PLAN DE CONTINGENCIA INFORMÁTICO DEL CNC

CNC
Consejo Nacional de Competencias

PLAN DE CONTINGENCIA INFORMÁTICO DEL CNC

PLAN DE CONTINGENCIA IRFORMÁTICO DEL CNC

Consejo Nacional de Competencias 2017

1ra Edición - Quito, 2017
32 páginas, 148,5mm x 210mm – (Línea de Documentos Institucionales)

EDICIÓN VIRTUAL SIN FINES COMERCIALES

De esta edición

Consejo Nacional de Competencias (CNC)
La Pinta E6-29 y La Rábida. Edificio Kywi (Alcatel-Lucent), piso 6
Quito - Pichincha - Ecuador
Telf.: (593) 22500 053
www.competencias.gob.ec

Elaborado por: Miguel Angel Moreno

Revisado por: Alaín Bustamante
Vanessa House

Aprobado por: María Caridad Vázquez

Diseño y Diagramación: Comunicación Social CNC

Mayo 2017

Contenido

Introducción

INTRODUCCIÓN

El alcance de este plan guarda relación con la infraestructura informática del Consejo Nacional de Competencias, así como los procedimientos relevantes de la gestión de Tecnología asociados con la plataforma tecnológica.

Entenderemos como infraestructura informática al hardware, software y elementos complementarios que soportan la información o datos críticos de todas las Direcciones del Consejo, tanto técnicas como de apoyo.

Entendemos también como procedimientos relevantes a la infraestructura informática a todas aquellas tareas que el personal de TIC del CNC, realiza frecuentemente cuando interactúa con la plataforma informática (entrada de datos, generación de reportes, consultas, etc.).

Uno de los más importantes activos de toda institución es la información que está genera en sus diferentes acciones y ámbitos. Conscientes de esta premisa, podemos indicar que se debe adoptar medidas de seguridad para la información y así mismo estar preparados para poder afrontar contingencias y desastres de tipo diverso.

La Gestión de Tecnología de la Información y de las Comunicaciones, en adelante GTIC, tiene, entre otros, el propósito de proteger la información y así asegurar su procesamiento y desarrollo de funciones institucionales. En base a ello presenta el Plan de Contingencia Informático del Consejo Nacional de Competencias.

El Especialista de TIC está obligado a hacer de conocimiento y explicar con lenguaje entendible a estos directivos las posibles consecuencias que la inseguridad insuficiente o inexistente pueda acarrear; de esa manera proponer y poner a consideración las medidas de seguridad inmediatas y a mediano plazo, que han de tomarse para prevenir los desastres que pueda provocar el colapso de los sistemas.

Objetivo

1 Objetivo

Formular un adecuado Plan de Contingencias, que permita la continuidad en los procedimientos informáticos de la GTIC, así como enfrentarnos a fallas y eventos inesperados; con el propósito de asegurar y restaurar los equipos e información con las menores pérdidas posibles en forma rápida, eficiente y oportuna; buscando la mejora de la calidad en los servicios que brinda la GTIC.

Alcance

2 Alcance

El Plan de Contingencias Informático está basado en la realidad que manifiesta el Consejo Nacional de Competencias, el mismo que puede servir como punto de partida hacia la adecuación y establecimiento de políticas. Un Plan de Contingencias debe ser diseñado y elaborado de acuerdo con las necesidades y realidad de cada institución, tener sus propios requerimientos, tener que adoptar un sitio especial para el procesamiento de la información o hasta tener que construirlo o implementarlo, requerirá además de pruebas de procedimientos nuevos y que sean compatibles con los procesos existentes, incluso muchas veces se requerirá contar con la participación de personal de otras direcciones o de otras gestiones de la Dirección Administrativa Financiera, para trabajar en conjunto cuando se desarrollen o implementen soluciones.

3 Análisis de Riesgos

Establecer los riesgos a los cuales está propensa la GTIC del CNC, de igual manera determinar el nivel o factor de riesgo, que lo clasificaremos en los siguientes:

Factor de Riesgo:

- Bajo
- Muy Bajo
- Alto
- Muy alto
- Medio

Ellos nos determinan nuestra tabla de riesgos y nivel de factores que a continuación detallamos:

RIESGO	Factor de Riesgo				
	Muy Bajo	Bajo	Medio	Alto	Muy Alto
Incendio					X
Inundación	x				
Robo Común					X
Vandalismo, daño de equipos y archivos.					X
Fallas en los equipos, daño de archivos.					X

RIESGO	Factor de Riesgo				
	Muy Bajo	Bajo	Medio	Alto	Muy Alto
Equivocaciones, daño de archivos.			x		
Virus, daño de equipos y archivo.					X
Terremotos, daño de equipos y archivos.				X	
Acceso no autorizado, filtración de información.					X
Robo de datos					X
Fraude, alteración de información.				X	
Desastre Total					X

En base a la tabla anteriormente presentada, concluimos que nuestro análisis de riesgo a modo general, nos hace ver que las posibles contingencias que pudieran presentarse en su mayoría van de un factor de ocurrencia medio y muy alto.

