ALCALDÍA MAYOR DE BOGOTÁ D.C.
MOVILIDAD
Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial

FORMATO DE APROBACIÓN DOCUMENTAL

CÓDIGO: SIG-FM-002 | **VERSIÓN: 9**

FECHA DE APLICACIÓN: JUNIO 2018

INFORMACIÓN DOCUMENTADA:		CÓDIGO:		VERSIÓN:		JUSTIFICACIÓN:		
TIPO	NOMBRE	ANTERIOR	VIGENTE	ANTERIOR	VIGENTE	ELABORA	ACTUALIZA	ANULA
Documento Interno	Políticas de escritorio limpio y bloqueo de pantallas	N/A	GSIT-DI-003	N/A	1	X		
Documento Interno	Política de buen uso de correo institucional	N/A	GSIT-DI-005	N/A	1	X		

DESCRIPCIÓN DE LA JUSTIFICACIÓN:

Se crean estos documentos internos de las Políticas de escritorio limpio y bloqueo de pantallas y Política de buen uso de correo institucional en el marco de la Política General de Tecnología y Seguridad de la Información y Comunicaciones. A cada uno de ellos se les describió en la casilla de control de cambios los ajustes realizados.

AVALA: RESPONSABLE DIRECTIVO SIG	ELABORA/ACTUALIZA/ANULA: *(Colaborador del proceso en compañía del enlace)*	ACOMPAÑAMIENTO: EQUIPO TÉCNICO SIG
(Firma)	*(Firma)*	*(Firma)*
Nombre: Marcela Rocío Márquez Arenas	*Nombre: Omar Garzón/Gloria Méndez*	*Nombre: Andrea Zambrano/Christian Medina*
Cargo: Secretaria General	*Cargo: Contratistas GSIT*	*Cargo: Contratistas DESI*

TRÁMITE DE APROBACIÓN DOCUMENTAL (DILIGENCIADO POR LA OFICINA ASESORA DE PLANEACIÓN)	¿ES APROBADO?	FECHA DE APROBACIÓN:	RESPONSABLE DEL SISTEMA DE GESTIÓN DE CALIDAD
	SI [X] NO [ ]	18-12-018	*(Firma)*
	OBSERVACIONES:		*Martha Patricia Aguilar Copete*
			REPRESENTANTE DE LA ALTA DIRECCIÓN PARA EL SIG

POLÍTICA DE SEGURIDAD DE ESCRITORIO LIMPIO Y BLOQUEO DE PANTALLAS

ALCALDÍA MAYOR DE BOGOTÁ D.C.

MOVILIDAD

Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial

Bogotá, D.C.,
(DICIEMBRE DE 2018)

CONTENIDO

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.

2. 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 de correo electrónico e incluso el domicilio en algunos casos. Aunque lo más común es usar este término para designar datos privados relacionados con Internet o la informática, sobre todo contraseñas, tanto de correo electrónico, conexión a Internet, IP privada, sesiones 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.

3. 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

4. OBJETIVOS ESPECIFICOS

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

5. 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.

6. 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* y la Comisión Electrotécnica 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.

7. 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 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.

8. 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.

8.1. 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 portatiles 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.

8.2. 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

8.3. 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 informacion 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		
Acompañamiento EQUIPO TÉCNICO SIG:	Firma:	Firma:
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

POLÍTICA DE RESPONSABILIDADES PARA EL BUEN USO DEL CORREO ELECTRÓNICO INSTITUCIONAL

ALCALDÍA MAYOR DE BOGOTÁ D.C.

MOVILIDAD

Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial

Bogotá, D.C.,
(DICIEMBRE DE 2018)

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El siguiente documento hace parte de la POLITICA GENERAL DE TECNOLOGÍA 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 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.

2. 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.

3. OBJETIVOS ESPECIFICOS

a) 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.

b) 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:

a) 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.

5. 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* 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, 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.

6. ROLES Y RESPONSABILIDADES

6.1 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.

6.2 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.

7. 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 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 los mismos, adicional tener instalado una herramienta de antivirus.

8. GLOSARIO DE TÉRMINOS

- **Disponibilidad:** Capacidad de un componente o servicio para realizar su función requerida durante un periodo de tiempo.
- **GSIT:** Proceso de 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		
Acompañamiento EQUIPO TÉCNICO SIG:	Firma:	Firma:
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 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