

**POLÍTICA DE RESPONSABILIDADES PARA EL BUEN USO DEL CORREO ELECTRÓNICO INSTITUCIONAL**

**Bogotá, D.C.,**

**(MAYO DE 2019)**

**CONTENIDO**

[1. INTRODUCCIÓN 3](#_Toc8995867)

[2. GLOSARIO DE TÉRMINOS 3](#_Toc8995868)

[3. OBJETIVO GENERAL 4](#_Toc8995869)

[4. OBJETIVOS ESPECIFICOS 4](#_Toc8995870)

[5. ALCANCE 4](#_Toc8995871)

[6. DECLARACIÓN 4](#_Toc8995872)

[7. ROLES Y RESPONSABILIDADES 5](#_Toc8995873)

[8. POLÍTICA DE SEGURIDAD PARA EL BUEN USO DEL CORREO ELECTRONICO INSTITUCIONAL. 5](#_Toc8995874)

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 Administración de la Seguridad de los Activos de Información y las buenas prácticas en las herramientas informáticas del proceso de apoyo “Gestión de Servicios de Infraestructura Tecnológica” (GSIT), en las políticas contenidas en este documento.

El Correo Electrónico es una herramienta Tecnológica proporcionada por la Entidad, con el propósito de apoyar el desarrollo de las actividades de los colaboradores en sus actividades de comunicación. El uso inapropiado de este recurso Tecnológico expone a la organización a riesgos tales como ataque de virus, compromiso de la red y sistemas de información e incluso peligros de índole jurídico a nivel nacional o internacional como consecuencia de una inadecuada comunicación. Estas directrices y recomendaciones buscan garantizar que el correo electrónico sea utilizado de forma racional, promoviendo una comunicación adecuada y efectiva, proporcionando a los usuarios una guía que describa sus responsabilidades relacionadas con la confidencialidad, privacidad y uso correcto de este servicio. Es responsabilidad de cada usuario conocer y aplicar las recomendaciones descritas aquí.

1. ****GLOSARIO DE TÉRMINOS****

* **Correo Masivo:** Envió de notificaciones de correo electrónico a toda la entidad.
* **Disponibilidad:** Capacidad de un componente o servicio para realizar su función requerida durante un período de tiempo.
* **EGTI:** Proceso de Estrategia de Gobierno de Tecnología de Información.
* **GSIT:** Proceso de Gestión de Servicios de Infraestructura Tecnológica.
* **Insidioso:** Que contiene un engaño oculto o disimulado para perjudicar a alguien.
* **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.
* **OAP**: Proceso de Oficina asesora de planeación.
* **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.

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

Garantizar el buen uso del correo electrónico y dar a conocer a los usuarios los riesgos asociados a la utilización inadecuada de este servicio, situación que puede comprometer la integridad y confidencialidad de la información.

1. ****OBJETIVOS ESPECIFICOS****
2. **Evitar el riesgo de la instalación de software nocivo en los equipos de cómputo de la entidad que los puedan infectar con algún tipo de virus y que puedan ser recibidos a través del correo electrónico.**
3. Usar el correo electrónico institucional con fines pertinentes a las funciones asignadas a cada funcionario.
4. ****ALCANCE****

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

1. El acceso a las cuentas de correo electrónico institucionales desde las instalaciones de la entidad y desde equipos de cómputo por fuera de la entidad.

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 asignada una cuenta de correo electrónico institucional. 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.13.2.3 Controles en la mensajería electrónica, 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 UAERMV y ayudar en el cumplimiento de los objetivos misionales.

***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 DE SEGURIDAD PARA EL BUEN USO DEL CORREO ELECTRONICO INSTITUCIONAL.

**Controles mensajería electrónica:**

Se debe proteger adecuadamente la información incluida en la mensajería electrónica.

