

**POLÍTICAS DE SEGURIDAD DE GESTIÓN DE ACTIVOS DE INFORMACIÓN**

**Bogotá, D.C.,**

**(OCTUBRE DE 2020)**

**Contenido**

[1. INTRODUCCIÓN 4](#_Toc51945068)

[2. OBJETIVOS. 5](#_Toc51945069)

[3. ALCANCE. 6](#_Toc51945070)

[4. GENERALIDADES. 6](#_Toc51945071)

[5. REFERENCIA NORMATIVA. 6](#_Toc51945072)

[6. GLOSARIO DE TERMINOS. 7](#_Toc51945073)

[7. ACTIVOS DE INFORMACIÓN. 10](#_Toc51945074)

[7.1. Registro De Activos de Información 11](#_Toc51945075)

[8. RESPONSABILIDADES. 13](#_Toc51945077)

[9. CLASIFICACIÓN DE LA INFORMACIÓN. 15](#_Toc51945079)

[10. ETIQUETADO DE LA INFORMACIÓN. 15](#_Toc51945080)

[11. ACTUALIZACIÓN DEL REGISTRO DE ACTIVOS DE INFORMACION. 15](#_Toc51945081)

[12. PUBLICACIÓN DEL REGISTRO DE ACTIVOS DE INFORMACIÓN. 16](#_Toc51945082)

[13. LINEAMIENTOS PARA EL USO DE ACTIVOS DE INFORMACIÓN. 16](#_Toc51945083)

[14. CUMPLIMIENTO. 18](#_Toc51945084)

[15. ACTUALIZACIONES DE LA POLÍTICA DE SEGURIDAD 19](#_Toc51945085)

I. [ANEXO METODOLOGÍA. 19](#_Toc51945086)

[1. Listar Inventario de Activos. 21](#_Toc51945090)

[2. Identificar el Dueño del Activo. 22](#_Toc51945091)

[3. Clasificar los Activos. 22](#_Toc51945092)

[4. Clasificar la Información. 22](#_Toc51945093)

[5. Determinar la Criticidad del Activo. 26](#_Toc51945097)

[6. Infraestructura Crítica Cibernética. 26](#_Toc51945098)

II. [ETIQUETADO. 26](#_Toc51945099)

**TABLAS E ILUSTRACIONES**

[Tabla N° 1. Roles y Responsabilidades. 13](#_Toc51863205)

[Tabla N° 2. Niveles de evaluación. 19](#_Toc51863214)

[Tabla N° 3. Niveles de clasificación. 19](#_Toc51863215)

[Tabla N° 4. Esquema de Clasificación Confidencialidad. 22](#_Toc51863221)

[Tabla N° 5. Esquema de Clasificación Integridad. 24](#_Toc51863222)

[Tabla N° 6. Esquema de Clasificación Disponibilidad. 24](#_Toc51863223)

[Tabla N° 7. Etiquetado de la información. 27](#_Toc51945100)

[Ilustración 1. Procedimiento para Registros de Activos de Información 11](#_Toc51863203)

[Ilustración 2. Metodología. 20](#_Toc51863216)

## **INTRODUCCIÓN**

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, a través de la presente política, establece la importancia de los activos de información al interior de la entidad, por medio de su identificación, clasificación, valoración y tratamiento de los mismos, estableciendo los lineamientos y mecanismos pertinentes para su adecuada protección.

Por medio de los lineamientos establecidos, la entidad puede controlar el grado de exposición a potenciales amenazas o vulnerabilidades sobre los activos de información en sus diferentes procesos, determinando el uso correcto y adecuado de cada uno de ellos, clasificándolos según su nivel de exposición al riesgo y su importancia en la misionalidad de la entidad. De esta manera, la entidad mantendrá de forma fácil y práctica el inventario de sus activos de información con su clasificación y valoración respectiva, cumpliendo con las regulaciones y/o normatividad vigente.

Adicional, en el presente documento se manifiesta la responsabilidad que tiene cada uno de los colaboradores de la entidad, en levantamiento de los activos de información en cada uno de los procesos a los cuales pertenecen, permitiendo establecer por el propietario del activo los mecanismos y/o lineamientos apropiados de seguridad para los mismos, mitigando de esta manera las amenazas y/o vulnerabilidades a los cuales se encuentra expuesto el activo de información.

