

**POLÍTICA DE SEGURIDAD DE ESCRITORIO LIMPIO Y BLOQUEO DE PANTALLAS**

**Bogotá, D.C.,**

**(ABRIL DE 2019)**

###

**CONTENIDO**

[1. INTRODUCCIÓN 3](#_Toc532282809)

[2. GLOSARIO DE TERMINOS 3](#_Toc532282810)

[3. OBJETIVO GENERAL 4](#_Toc532282811)

[4. OBJETIVOS ESPECIFICOS 4](#_Toc532282812)

[5. ALCANCE 4](#_Toc532282818)

[6. DECLARACION 5](#_Toc532282819)

[7. ROLES Y RESPONSABILIDADES 5](#_Toc532282824)

[8. POLITICA DE ESCRITORIO LIMPIO Y BLOQUEO DE PANTALLA 5](#_Toc532282827)

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, en las políticas contenidas en este documento; así mismo, como las buenas prácticas y herramientas informáticas que apoyen el proceso de apoyo: “Gestión de Servicios de Infraestructura Tecnológica” (GSIT).

Estos lineamientos definen las medidas preventivas de protección y las buenas prácticas, con respecto de las estaciones de trabajo y escritorios de todos los funcionarios, colaboradores y contratistas que desarrollan sus actividades en las instalaciones de la entidad.

La finalidad de esta política es proteger los documentos de la Entidad, tanto los físicos como los digitales, y todo tipo de almacenamiento, al reducir los riesgos de acceso no autorizado a la información, y la pérdida y/o daño de la misma. Este documento se basa en las buenas prácticas que permiten mantener el orden y la limpieza en el puesto de trabajo. Es una política de responsabilidad compartida entre el colaborador y la Entidad.

1. ****GLOSARIO DE TERMINOS****
* **Encargado de Seguridad:** 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.
* **Información sensible:** La información privada o sensible es el nombre que recibe la información critica en una entidad, por ejemplo ciertos datos personales y bancarios, [contraseñas](https://es.wikipedia.org/wiki/Autenticaci%C3%B3n_con_contrase%C3%B1a_de_un_solo_uso) de [correo electrónico](https://es.wikipedia.org/wiki/Correo_electr%C3%B3nico) e incluso el domicilio en algunos casos. Aunque lo más común es usar este término para designar datos privados relacionados con [Internet](https://es.wikipedia.org/wiki/Internet) o la informática, sobre todo [contraseñas](https://es.wikipedia.org/wiki/Contrase%C3%B1a), tanto de [correo electrónico](https://es.wikipedia.org/wiki/Correo_electr%C3%B3nico), [conexión a Internet](https://es.wikipedia.org/wiki/Conexi%C3%B3n_a_Internet), [IP privada](https://es.wikipedia.org/wiki/IP_privada), [sesiones](https://es.wikipedia.org/wiki/Sesi%C3%B3n) del PC, etc.
* **GSIT:** Gestión de Servicios de Infraestructura Tecnológica.
* **Tercero(s):** Cualquier persona natural o jurídica en calidad de proveedor, outsourcing o consultor.
* **TIC:** Tecnologías de la información y comunicaciones.
* **UAERMV:** Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial.
* **USB:** El Universal Serial Bus (USB) (bus universal en serie BUS) es un estándar industrial desarrollado en los años 1990 que define los cables, conectores y protocolos usados en un bus para conectar, comunicar y proveer de alimentación eléctrica entre ordenadores y periféricos y dispositivos electrónicos.
* **Usuario:** Este concepto cobija a todos los clientes internos, servidores públicos y contratistas que utilicen la red de la entidad.
1. ****OBJETIVO GENERAL****

Establecer las reglas para reducir los riesgos de acceso no autorizado, daño o pérdida, o divulgación no autorizada de la información, en cada uno de los puestos de trabajo, equipos y servidores de computo que están en las instalaciones de la entidad, en términos de garantizar la **confidencialidad, integridad y disponibilidad de los activos de información**

1. ****OBJETIVOS ESPECIFICOS****
2. **Proteger la información de los equipos de cómputo de la entidad.**
3. **Proteger la información de los documentos que reposan en los puestos de trabajo de la entidad.**
4. **Proteger la información almacenada en los servidores de computo de la entidad.**
5. **Concientizar a los usuarios de los riesgos asociados al mal manejo de la información.**
6. **Asegurar que la información reciba un nivel apropiado de protección de acuerdo con la importancia y criticidad para la entidad.**
7. ****ALCANCE****

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 se les haya asignado un escritorio de trabajo, un equipo de cómputo y que tengan acceso a los recursos y activos de información durante su ciclo de vida (creación, distribución, transmisión, almacenamiento, eliminación), y a los activos de información en todas sus formas (digital, impresa, escrita, y hablada) y está orientada a preservar la confidencialidad y disponibilidad de la información de la UAERMV, los cuales 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 las políticas de confidencialidad durante y una vez terminada su relación laboral y/o contractual con la UAERMV.