## 

1. Cada funcionario tendrá asignada una credencial de acceso conformada por un usuario y una clave asignada por el GSIT a través de los procedimientos establecidos.
2. El correo electrónico debe ser utilizado exclusivamente para fines laborales: para la difusión o el envío de circulares, memorandos, oficios y archivos de trabajo, cuando sea necesario en cumplimiento de las funciones asignadas.
3. El contenido de un mensaje de correo electrónico debe ser serio, claro, conciso, cortés y respetuoso. No se deben utilizar expresiones difamatorias o groseras en contra de personas, entidades públicas o privadas.
4. Los mensajes enviados a través del servicio de correo electrónico no deben contener material insidioso, ofensivo, obsceno, vulgar, racista, pornográfico, subversivo u otro material no-formal.
5. La información propia de la entidad que sea clasificada como información sensible o confidencial no debe ser enviada por medio de canales no seguros (no cifrados) como es Internet y/o las cuentas de correo de uso público (Gmail, Hotmail, Yahoo, etc.).
6. No se debe participar en la difusión de “cartas en cadenas”, en esquemas piramidales o de propagandas dentro y fuera de la institución.
7. No se deben realizar intentos no autorizados para acceder a una cuenta de correo electrónico de otro usuario.
8. No se debe descargar, enviar, imprimir o copiar documentos o contenidos en contra de las leyes de derechos de autor.
9. No se debe descargar software o archivos sin tomar las medidas de precaución para evitar el acceso de virus en el equipo y la red de la entidad.
10. Está prohibido el envío de correos SPAM (correo basura, correo no solicitado) de cualquier clase.
11. No se debe utilizar el correo electrónico para propósitos comerciales diferentes a los de la entidad.
12. No se deben utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del emisor de correo.
13. Se recomienda el uso del campo CCO: para mantener la privacidad de los correos electrónicos de los destinatarios. Este campo hace que los destinatarios reciban el mensaje sin aparecer en ninguna lista ni ser visibles a los demás.
14. No se permite enviar archivos con extensión .exe, .pif, .scr, .vbs, .cmd, .com, .bat, .hta, .dll debido a que este tipo de extensiones son propensas a ser utilizadas para propagación de virus. Este tipo de archivos serán eliminados automáticamente por el sistema de correo.
15. No se permite enviar contenidos multimedia (video o audio) con extensión .wav, .mp3, .mpge, .wma, .mov, .asf, .flv ya que estos documentos son muy pesados y ralentizan la red de comunicaciones. Igualmente, este tipo de archivos serán eliminados automáticamente.
16. Se recomienda comprimir los archivos a enviar a través del servicio de correo, para disminuir las exigencias técnicas en su transmisión.
17. El servidor de correo electrónico de la entidad debe contar con el filtrado de correo catalogado como SPAM o no deseado.
18. Se aplicarán políticas de filtrado de mensajes para evitar en la medida de lo posible la llegada de correo no deseado (SPAM) a los buzones de los usuarios.
19. Un mensaje no se aceptará cuando provenga de un servidor identificado como fuente de SPAM o como un servidor no válido para el envío de correo electrónico por alguna de las listas de bloqueo.
20. Se aplicarán políticas de filtrado de mensajes entrantes y salientes, rechazando el envío/recepción de mensajes que contengan virus. Cuando un mensaje es rechazado se envía una notificación al destinatario del mensaje, salvo en el caso de virus que falsifique el emisor del mensaje.
21. Un archivo adjunto se eliminará cuando, a través de los procesos automáticos de evaluación o revisión, sea identificado como portador de virus o cualquier otra amenaza para el destinatario, comunicándole al mismo este hecho mediante un mensaje al pie del correo electrónico.
22. Cada funcionario es responsable de conocer, adoptar y acatar esta política para el uso del servicio.
23. Cada colaborador es responsable de velar por el contenido de los correos electrónicos que se envíen a través de su cuenta.
24. El uso no autorizado de una cuenta de correo electrónico es ilegal y constituye una violación de esta política.
25. El colaborador debe usar correctamente sus credenciales de ingreso (usuario y clave). La cuenta de correo institucional es personal e intransferible, por lo que no debe proporcionarse a otros usuarios.
26. El colaborador debe cerrar totalmente su sesión de lectura y envío de correos para evitar la suplantación de identidad, cuando se retire del equipo en que se encuentre configurada la cuenta de correo.
27. El colaborador debe dar aviso al proceso de GSIT, a través de la mesa de ayuda o llamada telefónica, de cualquier fallo de seguridad en su cuenta de correo, incluyendo su uso no autorizado, pérdida de la contraseña, suplantación, etc.
28. Todo propietario de una cuenta de correo electrónico institucional de la entidad es responsable por la información o contenido que sea transmitido a través de ésta.
29. El uso inapropiado o el abuso en el servicio de correo electrónico pueden ocasionar la desactivación temporal o permanente de las cuentas.
30. La desactivación de la cuenta lleva consigo la imposibilidad de acceder a los mensajes de correo que estén en ese momento en el servidor y la imposibilidad de recibir nuevos mientras no vuelva a ser activada.
31. Cuando se accede a un correo electrónico desde un equipo por fuera de la entidad, no se debe hacer uso de la opción de guardar la contraseña cuando se utilicen computadores de uso compartido.
32. Cuando se accede a un correo electrónico desde un equipo por fuera de la entidad se debe borrar el historial de navegación y cerrar la sesión al terminar, siempre que se utilice un computador de uso compartido, para acceder al correo vía web.
33. Si se configura el correo electrónico en un dispositivo móvil se debe utilizar usuario y contraseña para bloquear el mismo, adicional tener instalado una herramienta de antivirus.
34. La creación de cuentas de correo debe ser solicitada por el proceso Gestión del Talento Humano de la entidad.
35. Cuando un funcionario se desvincule de la entidad, es responsabilidad del proceso Gestión del Talento Humano realizar la debida notificación al proceso de GSIT para inhabilitar el usuario y realizar la debida copia de seguridad de la información del correo electrónico.
36. Cuando un funcionario se encuentre en su periodo de vacaciones, las credenciales de la cuenta de correo electrónico deberán ser cambiadas, se debe configurar un reenvió a otra cuenta activa para que reciba y de respuesta a los posibles mensajes que lleguen a la cuenta del funcionario que se encuentra en vacaciones, de igual manera se debe configurar la respuesta automática notificando sobre la ausencia durante dicho periodo.

