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

# FORMATO DE APROBACIÓN DOCUMENTAL

**CÓDIGO: DESI-FM-008** | **VERSIÓN: 11**

**FECHA DE APLICACIÓN: MAYO 2019**

| INFORMACIÓN DOCUMENTADA: | | CÓDIGO: | | VERSIÓN: | | JUSTIFICACIÓN: | | |
|---|---|---|---|---|---|---|---|---|
| TIPO | NOMBRE | ANTERIOR | VIGENTE | ANTERIOR | VIGENTE | ELABORA | ACTUALIZA | ANULA |
| Procedimiento | Construcción de Soluciones | EGTI-PR-003 | EGTI-PR-003 | 3 | 4 | | X | |
| Plan | Plan de Seguridad y Privacidad de la información | EGTI-PL-001 | EGTI-PL-003 | 1 | 2 | | X | |

**DESCRIPCIÓN DE LA JUSTIFICACIÓN:**

Se modifica la versión del procedimiento EGTI-PR-003 Construcción de Soluciones debido a que fue necesario modificar el nombre del procedimiento de Construcción de Sistemas de Información a Construcción de Soluciones, ya que este presenta el paso a paso para realizar la tercera parte del proceso Desarrollo de Sistemas de Información.

Se cambia la codificación del plan EGTI-PL-001 Plan de Seguridad y Privacidad de la Información a EGTI-PL-003, debido a que este código se asignó en primera instancia al Plan Estratégico de Tecnologías de la Información PETI.

| AVALA: LÍDER DE PROCESO *(Puede ser el Líder Estratégico o Líder Operativo dependiendo del proceso)* | ELABORA/ACTUALIZA/ANULA: *(Colaborador del proceso en compañía del enlace)* | ACOMPAÑAMIENTO: ASESOR OAP *(Colaborador de la Oficina Asesora de Planeación a cargo de procesos)* |
|---|---|---|
| *(Firma)* | *(Firma)* | *(Firma)* Andrea del Pilar Zambrano |
| *Nombre: Marcela Rocío Márquez Arenas* | *Nombre: Gloria Méndez/ Andrea Bravo/ Omar Garzón/ Yuly González* | *Nombre: Andrea Zambrano/ Christian Medina* |
| *Cargo: Secretaría General* | *Cargo: Contratistas Proceso EGTI* | *Cargo: Contratistas Proceso DESI* |

| TRÁMITE DE APROBACIÓN DOCUMENTAL (DILIGENCIADO POR LA OFICINA ASESORA DE PLANEACIÓN) | ¿ES APROBADO? | FECHA DE APROBACIÓN: | RESPONSABLE DEL SISTEMA DE GESTIÓN DE CALIDAD |
|---|---|---|---|
| | SI [X] NO [ ] | 04-06-2019 | *(Firma)* |
| | OBSERVACIONES: | | *Martha Patricia Aguilar Copete* **REPRESENTANTE DE LA ALTA DIRECCIÓN** |

# ALCALDÍA MAYOR DE BOGOTÁ D.C.

MOVILIDAD

Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial

## PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

**Bogotá, D.C.,**
**(MAYO 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 implantación de su 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 de los componentes de información.

Se definen políticas y lineamientos con el propósito de cumplir con los objetivos de la institución en seguridad de la información 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 cómputo.
- 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 cómputo y el acceso a la red: Establece los lineamientos para el buen uso de los equipos de cómputo 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 IMPLEMENTACIÓN 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.<br>• 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.<br>• Inventario de activos.<br>• Generación de SOA (documento de aplicabilidad)<br>• Documentación básica inicial del SGSI.<br>• Comunicación y socialización a los usuarios de la entidad. |
| **Hito No 3** | Gestión de Riesgos | • Matriz de Gestión de Riesgos.<br>• Metodología de Gestión de Riesgos<br>• Definición del Plan de Tratamiento de Riesgos.<br>• Informe de Gestión de Riesgos.<br>• Comunicación y socialización a los usuarios de la entidad. |
| **Hito Nº 4** | Implementación y Operación del SGSI | • Actualización de documentación vigente.<br>• Informe de Medición del SGSI.<br>• Seguimiento del SGSI.<br>• Políticas específicas del SGSI.<br>• Seguimiento de los controles de seguridad de la información.<br>• Manual del SGSI.<br>• Medición, Métricas de procedimientos de seguridad.<br>• Comunicación y socialización a los usuarios de la entidad. |
| **Hito N.º 5** | Monitorear y Revisar | • Informe de auditoría interna.<br>• Planes de acción de auditoría del SGSI.<br>• Mejora continua.<br>• Acciones Correctivas, y de mejora. |
| **Hito N.º 6** | Mantener y Mejorar | • Implementar Mejoras. |

| | | |
|---|---|---|
| | | • Generar acciones correctivas.<br>• Comunicación y socialización a los usuarios de la entidad. |
| **Hito N° 7** | Acompañamiento en la Auditoria Externa (*) | • Preauditoria.<br>• Cierre de hallazgos<br>• 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 cláusulas o capítulos.
- 114 controles.
- 35 objetivos de control.

