


 <b>Comisión Federal de Telecomunicaciones</b>	<b>COMISIÓN FEDERAL DE TELECOMUNICACIONES</b>	<b>Codificación CFT-004RESREC-03</b>	
		<b>Revisión 003</b>	<b>Página 1 de 6</b>
		<b>18/02/2009</b>	

# **Política de Respaldo, Resguardo y Recuperación.**


*[Handwritten marks]*

 <b>Comisión Federal de Telecomunicaciones</b>	<b>COMISIÓN FEDERAL DE TELECOMUNICACIONES</b>	<b>Codificación CFT-004RESREC-03</b>	
		<b>Revisión 003</b>	<b>Página 2 de 6</b>
		<b>18/02/2009</b>	

## CONTENIDO

1.	INTRODUCCIÓN.....	1
2.	PROPÓSITO.....	1
3.	ALCANCE.....	1
4.	POLÍTICAS.....	1,2,3
5.	REVISIONES.....	3,4

Handwritten marks at the bottom of the page, including a vertical line, a stylized 'd', a diagonal slash, and a signature-like mark.

 <b>Comisión Federal de Telecomunicaciones</b>	<b>COMISIÓN FEDERAL DE TELECOMUNICACIONES</b>	<b>Codificación CFT-004RESREC-03</b>	
		<b>Revisión 003</b>	<b>Página 3 de 6</b>
		<b>18/02/2009</b>	

## 1. Introducción

La seguridad se ocupa de la identificación y valoración de los activos informáticos, así como de los riesgos a que estos pudieran ser vulnerables. También se encarga de proveer los mecanismos que coadyuven a la preservación de la integridad y disponibilidad de dichos activos, sin embargo, en ambientes de producción un servicio que no siempre se puede garantizar es la disponibilidad. Uno de los riesgos que afectan la disponibilidad es la pérdida parcial o total de la confianza o integridad de los activos, en cuyo caso la restauración al escenario último confiable es inminente. Es en este escenario en donde se hace necesario contar con una política de respaldo que garantice la recuperación a estados confiables con el mínimo de pérdidas de información lo más cercano al momento de la contingencia.

## 2. Propósito

El propósito de esta política es definir los lineamientos generales aplicables a los sistemas de información de la Comisión Federal de Telecomunicaciones, a quién en lo sucesivo se denominará como "**La Comisión**", en lo referente a los procedimientos de respaldo, resguardo y recuperación que se deberán observar en **La Comisión**.

Un punto importante de los respaldos que hay que asegurar es que estos sean efectuados a intervalos regulares, que los medios de respaldo sean usados en rotación y que se encuentren dispuestos en sitios alternos de forma regular.

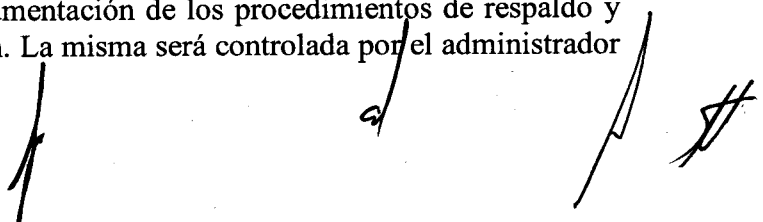
## 3. Alcance


Esta política es aplicable a todos los responsables de resguardar información en **La Comisión**, incluyendo todo el personal afiliado con terceros que tengan relación con la misma y servicios administrados por terceros.

Esta política deberá de ser dada a conocer al personal involucrado y manifestar expresamente el conocimiento de su contenido, alcance y sanciones.

## 4. Políticas

1. Todo sistema deberá contar con la documentación de los procedimientos de respaldo y recuperación antes de entrar en producción. La misma será controlada por el administrador



 <b>Comisión Federal de Telecomunicaciones</b>	<b>COMISIÓN FEDERAL DE TELECOMUNICACIONES</b>	<b>Codificación CFT-004RESREC-03</b>	
		<b>Revisión 003</b>	<b>Página 4 de 6</b>
		<b>18/02/2009</b>	

de la aplicación, para verificar que es clara y completa, deberá de contemplar como mínimo la recuperación de los siguientes elementos:

- 1.1. El remplazo de los servidores críticos .
- 1.2. El sistema operativo y su configuración (parámetros, file Systems, particiones, usuarios y grupos, etc)
- 1.3. Los parches y paquetes de software de base necesarios para que la aplicación se ejecute.
- 1.4. Los programas que componen la aplicación
- 1.5. Los archivos y/o bases de datos del sistema.
- 1.6. Horario de ejecución de la copia de respaldo.

No se pondrá en producción ningún sistema que no cumpla este requerimiento.

2. Todas las copias de respaldo deberán estar claramente identificadas, con etiquetas que indiquen como mínimo

- 2.1. Equipo al que pertenece
- 2.2. Fecha y hora de ejecución
- 2.3. Frecuencia: anual, mensual, semanal, diario
- 2.4. Número de secuencia
- 2.5. Tipo de backup
- 2.6. Nombre del sistema o aplicativo y otros datos necesarios para su fácil reconocimiento.

