamiento de los dispositivos

- Protección contra fuego

- Detectores de humo inadecuados

- Ausencia de aspersores (Halon)

- Sistema no probado regularmente

- Insuficiente extintores manuales

- Falta de monitoreo de las alarmas

- Falta de entrenamiento contra incendios

- Procedimientos inadecuados de evacuación
- Lejanía de las centrales de bomberos o acceso difícil al centro PED.
- No existen interruptores de energía para casos de emergencia.
- Paredes y puertas fabricadas con materiales combustibles.
- Peligros en el centro PED.
- Iluminación inadecuada.
- No existen reglas de seguridad o señales de peligro.
- Cajas de empalme en mal estado dentro del cielo raso.
- Red de distribución no revisada con regularidad

A.2.1.3 CONTROL DE INGRESO

- Ineficiencia o falta de vigilancia.
- Se carece de muros o cercas externas.
- No se hace uso de registro de visitantes.
- Falta de tarjetas de identificación.
- Falta de coordinación entre la vigilancia y los recursos ad hoc.
- Identificación no requerida a visitantes.
- Puertas y ventanas inseguras.
- Falta de control de vehículos que ingresan o salen
- Inadecuado control de acceso al centro PED.
- Areas del centro PED inseguras (sin llave).

A.2.1.4 PERSONAL

- No existe comprobación adecuada de experiencia del nuevo personal, de los suplidores y los contratistas.
- No se exige el contrato de empleo.
- Inadecuada revisión de procedimientos de entrenamiento del grupo o rotación del trabajo.
- Carencia de personal competente o está mal pagado.
- Existencia de personal mal intensionado.
- Existencia de baja moral de trabajo.
- Inadecuadas políticas de asignación de palabras claves.

A.2.1.5 ADMINISTRACION

- No se hace un análisis regular de los riesgos.

- No existen adecuadas políticas de seguridad.

- Los fraudes y otros problemas no son comunicados a las autoridades respectivas.

- No hay personal dedicado al manejo de los desastres.

A.2.1.6 PLAN DE CONTINGENCIAS

- No existe del todo un plan.

- No existe un respaldo del plan en algún medio, fuera del lugar o no existe documentación.

- No se cuenta con un sitio alterno de operaciones.

- El Plan está desactualizado o no ha sido probado.

- No existe un adecuado control de los activos y de los suministros.

- No existe identificación de los sistemas críticos.

A.2.1.7 DATOS Y PROGRAMAS

- No se establece un calendario para el respaldo de las aplicaciones o programas críticos

- Los lugares de almacenamiento dentro del cuarto del computador no son seguros.

- No se establecen políticas adecuadas para el manejo de datos importantes

- Se le permite al personal hacer sus trabajos personales (utilizar equipo).

- Documentación incompleta o inexistente.

- No se establece un calendario adecuado para el respaldo de programas fuente un objeto o de sistemas en desarrollo.

- Los programas son obsoletos los programas, tales como:

- No se destruye la información importante que no se usa.

- No se controlan los medios de almacenamiento.

- Inadecuados controles de calidad para los nuevos sistemas.

- No existen controles de acceso a los programas o sistemas.

- Los privilegios de los usuarios no están definidos.

A.2.1.8 HARDWARE (EQUIPO)

- No hay un inventario completo del hardware (equipo).

- Inadecuado mantenimiento.

- El equipo o el sistema operativo es obsoleto.

- En la comunicación de datos (teleproceso) existe.

- Inadecuado control de acceso.

- Líneas de comunicación privadas sin respaldo.

- Lineas de comunicación inseguras o con fallas.

- Existencia de interferencia electromagnética.

- Las terminales no se restringen para usuarios específicos o tareas específicas.

- Inadecuado o carencia total de control de claves de acceso.

A.2.1.9 ORGANIZACION INTERNA

- Se almacena documentación importante en medios inseguros.

- No hay controles de documentación o material importante (formularios sensibles).

- Carencia de respaldos de documentación importantes.

- Seguridad o las fallas de los equipos.

