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

FORMATO DE APROBACIÓN DOCUMENTAL

CÓDIGO: DESI-FM-008 | **VERSIÓN: 10**

FECHA DE APLICACIÓN: ENERO 2019

INFORMACIÓN DOCUMENTADA:		CÓDIGO:		VERSIÓN:		JUSTIFICACIÓN:		
TIPO	NOMBRE	ANTERIOR	VIGENTE	ANTERIOR	VIGENTE	ELABORA	ACTUALIZA	ANULA
Plan	Plan de seguridad y privacidad de la información.		EGTI-PL-001		1	X		
Plan	Plan de Tratamiento Riesgos		EGTI-PL-002		1	X		
Política	Políticas Generales De Tecnología Y Seguridad De La Información Y Comunicaciones	SIT-DI-001	EGTI-DI-001	2	3		X	

DESCRIPCIÓN DE LA JUSTIFICACIÓN:

Se realiza la actualización de Políticas Generales de Tecnología Y Seguridad de la Información y Comunicaciones, en donde se ajustó: introducción, el objetivo general, objetivos específicos y modificación del alcance, conforme a los lineamientos establecidos por MINTIC y la ISO 27001. Así mismo, se Realizaron los planes Plan de seguridad y privacidad de la información y Plan de Tratamiento Riesgos, conforme a lo estipulado por el MIPG.

AVALA: RESPONSABLE DIRECTIVO SIG	ELABORA/ACTUALIZA/ANULA: *(Colaborador del proceso en compañía del enlace)*	ACOMPAÑAMIENTO: EQUIPO TÉCNICO SIG
(Firma)	*(Firma)* Gloria Mendez	*(Firma)* Andrea del P. Zambrano B
Nombre: Marcela Rocío Márquez Arenas	*Nombre: Gloria Méndez/Omar Garzón*	*Nombre: Andrea del Pilar Zambrano Barrios*
Cargo: Secretaria General	*Cargo: Contratistas Procesos EGTI y GSIT*	*Cargo: Contratista OAP*

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 [ ]	13-02-2019	*(Firma)* Martha Patricia Aguilar Copete. *REPRESENTANTE DE LA ALTA DIRECCIÓN PARA EL SIG*
	OBSERVACIONES:		

ALCALDÍA MAYOR DE BOGOTÁ D.C.

MOVILIDAD

Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Bogotá, D.C.,
(FEBRERO DE 2019)

CONTENIDO

1. INTRODUCCIÓN

El presente documento corresponde al diagnóstico del estado actual de la seguridad de la información en la UNIDAD ADMINISTRATIVA ESPECIAL DE REHABILITACION Y MANTENIMIENTO VIAL (UAERMV). Para la evaluación se tiene como referencia las normas ISO 27001:2013, 27002, los lineamientos dados por MINTIC.

2. GLOSARIO DE TERMINOS

- **Análisis de brecha (GAP):** El GAP Análisis es un estudio preliminar que permite conocer la manera en la que se desempeña una empresa en **materia de seguridad de la información**, con relación a las mejores prácticas reconocidas en la industria, para esto se utilizan criterios establecidos en normas o estándares. El análisis establece las **diferencias entre el desempeño actual y el deseado**. Este análisis se puede aplicar a cualquier estándar certificable, lo normal es que se lleve a cabo para nuevos esquemas de certificación.
- **ISO 27001: ISO 27001** es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.
- **GAP:** Análisis de deficiencias, es un análisis que mide cómo una organización está llevando a cabo su desempeño con respecto a una serie de criterios establecidos en base a normas o procedimientos internos, controles seleccionados, las mejores prácticas de competencia, etc. El resultado de este análisis establece la diferencia entre el desempeño actual y el esperado, con un informe presentado con indicaciones sobre dónde están las deficiencias y "qué" falta para cumplir con cada requisito de la norma.
- **SOA:** Statement Of Applicability, en español DDA, documento de aplicabilidad.

3. OBJETIVO GENERAL

Verificar los alcances establecidos en el Modelo de Privacidad y Seguridad de la Información (MPSI) y la documentación base con la que cuenta la entidad para la implentacion de sun SGSI.

4. OBJETIVOS ESPECIFICOS.

- Identificar las orientaciones, directrices e instrumentos que le permiten a la UMV gestionar la seguridad de la información.
- Identificar los controles de seguridad de la información definidos en el anexo A de la norma ISO 27001:2013 que se aplican actualmente a la UMV.
- Identificar los controles y mecanismos de seguridad que utilizan actualmente los sistemas de información de la UMV.

- Identificar riesgos de seguridad asociados a los recursos tecnológicos a los que está expuesta la UMV.
- Describir los principales problemas de seguridad que presenta la entidad.
- Definir las medidas de seguridad más apropiadas a aplicarse.
- Definir políticas de seguridad encaminadas a minimizar los riesgos a los que está expuesta la información.
- Plantear un SGSI para la UMV bajo la norma ISO/IEC 27001 con el fin de garantizar confidencialidad, integridad y disponibilidad de la información.
- Implementar un SGSI para la UMV que permita proteger los activos de la entidad.
- Ser la guía que deben aplicar los usuarios para mantener un correcto uso de los recursos tecnológicos.
- Definir los lineamientos para ayudar a garantizar la seguridad de la información en la UAERMV.
- Lograr un adecuado nivel de confidencialidad, integridad, disponibilidad de la información que se produce o recibe en la entidad.
- Cumplir con los principios de seguridad de la información.
- Apoyar la innovación tecnológica.
- Proteger los activos de información, tecnológicos y de seguridad digital.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los servidores públicos, terceros, y demás usuarios externos de la UAERMV.
- Garantizar la continuidad del negocio frente a incidentes de seguridad.

5. ALCANCE

El presente documento describe el Plan de Seguridad y Privacidad de la entidad, alineado con los objetivos, metas, procesos, procedimientos y estructura organizacional, de tal forma que se asegure la confidencialidad, integridad y disponibilidad los componentes de información.

Se definen políticas y lineamientos con el propósito de cumplir con los objetivos de la institución en seguridad de la informacon y seguridad informática; y para ello se establecen:

- Políticas de seguridad: Para definir controles que proporcionan directivas y consejos de gestión para mejorar la seguridad de los activos de información.
- Políticas de navegación en internet: Establece la configuración de perfiles de navegación para optimizar el uso del canal de internet y reducir el riesgo de descarga de software nocivo.
- Políticas de tratamiento y manejo de datos personales: Establece los lineamientos para el manejo y tratamiento de los datos personales de acuerdo con la ley 1581 de 2012 de la SIC (Súper intendencia de industria y comercio).
- Políticas de seguridad de activos de información: establece controles para catalogar los activos y protegerlos eficazmente.

