ALCALDÍA MAYOR DE BOGOTÁ D.C.	PROCESO	GESTIÓN DE MEJORAMIENTO	CODIGO	E-MEJ-FT-009
			VERSIÓN	04
			PAGINA	
	FORMATO	MAPA DE RIESGOS	VIGENTE DESDE	05/02/2015

PROCESO	GESTIÓN TECNOLÓGICA Y DE LA INFORMACIÓN
OBJETIVO DEL PROCESO	Garantizar la implementación, administración y prestación de los servicios para la optimización de las herramientas informaticas, actividades de mantenimiento preventivo y correctivo de los activos de información, plataforma de comunicaciones y desarrollo de aplicaciones a la medida, asi mismo salvaguardar la información en sus criterios de confidencialidad, integridad y disponibilidad con el fin de garantizar la ejecución de los servicios informáticos que aporten al cumplimiento de la mision del Instituto.

FACTOR DE RIESGO (Contexto)	RIESGO	CLASIFICACIÓN DEL RIESGO	CAUSAS		EFECTOS	IMPACTO		PROBABILIDAD		EVALUACIÓN RIESGO		CONTROLES EXISTENTES	VALORACIÓN RIESGO		OPCIONES MANEJO	ACCIONES DE CONTINGENCIA
	Puede suceder …		INTERNO Dedido a..	EXTERNO Debido a…	Lo que podria ocasionar…											
- Bajo nivel de profesionalización y alto nivel de rotación de personal en misión. - Fragilidad de la comunicación interna y externa.	Perdida de Información por daños en el Hardware, Software e Infraestructura en los diferentes medios de almacenamiento utilizados en el Instituto (copias de seguridad, servidores, centro de computo)	TECNOLOGÍA	1) Infraestructura inadecuada para la puesta en servicio de los equipos que almacenan la información. 2) Fallas en el suministro de Energía 3) Manipulacion erradas por personal no capacitado para la prestación del servicio del mantenimiento de	- Desastres Naturales (Terremoto, Temblor, luz, Agua). - Desastres no Naturales (Incendio, Hurto, Terrorismo; Fallas en el suministro de energia, sabotaje, etc)	1) Retrazo en las actividades diarias de los procesos. 2) Que no se pueda tomar decisiones basadas en registros. 3) Sanciones, Multas	CATASTROFICO	5	IMPROBABLE	2	10	EXTREMO	*- Se tienen establecidas "Politicas de seguridad de la información" del proceso de TIC´s* *- Se cuenta con un Plan de Contingencia para atender cualquier evantualidad que pueda llegar a ocurrir y afecte la información del Instituto.*	5	ALTO	REDUCIR EL RIESGO	*- Restaurar las copias de seguridad que se tienen a través de terceros* *- Conexión virtual al centro de computo virtual resguardado por un tercero* *- Todas las acciones contempladas en el plan de contingencia*
- Fragilidad de la comunicación interna y externa. - Bajo nivel de profesionalización y alto nivel de rotación de personal en misión.	