VIGENCIA: 2024-12-11	CÓDIGO: P.P. 001	VERSIÓN: 01	PÁGINA: 1 de 32

PROCESO:

ADMINISTRATIVO

TIPO DE PROCESO:

PROCESO PRODUCTIVO

ALCANCE:

PERSONAL FONDO COMPLEMENTARIO PREVISIONAL CERRADO DE CESANTÍA DE LOS SERVIDORES CIVILES DEL TRÁNSITO NACIONAL FCPC-FONCETRA

MANUAL DE POLÍTICAS DE INFORMÁTICA

ETAPAS	NOMBRE Y CARGO	FIRMA
ELABORADO POR:	Ing. Marcela Patiño Ing. Viviana Paucar	
REVISADO POR:	Ing. Alejandro Palacios	
APROBADO POR:	Asamblea General de Participes	

1. INTRODUCCIÓN

El Manual de Políticas y Procesos de Informática es un documento guía para los procesos del Fondo Complementario Previsional Cerrado de Cesantía de los Servidores Civiles del Tránsito Nacional FCPC-FONCETRA que debe ser cumplido por todos los funcionarios del FCPC que participen en cada uno de los procesos descritos.

2. OBJETIVO

El objetivo es implantar políticas estándares, procesos y procedimientos en conjunción, orientados al fortalecimiento de las seguridades de la información apoyado en tecnología de punta, con el pleno compromiso de todos los funcionarios de la Organización.

Aplica a toda la información del Fondo de Cesantía y a la protección en cualquiera de sus presentaciones como documentos, archivos físicos, archivos magnéticos, correo electrónico, sistemas y aplicaciones propias.

3. ROLES Y RESPONSABILIDADES

Las principales responsabilidades son:

Representante Legal:

- Aprobar cambios y nuevas políticas de seguridad de la información.
- Aprobar Plan de contingencia

Asesor Informático

- Velar por el buen funcionamiento de las herramientas informáticas.
- Planificar, ejecutar y coordinar mantenimientos preventivos a equipos FCPC.
- Brindar soporte en temas informáticos a empleados FCPC con sus programas y proyectos.
- Establecer y revisar las políticas de uso de tecnología y seguridad de información.
- Planificar y ejecutar los procesos de respaldos de información.
- Dar seguimiento a contratos en el área tecnológica.
- Mantener actualizadas carpetas de archivos informáticos
- Capacitar al personal en uso de programas informáticos.

Auditor Interno

- Revisar y actualizar políticas y procedimientos, junto con el Asesor de Informática.
- Informar al Representante Legal sobre novedades de cumplimiento de políticas y procedimientos, generados a través del control previo y concurrente.
- Cumplir y hacer que se cumplan las políticas y procedimientos establecidos en este Manual.

4. POLÍTICAS DE PROCESOS

Es responsabilidad del Representante Legal y de los empleados del FCPC, el cumplimiento de los lineamientos aquí establecidos.

4.1 POLITICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

1. De la Organización

1. La seguridad de la información es responsabilidad del FCPC, es decir aplica a todos los usuarios que utilizan información, que manejan información, que administran, respaldan o dan mantenimiento a sistemas de información.

2. La información del FCPC, debe cumplir con la normatividad que determina las leyes y reglamentos de la legislación ecuatoriana para períodos de conservación y procedimientos de descarte de información.

3. Definir los privilegios de acceso a la información, de acuerdo a las funciones de los colaboradores, previo informe del Auditoría Interna.

2. Del Asesor Informático

1. Ejecutar el programa institucional de concientización en seguridad de la información.
2. Apoyar a los propietarios de la información en la clasificación de las misma
3. Mantener el inventario de clasificación de activos de información actualizable y accesible para el FCPC.
4. Resolver consultas y proporcionar recomendaciones sobre aspectos de seguridad de la información.
5. Identificar su información crítica, incluyendo los requerimientos de confidencialidad, integridad y disponibilidad.
6. Definir los requerimientos de protección de la información que posee.
7. Aplicar los privilegios de acceso a la información, de acuerdo a las funciones de los colaboradores, emitidos por la instancia.
8. Emitir directrices de seguridad de información dentro del proceso.
9. Identificar los riesgos a los que puede estar expuesta la información.