- Reportes incompletos o con error de las fallas del equipo.

- Inadecuada documentación de los sistemas, programas y sistema operativo.

- Procedimiento de encendido y apagado del equipo mal definidos.

- Malos hábitos permitidos en el cuarto del computador (comer, fumar, almacenar material inflamable, etc.).

- Falta de higiene en el lugar.

A.2.1.10 AUDITORIA

- No existen procedimientos o programas de auditoría.

- Inadecuados rastros de auditoría.

- Los reportes de Auditoría no se revisan.

- Inadecuados controles internos en los sistemas.

A.2.2 MEDIDAS PARA MITIGAR EL RIESGO

A 2.2.1 CONTROL DE INGRESO A LAS INSTALACIONES

- Contar con vigilancia de seguridad, debidamente preparados y entrenados (de preferencia empleados de la institución).

- Contar con puertas especiales preferentemente utilizar el sistema de doble puerta, de tal manera que al pasar la primera puerta, esta se cierra y la siguiente no se abre hasta que el guarda identifique a la persona.

- Llevar un registro de entradas y salidas de visitantes indicando nombre, propósito de la visita, hora de entreda y salida, sitio de trabajo (interno o externo) y persona que autorizó su ingreso.

- Controlar la entrada de personal autorizado mediante un gafete y otro medio de identificación, que indique el área a la que puede tener acceso.

- Mantener una relación constante entre los ejecutivos facultados para autorizar el ingreso de personal ajeno al centro PED y la salida de suministros.

- Las instalaciones colindantes con áreas descubiertas deben estar protegidas adecuadamente.

- Dejar una sola entrada debidamente controlada y el resto de las puertas como salidas de emergencia.

- En caso de que ingresen vehículos a las instalaciones, debe existir un control en donde se anote la placa del vehículo, nombre del

conductor, hora de entrada y salida, propósito de la visita y persona que autorizó el ingreso.

- Debe existir un circuito cerrado de televisión que permita vigilar al menos el acceso principal y el área de operación.

- El centro de procesamiento d datos debe considerarse como área de acceso restringido para personal no autorizado.

- Definir el personal autorizado con acceso al centro PED. Este podría ser:

- Empleados que laboren dentro del centro PED.

- Persona visitante de otras áreas de la institución, personal de limpieza, mantenimiento y proveedores que por razones de servicio deban tener acceso al centro PED, deberán contar con la debida autorización.

- Personal externo debidamente autorizado.

- Personal de ingeniería de Mantenimiento de equipo de cómputo y auxiliares.

- Contar con procedimientos alternos en caso de que personas con medios de acceso, extravíe éste o se le olvide.

A.2.2.2 LOCALIZACION GEOGRAFICA

- Analizar edificios vecinos, empresa y áreas adyacentes, con el fin de evitar instalar e PED en sitios propensos a incendios, explosiones, inundaciones, interferencias y otros riesgos que pudieran afectar sus operaciones del PED. Es conveniente realizar un análisis adecuado de las condiciones sismológicas y ambientales tales como contaminación, ruido y vibraciones.

- El lugar seleccionado deberá contar con bajo historial delictivo, vandalismo o disturbios sociales.

- El sitio seleccionado deberá contar con los medios de comunicación necesarios para tener un acceso rápido y oportuno, tomando en cuenta las contingencias que pudieran incomunicar al centro PED o para su evacuación. Es importante también conocer el área en lo que se refiere a la alimentación eléctrica y telefónica ya que de la primera depende toda la operación del centro PED y de la segunda el servicio de teleproceso.

A.2.2.3 EDIFICIO

- Es recomendable que el edificio cuente con:

- Espacios disponibles para instalación de equipos de soporte y auxiliares.

- Acceso razonable para la introducción y extracción del equipo, sin que sufra ningún daño.

- Potencial eléctrico adecuado.

- Servicios públicos adecuados.

- Buenas salidas de emergencia.

- El centro PED debe estar construido con materiales resistentes al fuego.

- Evitar el uso de alfombras, que producen electricidad estática.