Finalmente, se establece las acciones que la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, contempla por el incumplimiento de las políticas de seguridad de la información, por parte de sus colaboradores.

## **OBJETIVOS.**

* Proporcionar los criterios, formas, orientaciones y/o recomendaciones que deben ser utilizados por los líderes o responsables de los procesos o dependencias de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, para realizar la identificación, valoración y la clasificación de los activos de información.
* Clasificar los activos de información para garantizar una eficaz gestión de su seguridad con criterios de confidencialidad, integridad y disponibilidad.
* Mantener actualizado el inventario de activos de información de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial y asegurar que la información reciba un adecuado nivel de protección.
* Establecer las directrices y actividades generales para identificar, clasificar y valorar los activos de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, a través de los lineamientos establecidos en este documento, los cuáles serán utilizados por los servidores públicos, contratistas y terceros de la Entidad.

## **ALCANCE.**

Aplica para todos los colaboradores de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, que tengan acceso a los recursos y activos de información, en todas sus formas (digital, impresa, escrita, y hablada) durante su ciclo de vida (creación, distribución, transmisión, almacenamiento, eliminación), y está orientada a preservar la confidencialidad, integridad y disponibilidad de la información de la entidad, los cuales están sujetos a los mismos requerimientos de seguridad, y tienen las mismas responsabilidades de salvaguardar la información; por lo tanto, están obligados a continuar protegiendo y cumpliendo las políticas de confidencialidad durante y una vez terminada su relación laboral y/o contractual con la entidad.

## **GENERALIDADES.**

El presente documento establece las políticas de gestión de activos de información de la **Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial**,

dando cumplimiento a lo establecido en ley 1712 de 2014 “*por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones,* y al decreto reglamentario 103 de 2015, compilado en el decreto 1080 de 2015 “*por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones”.*

## **REFERENCIA NORMATIVA.**

El presente documento interno hace parte integral de las Políticas Generales de Tecnología de Seguridad y de Información, las cuales cuentan con el siguiente marco normativo:

* **Constitución Política de Colombia de 1991.** Artículos 15 del Habeas Data, 20 y 74 sobre acceso a la información.
* **Ley Estatutaria 1581 de 2012:** *“Por la cual se dictan disposiciones generales para la protección de datos personales”*
* **Ley Ordinaria 1273 de 2009: “***Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.*
* **Decreto Reglamentario 1377 de 2013, Compilado en el Decreto 1074 de 2015:** Protección de datos, decreto por el cual se reglamente parcialmente la Ley 1581 de 2012. Añade dos nuevos capítulos al Código Penal Colombiano. Derogado parcialmente por el Decreto 1081 de 2015.
* **Decreto Reglamentario 103 de 2015, Compilado en el Decreto 1081 de 2015:** *“Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones”.*