- Política de protección y respaldo de la información: Establece los lineamientos para garantizar las copias o respaldos de la información.
- Política del escritorio limpio y bloqueo de pantalla.: Establece los lineamientos para proteger los documentos ubicados en los escritorios y el bloqueo de los equipos de computo cuando el usuario no se encuentre en su puesto de trabajo.
- Política de seguridad para gestión de contraseñas: Establece los lineamientos para la gestión segura de las credenciales (usuario y contraseña) de los aplicativos y equipos de computo.
- Política de responsabilidades operacionales y control de cambios: Establece los lineamientos para cuando se requieren hacer cambios importantes en la infraestructura tecnológica o sistemas de información que pueden afectar la continuidad de la operación.
- Política de protección contra software nocivo: Establece los lineamientos para evitar la descarga, instalación y propagación de software nocivo (virus y sus variantes)
- Política de gestión de riesgos: Establece los lineamientos para la identificación y mitigación de los riesgos asociados a los activos de la entidad.
- Política para el buen uso del correo electrónico institucional: Establece los lineamientos para el uso eficiente y seguro del correo electrónico de la entidad.
- Política de registro histórico de actividades (log): Establece los lineamientos para almacenar los logs de los aplicativos críticos de la entidad, para en caso de presentarse un incidente de seguridad poder realizar un análisis forense.
- Política sobre el uso de equipos de computo y el acceso a la red: Establece los lineamientos para el buen uso de los equipos de computo de la entidad y la protección del acceso a la red lan o wifi de la entidad

6. METODOLOGÍA

Tomando como referencia la norma internacional ISO 27001:2013, 27002, los lineamientos del Ministerio de Tecnologías de Información y Comunicación (MINTIC), y la Alta Consejería, la unidad cuenta con el material suficiente para dar inicio a la implementación del SGSI.

7. PLAN PARA LA IMPLEMENTACION DEL SGSI EN LA ENTIDAD.

A continuación, se listan los HITOS definidos para la implementación del SGSI.

Tabla 1. Hitos implementación SGSI

Descripción	Actividad	Entregables
Hito Nº 1	Diagnóstico	• Diagnóstico de Seguridad de la Información. • Propuesta del Alcance del SGSI
Hito No 2	Establecimiento y Estructura del SGSI, Definición del Alcance	• Generación parcial de Políticas del SGSI. • Generación de formatos aplicables.

		• Inventario de activos. • Generación de SoA (documento de aplicabilidad) • Documentación básica inicial del SGSI. • Comunicación y socialización a los usuarios de la entidad.
Hito No 3	Gestión de Riesgos	• Matriz de Gestión de Riesgos. • Metodología de Gestión de Riesgos • Definición del Plan de Tratamiento de Riesgos. • Informe de Gestión de Riesgos. • Comunicación y socialización a los usuarios de la entidad.
Hito Nº 4	Implementación y Operación del SGSI	• Actualización de documentación vigente. • Informe de • Medición del SGSI. • Seguimiento del SGSI. • Políticas específicas del SGSI. • Seguimiento de los controles de seguridad de la información. • Manual del SGSI. • Medición, Métricas de procedimientos de seguridad. • Comunicación y socialización a los usuarios de la entidad.
Hito Nº 5	Monitorear y Revisar	• Informe de auditoría interna. • Planes de acción de auditoria del SGSI. • Mejora continua. • Acciones Correctivas, y de mejora.
Hito Nº 6	Mantener y Mejorar	• Implementar Mejoras. • Generar acciones correctivas.

		• Comunicación y socialización a los usuarios de la entidad.
Hito Nº 7	Acompañamiento en la Auditoria Externa (*)	• Preauditoria. • Cierre de hallazgos • Revisión, planes de acción, análisis y seguimiento a los hallazgos del Ente Certificador

Fuente: Proceso EGTI

8. DOMINIOS DE CONTROL

La norma ISO 27001:2013 en su anexo A tomado de la norma ISO 27002 nos habla de una serie:

- 14 dominios.
- 10 clausulas o capítulos.
- 114 controles.
- 35 objetivos de control.

Los lineamientos y buenas practicas para la implementación de los controles que apliquen a la entidad de acuerdo con los procesos y procedimientos establecidos para cada (proceso o dependencia de ésta), según MINTIC, la UMV para finales del año 2017 debe tener una calificación del 60% sobre 100% de acuerdo con los 14 dominios que menciona la norma.

Revisando los controles de seguridad que aplican a la entidad, ver tabla 4 (Dominios de control), la entidad obtuvo como calificación 6,57% del 60% que debería tener implementado de acuerdo a MINTIC para finales del año 2017, esto evidencia la brecha ente lo que se tiene y lo requerido, sin embargo la meta es cumplir el 100% de los controles de seguridad, alineados a la implementación del SGSI

Tabla 2. Dominios de control de la ISO 27001:2013

NOMBRE DOMINIOS DE CONTROL	RESULTADO	CALIFICACIÓN OBJETIVO
Políticas de seguridad de la información	10	60
Organización de la seguridad de la información	3	60
Seguridad de los recursos humanos	7	60
Gestión de activos	6	60
Control de acceso	14	60
Criptografía	0	60
Seguridad física y del entorno	23	60
Seguridad de las operaciones	9	60
Seguridad de las comunicaciones	9	60

Adquisición, desarrollo y mantenimiento de sistemas	0	60
Relación con los proveedores	0	60
Gestión de incidentes de seguridad de la información	0	60
Aspectos de la seguridad de la información de la gestión de la continuidad del negocio	0	60
Cumplimiento	9	60

Fuente: Proceso EGTI

9. DESARROLLO DE LAS POLITICAS

- Las estrategias en cuanto a seguridad de información de la UAEMRV son directrices de largo plazo, que sirven como base para la planeación adecuada y la definición de soluciones de seguridad para ajustarse a las necesidades de la entidad, tanto actuales como futuras.
- Las decisiones y disposiciones de seguridad de información estarán basadas en análisis de riesgos y métodos de evaluación.
- La seguridad de información considera revisiones continuas del valor para la institución de las medidas de seguridad en uso.
- La administración de la seguridad de información se desarrollará sobre lineamientos y guías dadas por las entidades del distrito como lo son el MINTIC, Alta Consejería, y otros.
- Las políticas de Seguridad deberán ser revisadas cada vez que se cumpla un ciclo de gestión de seguridad de la información.
- Las políticas de Seguridad deberán ser aprobadas por el(la) secretario(a) General de la entidad.

