

Política de Seguridad de Protección Contra Software Nocivo

**Bogotá, D.C.,**

**(ABRIL DE 2019)**

### ****TABLA DE CONTENIDO****

[1. INTRODUCCIÓN 3](#_Toc531083678)

[2. OBJETIVO GENERAL 3](#_Toc531083679)

[3. OBJETIVOS ESPECIFICOS 3](#_Toc531083680)

[4. ALCANCE 4](#_Toc531083681)

[5. DECLARACION 4](#_Toc531083682)

[6. ROLES Y RESPONSABILIDADES 5](#_Toc531083683)

[7. POLÍTICA DE SEGURIDAD DE PROTECCION CONTRA SOTWARE NOCIVO. 5](#_Toc531083684)

[8. GLOSARIO DE TERMINOS 7](#_Toc531083685)

1. ****INTRODUCCIÓN****

El siguiente documento hace parte de la POLITICA GENERAL DE TECNOLOGIA Y SEGURIDAD DE LA INFORMACION Y COMUNICACIONES de la entidad.

La UAERMV (Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial), basará la administración de la seguridad de los Activos de Información, así como las buenas prácticas en el uso de las herramientas informáticas involucradas en el proceso de apoyo: “Gestión de Servicios de Infraestructura Tecnológica” (GSIT) en las políticas contenidas en este documento

Un **virus informático** es un [*malware*](http://es.wikipedia.org/wiki/Malware) que tiene por objeto alterar el normal funcionamiento de los computadores sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan [archivos ejecutables](http://es.wikipedia.org/wiki/Archivo_ejecutable) por otros infectados con el [código](http://es.wikipedia.org/wiki/C%C3%B3digo_objeto) de este. Los virus pueden destruir de manera intencionada los [datos](http://es.wikipedia.org/wiki/Datos) almacenados en los equipos de cómputo. Aunque también existen otros *malwares* más inofensivos, que se caracterizan por ser molestos para el usuario.

Los virus informáticos tienen, básicamente, la función de propagarse a través de un software. Son muy nocivos y algunos contienen además una carga dañina con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas o bloquear las redes de la entidad, generando tráfico inútil.

Esta política se realiza con el fin de proteger los activos de información de la entidad contra el uso de software nocivo, que pueda comprometer los mismos.

1. ****OBJETIVO GENERAL****

Garantizar la no propagación o instalación de software con código malicioso o nocivo el cual pueda comprometer la disponibilidad, integridad y confidencialidad de los servicios soportados por la Infraestructura tecnológica de la entidad.

1. ****OBJETIVOS ESPECIFICOS****
2. Evitar el riesgo de la instalación de software nocivo en los equipos de cómputo de la entidad que puedan infectar el mismo con algún tipo de virus.
3. Controlar el acceso de los medios de almacenamiento externo, como memorias externas USB, CD (Discos Compactos) y DVD, sin la debida revisión o escaneo por parte de los Usuarios.

1. ****ALCANCE****

El alcance de los lineamientos que se definen en esta política da cubrimiento a los accesos que involucren:

1. Hardware (servidores, equipos de cómputo portátiles y de escritorio, medios de almacenamiento externo, como memorias externas USB, CD (Discos Compactos) y DVD.
2. Software no autorizado por el área de SIT.
3. Acceso a internet.

Aplica para todos los Servidores Públicos de la Unidad: Empleados públicos de planta (de carrera administrativa y los provisionales), funcionarios de libre nombramiento y remoción, trabajadores oficiales, contratistas y demás personal que tenga acceso a los equipos de cómputo y a la red de la entidad. Todos los colaboradores deberán preservar la confidencialidad y disponibilidad de la información de la UAERMV. Todos los tipos de colaboradores están sujetos a los mismos requerimientos de seguridad y tienen las mismas responsabilidades de salvaguardar la información de la Entidad. Están obligados a proteger y cumplir los acuerdos de confidencialidad durante y una vez terminada su relación laboral y/o contractual con la UAERMV.

Se tendrán en cuenta para esta política, los controles: A.12.2.1 Controles contra códigos maliciosos de la norma ISO 27001:2013.

1. ****DECLARACION****

En este documento se encuentran los lineamientos que aseguran una actuación adecuada para alcanzar un alto nivel de seguridad de la información en la UAERMV. La información es un activo importante para la entidad pues tiene un alto valor para la misma, por ello se han definido las directrices de seguridad para los Activos de Información que deben orientar todas las acciones a seguir. Estas directrices hacen parte del marco de POLÍTICAS GENERALES DE TECNOLOGÍA Y SEGURIDAD DE INFORMACIÓN Y COMUNICACIONES y están basadas en la NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27002 (anteriormente denominada ISO 17799) la cual es un estándar para la seguridad de la información y es publicada por la *International Organization for Standardization* y la Comisión Electrotécnica Internacional. La versión más reciente es la ISO/IEC 27002:2013).

Con lo anterior, se busca minimizar riesgos en la información, asegurar la continuidad de la UAERMV y ayudar en el cumplimiento de los objetivos misionales

**Acuerdo de confidencialidad:**

Todos los Usuarios que administren, leen, modifiquen o creen información en la UAERMV deben firmar un acuerdo de confidencialidad o de no divulgación como parte de sus términos y condiciones iníciales de empleo. Esta directriz también incluye a personal ocasional y los usuarios externos no contemplados en un contrato formalizado.

1. ROLES Y RESPONSABILIDADES
   1. **Encargado de seguridad de la información:** Persona delegada cuyas funciones principales son asesorar en materia de seguridad de la información a la UAERMV y supervisar el cumplimiento de la presente Política.

**6.2. Usuarios de la información.** Personas que tiene asignado un equipo de cómputo y/o escritorio de trabajo quienes deberán dar cumplimiento a los procedimientos que se deriven de esta Política.

