

Política de Seguridad Actualizaciones de Software

**Bogotá, D.C.,**

**DICIEMBRE 2022**

**CONTENIDO**

1. [**INTRODUCCIÓN** 3](#_Toc116308622)
2. [**OBJETIVOS** 4](#_Toc116308623)
3. [**ALCANCE** 4](#_Toc116308624)
4. [**GENERALIDADES** 4](#_Toc116308625)
5. [**OBLIGATORIEDAD** 4](#_Toc116308626)
6. [**REFERENCIA NORMATIVA.** 5](#_Toc116308627)
7. [**DEFINICIÓNES.** 5](#_Toc116308628)
8. [**LINEAMIENTOS PARA LA ACTUALIZACIÓN DE SOFTWARE.** 6](#_Toc116308629)
9. [**VIGENCIA DE LA POLÍTICA.** 8](#_Toc116308630)

## **INTRODUCCIÓN**

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, a través de la presente política, establece la importancia de tener todas las actualizaciones del firmware de dispositivos electrónicos, sistemas de información y sistemas operativos de la entidad, reduciendo posibles materializaciones de riesgos sobre los activos de información.

Adicional, manifiesta la importancia y necesidad que tiene la entidad de mantener permanentemente actualizado y parcheado todo el software que se procese al interior de la Unidad Administrativa Especial de Rehabilitación Vial, permitiendo de esta manera entre otras identificar posibles obsolescencias en sus diferentes servicios y/o dispositivos. evitando de esta manera ser un objetivo fácil para los ciberdelincuentes quienes, apoyados en técnicas, táctica y procedimientos, pueden comprometer los activos de información de una organización

Finalmente, establece una serie de lineamientos que se deben tener en cuenta con la finalidad prevenir que los activos de información de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial contengan vulnerabilidades que comprometan la confidencialidad, integridad y disponibilidad de los activos de información, causando interrupciones entre otros en la misionalidad de la entidad.

## **OBJETIVOS**

* Revisar la existencia de actualizaciones y parches de seguridad para el software de la entidad y elaborar procedimientos que permitan que tales actualizaciones y parches sean instalados en los equipos de forma segura y controlada.
* Proporcionar los criterios, orientaciones y/o recomendaciones que deben ser utilizados al interior de la entidad asegurando la corrección de las vulnerabilidades mediante la instalación de los parches de seguridad instalados.
* Determinar el software que debe ser actualizado al interior de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial.

# **ALCANCE**

Esta política aplica para todos los dispositivos electrónicos, sistemas de información, sistemas operativos y todos aquellos servicios y/o productos brindados por parte de proveedores con algún tipo de vínculo con la entidad y los generados internamente, que sean susceptibles de actualizaciones de seguridad al interior de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial

# **GENERALIDADES**

El presente documento establece los lineamientos de actualizaciones de software tanto en dispositivos electrónicos, sistemas de información y sistemas operativos, con la finalidad de proteger los activos de información de la **Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial**. Por lo anterior, la entidad divulga y exige el pleno cumplimiento de las políticas y procedimientos de seguridad de la información establecidas para la protección de los activos de información de la entidad.

## **OBLIGATORIEDAD**

Esta política es de obligatorio y estricto cumplimiento para la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, para sus servidores públicos, contratistas, proveedores y todas aquellas personas que guarden relación con la entidad que tengan a su cargo dispositivos electrónicos, sistemas de información y sistemas operativos de la Entidad.

# **REFERENCIA NORMATIVA.**

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

* **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 los datos” - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.*
* **Decreto Único 1078 de 2015:***“Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.*
* **Norma Técnica Colombiana NTC-ISO-IEC 27001:2013:**Norma técnica de sistemas de gestión de la seguridad de la información. Requisitos.
* **Norma Técnica Colombiana NTC-ISO-IEC 27002:2022:**Norma técnica de seguridad. Código de práctica para controles de seguridad de la información.

# **DEFINICIÓNES.**

* **Activos de Información:** Cualquier elemento de información o que interactúe con ella que sea necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste.
* **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.
* **Confidencialidad:** La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
* **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.
* **Incidente de seguridad de la información:** Un evento o serie de eventos de Seguridad de la Información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
* **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.
* **Proveedor:** Persona Natural o Jurídica que presta bienes o servicios a la entidad.
* **Proveedor de Servicios TIC:** Es el encargado de proporcionar servicios TIC a uno o más usuarios, internos o externos.
* **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.