## **GLOSARIO DE TERMINOS.**

* **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la entidad.
* **Activo de información:** Es todo aquello que las entidades consideran importante o de alta validez para la misma, ya que puede contener importante información como lo puede ser Bases de Datos con usuarios, contraseñas, números de cuentas, etc.
* **Amenaza:** Es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la organización.
* **Ciberseguridad:** la ciberseguridad se define como una **capa de protección para los archivos de información**, a partir de ella, se trabaja para evitar todo tipo de amenazas, las cuales ponen en riesgo la información que es procesada, transportada y almacenada en cualquier dispositivo.
* **Disponibilidad:** La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera esta, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso.
* **Categorías de información:** Toda información de contenido o estructura homogénea, sea física o electrónica, emanada de un mismo sujeto obligado como resultado del ejercicio de sus funciones y que pueda agruparse a partir de categorías, tipos o clases según sus características internas (contenido) o externas (formato o estructura). A nivel archivístico distrital, dicha categoría se reconoce como serie y subseries documental.
* **Colaboradores:** Todos los servidores públicos, trabajadores oficiales, orden de prestación de servicios y todas las personas que se encuentren vinculadas a la Entidad y que deban generar algún trabajo para la misma.
* **Clasificación de la información:** La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
* **Confidencialidad:** Es una propiedad que ostenta algún tipo de información y mediante la cual se garantizará el acceso a la misma solamente a aquellas personas que estén autorizadas a conocerla, y por consiguiente no será revelada ante aquellos que no cuenten con la autorización de conocerla.
* **Custodio:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.
* **Disponibilidad:** Propiedad de que la información sea accesible y utilizable cuando se requiera por los autorizados.
* **Documento de archivo (records):** Registro de información producida o recibida por una entidad pública o privada en razón de sus actividades o funciones.
* **Documento electrónico de archivo:** Es un documento cuyo soporte material es algún tipo de dispositivo electrónico o magnético, y en el que el contenido está codificado mediante algún tipo de código digital, que puede ser leído, interpretado, o reproducido, mediante el auxilio de detectores de magnetización.
* **Excepciones:** En este dato se indica si todo el documento es reservado o clasificado o solo una parte de él. Si solo un dato o información es reservado o clasificado dentro de un documento, esto no hace que todo lo que se contenga en él lo deba ser.
* **Índice de Información Clasificada y Reservada:** Es el registro de activos de la información pública que puede causar un daño a determinados derechos o intereses públicos (Reserva) o privados (Clasificación), por lo que no es publicable.
* **Información:** Según el Artículo 6°. Definiciones, de la Ley 1712 de 2014, *“Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen”.*
* **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.
* **Información pública clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o sami-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 del 2014.
* **Información pública reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos
* **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos. La integridad de un documento hace referencia a su carácter completo e inalterado. Es necesario que un documento este protegido contra modificaciones no autorizadas.
* **Inventario de Activos**: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.)
* **No clasificada:** Activos de Información que deben ser incluidos en el registro de activos y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.
* **Propiedad de los activos:** Los activos de información del registro de activos deben tener un propietario.
* **Registro:** Documento que presenta resultados obtenidos o proporciona evidencia de actividades ejecutadas.
* **Riesgo**: Es la definición de un escenario bajo el cual una amenaza puede explotar una vulnerabilidad, generando un impacto negativo al negocio (por ejemplo, pérdida de la continuidad, incumplimiento, pérdida de ingresos, entre otros).
* **Registro de Activos de Información:** Es el registro de activos de la información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
* **Tabla de Retención Documental - TRD:** Es un conjunto de unidades documentales homogéneas emanadas por un mismo órgano o sujeto productor en ejercicio de sus funciones ejemplo: contratos, historias laborales, actas.
* **Seguridad de la información:** Es el 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.
* **URL:** Son las siglas en inglés de Uniform Resource Locator, que en español significa Localizador Uniforme de Recursos. Como tal, el URL es la dirección específica que se asigna a cada uno de los recursos disponibles en la red con la finalidad de que estos puedan ser localizados o identificados.
* **Vulnerabilidad**: Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos de una organización.

## **ACTIVOS DE INFORMACIÓN.**

La información puede existir en muchas formas: Impresa, manuscrita, almacenada en disco o en medio magnético, en medios electrónicos, presentaciones, videos o conversaciones, entre otros, cualquiera que sea la forma de existencia de la información, ésta siempre debe estar protegida adecuadamente, para preservar la confidencialidad, integridad y la disponibilidad de la misma, para esto el dueño o el administrador de la información debe clasificarla para identificar la necesidad, prioridad y el grado de protección que requiere para comunicar el requerimiento de medios de tratamiento especial a la Secretaría General – Proceso Gestión de Servicios e Infraestructura Tecnológica.

## **Registro De Activos de Información**

La identificación del registro de activos de información permite clasificar los activos de la entidad a los que se debe brindar mayor protección, permitiendo reconocer sus características y validación del activo.