10. REFERENCIA NORMATIVA

- **Norma Técnica Colombiana NTC-ISO-IEC 27002:2015:** Norma técnica de seguridad. Código de practica para controles de seguridad de la información.
- **Decreto 1078 de 2015:** Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto No. 2573 de 2014:** establece como lineamiento la Seguridad y privacidad de la Información y comprende acciones transversales además de componentes enunciados, a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada.
- **Norma Técnica Colombiana NTC-ISO-IEC 27001:2013:** Norma técnica de sistemas de gestión de la seguridad de la información. Requisitos.
- **Decreto 1377 De 2013:** Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012. Añade dos nuevos capítulos al Código Penal Colombiano.

1. **Capitulo Primero:** De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos;
2. **Capitulo Segundo:** De los atentados informáticos y otras infracciones. Como se puede ver en el primer capitulo, esta Ley está muy ligada a la ISO27000, lo cual coloca al País a la vanguardia en legislación de seguridad de la información, abriendo así la posibilidad de nuevas entradas con este tema.

- **Articulo 230 de la ley 1450 de 2011:** Estableció que todas las Entidades deben adelantar acciones señaladas por el Gobierno Nacional, concernientes a implementar las estrategias de Gobierno en Línea que se definen por el Ministerio de Tecnologías de la Información y las comunicaciones.
- **Norma Técnica Colombiana NTC-ISO-IEC 31000:2018:** Norma técnica de gestión del riesgo. Principios directrices.
- **Ley 1341 del 30 de Julio de 2009:** Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
- **Ley 1273 DE 2009:** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado "de la protección de la información y los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Ley Estatutaria 1266 del 31 De diciembre de 2008:** Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales.
- **Ley 603 de 2000:** Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales. Ver esta ley.

11. IMPORTANCIA DE SU APLICACIÓN:

Este documento interno está orientado a brindar los lineamientos para:

- Proteger la información de la UAERMV ya sea dentro de las instalaciones o por fuera de ella.
- Garantizar el uso apropiado de los dispositivos tecnológicos (computadores de escritorio, portátiles, impresoras, tabletas, celulares de última generación, etc.) y de los servicios tecnológicos como el Internet, Correo Electrónico, pagina Web y demás aplicativos que pone a disposición la entidad para los funcionarios.
- Establecer pautas para la utilización eficiente y racional de los recursos tecnológicos.
- Minimizar los riesgos de que se materialice algún ataque informático o amenaza que pueda comprometer a la entidad en una eventual pérdida de información o indisponibilidad del servicio tecnológico.

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		
Acompañamiento EQUIPO TÉCNICO SIG:	Firma:	Firma:
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), versión inicial del documento conforme a los requerimientos de MINTIC.	Febrero 2019	Jefe Oficina Asesora de Planeación

ALCALDÍA MAYOR DE BOGOTÁ D.C.

MOVILIDAD

Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

Bogotá, D.C.,
(FEBRERO DE 2019)

CONTENIDO

1. INTRODUCCIÓN

La gestión integral de riesgos es un principio prioritario en la actuación de los colaboradores de la entidad.

La gestión de riesgos es la combinación de administrar el recurso humano, los procesos, los proyectos, las instalaciones y la implementación de mecanismos de prevención y mitigación de los riesgos identificados. Así mismo, la construcción de una cultura proactiva de conciencia y autocontrol frente al manejo del riesgo. Finalmente, la gestión integral de riesgos tiene como propósito reducir la probabilidad de ocurrencia y afectación en la continuidad de la operación de los procesos que utilicen los sistemas de información y la infraestructura tecnológica de la entidad.

El riesgo es un aspecto inseparable de los procesos y debe ser adecuadamente administrado y gestionado, siendo por ello necesario analizar y considerar la existencia de condiciones, situaciones o eventos que pueden desencadenarse y resultar en consecuencias negativas para la empresa, sus empleados, el medio ambiente, la comunidad o sus accionistas

2. GLOSARIO DE TERMINOS

- **Apetito de Riesgo (Tolerancia al Riesgo):** Es el nivel de riesgo que la entidad está dispuesta a tolerar para que no afecte el desarrollo de los objetivos estratégicos.
- **Control:** Medida que se toma para modificar la exposición al riesgo, bien sea para disminuir la probabilidad de ocurrencia del evento o para disminuir su impacto.
- **Disponibilidad:** Capacidad de un componente o servicio para realizar su función requerida durante un periodo de tiempo.
- **Gestión Integral de Riesgos:** Es el proceso de identificación, valoración y control de los riesgos que amenazan el logro de los objetivos de la entidad.
- **Identificación de riesgos:** Es el proceso de encontrar, reconocer y definir los escenarios de riesgo, sus causas y sus potenciales consecuencias.
- **Proceso:** Grupo de actividades relacionadas de manera lógica que, cuando se llevan a cabo, utilizan los recursos de la entidad para lograr resultados definitivos o transformar elementos de entrada, a través de una serie de actividades, en un producto o servicio.
- **Responsable del Riesgo:** Persona o entidad que tiene la responsabilidad y autoridad para gestionar el riesgo a través de la implementación de los planes de mitigación.
- **Riesgo:** El riesgo es el la exposición a una situación donde hay una posibilidad de sufrir un daño o de estar en peligro. Es esa vulnerabilidad y amenaza a que ocurra un evento y sus efectos sean negativos y que los activos puedan verse afectados por él.
- **Riesgo inherente:** Es el riesgo intrínseco de cada actividad, sin tener en cuenta los controles que de éste se hagan a su interior. Este riesgo surge de la exposición que se tenga a la actividad en particular y de la probabilidad que un impacto negativo afecte la rentabilidad, el capital de la compañía, y sus procesos.

- **Riesgo residual:** Es aquel riesgo que subsiste, después de haber implementado controles. Es importante advertir que el nivel de riesgo al que está sometido una entidad nunca puede erradicarse. Por ello, se debe buscar un equilibrio entre el nivel de recursos y mecanismos que es preciso dedicar para minimizar o mitigar estos riesgos y un cierto nivel de confianza que se puede considerar suficiente (nivel de riesgo aceptable). El riesgo residual puede verse como aquello que separa a la entidad de la seguridad absoluta.
- **Seguridad de la Información:** Conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.
- **Tratamiento del riesgo (Plan de Mitigación):** Selección y aplicación de medidas, con el fin de poder modificar la magnitud del riesgo, para evitar de este modo los daños intrínsecos de materializarse.
- **GSIT:** Gestión de Servicios de Infraestructura Tecnológica.
- **Impacto:** Es el resultado de la materialización de un evento.
- **Probabilidad:** Se refiere a la posibilidad de ocurrencia de un riesgo potencial.
- **Usuario:** Persona que utiliza los servicios diarios.