**PARAGRAFO: ENVÍO DE CORREOS MASIVOS**

Esta prohibido 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 asignada una cuenta de correo electrónico institucional, enviar correos masivos; las únicas dependencias autorizadas para enviar correos masivos a todos los procesos son: La Dirección General, la Oficina Asesora de Planeación a través de su proceso: Atención a Partes Interesadas y Comunicaciones, y la Secretaria General a través de su procesos Gestión de Servicios e Infraestructura Tecnológica y de Gestión del Talento humano.

**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 EGTI** | Firma: | Firma: |
| **Acompañamiento EQUIPO TÉCNICO SIG:** |
| **CHRISTIAN MEDINA FANDIÑO/**  **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 para el buen uso del correo electrónico institucional 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 para el buen uso del correo electrónico institucional. | Diciembre 2018 | Jefe Oficina Asesora de Planeación |
| 2 | Se realiza actualización del documento conforme al nuevo mapa de procesos. | Abril de 2019 | Jefe Oficina Asesora de Planeación |
| 3 | Revisado y actualizado por el Ing. Omar Fdo. Garzón Giraldo (Especialista en Seguridad de la Información), se cambia el orden del glosario de términos, se agregan políticas sobre él envió de correos masivos, inactivación y solicitud de cuentas por parte del proceso de Gestión del Talento Humano. | Mayo 2019 | Jefe Oficina Asesora de Planeación |