A continuación realizamos un deslinde de las causas por las cuales mayormente se presentan este tipo de contingencias, para ello realizamos la siguiente lista de preguntas:

1. Con respecto al fuego, que puede destruir los equipos y los archivos
   ¿La Institución cuenta con protección contra incendios?
   ¿Se cuenta con sistemas de aspersión automática?
   ¿Cuenta con diversos extintores?
   ¿Detectores de humo?
   ¿Los empleados están preparados para enfrentar un posible incendio?

2. Con respecto al robo común, llevándose los equipos y archivos
   ¿En qué tipo de edificio se encuentra la Institución?
   ¿Hay venta de drogas en el sector?
   ¿Los equipos de cómputo se ven desde la calle?
   ¿Hay personal de seguridad en la Institución?
   ¿Cuántos guardias de seguridad hay?
   ¿Los guardias de seguridad, están ubicados en zonas estratégicas?
   ¿Existe un sistema de seguridad para prevenir el ingreso de personas no autorizadas?

3. Con respecto al vandalismo, que dañen los equipos y archivos
¿Existe la posibilidad que un ladrón cause daños?
¿Hay la probabilidad que causen algún otro tipo de daño intencionado?

4. Con respecto a fallas en los equipos, que dañen los archivos
¿Los equipos tienen un 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?

5. A equivocaciones que dañen los archivos
¿Cuánto saben los empleados de computadoras o redes?
Los que no conocen del manejo de la computadora, ¿saben 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?

6. Con respecto a la acción de virus, que dañen los archivos
¿Se cuenta con antivirus corporativo?
¿Se prueba software en la oficina sin hacerle un examen previo?
¿Está permitido el uso de pendrives (memorias flash) en la oficina?
¿Se cuentan con procedimientos contra los virus?

7. Con respecto a terremotos, que destruyen los equipos y archivos
¿La Institución se encuentra en una zona sísmica?
¿El edificio cumple con las normas antisísmicas?
Un terremoto, ¿cuánto daño podría causar?

8. Con respecto a accesos no autorizados, filtrándose datos importantes
¿Existe registro de personal autorizado en el CNC?
¿Qué probabilidad hay que un colaborador intente hacer un acceso no autorizado?
¿Existe comunicación remota de la red? ¿Qué tipo de servicio se utiliza (Telnet, FTP, etc)?
¿Contamos con Sistemas de Seguridad en el Correo Electrónico o Internet?

9. Con respecto al robo de datos; y la posible difusión de estos.
¿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 los posibles sospechosos que pudieran efectuar el robo?

10. Con respecto al fraude, vía computadora.
¿Cuántas personas se ocupan de la contabilidad de la Institución?
¿Los sistemas son confiables?¿Pueden copiar datos en archivos?
Las personas que trabajan en las diferentes áreas, ¿qué tipo de antecedentes laborales tienen?
¿Existe acceso a los sistemas desde otros sistemas externos o por personas no autorizadas?

Plan de recuperación de desastres

4 Plan de recuperación de desastres

Ahora definimos las acciones a tomar para recuperarnos de la ocurrencia de un desastre. Este Plan de Recuperación contiene 3 etapas:

1 ACTIVIDADES PREVIAS AL DESASTRE
2 ACTIVIDADES DURANTE EL DESASTRE; y,
3 ACTIVIDADES DESPUÉS DEL DESASTRE

1. ACTIVIDADES PREVIAS AL DESASTRE

Como actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de información que nos asegure un proceso de recuperación con el menor costo posible a nuestra institución, tenemos que señalar las siguientes acciones que son precisas de realizar en la ejecución del presente plan.

a. Definición y Establecimiento de un Plan de Acción

Establecer los procedimientos relativos a:

(1). Sistemas de Información.- La GTIC tendrá una relación de los Sistemas de Información con los que cuenta. Debiendo identificar toda información sistematizada o manual, que sea necesaria para la buena marcha Institucional.