3. OBJETIVO GENERAL

Suministrar los lineamientos sobre las acciones que se deben adelantar al interior la entidad, encaminadas a establecer un plan de tratamiento de riesgos con el fin de disminuir la probabilidad de ocurrencia y el impacto de todas aquellas situaciones que puedan interferir con la continuidad de la operación de la infraestructura tecnológica y los sistemas de información que afecten el funcionamiento de los procesos de la entidad.

4. OBJETIVOS ESPECIFICOS

- Minimizar la materialización de los riesgos asociados infraestructura tecnológica y sistemas de información.
- Identificar las principales amenazas y vulnerabilidades a los que están expuestos los activos de información.
- 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 este documento da cubrimiento a:

a) Identificación de amenazas asociadas a los activos de información.
b) Identificación de vulnerabilidades asociadas a los activos de información.
c) Identificación del riesgo inherente.

d) Tratamiento del riesgo.
e) Aplicación de controles.

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 activos de información, deberán realizar la identificación de los riesgos inherentes de mencionados activos, así como aplicar los controles necesarios para minimizar el riesgo inherente.

6. 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* y la Comisión Electrotécnica Internacional. La versión más reciente es la ISO/IEC 27002:2013).

Por lo anterior, se busca minimizar los riesgos asociados a los activos de información, asegurar la continuidad de la UAERMV y ayudar en el cumplimiento de los objetivos misionales.

6.1. 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.

8. PLAN DE SEGURIDAD PARA LA GESTION DE RIESGOS.

Los riesgos de seguridad digital se basan en la afectación de 3 criterios en un activo o un grupo de activos dentro del proceso: "Integridad, confidencialidad o disponibilidad".

La entidad, se compromete a gestionar los riesgos, identificando y administrando los eventos potenciales que pueden afectar la plataforma estratégica, los objetivos institucionales y los macroprocesos y procesos de la entidad. Para la adecuada gestión integral del riesgo en la UAERMV, se presenta los siguientes lineamientos:

1. Se adoptará las metodologías para gestionar los riesgos de la entidad a través del análisis del contexto, entendido como el entorno externo e interno, y la valoración de los mismos, es decir, su identificación, análisis y evaluación, y su posterior tratamiento, todo esto manteniendo comunicación y consulta constante y permanente monitoreo y revisión, para evitar así su materialización.
2. Asegurar los recursos necesarios para ayudar a los responsables a gestionar y tratar los riesgos.
3. Los riesgos que se gestionan en la UAERMV son los siguientes:

    a) **Riesgos Estratégicos:** Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.
    b) **Riesgos gerenciales:** Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
    c) **Riesgos operativos:** Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
    d) **Riesgos financieros:** Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.
    e) **Riesgos tecnológicos:** Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
    f) **Riesgos de cumplimiento:** Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones
    g) contractuales.
    h) **Riesgo de imagen o reputacional:** posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización, ante sus clientes y partes interesadas.
    i) **Riesgos de corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
    j) **Riesgos de seguridad digital:** Posibilidad Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el

orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

4. Se deben identificar los activos de información por cada proceso.
5. Se deben identificar los dueños de los activos.
6. Se deben clasificar los activos.
7. Se debe determinar la criticidad de los activos.
8. Se deben identificar las vulnerabilidades de los activos.
9. Se deben identificar las amenazas de los activos.
10. Se deben identificar los riesgos de los activos.
11. Se debe realizar una descripción de los riesgos.
12. Se debe revisar la probabilidad y el impacto de ocurrencia de los riesgos.
13. Se debe calcular el riesgo inherente.
14. Se deben aplicar los controles a los riesgos identificados.
15. Los controles deben tener una frecuencia de aplicación.
16. La tolerancia es el nivel del riesgo que la entidad puede o está dispuesta a soportar, que corresponden a los riesgos que se encuentren en zona residual Baja y los que se encuentran en otra zona se trataran de acuerdo a los lineamientos establecidos en el procedimiento de Gestión de Riesgos de la entidad.
17. La entidad revisará y actualizará la política de Gestión de Riesgos de acuerdo con los cambios del entorno, las nuevas metodologías y los resultados de los indicadores de gestión asociados a la materialización de riesgos definidos.
18. Los riesgos identificados en la entidad deberán ser monitoreados permanentemente, para asegurar que los controles sean eficaces y eficientes, y obtener información para mejorar la evaluación y gestión de los riesgos e identificar la materialización oportuna de los riesgos.
19. Los niveles de responsabilidad sobre periodicidad de seguimiento y evaluación de los riesgos se llevarán a cabo de acuerdo procedimiento de Gestión de Riesgos.

20. Comunicar interna y externamente, los resultados de la gestión del riesgo desarrollada institucionalmente, reportando en el Mapa Institucional de Riesgos, los riesgos priorizados de acuerdo con los lineamientos establecidos en el procedimiento de Gestión de Riesgos.

21. Las opciones del tratamiento a los riesgos que se evalúan en la entidad son:

    a. **Evitar el riesgo:** Se logra cuando al interior de los procesos se genera cambios sustanciales por rediseño, eliminación o cancelación de una actividad o conjunto de actividades que causan el riesgo, resultado de unos adecuados controles y acciones emprendidas. Por ejemplo: el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.
    b. **Reducir el riesgo:** Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Por ejemplo: a través de la optimización de los procedimientos y la implementación de controles.
    c. **Compartir el riesgo:** Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones o dependencias, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar, la tercerización.
    d. **Asumir el riesgo**: Después de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso, el líder del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo. No aplica para los riesgos de corrupción, estos siempre deben conducir a un plan de acción o de tratamiento para mitigarlo.

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		
Acompañamiento EQUIPO TÉCNICO SIG:	Firma:	Firma:
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	Elaborado por el Ing. Omar Fdo. Garzón Giraldo (especialista en seguridad de la información), versión inicial del documento conforme a los requerimientos de MINTIC.	Febrero 2019	Jefe Oficina Asesora de Planeación

ALCALDÍA MAYOR DE BOGOTÁ D.C.

MOVILIDAD

Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial

POLÍTICAS GENERALES DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN Y COMUNICACIONES

Bogotá, D.C.,
(FEBRERO DE 2019)

CONTENIDO

1. INTRODUCCIÓN

Este documento es el resultado de la revisión de las políticas de seguridad de la información y comunicaciones aplicadas por primera vez en el mes de diciembre de 2007 y sus actualizaciones corresponderán a los cambios asociados al proceso de GSIT y EGTI.