- Evitar el paso de tuberías por encima o por debajo del centro PED con el fin de prevenir filtraciones.

- Se recomienda construir el mínimo de ventanas exteriores con el fin de evitar interferencias provenientes del exterior, también se reduce la posibilidad de entradas no autorizadas y la condensación de agua en días fríos.

A.2.2.4 CARACTERISTICAS DEL AREA DE OPERACION

- PISO

- Uso de piso falso sobre la estructura del piso.

- Deben instalarse sensores de humedad y un sistema de drenaje que impida problemas de inundación.

- No debe presentar problemas excesivos de pandeo.

- PAREDES

- Deben estar construídas con material resistente al fuego, capaces de soportar el mínimo aceptable de exposición al fuego.

- CIELOS

- Deben ser con características acústicas y no combustibles.

- Deben evitar la trasmisión de sonido.

- Aplicar retardantes al fuego.

- CINTOTECA

- Construída con un rango de resistencia aceptable.

- Debe ser utilizada únicamente con este fin.

- Sus puertas deberán ser diseñadas para resistir el fuego y con su respectivo cierre de seguridad. Además debecontar con sistema de detección y extinción.

- Los pisos, paredes y cielos deberán ser construidos con las mismas especificaciones del área de operación.

- Deben contar con controles de temperatura y humedad.

- DISEÑOS

- INSTALACIONES

- Todas las instalaciones deberán ser cosntruidas de acuerdo con los códigos y normas vigentes sobre esta materia (tierras físicas, capacidad máxima de conductores, ductos, códigos de colores, pararrayos, etc).

- NIVELES DE ILUMINACION

- Las oficinas, baños, pasillos, etc, deben contar con niveles adecuados de iluminación.

A.2.2.5 PROTECCION CONTRA EL FUEGO.

El fuego puede originarse intencional o accidentalmente, siendo esto último lo más frecuente y por lo general es debido al descuido en el mantenimiento de las instalaciones o en el manejo de materiales de naturaleza combustible, por lo que es necesario considerar los siguientes puntos:

- Almacenar el mínimo indispensable de materiales combustibles (papel, cajas de cartón, etc.) que se va a utilizar de inmediato dentro del centro PED.

- Evitar tener cables conductores de corriente eléctrica sueltos o con contactos en mal estado.

- Comprobar que las cortinas, muebles, piso falso, techo, filtros de aire acondicionado, aislantes eléctricos y acústicos estén fabricados con materiales no combustibles.

- Las paredes de la instalación deben estar fabricados con materiales retardantes al fuego.

- Detectar el fuego en su etapa inicial (a través de detectores de humo).

- Instalar alarmas que indiquen el lugar donde se ha desatado un incendio.

- Implementar procedimientos adecuados para entrenar al personal.

A.2.2.6 PROTECCION DE ARCHIVOS

A continuación se describen algunos métodos para asegurar la protección de la información reducir los riesgos de pérdidas, fuga o alteración de la misma.

- RESPALDOS

Se llama respaldo a una copia que se guarda y preserva usualmante en un medio de almacenamiento diferente a aquel en el que fue grabado originalmente como protección contra la destrucción de datos originales o de información previamente procesada. Generalmente los respaldos de información se hacen en cintas magnéticas.

Es conveniente considerar que conjuntamente con la atención que los programas y datos merecen para este respaldo, también debe considerarse la documentación mínima requerida de archivos, las descripciones de su contenido y el propio manejo de datos, ya que de otra manera la ineficiencia y eventualmente los errores serán múltiples durante el proceso de recuperación.

Deben existir respaldos bien protegidos de:

- Información
- Software de aplicaciones
- Software del sistema

- ELEMENTOS DE RESGUARDO

Para el resguardo de los respaldos de información, datos y programas, se cuenta con diversos mecanismos.

Los más importantes son:

- Muebles especiales
- Cintotecas integrales
- Cajas de seguridad

Estos construyen especialmente para el almacenaje de cintas y elementos magnéticos; su construcción debe garantizar su total protección contra accesos de personas no autorizadas y contra agentes destructivos tales como el agua y el fuego.