3. De todos los funcionarios del FCPC

1. No compartir sus claves de acceso con otras personas.
2. Tener instalado únicamente el software aprobado por el FCPC y que tenga la licencia apropiada.
3. Notificar en forma inmediata cualquier incidente o violación a la seguridad que descubra como virus, etc.
4. Dar el manejo adecuado a la información de acuerdo a su clasificación.
5. Todos los funcionarios del FCPC deben recibir una adecuada concientización, capacitación y actualizaciones periódicas en materia de seguridad de la información, incidentes de seguridad, responsabilidades legales y controles de la organización, y el uso correcto de los equipos.

6. Las pantallas de sus computadores deben estar protegidas con una CONTRASEÑA cuando el funcionario abandona su puesto de trabajo durante el horario normal o apagado cuando el funcionario ha terminado sus labores.
7. Todos los funcionarios del FCPC deben tomar precauciones para prevenir y detectar la introducción de software malicioso (como virus informático, etc.)
8. Tener su propia identificación y contraseña. La contraseña constituye un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a la información. La contraseña no debe ser compartida.
9. Además, todo funcionario del FCPC que realiza intercambio de información por otros medios de comunicación, de voz, fax y video debe tomar las debidas precauciones, respecto de no revelar información sensible y evitar dejar mensajes confidenciales en contestadores automáticos.

4.2 POLÍTICAS DE SEGURIDAD INFORMÀTICA

1. INTRODUCIÓN

Surgen como una herramienta organizacional para concienciar a los funcionarios del FCPC sobre la importancia y sensibilidad de la información. El proponer estás políticas de seguridad requiere un alto compromiso con el FCPC, agudeza técnica para establecer fallas y debilidades en su aplicación, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea al FCPC.

2. OBJETIVOS

Desarrollar un sistema de seguridad significa planear, organizar, dirigir y controlar las acciones para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los respaldos activos de la institución. Cuya implantación sugiere:

- Establecer un esquema de seguridad con perfecta claridad y transparencia bajo la responsabilidad del FCPC en la administración del riesgo.
- Establecer compromisos por parte de los funcionarios del FCPC con el proceso de seguridad.
- Ganar calidad con la presentación de servicios de seguridad

3. DISPOSICIONES GENERALES

Artículo 1.- El presente ordenamiento tiene por objeto estandarizar y contribuir al desarrollo informático del FCPC a través de los Representantes de los Partícipes.

Artículo 2.- Para los efectos de este instrumento se entenderá por Representantes de los Partícipes, a los partícipes que fueron elegidos en cada una de las provincias o agrupación de provincias, para su representación en las asambleas que el Representante Legal convoque, quienes a más de planificar, decidirán sobre:

- Adquisiciones de Hardware y software
- Establecimiento de estándares de la Institución tanto de hardware como de software.
- Establecimiento de lineamientos para concursos de ofertas
- Establecimiento de la Arquitectura tecnológica de grupo consistente en:

i. *Sistema operativo:* MS-Windows, Linux, Mac.
ii. *Bases de Datos:* SQL
iii. Utilitarios de oficina
- ✓ Microsoft Office

iv. Programas antivirus
- ✓ ESSET NOD 32
- ✓ KASPERSKY

v. Manejador de correo electrónico
- ✓ Microsoft Outlook
- ✓ Mail
- ✓ Google App

vi. Navegadores de Internet:
- ✓ Internet Explorer
- ✓ Google Chrome
- ✓ Mozilla

vii. Comprimidores de archivos:
- ✓ Winzip
- ✓ Winrar

Sólo se adquirirán las últimas versiones liberadas de los productos seleccionados con las respectivas autorizaciones. Todos los productos de Software que se adquieran deberán contar con su licencia de uso, documentación y garantía respectiva.