Los lineamientos y buenas prácticas 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 debía 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 entre 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 práctica 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. **Capítulo Primero:** De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos;
  2. **Capítulo Segundo:** De los atentados informáticos y otras infracciones. Como se puede ver en el primer capítulo, 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, página 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<br>Contratista / Proceso EGTI<br>Acompañamiento EQUIPO TÉCNICO SIG:<br>ANDREA DEL PILAR ZAMBRANO<br>Contratista/ Proceso DESI | Firma:<br>MARCELA ROCIO MARQUEZ ARENAS<br>(Secretaria General) | Firma:<br>MARTHA PATRICIA AGUILAR COPETE<br>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 |
| 2 | Se modifica la codificación del documento para adecuarlo a la estructura de documental de la nueva plataforma estratégica y debido a que el código EGTI-PL-001 se asignó en primera instancia al Plan Estratégico de Tecnologías de la Información PETI. | Mayo de 2019 | Jefe Oficina Asesora de Planeación |

| ALCALDÍA MAYOR DE BOGOTÁ D.C. MOVILIDAD Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial | PROCESO ESTRATÉGICO | Código: | EGTI-PR-003 | SIG SISTEMA INTEGRADO DE GESTIÓN |
|---|---|---|---|---|
| | Proceso Estrategia y Gobierno de TI | Versión: | 4 | |
| | Procedimiento Construcción de Soluciones | Fecha: | Mayo de 2019 | |

## 1. OBJETIVO

Desarrollar cada uno de los pasos requeridos en la generación de soluciones de software, con los criterios de calidad y funcionalidad necesarios de acuerdo a lo especificado en la fase de diseño.

## 2. ALCANCE

El procedimiento inicia con la programación de los sprints, incluye la elaboración de los procedimientos de operación y seguridad, la ejecución de pruebas unitarias, de integración y finaliza con la documentación de los diferentes manuales. La construcción de Sistemas de Información, se realiza al finalizar la aplicación de los procedimientos Gestión de Requerimientos de Automatización de los Procesos, el Diseño de soluciones, finalizando con la aplicación de las pruebas y la definición de los manuales o instructivos.

## 3. DEFINICIONES

***Capa de persistencia:** Hace referencia a todos los artefactos requeridos para almacenar los datos en una base de datos.
***EDT:** Estructura de Descomposición del trabajo.
***EGTI:** Estrategia y Gobierno de TI
***GSIT:** Gestión de Servicios e Infraestructura Tecnológica
***Modelo Físico:** Corresponde a un modelo entidad relación generado a partir del modelo lógico (ver procedimiento diseño de soluciones), incluye tablas, relaciones entre ellas, índices, llaves primarias, foráneas, disparadores y seguridad.
***Sprint:** Es una meta en el tiempo con tareas alcanzables (fuente: metodología SCRUM).

## 4. DESCRIPCIÓN DE LOS SIMBOLOS

| SÍMBOLO | SIGNIFICADO | SÍMBOLO | SIGNIFICADO | SÍMBOLO | SIGNIFICADO |
|---|---|---|---|---|---|
|  | Inicio y fin. |  | Conector página. |  | Conector de actividades |
|  | Operación: desarrollo de actividad o tarea. |  | Decisión: toma de decisión |  | Punto de control: se debe describir el control. Son medidas de seguridad o Prevenciones para ejecutar la actividad de acuerdo con las normas o requisitos establecidos |

| DESCRIPCIÓN (ACTIVIDAD Y/O TAREA) | PUNTO CONTROL | TIEMPO ESTIMADO | RESPONSABLE | DEPENDENCIA INVOLUCRADA | REGISTRO | OBSERVACIONES |
|---|---|---|---|---|---|---|
|  INICIO | | | | | | |
| 1. Establecer la programación de los sprints | | 3 días | Rol asignado (Líder de desarrollo) | Secretaría General Proceso EGTI | Herramienta para planeación SCRUM (tablero) | Se identifican todas las tareas técnicas en paquetes, alineado con la EDT del proyecto y se les asigna una posible priorización. |
| 2. Realizar modelo físico y capa de persistencia. | | Depende de la complejidad | Rol asignado (DBA, líder bases de datos) | Secretaría General Proceso EGTI | Herramienta para planeación SCRUM (tablero) Link script | Se basa en el modelo lógico generado en el procedimiento "Diseño de soluciones". Esta actividad genera unos archivos llamados "scripts". |
|  3. Generar código  | | Depende de la complejidad | Rol asignado (desarrolladores) | Secretaría General Proceso EGTI | Aplicación de control de código fuente | Se codifica lo necesario, es decir se construye el código para que la solución opere de acuerdo al diseño previamente establecido. |

