COMISION NACIONAL DE INVESTIGACIÓN Y DESARROLLO AEROESPACIAL

CONIDA

DIRECTIVA Nº 023 – 2011 CONIDA/OGA

"PLAN DE CONTINGENCIA DE EQUIPOS INFORMÁTICOS"

I. ASPECTOS GENERALES

El Plan de Contingencia implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos de cómputo y la información contenida en los diversos medios de almacenamiento.

II. OBJETIVO

Reducir el riesgo sobre la posibilidad de ocurrencia de siniestro de hardware, software, información y equipos periféricos.

III. FINALIDAD

Establecer los procedimientos que permitan reducir el riesgo de siniestro de cualquier índole.

IV. BASE LEGAL

3.1 Decreto Ley Nº 20643, Ley de Creación de CONIDA

3.2 Decreto Supremo Nº 004-88/SG, Estatuto de CONIDA

3.3 Decreto Legislativo N° 276 Ley de Bases de la Carrera Administrativa y de Remuneraciones del Sector Público

3.4 Ley N° 29296- Ley de Presupuesto del Sector Público para el año fiscal 2,011.

3.5 Resolución Jefatural N° 038-2010-JEINS-CONIDA Autoriza a partir de la fecha la aplicación del nuevo proyecto del Reglamento de Organización y Funciones de la Comisión Nacional de Investigación y Desarrollo Aeroespacial.

3.6 Resolución Jefatural N° 039-2010-JEINS-CONIDA, Autoriza a partir de la fecha la aplicación del Proyecto del Manual de Organización y Funciones de la Comisión Nacional de Investigación y Desarrollo Aeroespacial.

3.7 Resolución Jefatural N° 093–2011-JEINS-CONIDA que Aprueba el Plan de Prevención de Accidentes de la entidad.

V. ALCANCE

La presente Directiva es de observancia y estricto cumplimiento de todo el personal de CONIDA, sea cual fuere su régimen laboral.

VI. VIGENCIA

La presente Directiva tendrá vigencia desde la fecha de aprobación mediante Resolución Jefatural hasta su derogación o modificación con una norma similar ó de mayor jerarquía.

VII. PLAN DE CONTINGENCIA

7.1 El Plan de Contingencia de equipos de cómputo y bienes colaterales considera dos aspectos importantes:

a. Incluye las actividades que se deben realizar y los grupos de trabajo o responsables de operar.

b. El control, referido a las pruebas y verificaciones periódicas sobre la operatividad y actualización del plan de contingencia.

7.2 **Forman parte del plan de contingencias:** El plan de reducción de riesgos o plan de seguridad y el plan de recuperación de desastres.

7.3 **El plan de recuperación de desastres tiene tres fases claramente definidas:** Actividades previas al desastre; Actividades durante el desastre y Actividades después del desastre.

7.4 Las actividades previas al desastre son:

CONIDA V°B° Oficina de Asesoría Jurídica

CONIDA V°B° Oficina General de Administración

a. Establecimiento del plan de acción, que comprende:

a.1 Sistema de información: son los sistemas producidos en la Entidad y que son vitales para el adecuado funcionamiento del mismo.

a.2 Equipos de cómputo: Se cuenta con un sistema de información de Hardware y Software, con especificaciones técnicas, ubicación física y el área a la que está asignada. Se encuentran etiquetados los computadores de acuerdo a la importancia de su contenido, a fin de tener prioridad en caso de evacuación. Se cuenta con pólizas de seguros.
La Oficina de Telemática y Estadística es la responsable de identificar las computadoras de acuerdo a su importancia, en coordinación con las deferentes direcciones.

a.3 Obtención y almacenamiento de los Respaldos de Información (BACKUPS), que incluye: Dos Backups del Sistema Operativo por cada versión. Backup del Software Base (paquetes y/o lenguajes de programación con los cuales han sido desarrollados o interactúan los aplicativos Institucionales). Backup del Software Aplicativo. Backup de los Datos. Backup del Hardware. Procedimiento para los equipos, que por sus características técnicas y capacidades, son susceptibles de ser usados como equipos de emergencia.