3.1. INSTALACIONES DE LOS EQUIPOS DE CÓMPUTO

Artículo 3.- La instalación del equipo de cómputo, quedará sujeta a los siguientes lineamientos:

- Los equipos para uso interno se instalarán en lugares adecuados
- Las instalaciones están estrictamente con las especificaciones del cableado y de los circuitos de protección necesarios que el MAATE dispone.

3.2. LINEAMIENTOS EN INFORMÁTICA: *(INFORMACIÓN)*

Artículo 4.- La información almacenada en medios físicos se deberá inventariar, anexando la descripción y las especificaciones de la misma, clasificándola en tres categorías:

- Información histórica para auditorias.
- Información de interés de la Institución
- Información de interés exclusivo de alguna área en particular.

Artículo 5.-El Representante Legal, delimitará las responsabilidades de sus supervisados y determinará quien está autorizado a efectuar operaciones emergentes con dicha información tomando las medidas de seguridad pertinentes.

Artículo 6.- Se establecen tres tipos de prioridad para la información para respaldo:

6.1. La información vital para el funcionamiento del área, se deberá tener procesos colaborativos, así como tener el respaldo diario de las modificaciones efectuadas, rotando los dispositivos de respaldo y guardando respaldos históricos semanalmente.

6.2. La información necesaria pero no indispensable, deberá ser respaldada con una frecuencia mínima de una semana, rotando los dispositivos de respaldo y guardando respaldos históricos mensualmente.

6.2. El respaldo de la información ocasional o eventual queda a criterio del área.

Artículo 7.- La información almacenada en medios magnéticos, de carácter histórico, quedará documentada como activos del área y estará debidamente resguardada en su lugar de almacenamiento externo. Es obligación del responsable del área, la entrega conveniente de la información, a quien le suceda en el cargo.

Artículo 8.- Los sistemas de información en operación, como los que se desarrollen deberán contar con sus respectivos manuales. Un manual del usuario que describa los procedimientos de operación y el manual técnico que describa su estructura interna, programas, catálogos y archivos.

3.3 FUNCIONAMIENTO DE LOS EQUIPOS DE CÓMPUTO

Artículo 9.- Los funcionarios del FCPC al usar el equipo de cómputo, se abstendrán de consumir alimentos, fumar o realizar actos que perjudiquen el funcionamiento del mismo o deterioren la información almacenada en medios magnéticos, ópticos, o medios de almacenamiento removibles de última generación.

Artículo 10.- Por seguridad de los recursos informáticos se deben establecer seguridades:

- Físicas
- Sistema Operativo (licencias registradas de uso exclusivo de la institución)
- Software
- Comunicaciones
- Base de Datos
- Sistema Contable (Usuarios específicos)
- Aplicaciones (licencias registradas de uso exclusivo de la institución)

Bajo los siguientes lineamientos:

- Mantener claves de acceso propias y confidenciales que permitan el uso solamente al personal autorizado para ello.
- Verificar la información que provenga de fuentes externas a fin de corroborar que esté

libre de cualquier agente contaminante o perjudicial para el funcionamiento de los equipos
- Verificar que pólizas de seguros de los activos informáticos estén activas

Artículo 11.- En ningún caso se autorizará la utilización de dispositivos ajenos a los procesos informáticos. Por consiguiente, se prohíbe el ingreso y/o instalación de hardware y software particular, es decir que no sea propiedad del FCPC, excepto en casos emergentes que el Representante Legal lo autorice.

3.3. PLAN DE CONTINGENCIAS INFORMÀTICAS

Artículo 12.- El Representante Legal junto con el Asesor de Informática creará para los funcionarios del FCPC un plan de contingencias informáticas que incluya al menos los siguientes puntos:

Continuidad con la operación del área con procedimientos informáticos alternos.