La relación de Sistemas de Información detallará los siguientes datos:

Nombre del Sistema, es determinado por el analista-desarrollador asignado por la GTIC.

Lenguaje o Paquete con el que fue creado el Sistema, programas que lo conforman (tanto programas fuentes como programas objetos, rutinas, macros, etc.).

La Dirección, (área) que genera la información base (el <<dueño>> 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 realizará una lista priorizada (Ranking) de los Sistemas de Información necesarios para que el Consejo Nacional de Competencias recupere su operatividad perdida en el desastre (Contingencia).

(2). Equipos de Cómputo: Se tendrá en cuenta lo siguiente:

Inventario actualizado de los equipos de manejo de información (computadoras portátiles, computadoras de escritorio, servers, 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 hará por otro de mayor potencia (por actualización tecnológica), siempre y cuando esté 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.

Respaldo de PC´s, tener siempre una relación actualizada de PC´s requeridas como mínimo para cada sistema permanente de la institución (que por sus funciones constituye el eje central de los servicios informáticos), para cubrir las funciones básicas y prioritarias de cada uno de estos sistemas cuando se requiera.

(3). Obtención y Almacenamiento de los Respaldos de Información (BACKUPS): 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 del Consejo Nacional de Competencias, contando con:

Backups del Sistema Operativo. En caso de tener varios sistemas operativos o versiones se contará con una copia de cada uno de ellos.

Backups del Software Base. Paquetes y/o Lenguajes de Programación con los cuales han sido desarrollados o interactúan nuestros Aplicativos Institucionales.

Backups del Software Aplicativo. Considerando tanto los programas fuentes como los programas objeto correspondiente, y cualquier otro software o procedimiento que también trabaje con la data, para producir los resultados con los cuales trabaja el usuario final. Considerando las copias de los listados fuentes de los programas definitivos, para casos de problemas.

Backups de los Datos. Base de Datos, Índices, tablas de validación, passwords, y todo archivo necesario para la correcta ejecución del software aplicativo del CNC.

Backups del Hardware. Implementar mediante dos modalidades:

Modalidad Externa. Mediante convenio con otra Institución 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.

Modalidad Interna. Teniendo dos locales de almacenamiento, 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 probará y asegurará 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.

(4). Políticas (Normas y Procedimientos de Backups): Establecer los procedimientos, normas, y determinación de responsabilidades en la obtención

de los Backups mencionados anteriormente en el punto 3). Incluyéndose:

Periodicidad de cada tipo de Backups.

Respaldo de Información de movimiento entre los períodos que no se cuenta con Backups (backups incrementales).

Uso obligatorio de un formulario estándar para el registro y control de backups.

Correspondencia entre la relación de sistemas e informaciones necesarias para la buena marcha de la institución (mencionado en el punto a) y los backups efectuados.

Almacenamiento de los Backups en condiciones ambientales óptimas, dependiendo del medio magnético empleado.

Reemplazo de los Backups, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar (reciclaje o refresco).

Pruebas periódicas de los Backups (Restore), verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables.

b. Formación de Equipos Operativos para el Plan de Acción

Todas las áreas o Direcciones del CNC, que almacenen Información y que sirva para la operatividad institucional, designará un responsable de la seguridad de dicha información. Pudiendo ser el Director (a) del área o el colaborador que maneje directamente la información.

Entre las acciones a tomar por la GTIC conjuntamente con las oficinas 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 a archivos, bibliotecas, utilitarios, etc, para los principales sistemas,

subsistemas.

Supervisar procedimientos de respaldo y restauración.

Supervisar la carga de archivos de datos de las aplicaciones y la creación de los respaldos incrementales.

Coordinar líneas, terminales, modem, otros aditamentos para comunicaciones.

Establecer procedimiento de seguridad en los sitios de recuperación.

Organizar la prueba de hardware y software.

Ejecutar trabajos de recuperación.

Cargar y probar archivos del sistema operativo y otros sistemas almacenados en el local alternante.

Realizar procedimientos de control de inventario y seguridad de almacenamiento en el local alternante.

Establecer y llevar a cabo procedimientos para restaurar el lugar de recuperación.

Participar en las pruebas y simulacros de desastres.

Supervisar la realización periódica de los backups, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.