Se tendrán en cuenta para esta política especifica los controles A.11.2.9 POLITICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA tomado 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 en cuanto a seguridad de la información en la UAERMV. La información es un activo importante para la entidad, tiene un alto valor para la misma, por esto mismo la unidad ha definido las directrices de seguridad para los Activos de Información por medio de las cuales se 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) es un estándar para la seguridad de la información publicado 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).

## Por 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 administran, leen, modifican o crean 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

## ****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.

## 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, lo que incluye el resguardo de sus artículos personales.

1. POLITICA DE ESCRITORIO LIMPIO Y BLOQUEO DE PANTALLA

Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles (memorias USB, SD, micro SD, Discos duros externos, CD, DVD…), y una política de pantalla limpia en las instalaciones de la entidad donde se realicen procesos de información.

##

## Sobre el Escritorio Limpio durante la jornada laboral:

## Es responsabilidad de cada Usuario la protección de los sistemas de información a su cargo; con el fin de minimizar la exposición de la información sensible; los sistemas de información y elementos de procesamiento deberán tomar las medidas pertinentes para proteger la información, los datos, y los sistemas de información. Estas medidas se nombran a continuación:

1. Guardar documentos críticos, Tablet, celulares/móviles, portátiles en los cajones bajo llave, cuando no los estén utilizando.
2. Asegurar físicamente los computadores portátiles con cables de seguridad para evitar robos.
3. No publicar o dejar a la vista, documentos o datos críticos para la entidad, como: nombres de usuario, contraseñas, direcciones IP, contratos, números de cuentas, listas de clientes, archivos de propiedad intelectual, datos personales de los funcionarios Públicos y/o cualquier información importante para la UAERMV que no se desea publicar.
4. De haber ausencias de su lugar de trabajo, por tiempo prolongado, se debe asegurar que la información usada quede fuera del alcance de terceras personas.
5. Está prohibido tener sustancias o líquidos en el escritorio, ya que estos pueden dañar los equipos, así como la documentación.
6. Todos los equipos deberán tener una protección contra accesos no autorizados.
7. No dejar dispositivos de respaldo de información, como USB, discos duros externos, CD, DVD, etc, para el fácil acceso de cualquier persona.
8. No escribir contraseñas ni otros datos sensibles en papeles o documentos que queden a la vista.
9. El usuario es responsable de cerrar su sesión de trabajo y dejar el equipo bloqueado, cuando deje de usarlo por tiempo prolongado.
10. Desde el momento en que el usuario firma el acta de asignación de un equipo, la responsabilidad sobre el estado del equipo es completamente del usuario.
11. El usuario no tiene permitido hacer manipulación (traslados, desconexiones.) de las estaciones de trabajo, con excepción de los computadores nformació asignado para el desarrollo de sus funciones.
12. La estación de trabajo y equipos que están asignados a los usuarios, son activos de la entidad, por lo mismo el usuario no es dueño de mencionado activo.

## Sobre el escritorio limpio después de la jornada laboral: Los Usuarios de la UAERMV deberán:

1. Tomarse el tiempo necesario antes de abandonar la oficina para recoger y asegurar el material sensible, que pueda ser objeto de pérdida o robo.
2. Cerrar bajo llave gabinetes, cajones y oficinas.
3. Asegurar equipos costosos o medios de almacenamiento de información removible: Portátiles, Memorias micro SD, SD, Tablet Memorias USB entre otros

## Sobre el equipo de cómputo:

1. Cada Usuario de la UAERMV deberá bloquear la sesión al alejarse de su computador, aunque sea por poco tiempo, para prevenir el riesgo de la utilización y acceso a los sistemas de nformación de usuarios no autorizados o sin los privilegios requeridos y asi evitar exponer la información de la Unidad.
2. El escritorio del equipo de cómputo no debe tener información sensible o confidencial que pueda ser de fácil acceso, así como tener organizada la información que repose en el mismo.
3. Los usuarios de la entidad que utilicen conexión por escritorio remoto a servidores de computo de la entidad, deberán cerrar la sesión inmediatamente se deje de utilizar, cada vez que se realice la conexión deberá pedir las credenciales de acceso (Usuario y contraseña).
4. Se debe configurar en todos los equipos de la entidad un protector de pantalla institucional, que deberá activarse en el menor tiempo razonable de no uso del equipo.
5. El usuario, debe preocuparse por mantener su equipo en buenas condiciones de limpieza externa.
6. No está permitido pegar autoadhesivos ni figuras en las pantallas.

**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 POLITICA SEGURIDAD DE ESCRITORIO LIMPIO Y BLOQUEO DE PANTALLAS 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 POLITICA DE SEGURIDAD DE ESCRITORIO LIMPIO Y BLOQUEO DE PANTALLAS. | Diciembre 2018 | Jefe Oficina Asesora de Planeación |
| 2  | Se realizó actualización del documento conforme al nuevo mapa de procesos de la entidad.  | Abril de 2019 | Jefe Oficina Asesora de Planeación |