- Tener los respaldos de información en un lugar seguro, fuera del lugar en el que se encuentren los equipos.
- Tener el apoyo por medios magnéticos o en forma documental, de las operaciones necesarias para reconstruir los archivos dañados.
- Contar con un instructivo de reactivación del sistema contable, para que toda acción correctiva se efectúe con la mínima degradación posible de los datos.
- Contar con un directorio telefónico del personal interno y externo de soporte, el cual pueda recurrir en el momento en que se detecte cualquier anomalía.
- Ejecutar pruebas de la funcionalidad del plan.
- Mantener revisiones del plan a fin de efectuar las actualizaciones respectivas.

3.4 ESTRATEGIAS INFORMÁTICAS

Artículo 13.- La estrategia informática del FCPC se consolida en el Plan de Automatización Informática y está orientada hacia los siguientes puntos:

- Sistema Contable
- Esquemas de operación bajo el concepto multicapas (páginas Web).
- Estandarización de hardware, software base, utilitarios y estructuras de datos

Artículo 14.- Para la elaboración de los proyectos informáticos y para el presupuesto de los mismos, se tomarán en cuentan tanto las necesidades de hardware y software del área solicitante, como la disponibilidad de recursos con los que cuente el FCPC.

3.5. IDENTIFICADORES DE USUARIO Y CONTRASEÑAS

Artículo 15.- Todos los usuarios con acceso al sistema de información o a una red informática, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.

Artículo 16.- Ningún usuario recibirá un identificador de acceso a la Red de Comunicaciones,

Recursos Informáticos o Aplicaciones hasta que no acepte formalmente la Política de Seguridad vigente.

Artículo 17.- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el responsable de la información.

Artículo 18.- La longitud mínima de las contraseñas será igual o superior a seis caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.

3.6. RESPONSABILIDADES PERSONALES

Artículo 19.- Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.

Artículo 20.- Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.

Artículo 21.- Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.

Artículo 22.- Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar al Representante Legal y éste reportar al responsable de la administración de la red.

Artículo 23.- El Usuario debe utilizar una contraseña compuesta por un mínimo de seis caracteres constituida por una combinación de caracteres alfabéticos, numéricos.

Artículo 24.- La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos.

Artículo 25.- En caso que el sistema no lo solicite automáticamente, el usuario no debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.

Artículo 26.- En el caso que el sistema lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada año. En caso contrario, se le podrá denegar el acceso y se deberá contactar para solicitar al administrador de la red una nueva clave.

Artículo 27.- Proteger, en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.

Artículo 28.- Guardar por tiempo indefinido la máxima reserva y no se debe emitir al exterior datos de carácter personal contenidos en cualquier tipo de soporte.

Artículo 29.- Utilizar el menor número de listados que contengan datos de carácter personal y mantener los mismos en lugar seguro y fuera del alcance de terceros.

Artículo 30.- Cuando entre en posesión de datos de carácter personal, se entiende que dicha posesión es estrictamente temporal, y debe devolver los soportes que contienen los datos inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos.

Artículo 31.- Los usuarios sólo podrán crear ficheros que contengan datos de carácter personal para un uso temporal y siempre necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en unidades locales de disco de la computadora de trabajo y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.

Artículo 32.- Los usuarios deben notificar al Representante Legal cualquier incidencia que detecten que afecte o pueda afectar a la seguridad de los datos de carácter personal: pérdida de listados, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos.

Artículo 33.- Los usuarios únicamente introducirán datos identificativos y direcciones o teléfonos de personas en las agendas de contactos de las herramientas ofimáticas (por ejemplo, en Outlook)

3.7 SALIDA DE INFORMACIÓN

Artículo 34.- Toda salida de información (en soportes informáticos o por correo electrónico) sólo podrá ser realizada por personal autorizado y será necesaria la autorización formal del Representante Legal.

Artículo 35.- Además, en la salida de datos especialmente protegidos (como son los datos de los partícipes para los que el Reglamento requiere medidas de seguridad de nivel alto), se deberán cifrar los mismos o utilizar cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada durante su transporte.

