

**POLITICA DE SEGURIDAD SOBRE EL USO DE EQUIPOS DE COMPUTO Y EL ACCESO A LA RED**

**Bogotá, D.C.,**

**(MAYO DE 2019)**

**CONTENIDO**

[1. INTRODUCCIÓN 3](#_Toc7070606)

[2. GLOSARIO DE TÉRMINOS 3](#_Toc7070607)

[3. OBJETIVO GENERAL 4](#_Toc7070608)

[4. OBJETIVOS ESPECIFICOS 4](#_Toc7070609)

[5. ALCANCE 4](#_Toc7070610)

[6. DECLARACIÓN 5](#_Toc7070611)

[7. ROLES Y RESPONSABILIDADES 5](#_Toc7070612)

[8. POLÍTICA SOBRE EL USO DE EQUIPOS DE COMPUTO Y EL ACCESO A LA RED 6](#_Toc7070613)

1. ****INTRODUCCIÓN****

El siguiente documento hace parte de la POLÍTICA GENERAL DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN Y COMUNICACIONES de la entidad.

La UAERMV (Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial), basará la gestión de los equipos de cómputo y acceso a la red de apoyo “Gestión de Servicios de Infraestructura Tecnológica” (GSIT), en las políticas contenidas en este documento.

La conectividad de red hace parte de la infraestructura tecnológica mínima que debe tener la entidad para que los equipos de cómputo y servidores puedan estar conectados en una red local y la red de internet. El equipo de cómputo es la herramienta usada para que los usuarios de la entidad realicen las funciones asignadas como generación de documentos, informes, conexión a internet entre otros.

El uso inapropiado de estos recursos tecnológicos expone a la organización a riesgos tales como ataque de virus, compromiso de la red y sistemas de información. Estas directrices y recomendaciones buscan garantizar que la red y los equipos de cómputo sean utilizados de la mejor manera. Es responsabilidad de cada usuario conocer y aplicar las recomendaciones descritas aquí.

1. ****GLOSARIO DE TÉRMINOS****

* **Dirección IP:** Es un número que identifica, de manera lógica y jerárquica, a una [Interfaz](https://es.wikipedia.org/wiki/Interfaz) en red (elemento de comunicación/conexión) de un dispositivo ([computadora](https://es.wikipedia.org/wiki/Computadora), tableta, portátil, *smartphone*).
* **Dirección MAC:** (Control o control de acceso al medio) es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red.
* **Disponibilidad:** Capacidad de un componente o servicio para realizar su función requerida durante un periodo de tiempo.
* **EGTI:** Proceso de Estrategia de Gobierno de Tecnología de Información.
* **GSIT:** Proceso de Gestión de Servicios de Infraestructura Tecnológica.
* **UPS:** Fuentes ininterrumplibles de energía.
* **Usuario:** Persona que utiliza los servicios diarios.
* **VLAN:** Red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. ​
* **VPN:** (Virtual Private Network) es una conexión virtual segura usada para conectar la entidad con una red externa sin comprometer la seguridad de la información.

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

Garantizar el buen uso de los equipos de cómputo asignados por la entidad a los usuarios, para el desarrollo de sus funciones, así como el uso adecuado de la red de datos, dando a conocer a los usuarios los riesgos asociados a la utilización inadecuada de estos recursos tecnológicos, situación que puede comprometer la integridad y confidencialidad de la información de la entidad.

1. ****OBJETIVOS ESPECIFICOS****

* **Evitar los riesgos asociados al mal uso de los equipos de cómputo de la entidad.**
* **Evitar los riesgos asociados al mal uso de los equipos de la red de datos de la entidad.**
* **Proteger los activos de información de la entidad.**
* **Evitar la propagación de virus en la red de la entidad.**
* **Evitar ataques informáticos que pueden ocasionar la denegación de servicios.**

1. ****ALCANCE****

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

* El uso de los equipos de cómputo asignados por la entidad a los usuarios.
* El uso de la red de datos que dispone la entidad para la conexión de equipos de cómputo, servidores y dispositivos electrónicos que utilicen una conexión de red.

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 tengan asignados equipos de cómputo y que utilicen la red datos de la entidad.

Estas personas deberán preservar la confidencialidad de la información de la UAERMV, todos sin discriminación están sujetos a los mismos requerimientos de seguridad, y tienen las mismas responsabilidades de salvaguardar la información de la Unidad; por lo tanto, están obligadas a continuar protegiendo y cumpliendo 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.11.2 Equipos, A.13.1 Gestión de seguridad de redes, tomado de la norma ISO 27001:2013.

1. ****DECLARACIÓN****

En este documento se encuentran los lineamientos que aseguran una actuación adecuada para alcanzar un alto nivel en cuanto a 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*](http://es.wikipedia.org/wiki/International_Organization_for_Standardization) y la [Comisión Electrotécnica Internacional](http://es.wikipedia.org/wiki/Comisi%C3%B3n_Electrot%C3%A9cnica_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 operación de la UAERMV y ayudar en el cumplimiento de los objetivos misionales.

***6.1 Acuerdo de confidencialidad:***

Todos los Usuarios que administren, lean, 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 al personal ocasional y a los Usuarios externos no contemplados en un contrato formalizado.

1. ROLES Y RESPONSABILIDADES

**7.1 Encargado de seguridad de la información:** Persona delegada cuyas funciones principales son asesorar en materia de seguridad de la información a la UAEMRV y supervisar el cumplimiento de la presente Política.

