Fondo de Desarrollo Indígena Guatemalteco
Dirección de Informática

MANUAL DE NORMAS Y PROCEDIMIENTOS PARA LA ACTUALIZACIÓN DE ANTIVIRUS Y SOFTWARE

Octubre 2016.

INDICE

I. INTRODUCCIÓN

Como parte de la Seguridad de la Información del Fondo de Desarrollo Indígena Guatemalteco -FODIGUA- se deben establecer controles sobre los agentes maliciosos que puedan ingresar a la red de la Institución, así mismo mantener actualizado el Software instalado en el FODIGUA, estableciendo las actividades requeridas para detectar virus informáticos que puedan dañar o afectar los equipos, para garantizar así la disponibilidad e integridad de la información.

A continuación se presenta el Manual de Normas y Procedimientos para la actualización de Antivirus y Software del Fondo de Desarrollo Indígena Guatemalteco -FODIGUA-, en el cual se identifican cada una de las actividades que la Dirección de Informática deben realizar para un correcto control y monitoreo de las estaciones de trabajo, con actualizaciones de antivirus y Software.

II. OBJETIVO

Establecer un documento técnico administrativo que norme el procedimiento que debe seguir el personal del la Dirección de Informática, con el objetivo de controlar posibles daños por amenazas de virus informáticos en los procesos del equipo del Fondo de Desarrollo Indígena Guatemalteco, el cual garantizará el uso apropiado del equipo de cómputo y asimismo, la actualización de software instalado en la Institución.

III. TERMINOLOGÍA

AGENTES MALISIOSOS: conjunto de códigos, especialmente sentencias de programación, que tiene un fin malicioso. Esta definición incluye tanto programas malignos compilados, como macros y códigos que se ejecutan directamente, como los que suelen emplearse en las páginas web

SOFTWARE: Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

VIRUS: Un virus informático se adjunta a un programa o archivo de forma que pueda propagarse, infectando los ordenadores a medida que viaja de un ordenador a otro.

ANTIVIRUS: es un programa de seguridad que se instala en la computadora o dispositivo móvil para protegerlo de infecciones por malware.

MALWARE: Es una frase utilizada para cualquier tipo de software malintencionado, como virus, gusanos, troyanos.

IV. MARCO LEGAL

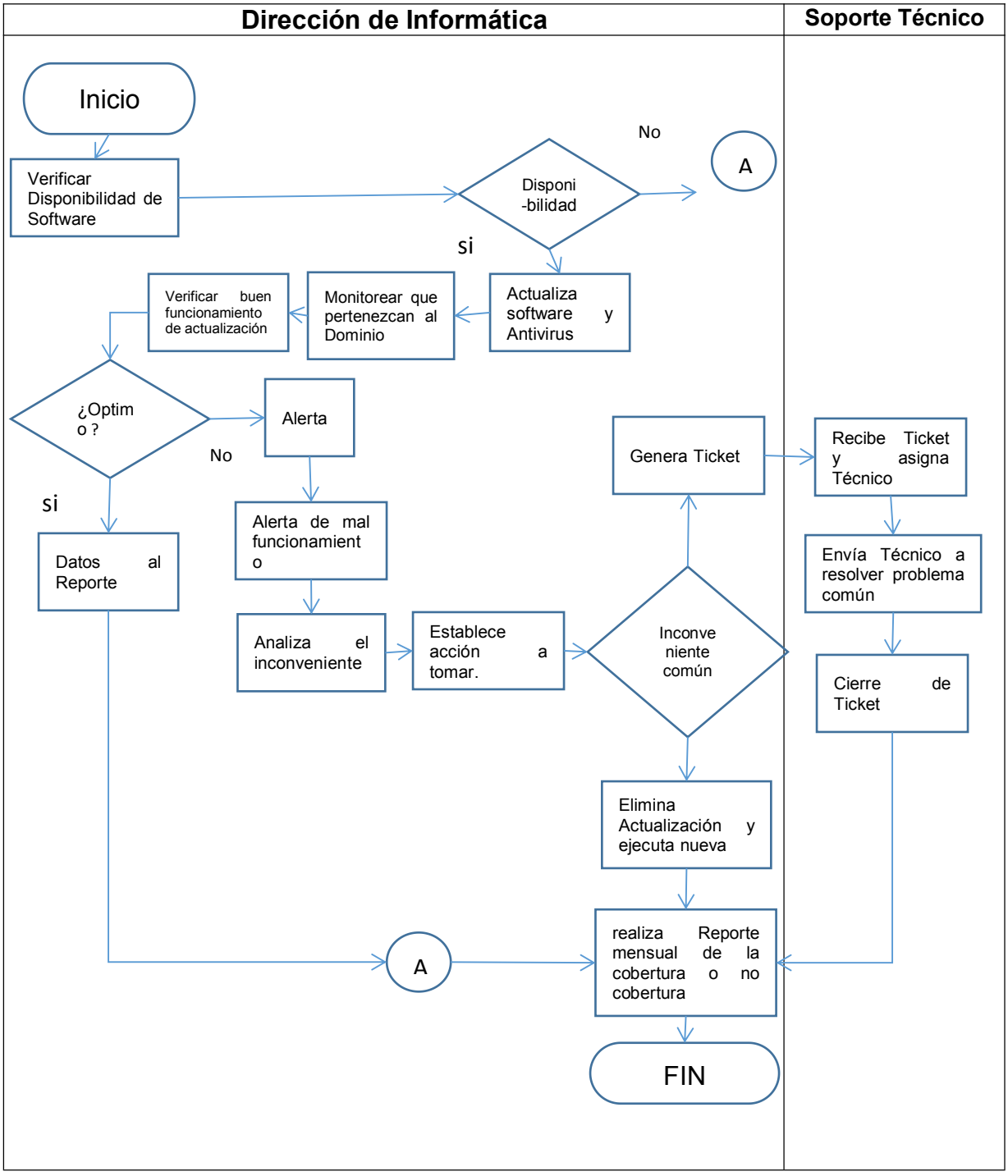
Acuerdo Gubernativo 435-94 del Fondo de Desarrollo Indígena y sus Reformas.