a.4 Políticas (normas y procedimientos de Backup), que considera: Determinación de responsabilidades en la obtención del Backup mencionado anteriormente; debiéndose incluir: El Backup se realizará cada tres meses, y en casos muy importantes con carácter mensual. Almacenamiento del Backup en condiciones ambientales óptimas, dependiendo del medio magnético empleado. Reemplazo del Backup, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar (reciclaje o refresco). Pruebas periódicas del Backup, verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables.

b. Formación de equipos operativos, mediante la designación del responsable de seguridad de la información en cada órgano. Las funciones de los responsables serán: Ponerse en contacto con los propietarios de las

aplicaciones y trabajar con ellos proporcionar soporte técnico para las copias de respaldo de las aplicaciones. Planificar y establecer los requerimientos de los sistemas operativos en cuanto archivos, bibliotecas, utilitarios, etc., para los principales sistemas y subsistemas. Supervisar procedimientos de respaldo y restauración. Supervisar la carga de archivos de datos de las aplicaciones, y la creación de respaldos incrementales. Coordinar líneas, terminales, modem y otros para comunicaciones. Establecer procedimientos de seguridad en los sitios de recuperación. Organizar la prueba de hardware y software. Realizar labor de recupero de inventario y seguridad del almacenamiento participar en las pruebas y simulacros de desastres.

c. Formación de equipos de evaluación para realizar la auditoría de los procedimientos de seguridad; cuyas funciones serán: Revisar la aplicación y cumplimiento de las normas y procedimientos con respecto a Backups, seguridad de equipos y data. Supervisar la realización periódica de los backups, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento. Revisar la correlación entre la relación de sistemas e información necesarios para la buena marcha de la Institución, y los backups realizados. Informar sobre el cumplimiento e incumplimiento de las normas, para las acciones de corrección respectivas.

7.5 Las actividades durante el desastre son:

a. Plan de emergencias: Señalización de los extintores. Cobertores contra el agua
b. Formación de equipos: El personal de la Oficina de Telemática y Estadística esta encargada de seleccionar, coordinar y ejecutar un plan de acción conjuntamente con las personas asignadas para este fin.
c. Entrenamiento: Establecer un programa de prácticas periódicas para el personal, en la lucha contra los diferentes tipos de siniestros, de acuerdo a los roles que se le haya asignado en los planes de evacuación de personal o equipos. Para este caso la Oficina de Logística deberá aprovechar las fechas de recarga de los extintores y propiciar charlas con organismos vinculados a siniestros. El personal debe tomar conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir, y deben asumir con seriedad y responsabilidad los entrenamientos. Los Funcionarios también están en la obligación de participar en los entrenamientos.

7.6 Las actividades después del desastre son:

a. Evaluación de los daños: Inmediatamente después de concluido el siniestro, se deberá evaluar la magnitud del daño producido. Qué sistemas se afectaron; qué equipos están no operativos; cuáles se pueden recuperar y en cuánto tiempo, etc. Comunicar a los organismos con los que se tiene convenio de respaldo a fin de preparar la reposición de equipos
b. Priorizar las actividades del plan de acción, si el plan de acción es general y contempla una pérdida total; la evaluación de daños reales y su comparación contra el plan, proporcionará la lista de las actividades a realizar en función de la prioridad. Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, a fin de asignarlos en forma temporal a las actividades afectadas, en apoyo al personal de los sistemas dañados y soporte técnico.

c. Ejecución de actividades: Conformación de equipos de trabajo para realizar las actividades previamente establecidas en el plan de acción. Cada uno de los equipos deberá contar con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, reportarlo de inmediato a la jefatura a cargo del Plan de Contingencias. El trabajo de recuperación consta de dos etapas: la primera, la restauración del servicio usando los recursos de la Institución o local de respaldo, y la segunda, volver a contar con los recursos en las cantidades y lugares apropiados, debiendo ser esta etapa lo suficientemente rápida y eficiente para no perjudicar la operatividad de la institución o local de respaldo.