No se cuenta con las acciones que atiendan oportuna y eficazmente los diferentes siniestros naturales y no naturales que puedan llegar a ocurrir en relación de Tecnología, Información e Infraestructua del Instituto	OPERATIVO	No se cuenta con personal suficiente de planta para la documentación y actualización del plan de contingencia y su respectivo plan de acción		Caos en el manejo de la información institucional	CATASTROFICO	5	IMPROBABLE	2	10	EXTREMO	*- Se cuenta con copias de seguridad ejecutadas mediante el DATA PROTECTOR el cual realiza copias de forma automática con una periodicidad diaria y de forma manual con una periodicidad mensual*	5	ALTO	REDUCIR EL RIESGO	*- Restaurar las copias de seguridad que se tienen a través de terceros* *- Conexión virtual al centro de computo virtual el cual es resguardado por un tercero* *- Restauración de Servidores* *- Gestionar el personal necesario* *- Todas las acciones contempladas en el plan de*
- Inexistencia de normatividad interna tales como seguridad, manejo y disposición de la información orientada a la atención del usuario y del ciudadano	Incumplimiento de normatividad interna y la establecida por los entes que rigen y controlan el Instituto	CUMPLIMIENTO	1) Falta de verificación, información y aplicación de normas establecidas y a su vez desconocimiento de actualizaciones que se realicen a las mismas por los Entes reguladores y las dictadas por el Instituto		- Sansiones. - Multas. - Perdida de imagen Institucional - Cierre parcial o total del Instituto	CATASTROFICO	5	IMPROBABLE	2	10	EXTREMO	*- Realización de seguimiento a los lineamientos establecidos en Decretos, Acuerdos y Resoluciones establecidas por el Intituto, asi mismo nos regimos por la Resolución 305 de 20 de Octubre de 2008 Establecida por la Comisión Distrital de Sistemas y demás Externas*	5	ALTO	EVITAR EL RIESGO	*- Realizar los ajustes necesarios de acuerdo a la normatividad vigente en materia de TIC´s*
- Inexistencia de politicas de seguridad de activos informaticos adecuados para la protección de la información del Instituto. - Inexistencia de normatividad interna para la seguridad, manejo y disposición de la informacion y los activos informáticos orientada a la aterción del usuario.	Fallas en los activos informaticos	TECNOLOGÍA	1) Manipulacion errada del usuario hacia el activo fisico 2) Incumplimiento de garantias	- Desastres Naturales (Terremoto, Temblor, luz, Agua). - Desastres no Naturales (Incendio, Hurto, Terrorismo; Fallas en el suministro de energia, sabotaje, etc)	1) Entrega inoportuna de la información entre los procesos. 2) Reatraso en la actividades diarias de los procesos. - multas. - sanciones	CATASTROFICO	5	IMPROBABLE	2	10	EXTREMO	*- Control de hojas de vida de equipos de compútos.* *- Control del rendimiento de los equipos.* *- Mantenimiento preventivo y correctivo.* *- Capacitación del equipo de sistemas a los usarios finales para el manejo y/o utilización de los equipos de compúto.* *- Control de licencias de software .*	5	ALTO	REDUCIR EL RIESGO	*- Aplicación de garantia, polizas para los activos informaticos de Hardware y Software.* *- Realizar y/o solicitar soporte a los sistemas de Información y activos informáticos.* *- Realizar la reparación y restauracion del recurso en caso de ser necesario* *- Validar y ejecutar las garantias en caso*