| | | | | | | |
|---|---|---|---|---|---|---|
| A<br>4. Ejecutar casos de prueba. |  | Depende de la complejidad | Rol asignado (oficial de pruebas) | Secretaría General Proceso EGTI | Formato Pruebas Casos de Uso | Se realizan todas las pruebas conforme el plan y prácticas de pruebas, incluyendo la integración de los procesos de negocio, los componentes de la solución TI y los requerimientos no funcionales (por ejemplo, seguridad, interoperabilidad, usabilidad).<br>Se identifica, registra y clasifica (por ejemplo, fallos menores, significativos, críticos) los errores que se evidencian durante las pruebas. Se repiten las pruebas hasta que todos los errores significativos hayan sido resueltos, se supervisan todas las excepciones de calidad y se relacionan todas las acciones correctivas. Se debe mantener un registro con todas las revisiones, resultados, excepciones y correcciones. |
| ¿Los casos de prueba son satisfactorios? NO → 1 | | | | | Formato Pruebas Casos de Uso | En el procedimiento de diseño se contempla la creación de los casos de prueba y en ellos se especifican los criterios de éxito. En este procedimiento sólo se ejecutan las pruebas para evaluar dichos criterios. |
| SI<br>5. Ejecutar pruebas de usuario. |  | Depende de la complejidad | Usuario líder | Secretaría General Proceso EGTI Procesos UAERMV | Formato de Acta | Se debe mantener un registro con todas las revisiones, resultados, excepciones y correcciones. Esta actividad tiene acompañamiento del rol asignado (analista) |
| ¿Las pruebas de usuario son satisfactorias? NO → 1 | | | | | | |
| SI<br>6. Aprobar y comunicar resultados a los interesados | | Depende de la complejidad | Usuario líder | Procesos UAERMV | Correo electrónico | Registrar los resultados de las pruebas y comunicarlos a las partes interesadas conforme al plan de pruebas. |
| 7. Documentar manuales | | Depende de la complejidad | Rol asignado (documentador) | Secretaría General Proceso EGTI | | Se documenta el manual del usuario y el técnico. En caso de ser necesario, se debe completar y actualizar el proceso de negocio y los manuales de operaciones, para registrar cualquier personalización o condiciones especiales únicas en la implementación. Los manuales deben estar alojados en cada solución, es decir hacen parte de la opción desarrollada. |
| FIN | | | | | | |

| ALCALDÍA MAYOR DE BOGOTÁ D.C. MOVILIDAD Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial | PROCESO ESTRATÉGICO | Código: | EGTI-PR-003 | SIG UNIDAD DE MANTENIMIENTO VIAL |
|---|---|---|---|---|
| | Proceso Estrategia y Gobierno de TI | Versión: | 4 | |
| | Procedimiento Construcción de Soluciones | Fecha: | Mayo de 2019 | |

**REVISIÓN Y APROBACIÓN**

| Elaborado y/o actualizado por: | Validado por RESPONSABLE DIRECTIVO SIG del Proceso: | Aprobado: |
|---|---|---|
| GLORIA MÉNDEZ RUÍZ / ANDREA SULEMA BRAVO ALVARADO<br>Contratistas/ Proceso Estrategia y Gobierno de TI | | Firma: |
| Acompañamiento EQUIPO TÉCNICO SIG: | | |
| ANDREA DEL PILAR ZAMBRANO/ CHRISTIAN MEDINA<br>Contratistas/ Proceso Direccionamiento Estratégico e Innovación | MARCELA ROCÍO MÁRQUEZ ARENAS<br>Secretaría General | MARTHA PATRICIA AGUILAR COPETE<br>Representante de la Alta Dirección |

**Participo en la Elaboración del Procedimiento**

| Nombre | Cargo | Firma |
|---|---|---|
| Gloría Méndez | Contratista | |
| Andrea Sulema Bravo | Contratista | |
| Fernando Camargo | Contratista | |
| Yuly Andrea González | Contratista | |

**CONTROL DE CAMBIOS**

| VERSIÓN | DESCRIPCIÓN | FECHA | APROBADO Representante de la Alta Dirección SIG |
|---|---|---|---|
| 001 | Creación y aprobación | dic-12 | Mónica Rubio |
| 002 | Se ajustaron los siguientes cambios:<br>-Se ingresan en registros los formatos SIT-FM-001, SIT-FM-002, SIT-FM-004, GDO-FM-016 , SIT-FM-005, SIT-FM-006, SIT-FM-007 Solicitud y Priorización de copias de seguridad y SIT-FM -008 Cronograma Copias de Seguridad<br>-Nombre, Cargos, Firmas de Revisión, Firmas de Aprobación Versión, Logos del nuevo Plan de Desarrollo | ago-13 | Gloria Cecilia Valbuena Torres |
| 003 | Se realizaron los siguientes cambios:<br>-Se rediseño el flujo del procedimiento.<br>-Se dividió el procedimiento SIT-PR-003 Desarrollo de Sistemas de Información en tres partes, la inicial Gestión de Requerimientos EGTI-PR-002, la siguiente Diseño de Soluciones EGTI-PR-004 y la final, es decir, el presente documento EGTI-PR-003 "Construcción de Soluciones", además de establecer responsables y el rol asignado a cada colaborador que participa en el desarrollo de la opción seleccionada. | may-19 | Jefe de la Oficina Asesora de Planeación. |
| 4 | Fue necesario modificar el nombre del procedimiento, y se elimina el código de los formatos. | may-19 | Jefe de la Oficina Asesora de Planeación. |
| | | | |
| | | | |