d. Evaluación de resultados: Concluida la labor de recuperación del sistema afectada por el siniestro, se debe evaluar objetivamente, todas y cada una de las actividades realizadas, considerándose entre otros aspectos: ¿Qué tan bien se hicieron; qué tiempo demando; qué circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción; cómo se comportaron los equipos de trabajo. De la Evaluación de resultados y del siniestro en si, deben obtenerse dos tipos de recomendaciones: una la retroalimentación del plan de Contingencias y otra una lista de recomendaciones para minimizar la pérdida que ocasionó el siniestro.

e. Retroalimentación del plan de acción: Con la evaluación de resultados, debe optimizarse el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente. Evaluar cual hubiera sido el costo de no tener un plan de contingencias.

7.7 El riesgo es la probabilidad de ocurrencia de eventos negativos que perjudiquen los equipos informáticos y periféricos. El análisis supone obtener una evaluación económica del impacto de dichos sucesos negativos. El valor calculado se utiliza para contrastar el costo de la protección de la información con el costo de una nueva producción.

7.8 Se considerarán los siguientes factores de riesgo
Factor de riesgo muy bajo
Factor de riesgo bajo
Factor de riesgo medio
Factor de riesgo alto
Factor de riesgo muy alto
Se efectuará un resumen de los riesgos ordenados por el factor de riesgo de cada uno de ellos contemplados en el numeral 6.12 de la presente Directiva

7.9 El análisis de riesgos supone responder a preguntas y determinar su grado de confiabilidad:
Qué puede ir mal?
Con qué frecuencia puede ocurrir?
Cuáles serían las consecuencias?

7.10 La evaluación de riesgos supone responder a preguntas con la mayor confiabilidad:
Qué se intenta proteger?
Cuál es el valor para la organización o para la persona?
Frente a qué se intenta proteger?
Cuál es la probabilidad de un ataque?

7.11 Los órganos de la institución, sin excepción, están obligados a brindar todo el apoyo necesario a la Oficina de Telemática y Estadística de la Oficina de Administración General.

7.12 Los Directores Técnicos o Jefes de Oficina, según sea el caso, designarán a los responsables de cada área usuaria para que brinden apoyo al personal de la Oficina de Telemática y Estadística en los siguientes aspectos:

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

Al fuego, que puede destruir los equipos y archivos:

- La Institución cuenta con protección contra incendios
- Se cuenta con sistemas de aspersión automática
- Diversos extintores
- Detectores de humo
- Los empleados están preparados para enfrentar un posible incendio

Al robo común, llevándose los equipos y archivos.

- En qué tipo de vecindario se encuentra la Institución
- Hay venta de drogas
- Las computadoras se ven desde la calle
- Hay personal de seguridad en la Institución
- Cuántos vigilantes hay
- Los vigilantes, están ubicados en zonas estratégicas

Al vandalismo, que dañen los equipos y archivos.

- Existe la posibilidad qué un ladrón frustrado cause daños
- Hay la probabilidad qué causen algún otro tipo de daño intencionado

A fallas en los equipos, que dañen los archivos

- Los equipos tienen mantenimiento continuo por parte de personal calificado
- Cuáles son las condiciones actuales del hardware
- Es posible predecir las fallas a que están expuestos los equipos

A equivocaciones, que dañen los archivos.

- Cuánto saben los empleados de computadoras o redes
- El que no conocen el manejo de la computadora, sabe a quién pedir ayuda
- Durante el tiempo de vacaciones de los empleados, ¿qué tipo de personal los sustituye y qué tanto saben del manejo de computadoras?

A la acción de virus, que dañen los equipos y archivos.

- Se prueba software en la oficina sin hacerle un examen previo
- Está permitido el uso de disquetes en la oficina
- Todas las máquinas tienen unidades de disquetes
- Se cuentan con procedimientos contra los virus

A terremotos, que destruyen el equipo y los archivos.

- La Institución se encuentra en una zona sísmica?
- El edificio cumple con las normas antisísmicas?
- Un terremoto, ¿cuánto daño podría causar?

A accesos no autorizados, filtrándose datos no autorizados.