**7.2 Usuarios de la información.** Personas que tienen 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 SOBRE EL USO DE EQUIPOS DE COMPUTO Y EL ACCESO A LA RED

**Controles para el uso de equipos de cómputo y acceso a la red:**

## 

1. Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
2. Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
3. Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
4. Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó.
5. Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.
6. Solo permite el uso de equipos de cómputo que sean de propiedad de la entidad o que estén en arriendo por medio de la entidad.
7. En caso de que algún funcionario utilice un computador personal en las instalaciones de la entidad, deberá ser autorizado por el líder del proceso, llevar el equipo a soporte técnico del proceso de GSIT para ser revisado.
8. Los equipos de cómputo que no sean asignados por la entidad que se vayan a utilizar en las instalaciones de la UAERMV, deben tener al menos un antivirus instalado, y se debe correr un proceso de ejecución del antivirus antes de conectarse a la red de la entidad.
9. El uso del equipo de cómputo será exclusivamente para realizar las actividades relacionadas con las funciones asignadas.
10. La instalación o reubicación del equipo al interior de una misma área, será realizada únicamente por personal del área de tecnología, y debe ser tramitado a través de la mesa de ayuda.
11. Los inventarios de los equipos de cómputo deben permanecer actualizados.
12. Cada equipo de cómputo deberá tener una cuenta de usuario y contraseña para el acceso al mismo, la cual únicamente será de conocimiento de la persona asignada y ésta no se deberá compartir con ninguna persona, (de acuerdo a la política de seguridad de gestión de contraseñas).
13. El equipo de cómputo (computadores, servidores) deberá estar conectado a un tomacorriente regulado (con protección de UPS). En las áreas que no cuenten con tomacorrientes de este tipo, el equipo deberá ser conectado a un regulador de voltaje adecuado a la carga del equipo.
14. Las impresoras siempre deberán estar conectadas a tomacorriente normal y protegidos con tierras físicas.
15. No se deben ingerir alimentos o bebidas cerca de los equipos de cómputo.
16. No se deben ingerir alimentos o bebidas en los centros de cableado.
17. Está prohibido conectar aparatos o equipos que no sean computadores a los tomacorrientes regulados y fuentes ininterrumplibles de energía (UPS).
18. Los equipos deben estar apagados antes de ser conectados o desconectados del tomacorriente, así como para efectuar cualquier mantenimiento, instalación o actualización física de los mismos.
19. Los equipos de cómputo deben tener un usuario y contraseña de administrador para la instalación de programas, la cual debe ser administrada por personal de soporte técnico.
20. No se debe realizar la instalación de programas no autorizados por el proceso de GSIT.
21. No se deben instalar programas no licenciados.
22. El uso de periféricos y medios de almacenamiento en los computadores de escritorio, computadores portátiles, y demás recursos informáticos de la entidad, debe ser restringido acorde con las funciones realizadas por los empleados.
23. Es responsabilidad de infraestructura tecnológica, mantener actualizados el sistema operativo y el software instalado en los computadores de escritorio, computadores portátiles y demás recursos informáticos de propiedad de la UAERMV, con el fin de prevenir problemas de seguridad informática relacionados con los mismos y que pongan en riesgo la disponibilidad y continuidad de los recursos informáticos.
24. Se recomienda la actualización del sistema operativo de los equipos de cómputo a través de un servidor de actualizaciones centralizado, y realizar la actualización en ambientes de pruebas contralados antes de ser replicados a los equipos de cómputo de la entidad.
25. El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.
26. La conexión a la red de los equipos que no son propios (portátiles, celulares, tablets, autorizados) de la entidad, se realizará por medio de conexión por wifi a una VLAN o red diferente a la red administrativa y se concederá el acceso a internet en el perfil bajo.
27. Los puertos de red de los puestos de trabajo no deben estar habilitados para conexión directa, se recomienda la configuración en los switches de acceso para que el puerto se habilite por la dirección MAC del equipo autorizado.
28. Se recomienda la asignación de direccionamiento IP a los dispositivos de red, a través del servidor de DHCP teniendo previamente la reserva por la dirección MAC de cada equipo.
29. Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
30. Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.
31. Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
32. Se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
33. Se prohíbe la instalación de cables, switches genéricos, derivaciones a través de conectores en “T” o cualquier tipo de derivación de datos por parte de los usuarios. Así mismo, no se permite la instalación de ningún servicio que intervenga directamente sobre el cableado de datos de la entidad. Sin excepción, las conexiones deberán ser realizadas por el personal autorizado de infraestructura tecnológica.
34. En caso de requerirse una conexión remota de algún funcionario de la entidad, se debe realizar a través de una VPN la cual debe ser solicitada previamente a través del líder del proceso.
35. Para conexiones remotas de empresas contratistas o proveedores de servicios tecnológicos de la entidad, se debe realizar a través de programas licenciados previa revisión de estos, siempre y cuando no afecten a seguridad de los activos de la UMV.

**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**  **Contratistas / Proceso EGTI** | Firma: | Firma: |
| **Acompañamiento EQUIPO TÉCNICO SIG:** |
| **ANDREA DEL PILAR ZAMBRANO**  **Contratista/ Proceso DESI** |
| **MARCELA ROCÍO MÁRQUEZ ARENAS**  **(Secretaría 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 seguridad sobre el uso de los equipos de cómputo y el acceso a la red 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 sobre el uso de los equipos de cómputo y el acceso a la red. | Mayo 2019 | Jefe Oficina Asesora de Planeación |