Las actividades a realizar para obtener un registro de activos inician con la Definición, Revisión, Actualización y Publicación, las cuales se reflejan documentalmente en **Formato Matriz De Activos De Información EGTI-FM-009[[1]](#footnote-1).**

## **Ilustración 1. Procedimiento para Registros de Activos de Información**



**Fuente: Guía 5 – Gestión Clasificación de Activos.**

Con relación a la información que se recibe, transforma y produce en la Entidad, se identifican los siguientes tipos de activos de información:

* **Documental:** se realiza a través del reconocimiento de la producción documental de la Entidad.
* **Software:** Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en un computador.
* **Físico (Hardware):** Medio utilizado para realizar la captura, procesamiento, almacenamiento, difusión y divulgación de la información, es deseable que se utilicen las tecnologías de punta para lograr una gestión oportuna y eficiente en almacenaje y procesamiento de datos y en la ampliación de la cobertura de información a difundir. En este sentido, se refiere a todos los elementos físicos que permiten el correcto funcionamiento de un medio informático. Incluye redes de datos, discos duros o extraíbles, impresoras, servidores, computadores, dispositivos móviles, entre otros. Para facilidad de manejo de este tipo de activos, los mismos pueden ser agrupados según sus características (por ejemplo: equipos de cómputo personales; dispositivos móviles o celulares).
* **Persona:** Cargo de aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información.
* **Servicios:** Hace referencia a aquellas actividades realizadas por personas, dependencias o entidades ajenas al proceso, que facilitan la administración o flujo de la información generada por el proceso. En esta tipología se encuentra la intranet, el internet, el correo electrónico, el servicio de fotocopiado, el servicio de correspondencia, el servicio de ingreso a la entidad, entre otros.
* **Red de datos:** Elementos de la infraestructura de telecomunicaciones.

## **RESPONSABILIDADES.**

Se identifican los activos de información de mayor importancia asociados a cada Sistema de Procesamiento de la Información en su respectivo proceso, con sus responsables y su Ubicación, para luego elaborar un inventario con dicha información.

El Inventario se deberá identificar, documentar y actualizar ante cualquier modificación de la información y los activos asociados con los medios de procesamiento. Este debe ser revisado con una periodicidad no mayor a un (1) año.

La responsabilidad de realizar y mantener actualizado el inventario de activos de información es de cada responsable de proceso de la entidad por medio del diligenciamiento de **Formato Matriz De Activos De Información EGTI-FM-009.**

El uso de los activos de información pertenecientes a la entidad es responsabilidad del propietario asignado; es su deber proteger y mantener la confidencialidad, integridad y disponibilidad de los activos de información.

## **Tabla N° 1. Roles y Responsabilidades.**

| **Rol** | **Responsabilidad** | **Actividad** |
| --- | --- | --- |
| Área o dependencia responsable o **creadora** de la información. (Gerentes, Jefes de Oficina, subdirectores, Líderes de Procesos). | Identificar y determinar los controles de seguridad de los activos que forman parte del área. | * Identificar los activos de información del área.
* Dar los lineamientos sobre el buen uso de la información.
* Garantizar que la información sea íntegra y que esté disponible para la consulta y/o acceso para el público autorizado.
* Hacer revisión y/o actualización periódica de la valoración y clasificación de los activos de información.
 |
| Área o dependencia que **custodia** la información. (Gerentes, Jefes de Oficina, subdirectores, Líderes de Procesos). | Responsable de la protección de la confidencialidad, integridad, disponibilidad y privacidad de los activos que están bajo su custodia. | * Administrar y hacer efectivo los controles que el propietario del activo haya definido.
* Garantizar que los activos de información se encuentren disponible e íntegros y que solo personal autorizado acceda a ellos.
* Cumplir con los controles de seguridad establecidos para la protección de la información.
* Ejecutar las actividades propias de su cargo, de acuerdo a la custodia de la información.
 |
| Colaboradores (Usuario final) | Aplicar lineamientos de uso de la información. | * Hacer buen uso de los activos de información.
* Garantizar la confidencialidad, integridad y disponibilidad del activo de información.
* Reportar cualquier evento que atente contra la seguridad de la información.
 |

**Fuente: Desarrollo Propio.**

## **CLASIFICACIÓN DE LA INFORMACIÓN.**

Para la Clasificación de la Información se debe tener en cuenta los criterios de Confidencialidad, Integridad y Disponibilidad, conforme a la normatividad vigente, permitiendo establecer los niveles de protección adecuados para asegurar que la información institucional se encuentre protegida contra divulgación no autorizada, exposición, pérdida, robo o daño intencional o accidental, teniendo en cuenta las características y lineamientos de los estándares y normatividad relacionada con seguridad y privacidad de la información.