- Cuánta competencia hay para la Institución
- Qué probabilidad hay que un extraño intente hacer un acceso no autorizado
- El MODEM se usa para comunicarse hacia fuera y hacia dentro
- Se cuenta con Sistemas de Seguridad en el Correo Electrónico o Internet

Al robo de datos, difundiéndose los datos sin cobrarlos.

- Cuánto valor tienen actualmente las Bases de Datos
- Cuánta pérdida podría causar en caso de que se hicieran públicas
- Se ha elaborado una lista de posibles sospechosos que pudieran robar
- La lista de sospechosos, ¿es amplia o corta?

Al fraude, desviando fondos merced a la computadora
- Cuántas personas se ocupan de la contabilidad de la Institución
- El sistema de contabilidad es confiable
- Los que trabajan en contabilidad, tienen antecedentes laborales, de qué tipo
- Existe acceso al sistema contable desde otros sistemas o personas

7.13 La Oficina de Telemática y Estadística evaluará las probables fallas en el sistema de seguridad.

7.14 Las Direcciones Técnicas y Oficinas, según sea el caso, dispondrán que el personal realice con carácter obligatorio las siguientes acciones de protección de los equipos e información.

Generales: Una copia mensual de los archivos que son vitales para la Institución

Robo común: Cerrar las puertas de entrada y ventanas de cada Oficina. Se cuenta con personal de seguridad en la entrada del local y cerco eléctrico perimétrico

Vandalismo: Cerrar las puertas de ingreso

Falla de los equipos: Tratar con cuidado, realizar el mantenimiento en forma regular, no fumar, debe estar previsto el préstamo de otros equipos.

Daño por virus: Todo el software que llega se analiza en un sistema utilizando software antivirus. Los programas de dominio público y de uso compartido (Shareware), sólo se usan si proceden de una fuente fiable.

Equivocaciones: El servidor debe tener buena formación.

Terremoto: Aplicar la protección contra incendio.

Acceso no autorizado: Cerrar la puerta de entrada, la vigilancia debe rondar por todo el perimetro de las Instalaciones de CONIDA.

Robo de datos: Mantener cerrada la puerta principal. Todas las Pc's deben estar bloqueadas con claves de acceso.

Fuego: Colocar extintores en sitios estratégicos y la oficina de Logística debe propender a entrenamiento para el uso de los mismos.

VIII. DISPOSICIONES ESPECÍFICAS

8.1 La Oficina de Administración General a través de la Oficina de Telemática y Estadística es la responsable de formular, programar, realizar, coordinar, ejecutar, evaluar y controlar el Plan de Contingencias de equipos informáticos y periféricos.

8.2 La Oficina de Administración General a través de la Oficina de Logística es la responsable del entrenamiento en el uso de extintores, para lo cual deberá programar las fechas en que se realizará tal entrenamiento.

8.3 La Oficina de Administración General a través de la Oficina de Control Patrimonial es la responsable de proporcionar a la Oficina de Telemática y Estadística el inventario de equipos informáticos y periféricos debidamente actualizados.

8.4 Los Directores Técnicos y Jefes de Oficina, según sea el caso, brindarán a su personal las facilidades para el cumplimiento de los objetivos.

IX. DISPOSICIONES COMPLEMENTARIAS

9.1 El Plan de Contingencias de equipos informáticos y periféricos tiene la clasificación de prioridad muy alta.

9.2 El Director de Administración es el responsable de velar por el estricto cumplimiento de lo dispuesto en la presente Directiva.

9.3 El personal de la Entidad, independientemente de su nivel y cargo forma parte como un Todo del plan de contingencias.

9.4 El personal de la Entidad hará suyo lo establecido en la presente Directiva, bajo responsabilidad.

X. DISPOSICION FINAL

CONIDA V°B° Oficina de Asesoría Jurídica

Las Direcciones Técnicas, Oficina de Administración General y Direcciones de Línea son responsables, del cumplimiento de lo dispuesto en la presente Directiva, en materia de su competencia.

Abogado
Daniel Fernando Bolaños Galindo
Director de Administración General
CONIDA