A.2.2.7 SOPORTE AMBIENTAL

Las condiciones ambientales que se deben mantener dentro del centro PED y particularmente en el área de operación, son factores importantes de vigilar y controlar dentro de un programa de seguridad física, ya que un cambio en la temperatura puede dañar, temporal o permanentemente, dispositivos magnéticos de información y alterar el servicio del centro PED. Al respecto se hacen las siguientes recomendaciones:

- Se recomienda que la temperatura ideal de operación de los equipos de cómputo oscile entre 18 y 22 grados centígrados; la humedad relativa debe ser del 50% con una desviación de hasta 5%.

- El aire fresco producido por los equipos de aire acondicionado debe ser filtrado con el fin de evitar el ingreso de gases y vapores contaminados.

- Los filtros y los forros de los ductos del sistema de aire acondicionado deben estar hechos de materiales no combustibles.

- El mantenimiento preventivo debe hacerse al menos una vez al mes.

- Las conexiones eléctricas y las cajas de los circuitos que alimentan a los equipos de aire acondicionado deben estar protegidos y deben ser independientes de las conexiones del resto del equipo.

- Se debe contar con un respaldo adecuado de aire acondicionado, con el fin de que en caso de falla, no se deje inoperante a la unidad central de proceso.

- Aislar adecuadamente las tuberías de agua que abastecen a los equipos de aire acondicionado de manera que no produzcan derrames cerca del equipo o de los materiales relacionados con la computadora.

A.2.2.8 CLAVES DE ACCESO Y CODIGOS DE USUARIO

Hoy en día, la técnica más adecuada para controlar elacceso a los sistemas de información es mediante la utilización de claves de acceso y códigos de usuarios (password).

Una clave de acceso es un conjunto de números o caracteres o combinación de los mismos, que se asignan a un usuario o recurso del sistema de cómputo. Estas establecen las prioridades de acceso hacia los programas, archivos y bases de datos; además limitan los procesos a que los usuarios tienen autorización de ingresar. Muchos de los productos que se encuentran en el mercado, contemplan este tipo de protección.

La contraseña debe ser personal e intransferible, cada usuario es responsable.del uso que se haga de misma.

Para controlar en una forma adecuada el acceso a los sistemas de información, debe existir una unidad orgánica responsable de la seguridad de los datos que tendrá a su cargo la siguientes funciones:

- Elaborar procedimientos escritos para la asignación y administración de la claves de acceso.

- Conocer qué información debe estar protegida y el grado de protección que requiere. usuarios.

- Instruir al personal sobre la importancia de la seguridad.

- Cambiar las claves de acceso al menos cada 60 días o elaborar procedimientos interactivos que permitan a los usuarios modificar las mismas en el momento qu se requiera.

Algunas otras recomendaciones que se pueden dar al respecto son:

- El archivo que contiene las claves de acceso debe estar encriptado y debe tener su propia clabe de acceso.

- Debe existir una bitácora que registre todos los accesos ocurridos a fin de detectar intentos no autorizados.

A.2.2.9 CRIPTOGRAFIA

A la fecha la mejor defensa contra accesos no autorizados a la información procesada en los centros de cómputo, consiste en implantar medidas de seguridad, tanto físicas como lógicas, que reduzcan la posibilidad de que ocurra un evento que pueda repercutir en una pérdida para la institución.

En el ambiente del teleproceso la criptografía e la única técnica disponible para proteger la información sensitiva que se transmite a través de la red; aunque también puede ser usada para proteger información almacenada en dispositivos magnéticos.

Los términos de encripción y decripción son sinónimos de cifrado y descrifrado, existiendo básicamente dos métodos para transformación de mensajes:

- A través de códigos.
- A través de cifras.

En este último caso los caracteres pueden ser SUSTITUIDOS o TRANSPUESTOS.