## **ETIQUETADO DE LA INFORMACIÓN.**

Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la entidad.

## **ACTUALIZACIÓN DEL REGISTRO DE ACTIVOS DE INFORMACION.**

De acuerdo con el Modelo de seguridad y Privacidad de la Información, la actividad de actualización se refiere a la verificación que se lleva a cabo para determinar si un activo de información continua o no siendo parte del inventario, o si los valores de evaluación asignados deben ser modificados. En general, el inventario de activos puede ser revisado o validado en cualquier momento por parte de la dependencia responsable. Algunas de las razones por las cuales se debería realizar la revisión o validación son las siguientes:

* Actualizaciones al proceso al que pertenece el activo.
* Adición de actividades al proceso.
* Inclusión de nuevos registros, procesos y procedimientos.
* Inclusión de un nuevo activo.
* Supresión de un área, proceso o cargo en la entidad que tenía asignado el rol de propietario o custodio.
* Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados.
* Cambios físicos de la ubicación de activos de información.

La actualización de la información del registro de activos de información se encuentra enmarcada en la siguiente normatividad:

* Modelo de Seguridad y Privacidad de la Información, Guía No. 5 Gestión y Clasificación de Activos de Información, Numeral 6.3. actualización *“Una vez se ha definido qué cambios se realizarían en el inventario, desde cada proceso, se procede a actualizar el inventario de activos de información”.[[2]](#footnote-2)*
* Decreto 103 de 2015 en el Capítulo 1. Articulo 38 parágrafo 2. “*El sujeto obligado, debe actualizar el Registro de Activos de Información de acuerdo con los procedimientos y lineamientos definidos en su Programa de Gestión Documental.[[3]](#footnote-3)”*

## **PUBLICACIÓN DEL REGISTRO DE ACTIVOS DE INFORMACIÓN.**

Se debe publicar el Registro de activos de la información y el Índice de información clasificada y reservada de acuerdo el artículo 13 de la Ley 1712 de 2014 que determina *“Todo sujeto obligado deberá crear y mantener actualizado el Registro de Activos de Información...”* así como el Decreto 1081 de 2015 articulo 2.1.1.2.1.4.y el Decreto 103 de 2015 artículo 4.

## **LINEAMIENTOS PARA EL USO DE ACTIVOS DE INFORMACIÓN.**

Los activos de información pertenecen a la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, y el uso de los mismos debe emplearse exclusivamente con propósitos laborales.

Los colaboradores de la entidad deberán utilizar únicamente los programas y equipos autorizados por el proceso de Gestión de Servicios e Infraestructura Tecnológica.

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, proporcionará a los colaboradores, los equipos informáticos y los programas instalados en ellos; los datos (información) creados, almacenados y recibidos, serán propiedad de la entidad; los colaboradores no podrán realizar Backup de sus archivos personales o de información pública, para copiar cualquier tipo de información clasificada o reservada debe solicitar autorización a su Jefe inmediato o Supervisor, de acuerdo a las normas sobre clasificación de la información y conforme a los niveles de seguridad establecidos por la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial; Su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la entidad, serán sancionadas de acuerdo con las normas y legislación vigentes.

Periódicamente, el proceso de Gestión de Servicios e Infraestructura Tecnológica efectuará la revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos NO autorizados, será considerado como una violación a las Políticas de Seguridad de la Información de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial.

Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados por el Jefe de la dependencia o Supervisor a través de la Mesa de Servicios del proceso Gestión de Servicios e Infraestructura Tecnológica.

Los recursos informáticos de la entidad no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.

Los colaboradores no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos o que vayan en contravía de las políticas de seguridad de la información, entre ellos envíos o reenvíos masivos de correos electrónicos o spam, practica de juegos en línea, uso permanente de redes sociales personales, conexión de periféricos o equipos que causen molestia a compañeros de trabajo, etc.

