******

POLÍTICA DE SEGURIDAD PARA LA GESTION DE CONTRASEÑAS

**Bogotá, D.C.,**

**(ABRIL DE 2019)**

**CONTENIDO**

[1. INTRODUCCIÓN 3](#_Toc529806932)

[2. GLOSARIO DE TERMINOS 4](#_Toc529806933)

[3. OBJETIVO GENERAL 4](#_Toc529806936)

[4. OBJETIVOS ESPECIFICOS 5](#_Toc529806937)

[5. ALCANCE 5](#_Toc529806941)

[6. DECLARACION 5](#_Toc529806942)

[7. ROLES Y RESPONSABILIDADES 6](#_Toc529806947)

[8. POLÍTICA DE SEGURIDAD PARA LA GESTION DE CONTRASEÑAS 6](#_Toc529806950)

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).

El tratamiento diario de la información de la entidad requiere el acceso a distintos servicios, dispositivos y aplicaciones por parte de los usuarios, para los cuales utilizamos las credenciales de acceso compuesta por un usuario y una contraseña. Por la seguridad de los servicios y sistemas en los que existen cuentas de usuarios para la autenticación, tenemos que garantizar que las credenciales de autenticación se generan, actualicen y revoquen de forma óptima y segura.

1. ****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.
* **Single Sign On (SSO):** Es un procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con una sola instancia de identificación. Su traducción literal sería algo como «autenticación única» o «validación única».
* **Usuario:** Persona que utiliza los servicios diarios.
1. ****OBJETIVO GENERAL****

Establecer, difundir y verificar el cumplimiento de buenas prácticas en el uso de contraseñas para los usuarios estándar y para los usuarios con privilegios de administrador de los diferentes sistemas de información.

1. ****OBJETIVOS ESPECIFICOS****
2. **Evitar el riesgo de perdida de las credenciales de acceso de los usuarios a los diferentes sistemas de información que lo requieran.**
3. **Evitar el riesgo asociado a la ausencia de un administrador con privilegios a los sistemas de información, bases de datos, aplicativos, elementos de infraestructura tecnológica.**
4. **Garantizar la disponibilidad, confidencialidad e integridad de los activos de información de la entidad minimizando el riesgo que se pueda generar por la fuga o perdida de alguna credencial de acceso.**
5. ****ALCANCE****

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

1. Acceso a alguno de los siguientes sistemas:
	* Bases de datos.
	* Aplicativos.
	* Sistemas de información.
	* Elementos de infraestructura tecnológica (Firewall, Router, Switch…).
	* Equipos de computo.

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 asignado un usuario y contraseña para el ingreso a algunos de los sistemas de información, bases de datos, equipos de computo o aplicativos que soliciten la autenticación. Estos deberán preservar la confidencialidad 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; así como están obligados a continuar protegiendo y cumpliendo los acuerdos de confidencialidad durante y una vez terminada su relación laboral y/o contractual con la UAERMV.

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, 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.