3. Se llevará un registro diario de las cintas en uso indicado al menos.



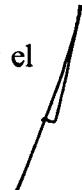

- 3.1. Fecha de ejecución del respaldo
- 3.2. Que cintas integran el backup de los equipos.
- 3.3. Cantidad de veces que se uso la cinta. Una cinta tiene un máximo de 25 veces (vida útil)  
Luego de lo cual se procederá a remplazarlas.
- 3.4. Lugares asignados para su almacenamiento


El administrador de servidores revisara periódicamente que se cumpla con este registro en tiempo y forma. En el caso de base de datos ver bitácora de respaldos.

4. Todos los procedimientos de respaldo deberán generar un registro en el equipo que permita la revisión del resultado de la ejecución y dentro de lo posible, se realizaran con la opción de verificación de integridad (lectura posterior a la escritura.)

5. Los sitios donde se almacena las copias de respaldo deberán ser físicamente seguros, con los controles físicos y ambientales según normas estándares; las cintas deben guardarse dentro de la caja fuerte.

6. Se realizaran copias del respaldo del sistema completo de acuerdo a lo indicado por el

 <b>Comisión Federal de Telecomunicaciones</b>	<b>COMISIÓN FEDERAL DE TELECOMUNICACIONES</b>	<b>Codificación CFT-004RESREC-03</b>	
		<b>Revisión 003</b>	<b>Página 5 de 6</b>
		<b>18/02/2009</b>	

administrador de la aplicación, en la frecuencia asignada a cada aplicación o sistema, previendo la conservación de estos backups por el periodo de tiempo también estipulado previamente conforme a la criticidad de la información.

7. En caso de utilizar backups incrementales se deberá tener en cuenta lo siguiente:

- 7.1. Se documentara la identificación de secuencia de los backups incrementales.
- 7.2. Deberán existir controles para prevenir la carga de cintas en una secuencia equivocada.
- 7.3. Se realizara un backup del sistema completo cada 7 días.

8. Se efectuarán pruebas de recuperación de las copias de respaldo por parte del administrador de servidores al menos una vez cada 90 días y serán supervisadas por el administrador de aplicaciones.

Estas pruebas servirán para constatar que se puedan obtener correctamente los datos grabados en la cinta al momento de ser necesarios, de forma de garantizar su propósito.

Las pruebas se deberán formalizar en un acta escrita y firmada por el responsable del sector técnico y el encargado de realizar la recuperación. Eventualmente el área responsable de la seguridad tecnológica presenciara las pruebas y firmara el acta.

9. Los periodos de retención de la información histórica son los siguientes:

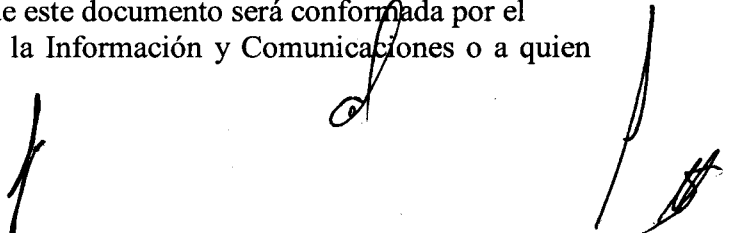
- Lotes de transacción: perpetuo
- Actividades de los usuarios y pistas de auditoría: 3 años.


10. El respaldo de la información histórica se realizara utilizando soportes magnéticos de preferencia no reutilizables (CDs, discos ópticos, etc)

11. Los procedimientos de generación y grabación de estos archivos serán automáticos, a fin de evitar su modificación.

## 5. Revisiones

Las revisiones al presente documento se realizarán durante la primera semana laborable de cada trimestre según calendario. La revisión de este documento será conformada por el Director General Adjunto de Tecnologías de la Información y Comunicaciones o a quien



 <b>Comisión Federal de Telecomunicaciones</b>	<b>COMISIÓN FEDERAL DE TELECOMUNICACIONES</b>	<b>Codificación CFT-004RESREC-03</b>	
		<b>Revisión 003</b>	<b>Página 6 de 6</b>
		<b>18/02/2009</b>	

este designe. En caso de haber mejoras al documento se generará una nueva versión de este y en caso contrario se mantendrá la anterior.

En el caso que durante la observación de dicho documento se encontrara una falla que atente contra la integridad del asunto que trata el presente documento se creará un grupo revisor emergente designado por el área responsable.

<b>REV.</b>		<b>200902-10</b>
01	Propuesta de mejora de procedimientos en la Dirección de Análisis y Desarrollo.  Ing. Andres Falcón García Ing. Enrique Javier Blum Tadeo Lic. José Moisés León Hernández	2004-11-29
02	Adaptación para incluir la política dentro del esquema general del Plan de Seguridad Informática.  Ing. Andres Falcón García	2005-01-15
03	Actualización de la política  Ing. Andres Falcón García L.C.C. Guillermo Rodriguez Contreras Ing. Cesar Vicente Pérez Gaytán	2009-02-10

**Elaboro**

\_\_\_\_\_  
L.C.C. Guillermo Rodriguez Contreras  
Director de Sistemas Informáticos

**Reviso**

\_\_\_\_\_  
Ing. Andres Falcón García  
Director General de Tecnologías de  
la Información y Comunicaciones

**Responsables**

\_\_\_\_\_  
Cesar Vicente Pérez Gaytán  
Soporte Técnico

\_\_\_\_\_  
Manuel Samano Rodríguez  
Soporte Técnico