Los colaboradores no podrán efectuar ninguna de las siguientes labores sin previa autorización del proceso de Gestión de Servicios e Infraestructura Tecnológica:

* Instalar software en cualquier equipo de la entidad.
* Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo de la entidad.
* Modificar, revisar, transformar o adaptar cualquier software propiedad de la entidad.
* Descompilar o realizar ingeniería inversa en cualquier software de propiedad de la entidad.
* Copiar o distribuir cualquier software de propiedad de la entidad.
* Cambiar la configuración de hardware de propiedad de la entidad.

Los colaboradores deberán informar al proceso de Gestión de Servicios e Infraestructura Tecnológica a través de la Mesa de Servicios o correo electrónico mesadeayuda@umv.gov.co y al Jefe Inmediato o Supervisor, sobre cualquier violación de las políticas de seguridad, uso indebido y debilidades de seguridad de la información de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, que tenga conocimiento.

Los colaboradores serán responsables de todas las transacciones o acciones efectuadas con su “cuenta de usuario”.

Ningún colaborador deberá acceder a la red o a los servicios TIC de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, utilizando una cuenta de usuario o clave de otro usuario.

Los colaboradores no están autorizados para hacer uso de redes externas a través de dispositivos personales en las instalaciones de la entidad (modem USB, Router, wifi público, etc), esto compromete la seguridad de los recursos informáticos de la entidad.

La eliminación o destrucción de los activos de información, sean estos documentos en papel, bienes muebles (equipos, computadores, notebook, u otros similares), deberá efectuarse de acuerdo con la normatividad vigente.

Los colaboradores deberán realizar la devolución de todos los activos físicos y/o electrónicos asignados por la entidad, en el proceso de desvinculación, de igual manera deberán documentar y entregar a la entidad, los conocimientos importantes que posee de la labor que ejecutan.

## **CUMPLIMIENTO.**

Los diferentes aspectos contemplados en esta política son de obligatorio cumplimiento para todos los colaboradores de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial.

En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, tomará las acciones disciplinarias y legales correspondientes.

## **ACTUALIZACIONES DE LA POLÍTICA DE SEGURIDAD**

Debido a la propia evolución de la tecnología y las amenazas de seguridad, y a las nuevas aportaciones legales en la materia, la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, se reserva el derecho a modificar esta política cuando sea necesario. En todo caso, los cambios realizados en esta política serán divulgados a los colaboradores de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial.

Es responsabilidad de cada uno de los usuarios la lectura y conocimiento de las Políticas de Seguridad contempladas en este documento.

# **ANEXO METODOLOGÍA.**

El sistema de clasificación definido, se basa en la confidencialidad como principio rector en la selección, e incluye el tratamiento de la información en cuanto a la Confidencialidad, la Integridad y la Disponibilidad de cada activo. Asimismo, contempla el impacto que causaría la pérdida de alguna de estas propiedades.

Para cada propiedad se establecieron criterios específicos y lineamientos para el tratamiento adecuado del activo. Asimismo, en este documento se definieron tres (3) niveles que permiten determinar el valor general del activo en la entidad: Alta, Media y Baja, con el fin identificar qué activos deben ser tratados de manera prioritaria (ver Tabla N° 1: Niveles de evaluación).

# **Tabla N° 2. Niveles de evaluación.**

|  |  |  |
| --- | --- | --- |
| **CONFIDENCIALIDAD** | **INTEGRIDAD** | **DISPONIBILIDAD** |
|
| **INFORMACION PUBLICA RESERVADA** | **ALTA (A)** | **ALTA (1)** |
|
|
| **INFORMACION PUBLICA CLASIFICADA** | **MEDIA (M)** | **MEDIA (2)** |
|
|
| **INFORMACION PUBLICA** | **BAJA (B)** | **BAJA (3)** |
|
|
| **NO CLASIFICADA** | **NO CLASIFICADA** | **NO CLASIFICADA** |
|
|

**Fuente: Guía 5 – Gestión Clasificación de Activos.**

# **Tabla N° 3. Niveles de clasificación.**

|  |  |
| --- | --- |
| **ALTA**  | Activos de información en los cuales la clasificación de lainformación en dos (2) o todas las propiedades(confidencialidad, integridad, y disponibilidad) es alta. |
|
|
| **MEDIA**  | Activos de información en los cuales la clasificación de lainformación es alta en una (1) de sus propiedades o al menosuna de ellas es de nivel medio. |
|
|
| **BAJA**  | Activos de información en los cuales la clasificación de lainformación en todos sus niveles es baja. |
|
|

**Fuente: Guía 5 – Gestión Clasificación de Activos.**

A continuación, se describen las actividades que se desarrollan para realizar la identificación y clasificación de los activos de información en la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial. El siguiente esquema de clasificación atiende a los requerimientos de clasificación de los activos de información con miras a una adecuada gestión de riesgos de seguridad de la información y clasificación de la información almacenada en los activos.