La 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 los procesos: "Estrategia y Gobierno de TI (EGTI) y Gestión de Servicios de Infraestructura Tecnológica (GSIT), cual contendrá las condiciones, normas y correcciones para quienes las incumplan.

De igual manera, se relacionan los principios de actuación para las personas que tengan acceso a los sistemas de información o recursos informáticos, y por lo tanto el mismo se constituye en la normativa que regulará toda la Administración de la Seguridad de los Activos de Información y los correctivos adecuados.

Este documento se refiere a una regla de definición general y debe cumplir con las directrices de la Comisión Distrital de Sistemas (organismo rector de las políticas y estrategias que a nivel de Tecnología informática y de comunicaciones se adopten en todas las entidades del Distrito Capital y asesor técnico) quien implementó el Sistema Distrital de Información – SDI: integrado por el conjunto de políticas, estrategias, metodología, procedimientos, bases de datos, plataformas; por lo cual este Documento Interno debe revisarse con frecuencia y está sujeto a modificaciones y cambios estructurales.

La seguridad de la informacion pretende proteger los recursos informáticos valiosos de la entidad, tales como la información, el hardware o el software. A través de la adopción de las medidas adecuadas, la Política General de Tecnología y Seguridad de la Información y Comunicación ayuda a la organización cumplir sus objetivos, protegiendo sus recursos financieros, sus sistemas, su reputación, su situación legal, y otros bienes tanto tangibles como intangibles. Debe verse a la seguridad informática, no como un objetivo en sí mismo, sino como un medio de apoyo a la consecución de los objetivos de la entidad.

La Política General de Tecnología y Seguridad de la Información y Comunicación es una invitación a cada uno de los miembros de la entidad a reconocer la información entre otras como uno de los activos principales. Esta política debe concluir en una posición consciente y

vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la entidad.

Este documento recoge las políticas relacionadas con la infraestructura tecnológica de entidad en cuanto a los lineamientos referentes a temas como manejo de correo electrónico, estudio y manejo de nuevas adquisiciones, responsabilidades administrativas, integración con diferentes áreas de la organización, lineamientos sobre gestión de incidencias y revisión de aspectos relevantes frente a mecanismos preventivos y correctivos, todo bajo los conceptos de seguridad informática. Desarrollar una política de seguridad de la informacion significa planear, organizar, dirigir y controlar las actividades tecnológicas para mantener y garantizar la integridad física de los recursos tecnologicos, así como resguardar los activos de la entidad.

2. GLOSARIO DE TERMINOS

- **Acuerdo de Confidencialidad:** Contrato suscrito entre las partes con el fin de compartir material confidencial o conocimiento para ciertos propósitos, pero restringiendo su uso publico.
- **BACKUP:** En tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperación en caso de su pérdida.
- **Batch:** Archivo magnético que tiene almacenada una secuencia de comandos. Al
- **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.
- **Firewall:** Dispositivo tecnológico que tiene como función proteger la red interna de una compañía de accesos no autorizados del exterior vía Internet.
- **LAN:** Local área network o red de área local, es la interconexión de una o varias computadoras y periféricos.
- **Seguridad de la Información:** Protección que se brinda a los activos de información mediante medidas preventivas con el fin de asegurar la continuidad del negocio y evitar la materialización de los riesgos.
- **Seguridad Informática:** Se encarga del aseguramiento de la infraestructura tecnológica mediante herramientas o elementos físicos, para evitar que se materialización las amenazas que se propagan por la red.
- **SGSI:** Sistema de Gestión de la Seguridad de la Información.
- **GSIT:** Gestión de Servicios de Infraestructura Tecnológica.
- **SPAM:** Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming.
- **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.
- **VPN:** Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.
- **WAN:** Wide área network o red de área amplia, es una red de computadoras que abarca varias ubicaciones físicas, proveyendo servicio a una zona, un país, incluso varios continentes. Es cualquier red que une varias redes locales (LAN).

3. OBJETIVO GENERAL

Establecer LAS POLÍTICAS GENERALES DE TECNOLOGIA Y SEGURIDAD DE LA INFORMACIÓN Y COMUNICACIÓN con las cuales se defina el uso adecuado de los recursos tecnológicos de la UAERMV, para reducir los riesgos que pueden afectar la continuidad de la operación en cuanto a infraestructura tecnológica y sistemas de información.

3.1 OBJETIVOS ESPECÍFICOS:

a) Ser la guía que deben aplicar los Usuarios para mantener un correcto uso de los recursos tecnológicos.
b) Definir los lineamientos para ayudar a garantizar la seguridad de la información en la UAERMV.
c) Lograr un adecuado nivel de confidencialidad, integridad, disponibilidad de la información que se produce o recibe en la entidad.
d) Cumplir con los principios de seguridad de la información.
e) Minimizar el riesgo de seguridad de la información que pueda afectar las funciones más importantes de la entidad.
f) Apoyar la innovación tecnológica.
g) Ser un lineamiento para implementar el sistema de gestión de seguridad de la información, (SGSI).
h) Proteger los activos de información, tecnológicos y de seguridad digital.
i) Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
j) Fortalecer la cultura de seguridad de la información en los servidores públicos, terceros, y demás usuarios externos de la UAERMV.
k) Garantizar la continuidad del negocio frente a incidentes de seguridad.
l) Establecer las sanciones respectivas por incumplimiento de las directrices presentadas en este documento y que atenten contra sus principios básicos.

4. NIVEL DE CUMPLIMIENTO

a) Definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, alineados a las necesidades de la entidad, y a los requerimientos regulatorios.
b) Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de sus servidores públicos, contratistas, terceros y proveedores de servicios.
c) Proteger la información generada, procesada o resguardada por los procesos de la entidad, su infraestructura tecnológica y activos, del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores), o como resultado de un servicio interno en outsourcing.
d) Proteger la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
e) Proteger la información de las amenazas.
f) Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta los procesos críticos.
g) Controlar la operación de los procesos de la entidad garantizando la seguridad de los recursos tecnológicos y las redes de datos.
h) Implementar control de acceso a la información, sistemas y recursos de red.
i) Garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
j) Garantizar que a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva del modelo de seguridad.
k) Garantizar la disponibilidad de los procesos de la entidad y la continuidad de su operación basada en el impacto que pueden generar los eventos.
l) Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

5. ALCANCE

Se definen políticas y lineamientos con el propósito de cumplir con los objetivos de la institución en seguridad de la informacon y seguridad informática; y para ello se establecen:

- Políticas de seguridad: Para definir controles que proporcionan directivas y consejos de gestión para mejorar la seguridad de los activos de información.
- Políticas de navegación en internet: Establece la configuración de perfiles de navegación para optimizar el uso del canal de internet y reducir el riesgo de descarga de software nocivo.
- Políticas de tratamiento y manejo de datos personales: Establece los lineamientos para el manejo y tratamiento de los datos personales de acuerdo con la ley 1581 de 2012 de la SIC (Súper intendencia de industria y comercio).
- Políticas de seguridad de activos de información: establece controles para catalogar los activos y protegerlos eficazmente.
- Política de protección y respaldo de la información: Establece los lineamientos para garantizar las copias o respaldos de la información.
- Política del escritorio limpio y bloqueo de pantalla.: Establece los lineamientos para proteger los documentos ubicados en los escritorios y el bloqueo de los equipos de computo cuando el usuario no se encuentre en su puesto de trabajo.
- Política de seguridad para gestión de contraseñas: Establece los lineamientos para la gestión segura de las credenciales (usuario y contraseña) de los aplicativos y equipos de computo.
- Política de responsabilidades operacionales y control de cambios: Establece los lineamientos para cuando se requieren hacer cambios importantes en la infraestructura tecnológica o sistemas de información que pueden afectar la continuidad de la operación.
- Política de protección contra software nocivo: Establece los lineamientos para evitar la descarga, instalación y propagación de software nocivo (virus y sus variantes)
- Política de gestión de riesgos: Establece los lineamientos para la identificación y mitigación de los riesgos asociados a los activos de la entidad.
- Política para el buen uso del correo electrónico institucional: Establece los lineamientos para el uso eficiente y seguro del correo electrónico de la entidad.
- Política de registro histórico de actividades (log): Establece los lineamientos para almacenar los logs de los aplicativos críticos de la entidad, para en caso de presentarse un incidente de seguridad poder realizar un análisis forense.
- Política sobre el uso de equipos de computo y el acceso a la red: Establece los lineamientos para el buen uso de los equipos de computo de la entidad y la protección del acceso a la red lan o wifi de la entidad.

Aplica para todos los colaboradores 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 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.

5.1 ACTIVOS DE INFORMACION SON:

ACTIVOS HUMANOS

- **Empleados:** Empleados públicos de planta (de carrera administrativa y los provisionales), funcionarios de libre nombramiento y remoción, trabajadores oficiales, contratistas.
- **Externos:** Consultores, asesores, especialistas, trabajadores temporales, proveedores.

ACTIVOS FISICOS

- **Infraestructura de TI:** Edificios, oficinas, centro de datos, cuartos de servidores y equipos, armarios de red (Racks), cableado, escritorios, cajones, archivadores, salas de almacenamiento de medios físicos, dispositivos de identificación y autentificación, control de acceso del personal y otros dispositivos de seguridad como por ejemplo las cámaras (circuito cerrado de TV, lectores biométricos...).
- **Controles del entorno de TI:** Alarmas, sistema de refrigeración, supresión contra incendio, sistemas de alimentación ininterrumpida (UPS), planta eléctrica, alimentación de potencia y de red.
- **Hardware de TI:** Computadores de escritorio y portátiles, dispositivos de almacenamiento, servidores, firewall, routers, dispositivos de comunicaciones, impresoras, faxes, scanners, fotocopiadoras.
- **Documentación:** Procedimientos, programas, guías, formatos, manuales y demás documentación física de propiedad de la entidad.

ACTIVOS DE SERVICIOS DE TI

- Servicios de autenticación y administración de usuario, aplicaciones, servidores proxy, servicios de red, servicios web, servicios inalámbricos, antivirus, antispyware, antispam, detección y prevención de intrusiones, seguridad, FTP, bases de datos, correo electrónico y mensajería instantánea, herramientas de desarrollo, contratos de soporte y mantenimiento de software.

Las políticas de seguridad de la información descritas en este documento aplican a todos los activos de información durante su ciclo de vida, incluyendo creación, distribución, transmisión, almacenamiento y eliminación.

De igual manera, estas políticas están orientadas a garantizar el uso apropiado de los dispositivos tecnológicos (computadores de escritorio, portátiles, etc.) y de servicios como el internet, el correo electrónico, el Orfeo, y demás aplicativos brindando a los servidores públicos, contratistas, terceros, lineamientos para la utilización apropiada de dichos recursos, permitiendo así minimizar los riesgos de una eventual perdida de activos de información sensible para la UAEMRV.

Estas políticas aplican a todos los servidores públicos, contratistas, terceros que acceden a activos de información de la UAEMRV los cuales están sujetos a los mismos requerimientos de seguridad, y tienen las mismas responsabilidades de seguridad de la información que los funcionarios de la entidad.

La información utilizada para el desarrollo de las actividades y funciones diarias o contratadas por la UAEMRV es propiedad de la entidad, por tal razón, todos los servidores públicos, contratistas y terceras partes están obligados a proteger dicha información, incluso una vez haya terminado su relación contractual y/o legal con la entidad.

6. AUTORIDAD Y LIDERAZGO

Para efectos la definición de roles y responsabilidades para la aplicación de este documento interno, se designa la administración estratégica y orientación general de las POLÍTICAS GENERALES DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN Y COMUNICACION, además de su implementación, al proceso de GSIT y EGTI con el apoyo de la Secretarial general de la entidad.

7. POLÍTICAS GENERALES DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN Y COMUNICACION

7.1 PROPÓSITO:

La implementación de este documento de POLÍTICAS GENERALES DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN Y COMUNICACIONES, busca reducir la materialización de los riesgos, respecto a una amplia gama de amenazas que pueden ser accidentales o intencionales, estableciendo normas claras respecto de su divulgación, modificación o eliminación de la información considerada crítica sensible para el logro de los objetivos misionales de la Unidad, y proveer a la UAERMV de un documento formal en donde se contengan las buenas prácticas para una administración adecuada de los recursos tecnológicos, soporte a Usuarios, seguridad de la información y las comunicaciones de la Unidad.

7.2 REFERENCIA NORMATIVA

- **Norma Técnica Colombiana NTC-ISO-IEC 27002:2015:** Norma técnica de seguridad. Código de practica para controles de seguridad de la información.
- **Decreto 1078 de 2015:** Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto No. 2573 de 2014:** establece como lineamiento la Seguridad y privacidad de la Información y comprende acciones transversales además de componentes enunciados, a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada.
- **Norma Técnica Colombiana NTC-ISO-IEC 27001:2013:** Norma técnica de sistemas de gestión de la seguridad de la información. Requisitos.
- **Decreto 1377 De 2013:** Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012. Añade dos nuevos capítulos al Código Penal Colombiano
  1. **Capitulo Primero:** De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos;
  2. **Capitulo Segundo:** De los atentados informáticos y otras infracciones. Como se puede ver en el primer capitulo, esta Ley está muy ligada a la ISO27000, lo cual coloca al País a la vanguardia en legislación de seguridad de la información, abriendo así la posibilidad de nuevas entradas con este tema.