## **LINEAMIENTOS PARA LA ACTUALIZACIÓN DE SOFTWARE.**

Los siguientes lineamientos tienen como finalidad prevenir que los activos de información de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial contengan vulnerabilidades que comprometan la confidencialidad, integridad y disponibilidad de los activos de información, causando interrupciones entre otros en la misionalidad de la entidad:

* 1. Todos los colaboradores de la entidad deberán cumplir las políticas de seguridad de la información definidas por la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial.
  2. Todas las áreas y/o procesos de la entidad, deberán aplicar lo establecido en **EGTI-PR-016 Procedimiento Actualizaciones de Software.**
  3. Todos los servidores deben ser configurados con el mínimo de servicios necesarios y obligatorios para desarrollar las funciones designadas.
  4. Las actualizaciones de seguridad críticos de los dispositivos electrónicos, sistemas de información y sistemas operativos deben instalarse en el momento de publicarse, siguiendo los lineamientos de **EGTI-PR-016 Procedimiento Actualizaciones de Software.**
  5. Las actualizaciones de seguridad que no represente un riesgo para los servicios y/o información de la entidad, se realizarán su instalación de manera acumulativa mínimo de forma mensual, siguiendo los lineamientos de **EGTI-PR-016 Procedimiento Actualizaciones de Software.**
  6. Se prohíbe la utilización de dispositivos electrónicos, sistemas de información y sistemas operativos obsoletos que no cuenten con actualizaciones de seguridad y/o soporte por parte del proveedor.
  7. Realizar un listado y/o inventario de software existente al interior de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, susceptibles de actualizaciones de seguridad.
  8. Revisar las características y los requisitos de las actualizaciones y parches antes de instalarlo.
  9. Analizar y contrastar en un entorno de pruebas las actualizaciones correspondientes antes de instalar.
  10. Contar con mecanismos y procedimientos para deshacer los cambios sufridos en alguna actualización en caso de presentar algún inconveniente.
  11. Se recomienda utilizar herramientas de autodiagnóstico para detectar software no actualizado en dispositivos electrónicos, sistemas de información y sistemas operativos.
  12. Se recomienda tener configurado un sistema de alertas para recibir avisos y notificaciones sobre vulnerabilidades, actualizaciones y parches de seguridad.
  13. Registrar cada una de las actualizaciones y parches de seguridad instaladas en los dispositivos electrónicos, sistemas de información y sistemas operativos.

# **VIGENCIA DE LA POLÍTICA.**

La Política de seguridad Actualización de Software de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, estará vigente a partir de su publicación. La entidad se reserva el derecho a modificarla cuando se considere necesario, para lo cual, estas modificaciones entrarán en vigor y tendrán efectos desde su publicación, a través de los mecanismos dispuestos por la entidad.

|  |  |  |
| --- | --- | --- |
| **Elaborado y/o Actualizado por:** | **Validado por**  **Líderes (Estratégico u Operativo) del Proceso:** | **Aprobado:** |
| **LUIS ENRIQUE PARIS GARCIA /**  **GLORIA MENDEZ**  **Contratistas / Proceso EGTI** | Firma: | Firma: |
| **Acompañamiento Asesor OAP:** |
| **CHRISTIAN MEDINA FANDIÑO**  **Contratistas/ Proceso DESI** |
| **MARTHA PATRICIA AGUILAR COPETE**  **(Secretaria General)** | **MARTHA PATRICIA AGUILAR COPETE**  **Jefe Oficina Asesora de Planeación (e)** |

**CONTROL DE CAMBIOS:**

|  |  |  |  |
| --- | --- | --- | --- |
| **VERSIÓN** | **DESCRIPCIÓN** | **FECHA** | **APROBADO** |
| 1 | Se realiza la elaboración de la política de Actualizaciones de Software, definendo los lineamientos mínimos que deben cumplir los colaboradores responsables de los dispositivos electrónicos, sistemas de información y sistemas operativos la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial. | DICIEMBRE  2022 | Jefe Oficina Asesora de Planeación |