# **Ilustración 2. Metodología.**



**Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones.**

# **Listar Inventario de Activos.**

En Cada proceso, deberán listarse los activos, indicando algún consecutivo, nombre y descripción breve de cada uno,la cual permitirá identificar, valorar, y clasificar los activos de información, servicios, medios de procesamiento, que soportan la gestión de los procesos y establecer su nivel de clasificación.

El Inventario debe actualizarse como mínimo una vez al año y ser avalado por el Comité Institucional de Gestión y Desempeño.

## **Identificar el Dueño del Activo.**

Cada uno de los activos identificados deberá tener un dueño designado, si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente. El dueño del activo debe identificar, valorar y clasificar sus activos de información dentro del inventario, manteniendo la información detallada para cada activo sobre su valoración y clasificación en Confidencialidad, Integridad, Disponibilidad. Igualmente deberá hacer el tratamiento adecuado correspondiente a su clasificación y corrección de inconsistencias detectadas.

## **Clasificar los Activos.**

Cada uno debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: Información, Software, Hardware, Componentes de Red entre otros, está clasificación permitirá establecer su importancia dentro de la entidad y lograr establecer los niveles de protección necesarios en función de su importancia.

## **Clasificar la Información.**

Una vez identificados los activos de información, se deben establecer niveles de protección para asegurar que la información institucional se encuentre protegida contra divulgación no autorizada, exposición, pérdida, robo o daño intencional o accidental, teniendo en cuenta las características y lineamientos de los estándares y normatividad relacionada con seguridad y privacidad de la información.

NTC-ISO/IEC 27001 establece la seguridad de la información como la “preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.”, para lo cual se establecen criterios para la valoración y clasificación de los activos teniendo en cuenta estas características principales.

La clasificación de la información se debe realizar teniendo en cuenta los principios de seguridad:

* **CONFIDENCIALIDAD:** propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

# **Tabla N° 4. Esquema de Clasificación Confidencialidad.**

|  |
| --- |
| **CONFIDENCIALIDAD** |
| **INFORMACION PUBLICA RESERVADA** | Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica. |
|
|
| **INFORMACION PUBLICA CLASIFICADA** | Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario. |
|
|
|
|
| **INFORMACION PUBLICA** | Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad. |
|
|
| **NO CLASIFICADA** | Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA. |
|
|

**Fuente: Guía 5 – Gestión Clasificación de Activos.**

* **Información Pública Clasificada**

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley; en este sentido se consideran las siguientes definiciones:

* + **Dato Público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio ya su calidad de comerciante o de servidor público. (Ley 1581 de 2012). Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013).
	+ **Dato Semiprivado:** Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios. (Ley 1266 de 2008).
	+ **Dato Privado:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1266 de 2008).
	+ **Datos Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Ley 1581 de 2012 – Decreto 1377 de 2013).
* **Información Pública Reservada.**

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en la ley 1712 de 2014.

* **INTEGRIDAD:** La integridad se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción.

# **Tabla N° 5. Esquema de Clasificación Integridad.**

|  |
| --- |
| **INTEGRIDAD** |
| **A (ALTA)** | Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad. |
|
|
| **M (MEDIA)** | Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad. |
|
|
|
|
| **B (BAJA)** | Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos. |
|
|
| **NO CLASIFICADA** | Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA. |
|
|

**Fuente: Guía 5 – Gestión Clasificación de Activos.**

* **DISPONIBILIDAD:** La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera esta, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso.