1. POLÍTICA DE SEGURIDAD DE PROTECCION CONTRA SOTWARE NOCIVO.

**Controles Contra códigos maliciosos:**

Se deben implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.

1. Todos los equipos de cómputo de la entidad sin excepción alguna deben tener un programa de antivirus instalado, licenciado y actualizado con la versión más reciente de las bases de datos del fabricante.
2. El programa de antivirus debe ejecutarse automáticamente cuando se conecte un dispositivo de almacenamiento externo, como memorias externas USB, CD (Discos Compactos) y DVD, en caso de no realizarse de forma automática se deberá realizar el procedimiento de forma manual sin excepción alguna y realizar un escaneo de virus.
3. Todos los equipos de cómputo de la entidad deben tener habilitado la solicitud de clave de administrador cuando se intente realizar la instalación de un programa ejecutable.
4. Las credenciales de acceso para la instalación de programas deben ser cambiadas periódicamente, estas credenciales no deben ser conocidas por los usuarios estándar de la entidad.
5. Los usuarios no deben descargar software desde internet.
6. Los usuarios no deben utilizar software obtenido externamente desde Internet o de una persona u organización diferente al área de GSIT.
7. Debe certificarse que todo el software, archivos o ejecutables, se encuentran libres de virus antes de ser enviados a una entidad externa.
8. Cualquier archivo Cifrado suministrado por instituciones externas a la UAERMV, debe ser descifrado antes de ser sometido al análisis con sistemas antivirus.
9. Antes que cualquier archivo sea restaurado en un sistema de la UAERMV, desde un medio de almacenamiento de respaldo, éste debe ser analizado con un sistema antivirus actualizado.
10. Los usuarios no deben intencionalmente escribir, generar, compilar, copiar, almacenar, propagar, ejecutar o intentar introducir cualquier código de computador diseñado para auto replicarse, deteriorar o que obstaculice el desempeño de cualquier sistema de la UAERMV.
11. La plataforma de correo electrónico de la entidad debe contar con el servicio de anti-SPAM habilitado y funcionando, y a su vez la generación de reportes mensuales sobre la prevención de estos.
12. Cuando se reciba un correo sospechoso por el nombre, la extensión de este, el remitente o con otras características anormales, se recomienda no hacer la apertura o descarga de los archivos adjuntos y mucho menos la ejecución de estos, en estos casos solicitar la revisión inmediata del personal de soporte técnico del grupo e GSIT.
13. Si un usuario sospecha de una infección por un virus en el computador, debe desconectar el cable de red, llamar al personal de soporte del grupo de GSIT para que sea revisado inmediatamente.
14. ****GLOSARIO DE TERMINOS****

* **Disponibilidad:** Capacidad de un componente o servicio para realizar su función requerida durante un periodo de tiempo.
* **GSIT:** Gestión de Servicios de Infraestructura Tecnológica.
* **Software malicioso**: También conocido como programa malicioso o malware, contiene virus, spyware y otros programas indeseados que se instalan en el computador, teléfono o aparato móvil sin el consentimiento del usuario. Estos programas pueden colapsar el funcionamiento de los equipos y se pueden utilizar para monitorear y controlar la actividad del usuario en internet. Además, con estos programas los equipos pueden quedar expuestos al ataque de virus y enviar anuncios indeseados o inapropiados. Los delincuentes usan programas maliciosos para robar información personal, enviar spam y cometer fraude.
* **SPAM:** O información basura, hace referencia a aquellos mensajes, con remitente desconocido, que no son solicitados ni deseados por el usuario y que, además, por norma general, son enviados en grandes cantidades. Por consiguiente, el spam se caracteriza por ser anónimo, masivo y no demandado.
* **Usuario:** Persona que utiliza los servicios diarios.

**REVISIÓN Y APROBACIÓN:**

|  |  |  |
| --- | --- | --- |
| **Elaborado y/o Actualizado por**  **EQUIPO OPERATIVO SIG del Proceso:** | **Validado por**  **RESPONSABLE DIRECTIVO SIG**  **del Proceso:** | **Aprobado por:** |
| **OMAR FERNANDO GARZON /**  **GLORIA MENDEZ**  **Contratista / Proceso GSIT** | Firma: | Firma: |
| **Acompañamiento EQUIPO TÉCNICO SIG:** |
| **CHRISTIAN MEDINA FANDIÑO/**  **ANDREA DEL PILAR ZAMBRANO**  **Contratista/ Proceso DESI** |
| **MARCELA ROCIO MARQUEZ ARENAS**  **(Secretaria General)** | **MARTHA PATRICIA AGUILAR COPETE**  **Representante de la Alta Dirección** |

**CONTROL DE CAMBIOS:**

|  |  |  |  |
| --- | --- | --- | --- |
| **VERSIÓN** | **DESCRIPCIÓN** | **FECHA** | **APROBADO**  **Representante de la Alta Dirección SIG** |
| 1 | Revisado y actualizado por el Ing. Omar Fdo. Garzón Giraldo (especialista en seguridad de la información), se realizó la separación de la Política de protección contra software nocivo de la POLITICA GENERAL DE TECNOLOGIA Y SEGURIDAD DE LA INFORMACION Y COMUNICACIONES, se agregó introducción, se modificó el objetivo general, se agregaron los objetivos específicos, se realizó modificación del alcance, se agregaron roles y responsabilidades y las generalidades de la Política de seguridad de protección contra software nocivo. | Diciembre 2018 | Jefe Oficina Asesora de Planeación |
| 2 | Se realiza actualización de documento conforme al nuevo mapa de procesos de la entidad. | Abril de 2019 | Jefe Oficina Asesora de Planeación |