V. DESCRIPCIÓN DEL PROCESO

Responsable	No de paso	Actividad
Dirección de Informática	1	Verificar si existen licencias disponibles tanto de Software y Antivirus.
	2	**Si** existe licenciamiento disponible continuar con paso 4
	3	**No** existe licenciamiento disponible continua con paso No. 17
	4	Actualiza Versión del Software Instalado y de la misma manera el Antivirus.
	5	Monitorea que los equipos estén agregados al Dominio de la Institución y comprobar que los equipos estén completamente inventariados
	6	Verificar el buen funcionamiento de las actualizaciones.
	7	**Si** el funcionamiento es optimo, agrega datos al reporte y continúa con el paso ultimo
	8	**No** es óptimo por mal funcionamiento, genera alerta de forma automática.
	9	Alerta por mal funcionamiento en el equipo.
	10	Identifica la causa del mal funcionamiento y analiza el tipo de inconveniente detectado.
	11	Establece la acción a tomar, considerando el inconveniente detectado.
	12	Si el inconveniente es común, genera ticket en la mesa de ayuda y continúa con el paso No. 14
	13	No es infección común. Elimina actualización del Software o antivirus y ejecuta una nueva actualización. Continua con paso No. 17
Soporte Técnico	14	Recibe ticket y asigna técnico.
	15	Envía técnico para solventar incidente común.

	16	Cierre de caso o Cierre de Ticket.
	17	Realiza reporte mensual de la cobertura o no cobertura en el equipo de la institución y de las alertas detectadas.
		Fin del Proceso.

VI. DIAGRAMA DE FLUJO



VII.ANEXOS

a. Normas

1.1.1. Todas las computadoras de escritorio, servidores y computadoras portátiles deberán tener instalado Software actualizado y antivirus autorizado y vigente por la Dirección de Informática.

1.1.2. Todo equipo de cómputo que sea configurado por primera vez a la red del FODIGUA, deberá instalarse el software de antivirus la responsabilidad del Área de Infraestructura de la Dirección de Informática.

1.1.4. La administración del servidor del software de Antivirus está a cargo del encargado de Infraestructura de la Dirección de Informática, asimismo es responsable de mantener contratos vigentes del Software instalado en la Institución.

1.1.5. Las contraseñas de licenciamiento del Software instalados en el Fondo y antivirus son administradas únicamente por el Departamento de Infraestructura quien configura la consola y establece los tiempos de actualización de acuerdo a la licencia vigente.

1.1.7. Las actualizaciones correspondientes se realizarán por medio de un servidor donde estará instalada la consola principal de antivirus, mediante el cual se establece el horario de actualización y configuración para el debido control.

1.1.11. El usuario no está autorizado para instalar software ajeno a la Institución de la misma manera conectar a la red de la Institución, computadoras que no contengan el antivirus establecido por la Dirección de Informática.

1.1.13. Queda prohibido cambiar la configuración o parámetros de los equipos de cómputo, sistemas operativos o aplicaciones de la Institución. Este procedimiento debe realizarlo personal autorizado de la Dirección de Informática.

1.1.14. El Departamento de Seguridad Informática debe llevar el control de la cantidad de licencias Instaladas del software y antivirus, a menos que la licencia sea ilimitada