# **Tabla N° 6. Esquema de Clasificación Disponibilidad.**

|  |
| --- |
| **DISPONIBILIDAD** |
| **1 (ALTA)** | La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos. |
|
|
| **2 (MEDIA)** | La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad. |
|
|
|
|
| **3 (BAJA)** | La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen. |
|
|
| **NO CLASIFICADA** | Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA. |
|
|

**Fuente: Guía 5 – Gestión Clasificación de Activos.**

## **Determinar la Criticidad del Activo.**

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, debe evaluar la criticidad de los activos, a través de preguntas que le permitan determinar el grado de importancia de cada uno, para posteriormente, durante el análisis de riesgos tener presente esta criticidad para hacer una valoración adecuada de cada caso.

Definir las escalas (que significa criticidad ALTA, MEDIA y BAJA) para valorar los activos respecto a la confidencialidad, integridad y disponibilidad e identificar su nivel de importancia o criticidad para el proceso. (Ver Tabla N°3 Niveles de Clasificación).

## **Infraestructura Crítica Cibernética.**

Identificar y reportar a las instancias y autoridades respectivas en el Gobierno nacional si poseen ICC. Un activo es considerado infraestructura crítica si su impacto o afectación podría superar alguno de los 3 criterios:

**Se considera como infraestructura crítica a todo activo que sea afectado por uno o más de los siguientes tres tipos de impacto:**

* Impacto social, (0,5%) correspondiente a 250.000 personas de la Población Nacional.
* Impacto económico, PIB de un día o 0,123% del PIB Anual.
* Impacto ambiental, de 3 años o más en recuperación.

# **ETIQUETADO.**

Teniendo en cuenta el inventario de activos de información, se realiza el etiquetado de la información de la siguiente manera:

**CONFIDENCIALIDAD**

* **IPC =** Información Pública Clasificada.
* **IPR =** Información Pública Reservada.

**Nota:** La Información Pública no se Etiqueta.

**INTEGRIDAD**

* **A =** Alta.
* **M =** Media.
* **B =** Baja.

**DISPONIBILIDAD**

* **3 =** Alta.
* **2 =** Media.
* **1 =** Baja.

El etiquetado de los documentos se realiza al píe de página o al final de documento: **INFORMACION\_IPR\_M\_3\_100\_110\_Cuenta de Cobro.**

# **Tabla N° 7. Etiquetado de la información.**



**Fuente: Desarrollo Propio.**

**REVISIÓN Y APROBACIÓN:**

|  |  |  |
| --- | --- | --- |
| **Elaborado y/o Actualizado por:** | **Validado por** **RESPONSABLE DIRECTIVO del Proceso:** | **Aprobado****Representante de la Alta Dirección:** |
| **LUIS ENRIQUE PARIS GARCIA /** **GLORIA MÉNDEZ****Contratista / Proceso EGTI** | Firma: | Firma: |
| **Revisado por:** |
| **ANDREA DEL PILAR ZAMBRANO****Contratista/ Proceso DESI** |
| **MARTHA PATRICIA AGUILAR COPETE** **Secretaría General**  | **DIANA MARCELA REYES TOLEDO****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 GESTIÓN DE ACTIVOS DE INFORMACIÓN de la POLÍTICA GENERAL DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN Y COMUNICACIONES, se agregó introducción, se modificó el objetivo general, se agregaron los objetivos específicos, se efectuó la modificación del alcance, se agregó: la definición de activos de información, glosario de términos, roles y responsabilidades, clasificación de la información, manejo de medios. | Mayo 2019 | Jefe Oficina Asesora de Planeación |
| 2 | Se realiza modificación en introducción, objetivos, roles y responsabilidades, normatividad, se incorporan lineamientos específicos, cumplimiento, generalidades. | Octubre 2020 | Jefe Oficina Asesora de Planeación |

1. **Nota:** Para el caso del proceso *Gestión de Servicios e Infraestructura Tecnológica,* se debe realizar el diligenciamiento adicional de **EGTI-FM-010 FORMATO INVENTARIO DE ACTIVOS DE RED.** [↑](#footnote-ref-1)
2. https://www.mintic.gov.co/gestionti/615/articles-5482\_G5\_Gestion\_Clasificacion.pdf [↑](#footnote-ref-2)
3. Decreto 103 de 2015 Capitulo 1. Articulo 38 parágrafo 2 [↑](#footnote-ref-3)