A.2.2.10 ESTANDARES DE SEGURIDAD

Con el propósito de minimizar los riesgos de pérdida, divulgación, destrucción o modificación de información que se maneja en un centro PED y para que las medidas de seguridad tanto físicas como lógicas cumplan su objetivo, es necesario establecer estándares que se enfoquen a controlar las diferentes actividades que se realizan en las áreas de mesa de control, captura de datos y operación.

- Mesa de control.

1- Recepción de documentos:

El usuario debe entregar al encargado de recepción y de acuerdo a los horarios establecidos la siguiente información:

....Solicitud de proceso autorizada por el usuario responsable.
La información fuente.
Una forma de control de documentos por lote.
Una forma de control de lotes por sistema.

El controlista de recepción deberá:

. Verficar que los datos en las formas entregadas sean claros y completos.
. Verificar el nombre y firma del usuario que autoriza.
. Entregar al usuario una contraseña que será exigida al momento de entregar los reportes solicitados.

2- Destrucción de información innecesaria.

El encargado de mesa de control deberá:

Obtener el visto bueno del responsable paradestruir el material que ya no se utilice.
Triturarlo dentro del ámbito del centro PED.
Guardar una copia de la autorización en el archivo de mesa de control.

3- Emisión y entrega de reportes.

El área de operación deberá entregar los reportes tomando en cuenta:

La información contenida en la solicitud de proceso.
El calendario de producción (horario y prioridades).
La documentación del sistema.

El responsable de mesa de control deberá:

Preparar los reportes de acuerdo a lasinstrucciones del usuario y a la documentación del sistema.

Entregar los reportes al usuario a cambio de la contraseña de la solicitud de proceso, registrar la hora de entrega y firma de usuario que recibe.

- Area de captura.

1- Captura de la información fuente.

El capturista NO deberá hacer correcciones por iniciativa propia.

Cargar sus cifras de control al sistema para que se verifiquen por programa.

Respetar los dígitos codificados en el documento fuente.

Comparar las cifras fuente al final de lacaptura contra las cifras de control cargadas inicialmente.

Anotar la diferencia en el control de documentos de la información fuente, en el caso de que las cifras no coincidan.

- Area de operación.

1- Identificación de archivos de producción en diskettes y cintas magnéticas.

Todos los diskettes deberán ser identificados y controlados por el responsable de operación de acuerdo a lo siguiente:

. Tener un mueble para ordenar los diskettes.
. Asignar un número de inventario a los diskettes existentes y los que se adquieran posteriormente.
. Identificar los diskettes por medio de etiquetas externas engomadas de un color fijo para cada sistema que esté en producción.

2- Acceso a los archivos de producción y extracción de información.

Toda la información que sea necesario extraer de los centros de procesamiento de la institución, en cualquiera de los medios que esté contenida, debe ampararse en una forma especial diseñada por la unidad encargada de la seguridad de la información, en la que se especificará el asunto, motivo y los requerimientos de acceso o extracción de información.

3- Programas fuente en medios magnéticos.

Los programas fuente deberán ser copiados de disco a cinta o diskette una vez que el sistema a que pertenecen haya sido trasladado a producción.

A.2.2.11 MATENIMIENTO A INSTALACIONES ELECTRICAS

El mantenimiento y atención oportuna a las instalaciones y equipos son de gran importancia para el centro PED, ya que de estos depende la continuidad operacional del mismo. Es importante contar con procedimientos y controles que contemplen todos los puntos que tengan relación con la operación del centro PED para prevenir fallas o problemas.

Para la elaboración de programas de mantenimiento a instalaciones y equipos se deben tomar en cuenta no sólo los puntos significativos, sino también aquellos aque son menos relevantes pero que en determinado momento pueden afectar la continuidad del centro PED.

- El suministro de energía eléctrica para el centro PED debe ser:

. Independiente.
. Regulado.
. Debe contar con tierra física en toda la red de alimentación eléctrica.
. Centros de distribución de carga para todos los equipos debidamente identificados mediante diagramas (planos) de distribución.

- Deberá contarse con interruptor general de energía eléctrica para desactivar el suministro en casos de emergencia.