3.8 USO APROPIADO DE LOS RECURSOS INFORMÁTICOS

Artículo 36.- Los Recursos Informáticos, Datos, Software, Red Corporativa y Sistemas de Comunicación electrónica están disponibles exclusivamente para complementar las obligaciones y propósito de la operativa para la que fueron diseñados e implantados. Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso.

3.9 PROHIBICIONES DE USO DE RECURSOS INFORMÁTICOS: En relación a:

Artículo 37.- El uso de estos recursos para actividades no relacionadas con el propósito del FCPC, o bien con la extralimitación en su uso.

Artículo 38.- Las actividades, equipos o aplicaciones que no estén directamente especificados como parte del Software o de los Estándares de los Recursos Informáticos propios del FCPC.

Artículo 39.- Introducir en los Sistemas de Información o la Red Corporativa contenidos obsceno, amenazador, inmoral u ofensivo.

Artículo 40.- Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos Informáticos. El personal contratado por el FCPC tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los Sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.

Artículo 41.- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos del FCPC

3.10 SOFTWARE

Artículo 42.- Todo el personal que accede a los Sistemas de Información del FCPC debe utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de utilización.

Artículo 43.- Todo el personal tiene prohibido instalar copias ilegales de cualquier programa, incluidos los estandarizados. Así como también borrar cualquiera de los programas instalados legalmente.

3.11 RECURSOS DE RED

De forma rigurosa, ninguna persona debe:

Artículo 44.- Intentar obtener otros derechos o accesos distintos a aquellos que les hayan sido asignados.

Artículo 45.- Intentar acceder a áreas restringidas de los Sistemas de Información o de la Red Institucional.

Artículo 46.- Intentar distorsionar o falsear los registros "log" de los Sistemas de Información.

Artículo 47.- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos.

Artículo 48.- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros Usuarios, ni dañar o alterar los Recursos Informáticos.

3.12 CONECTIVIDAD A INTERNET

Artículo 49.- La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos los funcionarios del FCPC tienen las mismas responsabilidades en cuanto al uso de Internet.

Artículo 50.- El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello.

No está permitido acceder a Internet llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de Internet conectándose con un módem.

Artículo 51.- Internet es una herramienta de trabajo. Todas las actividades en Internet deben estar en relación con tareas y actividades del trabajo desempeñado.

Artículo 52.- Sólo puede haber transferencia de datos de o a Internet en conexión con actividades propias del trabajo desempeñado.

Artículo 53.- En caso de tener que producirse una transmisión de datos importante, confidencial o relevante, sólo se podrán transmitir *en forma encriptado o codificada.*

3.13 ACTUALIZACIONES DE LA POLÍTICA DE SEGURIDAD

Artículo 54.- Debido a la propia evolución de la tecnología y las amenazas de seguridad, y a las nuevas aportaciones legales en la materia, el FCPC se reserva el derecho a modificar esta Política cuando sea necesario.

Artículo 55.- Es responsabilidad de cada uno de los funcionarios del FCPC la lectura y conocimiento de la Política de Seguridad más reciente.

3.14 BENEFICIOS DE IMPLANTAR POLÍTICAS DE SEGURIDAD INFORMÁTICA

Los beneficios de un sistema de seguridad con políticas claramente concebidas bien elaboradas son inmediatos, ya que el FCPC trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

3.14.1 Aumento de la productividad laboral.
3.14.2 Aumento de la motivación del personal.
3.14.3 Compromiso con la misión de la institución.
3.14.4 Información confiable.

Aprobado en el Distrito Metropolitano de Quito, en Asamblea General Ordinaria Virtual de Partícipes de fecha 11 de diciembre de 2024.

Ing. Alejandro Palacios
Representante Legal
FCPC de Cesantía de los Servidores Civiles del Tránsito Nacional FCPC-FONCETRA