1. POLÍTICA DE SEGURIDAD PARA LA GESTION DE CONTRASEÑAS

1. El administrador de cada sistema de información es responsable de asegurar que se solicite las credenciales de acceso (usuario y contraseña) para permitir el acceso.
2. El administrador de cada sistema es responsable de asegurar que el mismo solicite cambio de contraseña cada vez que esta es reestablecida manualmente a un usuario.
3. El colaborador es responsable de asegurar la privacidad de las contraseñas asignadas para acceder a los sistemas de información.
4. Las credenciales de acceso para los diferentes sistemas de información son personal e intransferible.
5. El administrador de cada sistema es responsable de asegurar que las contraseñas que se transmitan a través de redes públicas, estén protegidas contra acceso no autorizado mientras se encuentren en tránsito.
6. El usuario de los sistemas de información es responsable de establecer una contraseña segura, que cumpla con las siguientes características:
	1. La longitud de la contraseña debe ser mínimo de 8 caracteres, entre mas caracteres tenga la contraseña es mas difícil de descifrar por algún delincuente informático (hacker.)
	2. Las aplicaciones en las cuales la tecnología utilizada no contemple una longitud mínima de ocho caracteres, la longitud mínima deberá ser la máxima contemplado por el sistema.
	3. La contraseña debe estar compuesta por una combinación de letras Mayúsculas, minúsculas, caracteres numéricos y símbolos especiales como los siguientes: ` ~ ! @ # $ % ^ & \* ( ) \_ + - = { } | [ ] \ : " ; ' < > ? , . /.
	4. Hay que evitar utilizar secuencias básicas de teclado (por ejemplo: ”qwerty”, “asdf” o las típicas en numeración: “1234” ó “98765”)
	5. No repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).
	6. No enviar nunca la contraseña por correo electrónico o en un sms. Tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo.
	7. No deben usarse palabras o nombres comunes que aparezcan en los diccionarios.
	8. No debe haber una relación obvia con el usuario, sus familiares, nombre de la entidad, abreviaciones relacionadas a la entidad, ciudad, país, año, fecha de nacimiento, el grupo de trabajo u otras asociaciones parecidas, ya que pueden ser identificadas de manera fácil a través de un ataque de ingeniería social.
	9. Debe ser cambiada con una periodicidad de mínima de 60 días.
	10. El administrador del sistema debe utilizar contraseñas diferentes como usuario y como administrador.
	11. Si hay indicios para creer que una contraseña ha sido comprometida, debe cambiarse inmediatamente.
	12. No deben usarse contraseñas que sean idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que sea posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores, esto se debe gestionar desde el sistema que asigne las credenciales.
	13. Es responsabilidad del administrador de cada sistema establecer los mecanismos para que la contraseña asignada al usuario le sea transmitida de la manera más confidencial posible.
	14. No se debe escribir la contraseña en papeles y dejarla en sitios donde pueda ser encontrada por terceros.
	15. No se debe almacenar la contraseña en la computadora. Algunos cuadros de diálogo o ventanas emergentes de los navegadores presentan una opción para guardar o recordar la contraseña; no debe seleccionarse esa opción.
	16. Las aplicaciones deben almacenar las contraseñas en forma cifrada.
	17. Las contraseñas predefinidas que traen los equipos y aplicaciones, deben cambiarse inmediatamente al ponerse en operación.
	18. Las contraseñas deben cambiarse cuando una persona que tiene acceso a cuentas privilegiadas compartidas, ya no hace parte de la entidad como colaborador.
	19. Las credenciales asociadas a un usuario que se encuentre en vacaciones deberán ser inactivadas durante el periodo de vacaciones del colaborador.
7. En caso de utilizar autenticación SSO (Single Sign On), para dos o mas sistemas de información como es el caso del acceso al equipo de computo y el paquete de office 365 (Outlook, correo, skype..), las contraseñas deben cumplir los numerales mencionados con anterioridad.
8. Para los administradores de los sistemas de información, aplicaciones, equipos de infraestructura tecnológica, bases de datos se recomienda la creación de un usuario alterno o de contingencia con los privilegios mínimos de administración.
9. Las credenciales de acceso deberán ser almacenadas en un sobre sellado entregado al director de tecnología o cargo equivalente en la entidad y ser almacenadas en una caja fuerte.
10. En caso de que algún administrador mencionado en el numeral 7 no se encuentre en la entidad y se requiera realizar alguna configuración urgente, se tendrá acceso al sobre y se realizara la configuración requerida por otra persona con los conocimientos mínimos en el tema.
11. Una vez se abra el sobre y realice la configuración requerida el administrador principal debe realizar el cambio de la contraseña y ser entregado de nuevo como se menciono en el numeral 9.
12. Cada vez que se realicen los cambios de las credenciales de acceso de las bases de datos, sistemas de información o aplicativos, elementos de infraestructura tecnológica, deben ser entregadas como se menciona en el numeral 9.
13. El usuario es responsable de bloquear su equipo en el momento en que se retire de su puesto de trabajo a una zona donde pierda visibilidad de este.

**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:** |
| **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 | Elaborada por el Ing. Omar Fdo. Garzón Giraldo (especialista en seguridad de la información), se realizó el documento de Política de seguridad para la gestión de contraseñas que hace parte de la POLITICA GENERAL DE TECNOLOGIA Y SEGURIDAD DE LA INFORMACION Y COMUNICACIONES. | Diciembre 2018 | Jefe Oficina Asesora de Planeación |
| 2 | Se realiza recodificación del documento, según el nuevo mapa de procesos de la entidad.  | Abril de 2019 | Jefe Oficina Asesora de Planeación |