- **Articulo 230 de la ley 1450 de 2011:** Estableció que todas las Entidades deben adelantar acciones señaladas por el Gobierno Nacional, concernientes a implementar las estrategias de Gobierno en Línea que se definen por el Ministerio de Tecnologías de la Información y las comunicaciones.
- **Decreto 2573 de 2014:** Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
- **Norma Técnica Colombiana NTC-ISO-IEC 31000:2018:** Norma técnica de gestión del riesgo. Principios directrices.
- **Ley 1341 del 30 de Julio de 2009:** Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
- **Ley 1273 DE 2009:** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado "de la protección de la información y los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Ley Estatutaria 1266 del 31 De diciembre de 2008:** Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales.

Ley 603 de 2000: Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales. Ver esta ley.

7.3 IMPORTANCIA DE SU APLICACIÓN:

Este documento interno está orientado a brindar los lineamientos para:

- Proteger la información de la UAERMV ya sea dentro de las instalaciones o por fuera de ella.
- Garantizar el uso apropiado de los dispositivos tecnológicos (computadores de escritorio, portátiles, impresoras, tabletas, celulares de última generación, etc.) y de los servicios tecnológicos como el Internet, Correo Electrónico, pagina Web y demás aplicativos que pone a disposición la entidad para los funcionarios.
- Establecer pautas para la utilización eficiente y racional de los recursos tecnológicos.

- Minimizar los riesgos de que se materialice algún ataque informático o amenaza que pueda comprometer a la entidad en una eventual pérdida de información o indisponibilidad del servicio tecnológico.
- La Dirección General de la UAERMV deberá dotar a los Servidores Públicos, de los recursos tecnológicos, humanos y de capacitación, necesarios para llevar a cabo la completa difusión y entendimiento de las políticas que se describen en este documento.

7.4 CUMPLIMIENTO:

Las POLÍTICAS GENERALES DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN Y COMUNICACIONES son de obligatorio cumplimiento y ningún Servidor Público está exento de su acatamiento.

Si una persona o entidad viola las disposiciones de las Políticas, por indiferencia o intencionalmente, la UAERMV se reserva el derecho de tomar las medidas correspondientes.

7.5 PRINCIPIOS:

Los siguientes principios básicos fundamentan las POLÍTICAS GENERALES DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN Y COMUNICACIONES de la UAERMV.

7.5.1 ***Propiedad de la información:*** Los activos de información tanto físicos como digitales que son propiedad de la UAERMV, son entregados a los Servidores Públicos y contratistas para su buen uso, operación o custodia, mas esto no modifica la propiedad de estos que seguirá estando a nombre de la UAERMV. La información generada por Servidores Públicos y contratistas durante la ejecución de sus funciones es propiedad intelectual de la UAERMV como parte del proceso laboral de las personas.

7.5.2 ***Protección de la información***: Los activos de información serán protegidos con el nivel necesario en proporción a su riesgo de pérdida y valor para el logro de los objetivos misionales, acentuando la confidencialidad, integridad y disponibilidad que se requiera.

7.5.3 ***Protección de los recursos tecnológicos***: Los recursos tecnológicos serán protegidos con el nivel necesario en proporción a su valor para el logro de los objetivos misionales y el riesgo de pérdida de la Unidad. Dichos recursos deben

ser utilizados exclusivamente para desarrollar actividades laborales; así mismo, su utilización se hará en forma adecuada, responsable y cuidando de su integridad.

7.5.4 ***Autenticación de Usuarios***: Todos los Usuarios incluido el personal de los procesos Estrategia y Gobierno de TI y Gestión de Servicios e Infraestructura Tecnológica, deben tener un identificador único (ID de Usuario) solamente para su uso personal exclusivo y las contraseñas personales deben proveer la autenticación al sistema, sobre la base de un secreto que solo debe conocer el Usuario.

7.5.5 ***Responsabilidad:*** Los Usuarios y custodios de los activos de información de la UAERMV, son responsables por el uso apropiado, protección y privacidad de estos activos.

7.5.6 ***Disponibilidad***: Los activos de información deben estar disponibles para soportar los objetivos misionales de la UAERMV, garantizando que solo los Usuarios autorizados tengan acceso a la información o a los recursos informáticos.

7.5.7 ***Integridad***: Los activos de información deben estar adecuadamente protegidos para asegurar la exactitud y totalidad de la información y de los métodos de procesamiento. Las medidas de validación definidas (como LOG y copias de seguridad) permitirán detectar la modificación inapropiada, eliminación o adulteración de los activos de información.

7.5.8 ***Confidencialidad***: Los activos de información de la UAERMV, deben ser accedidos únicamente por personal autorizado. Las medidas de confidencialidad definidas en este documento garantizaran este principio.

7.5.9 ***Esfuerzo de Equipo***: La seguridad de información debe ser un esfuerzo de *equipo* donde debe participar en forma activa cada Servidor Público y contratista que tenga interacción con la información o los sistemas de información de la Unidad. Todos los Servidores Públicos y contratistas de la UAERMV deben cumplir con las Políticas de Seguridad y más que eso, desempeñar un papel proactivo para su protección, divulgación de estas políticas, y el de informar cualquier acto indebido que vaya en contra de la política establecida.

7.5.10 ***Soporte Primario para la Seguridad de Información***: La Secretaría General deberá proveer dirección y experiencia técnica para asegurar que la información

de la UAERMV se encuentre protegida apropiadamente. Esto incluye considerar la confidencialidad, la integridad y la disponibilidad de la información y de los recursos tecnológicos que la soportan, y de igual manera garantizar el presupuesto para el sostenimiento de la Infraestructura Tecnológica y la inversión en nuevas tecnologías en pro de proteger la entidad.

El personal de los procesos Estrategia y Gobierno de TI y Gestión de Servicios e Infraestructura Tecnológica, encargados de la Seguridad de la Información debe gestionar y desarrollar las iniciativas sobre seguridad de información en la Unidad.

Las políticas generadas por el encargado de la seguridad de la información del proceso de GSIT, deben ser validadas por el Comité de la Secretaría General, antes de ser aprobadas por la Dirección General de la UAERMV.