2. ACTIVIDADES DURANTE EL DESASTRE

Una vez presentada la contingencia, se ejecutará las siguientes actividades:

a. Plan de Emergencia

Establecer las acciones que se deben realizar cuando se presente un siniestro, así como la difusión de las mismas.

Conviene prever los posibles escenarios de ocurrencia del Siniestro:

- Durante el día.
- Durante la Noche o madrugada.

Este plan incluirá la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre la contingencia.

Si bien es cierto la integridad de las personas es lo primordial, se deben adoptar medidas con el fin de asegurar la información detallando:

- Vías de salida o escape.
- Plan de Evacuación de Personal.
- Plan de puesta a buen recaudo de los activos (incluyendo los activos de información) del CNC (si las circunstancias del siniestro lo posibilitan).
- Ubicación y señalización de los elementos contra el siniestro (extinguidores, cobertores contra agua, etc)
- Secuencia de llamadas en caso de siniestro, tener a la mano: elementos de iluminación (linternas), lista de teléfonos de bomberos/ ambulancias, 911, Policía Nacional y de su personal (equipos de seguridad) nombrados para estos casos.

En caso de contingencias como fallas en equipos de cómputo, fallas humanas, acción de virus, etc.; solicitar la ayuda del personal de la GTIC, si es que en el área no existe una persona capacitada para resolver el problema.

b. Formación de Equipos

Establecer claramente cada equipo (nombres, puestos, ubicación, etc.) con funciones claramente definidas a ejecutar durante el siniestro.

Si bien la premisa básica es la protección de la Integridad del personal, en caso de que el siniestro lo permita (por estar en un inicio o estar en una área cercana, etc.), deberá de existir dos equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y otro para el salvamento de los recursos Informáticos., de acuerdo a los lineamientos o clasificación de prioridades, para salvar los equipos señalados en el acápite 4.1.a. (Definición y Establecimiento del Plan de Acción)

c. Entrenamientos

Establecer un programa de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestro, de acuerdo a los roles que se le hayan asignado en los planes de evacuación de personal o equipos para minimizar costos, se puede aprovechar las fechas de recarga de extinguidores o las charlas de los proveedores, etc.

Un aspecto importante es que el personal tome conciencia de los siniestros (incendios, inundaciones, terremotos, apagones, y/o atentados terroristas, etc.) pueden realmente ocurrir y tomar con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen todas las autoridades y Directores del CNC, dando el ejemplo de la importancia que la alta dirección otorga a la Seguridad Institucional.

3. ACTIVIDADES DESPUÉS DEL DESASTRE

Durante la contingencia, se tomará en cuenta lo planificado en el plan de Emergencia.

a. Evaluación de Daños.

Inmediatamente después que la contingencia ha concluido, se evaluará la magnitud de los daños producidos, estableciendo que sistemas están afectados,

que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc.

Adicionalmente se lanzará un pre-aviso a la institución con la cual tenemos el convenio de respaldo, para ir avanzando en las labores de preparación de entrega de los equipos por dicha institución.

b. Priorización de actividades del Plan de Acción

Toda vez que el Plan de acción contemple una pérdida total, la evaluación de daños reales y su comparación con el Plan, nos dará la lista de actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de nuestra institución.

Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, para su asigna miento temporal a las actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.

c. Ejecución de Actividades.

La ejecución de actividades implica la creación de equipos de trabajo para realizar las actividades previamente planificadas en el Plan de acción.

Cada uno de estos equipos contará con un coordinador que reportará diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, informará de inmediato al encargado del Plan de Contingencias (GTIC).

Los colaboradores de recuperación tendrán dos etapas:

- La primera, la restauración de los servicios usando los recursos del CNC o local de respaldo.

- La segunda, es volver a contar con los recursos en las cantidades y lugares propios de los sistemas de información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar el buen servicio de nuestro sistema e imagen institucional, como para no perjudicar la operatividad del CNC o local de respaldo.

d. Evaluación de Resultados.

Una vez concluidas las labores de recuperación del (los) sistema(s) que fueron afectados por la contingencia, se evaluará objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción, como se comportaron los equipos de trabajo, etc.

De la evaluación de resultados y del siniestro, saldrán dos tipos de recomendaciones, una la retroalimentación del Plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro.

e. Retroalimentación del Plan de Acción.

Con la evaluación de resultados, se optimizará el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

PLAN DE CONTINGENCIA INFORMÁTICO DEL CNC

PLAN DE CONTINGENCIA INFORMÁTICO DEL CNC

CNC
Consejo Nacional de Competencias