- Si se cuenta con sistema ininterrumpido de potencia o planta de emergencia, los equipos y las áreas indispensables deben estar conectadas a éstos pa que cuando ocurra una interrupción de energía eléctrica, no ofrece la operación del centro PED.

- Deberá contarse con un programa de mantenimiento preventivo que revise:

Balanceo de fases de alimentación al centro PED.
Medición de tierra física.
Contactos, aislamientos limpieza en interruptores.
Sistema de iluminación de emergencia.
Consumo de energía.

- Plan de mantenimiento de planta de emergencia.

Tensión de salida
Temperatura de arranque
Presión
Tiempo y sistema de arranque
Secuencia de fases

- Plan de mantenimiento preventivo a Sistema Ininterrumpido de Potencia (UPS).

Pruebas
Frecuencia
Secuencia de fases
Tensión del banco baterías

- Plan de mantenimiento preventivo a reguladores del voltaje.

Tensión de entrada/salida
Borneo de Conexión
Tensión del banco de baterías

- Contar con plan de mantenimiento correctivo a las instalaciones eléctricas que puede ser proporcionado interna o externamente dependiendo del tipo de problema.

A.2.2.12 MANTENIMIENTO A EQUIPO DE COMPUTO.

- Deberá contarse con un servicio (contrato) de mantenimiento preventivo y correctivo para el equipo de cómputo que controle:

Temperatura
Humedad
.Limpieza de la sala de cómputo
Limpieza de filtros
Entradas de polvo y humo.
Equipo portátil de extinción

A.2.2.13 MANTENIMIENTO A EQUIPOS ESPECIALES.

- Deberá contarse con servicio (contrato) de mantenimiento preventivo y correctivo para el equipo especial y auxiliar.

- El plan de mantenimiento preventivo debe controlar:

Sistema de detección y extinción de incendios.
Sistema de control de acceso.
Equipos auxiliares:
Cortadora de papel
.Descarbonadora
Trituradora
Limpiadora de cintas magnéticas

A.2.2.14 MANTENIMIENTO A EQUIPO DE AIRE ACONDICIONADO

- Deberá contarse con un plan de mantenimiento preventivo y correctivo para el equipo de aire acondicionado que contemple:

Limpieza de filtros
Revisión de válvulas, compresores y ventiladores
Rango de temperatura y humedad
Monitoreo de temperatura y humedad
Nivel de agua
Ruidos anormales
Bitácora de servicio

A.2.2.15 MANTENIMIENTO DE PISO FALSO

Deberá existir un procedimiento adecuado par la limpieza y mantenimiento del piso falso, teniendo en cuenta:

- No utilizar agua sobre el piso.
- Nunca encerar o pulir el piso.
- Limpiar diariamente con una tela humedecida la superficie del piso.
- Limpiar periódicamente el piso con tela humedecida conagua y jabón y luego con tela limpia enjuagada con agua simple.
- Limpiar cámara plena (debajo del piso falso) mínimo cada tres meses tomando en cuenta:
  Limpieza de soportes
  Utilización de aspiradoras
  Desactivar el suministro de energía
- Contar con herramientas de succión para remover el pisofalso.

A.2.2.16 USO DE PASILLOS Y SALIDAS DE EMERGENCIA.

Mantener los pasillos y salidas de emergencia en buen estado para que cuando sea necesario utilizarlos permitan el desalojo rápido de personas. Deberán estar siempre sin obstáculos, limpios y señalados.

A.2.2.17 ABASTECIMIENTO DE PAPALERIA.

El área de abastecimiento de papalería para la continuidad operativa del centro PED debe ser única y debe contar con los elementos de seguridad contra incendios. Debe existir únicamente la cantidad necesaria para el turno en cuestión y al término de éste volver a surtir para que no aumente el riesgo en caso de incendio.

- Debe ser sólo una persona la que realice el acarreo de papalería dentro del centro PED.

- Dependiendo del consumo y del tamaño del área, se debe contar con un inventario mínimo que asegure la continuidad opertiva.

- Identificar a más de un proveedor para los casos de escacez y abastecimiento oportuno.