Los Usuarios son responsables de familiarizarse y cumplir con las Políticas de Seguridad; las dudas que puedan surgir alrededor de éstas deben ser consultadas al encargado que tiene a cargo la seguridad de la Información.

7.5.11 **Monitoreo de la seguridad de la información:** La entidad deberá efectuar revisiones por lo menos una vez al año donde se realicen las pruebas para evaluar el cumplimento de la POLITICA GENERAL DE TECNOLOGIA Y SEGURIDAD DE LA INFORMACION, y las políticas puntuales generadas para verificar el cumplimiento de estas y el aseguramiento de los diferentes componentes que hacen parte de la infraestructura tecnológica de la entidad.

De igual manera se realizarán actualizaciones periódicas de acuerdo con los diferentes lineamientos de la entidad y su necesidad de seguridad.

7.5.12 Clasificación de la información: En seguridad de la información se manejan tres conceptos o pilares importantes que son: confidencialidad, integridad y disponibilidad, definiendo tres niveles de clasificación para la información, además de la Ley 1712 de 2014 - Ley de Transparencia y Acceso a la Información Pública y Ley 1581 de 2012 – Protección de datos personales.

La POLÍTICA GENERAL DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN Y COMUNICACIÓN define un esquema de clasificación de información de la siguiente manera:

- **Confidencial:** Esta información estará disponible para un grupo especifico de personas (definidos por la entidad y el propietario), la indisponibilidad, divulgación o alteración sin autorización puede impactar negativamente, de índole legal, operativo, económico o que afecte la imagen de la entidad, en caso de que la información sea suministrada a un tercero se debe hacer con un acuerdo de confidencialidad firmado.
- **Uso Interno:** Esta información puede ser suministrada a terceros si se ha firmado un acuerdo de confidencialidad, su acceso es libre para los empleados de la entidad a través de la intranet. Esta información por su contenido solo le interesa a quienes va dirigida, la indisponibilidad, divulgación o alteración sin autorización puede afectar a una entidad o personas.
- **Publica:** Esta información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad sin que esto conlleve un impacto negativo de ninguna índole.

7.6 DESARROLLO DE LAS POLITICAS

- Las estrategias en cuanto a seguridad de información de la UAEMRV son directrices de largo plazo, que sirven como base para la planeación adecuada y la definición de soluciones de seguridad para ajustarse a las necesidades de la entidad, tanto actuales como futuras.
- Las decisiones y disposiciones de seguridad de información estarán basadas en análisis de riesgos y métodos de evaluación.
- La seguridad de información considera revisiones continuas del valor para la institución de las medidas de seguridad en uso.
- La administración de la seguridad de información se desarrollará sobre lineamientos y guías dadas por las entidades del distrito como lo son el MINTIC, Alta Consejería, y otros.
- Las políticas de Seguridad deberán ser revisadas cada vez que se cumpla un ciclo de gestión de seguridad de la información.
- Las políticas de Seguridad deberán ser aprobadas por el(la) secretario(a) General de la entidad.

7.7 POLITICAS ESPECIFICAS.

La UAEMRV para el fortalecimiento de la POLÍTICA GENERAL DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN Y COMUNICACIÓN, elaborara las siguientes políticas

puntuales con el objetivo de proteger los activos, siguiendo como guía la norma ISO 27001 de 2013, estas políticas serán anexos a este documento principal.

1. Políticas de navegación en internet.
2. Políticas de tratamiento y manejo de datos personales.
3. Políticas de seguridad de activos de información.
4. Política de protección y respaldo de la información.
5. Política del escritorio limpio y bloqueo de pantalla.
6. Política de seguridad para gestión de contraseñas
7. Política de responsabilidades operacionales y control de cambios.
8. Política de protección contra software nocivo.
9. Política de gestión de riesgos.
10. Política para el buen uso del correo electrónico institucional.
11. Política de registro histórico de actividades (log).
12. Política sobre el uso de equipos de computo y el acceso a la red.

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:		
ANDREA DEL PILAR ZAMBRANO/ CHRISTIAN MEDINA Contratista/ Proceso DESI	MARCELA ROCIO MARQUEZ ARENAS (Secretaria General)	MARTHA PATRICIA AGUILAR COPETE (Representante de la Alta Dirección)

CONTROL DE CAMBIOS:

VERSION	DESCRIPCIÓN	FECHA	APROBADO Representante de la Alta Dirección SIG
1.0	Elaborado por MARISOL LONDOÑO LOPEZ – Profesional Especializada Sistemas: Actualización de la Resolución 558 del 14 de diciembre de 2007 y a las Normas ISO/IEC 17799: 2005, ISO/IEC 27001	Diciembre de 2007	Comité de Gestión Integral
1.01	Revisión no documentada en el Sistema de Gestión de Calidad: MARISOL LONDOÑO LOPEZ – Profesional Especializada Sistemas	Enero de 2008	Proceso SIT
1.02	Revisión no documentada en el Sistema de Gestión de Calidad: MARISOL LONDOÑO LOPEZ – Profesional Especializada Sistemas.	Marzo de 2009	Proceso SIT
1.03	Revisión no documentada en el Sistema de Gestión de Calidad: JOSE GABRIEL GUERRA – Profesional Universitario Sistemas	Marzo de 2010	Proceso SIT
1.04	Revisión no documentada en el Sistema de Gestión de Calidad: JOSE GABRIEL GUERRA – Profesional Universitario SIT / PAOLA MONTENEGRO - Contratista	Agosto de 2011	Proceso SIT
1.05	Revisión no documentada en el Sistema de Gestión de Calidad: JUAN CARLOS ALBA ALBARRACÍN – Profesional Especializado SIT / JOSE GABRIEL GUERRA – Profesional Universitario SIT	Febrero de 2013	Proceso SIT

2.0	Revisado con el Acompañamiento OAP: Se actualiza a la normatividad vigente Normas NTC-ISO/IEC 27002, ISO/IEC 27001. Por: JUAN CARLOS ALBA ALBARRACÍN – Profesional Especializado SIT / JOSE GABRIEL GUERRA – Profesional Universitario SIT	Febrero 2015	JEFE OAP
3	Revisado y actualizado por el Ing. Omar Fdo. Garzón Giraldo (especialista en seguridad de la información), se desagregaron las políticas puntuales de la POLITICA GENERAL DE TECNOLOGIA Y SEGURIDAD DE LA INFORMACION Y COMUNICACIONES, se agrego introducción, se modifico el objetivo general, se agregaron los objetivos específicos, se realizo modificación del alcance, la introducción.	Diciembre 2018	Jefe Oficina Asesora de Planeación