ALCALDÍA MAYOR DE BOGOTÁ D.C.	PROCESO	GESTIÓN DE MEJORAMIENTO	CODIGO	E-MEJ-FT-009
			VERSIÓN	04
			PAGINA	
	FORMATO	MAPA DE RIESGOS	VIGENTE DESDE	05/02/2015

PROCESO	GESTIÓN TECNOLÓGICA Y DE LA INFORMACIÓN
OBJETIVO DEL PROCESO	Garantizar la implementación, administración y prestación de los servicios para la optimización de las herramientas informaticas, actividades de mantenimiento preventivo y correctivo de los activos de información, plataforma de comunicaciones y desarrollo de aplicaciones a la medida, asi mismo salvaguardar la información en sus criterios de confidencialidad, integridad y disponibilidad con el fin de garantizar la ejecución de los servicios informáticos que aporten al cumplimiento de la mision del Instituto.

FACTOR DE RIESGO (Contexto)	RIESGO	CLASIFICACIÓN DEL RIESGO	CAUSAS		EFECTOS	IMPACTO		PROBABILIDAD		EVALUACIÓN RIESGO		CONTROLES EXISTENTES	VALORACIÓN RIESGO		OPCIONES MANEJO	ACCIONES DE CONTINGENCIA
	Puede suceder …		INTERNO Debido a..	EXTERNO Debido a…	Lo que podria ocasionar…											
- Bajo nivel de profesionalización y alto nivel de rotación de personal en misión. - Fragilidad de la comunicación interna y externa.	**CORRUPCIÓN**: Acceso no autorizado al centro de computo y cuartos de comunicaciones tanto físico como lógico por servidores públicos o terceros	TECNOLOGÍA	1) Desconocimiento de las politicas de seguridad interna del Instituto 2) No se cuenta con el procedimiento documentado de acceso al centro de computo y cuartos de comunicación	1) Robo por parte de personal externo	1) Destrucción, manipualción y extracción de la información y los recursos informaticos en beneficio propio 2) Retrazo en las actividades diarias de los procesos. 3) Que no se pueda tomar decisiones basadas en registros. 4) Sanciones, Multas	**MAYOR**	4	**PROBABLE**	4	**16**	**EXTREMO**	*- Se tienen establecidas "Politicas de seguridad de la información" del proceso de TIC´s* *- Se cuenta con un Plan de Contingencia para atender cualquier evantualidad que pueda llegar a ocurrir y afecte la información del Instituto.*	12	ALTO	REDUCIR EL RIESGO	*-Todas las acciones contempladas en el plan de contingencia* *- Aplicar politicas de seguridad de la información*
- Definiciones imprecisas de roles de usuarios	**CORRUPCIÓN:** Sistemas de información (SYSMAN, SIMI y roles de acceso a la red) susceptibles de manipulación o adulteración	TECNOLOGÍA	1) Falta de cumplimiento al reglamento interno de trabajo en el tema de seguridad de la información. 2) Ausencias y falta de de definiciones claras de roles y permisos de los usuarios dentro de los sistemas de información	- Acceso de terceros a la informacion del Instituto para beneficio propio	1) Generación de informes imprecisos y poco confiables que no reflejan la verdadera situación del Instituto 2) Manipulación de información sensitiva, crítica o valiosa del Instituto para la materialización de fraudes 3) Sanciones y multas para el Instituto	**MAYOR**	4	**PROBABLE**	4	**16**	**EXTREMO**	*- Definicion y aplicabilidad de horario y roles de acceso dentro del servidor de directorio activo de la red* *- Creación de los roles y permisos a los usuarios en los sistemas de información*	12	ALTO	REDUCIR EL RIESGO	*Restauración de Backups y segumiento a los Log`s del Directorio Activo de la red.*

CONTROL DE CAMBIOS			
ACTUALIZACIÓN	**DESCRIPCIÓN DE CAMBIOS**	**FECHA (DD/MM/AA)**	**ELABORÓ**
1	Se creo	24/11/2011	
2	Se incluyó los riesgos de corrupción	30/04/2013	
3	1. Se modifica el nombre del Proceso de Tecnologías de Información y Comunicaciones TIC´S a Gestión Tecnológica y de la Informacón. 2. Se adecúa el contenido a la Plantilla vigente. 3. Se incluyen los riesgos que estaban contenidos en el Mapa de Riesgos del año 2011 versión 01. 4. Se elimina del tercer riesgo del mapa de riegos, la causa interna N° *2) Incumplimiento a la norma*, Porque no es una causa originaria del riesgo que se está evaluando, sino un efecto o una consecuencia del mismo. 5. Se elimina del segundo riesgo de Corrupción (riesgo N°6 del mapa) la causa interna N° 3 *Cargue de informacion errada en los sistemas de información*. Porque esta no es una causa originaria del riesgo que se está evaluando.	09 de febrero de 2015	FIRMA EN ORIGINAL ORALIA FRANCO GÓEZ PROFESIONAL UNIVERSITARIO ÁREA DE SISTEMAS

APROBACIÓN		
PERSONA SOLICITANTE DEL CAMBIO	**REVISIÓN OFICINA ASESORA DE PLANEACIÓN**	**APROBACIÓN LIDER DEL PROCESO**
FIRMA: FIRMA EN ORIGINAL	FIRMA: FIRMA EN ORIGINAL	FIRMA: FIRMA EN ORIGINAL
NOMBRE: RAFAEL SEGUNDO MIER DELGADILLO	NOMBRE: ANY JACKELINE ROJAS PINILLA	NOMBRE: ROBERTO ANTONIO CONTRERAS MORA
CARGO: RESPONSABLE DEL ÁREA DE SISTEMAS	PROFESIONAL SIGID	CARGO: SUBDIRECTOR ADMINISTRATIVO

** Se debe llevar la trazabilidad de todas las versiones que se realicen al mapa de riesgos