SERVICIUDAD	**Serviciudad E.S.P.**	**Código CIFO -01**	**Versión 03**
	Mapa de Riesgos	**Página 1 de 1**	

PROCESO: Mantenimiento de Equipo Tecnológico

OBJETIVO: Garantizar el adecuado mantenimiento y calibraciòn de los equipos tecnológicos que inciden en la calidad de la prestación de los servicios que presta la empresa.

ALCANCE: El proceso abarca desde la planificaciòn del mantenimiento correctivo y preventivo de los equipos hasta la puesta en funcionamiento de los mismos.

RESPONSABLE: Subgerente de Planeaciòn /Profesional en sistemas

CLASIFICACIÓN	CAUSAS	RIESGO	EFECTOS	CONTROLES	CALIFICACION		Evaluación	OPCIONES DE MANEJO	ACCIONES	SEGUIMIENTO		
					PROBABILIDAD	IMPACTO				AUTOEVALUACIÓN DEL PROCESO (Líder de Proceso)	OFICINA DE CONTROL INTERNO	REGISTRO EVIDENCIA DEL SEGUIMIENTO
Riesgo de Informática y Tecnología	1.Falta de programación de mantenimientos preventivos y correctivos de los equipos 2.Personal sin competencia 3. Equipos obsoletos 4.Falta de contrato para el mantenimiento del software 5- Ausencia de respaldo de energía eléctrica para los equipos y servidores.	**Inadecuado mantenimiento de los equipos tecnológicos (Hardware y Software)**	1.Equipos en mal estado 2.Retraso en las actividades y procesos 3.insatisfacción del cliente interno y externo 4-Pérdida de información y de bases de datos fuentes vitales para los procesos Institucionales.	1.Programación de mantenimientos preventivos 2.Personal competente. 3.Contratación de técnico de apoyo en sistemas. 4.Optimización de las redes de voz y datos a categoria 6A 5-Compra de UPS de 10 KVA para respaldo de energía	2	3	MODERADA	M: Zona de riesgo Moderada: Asumir el riesgo, Reducir el riesgo	1.Implementación del FORTINET para seguridad perimetral 2.Solictud en presupuesto próxima vigencia para la adquisición de hardware y software. 3-Elaboración de plan de mantenimiento preventivo y correctivo.	1.Se hace seguimiento cada tres meses siguiendo la cronología que se realiza en sistemas para hacer mantenimiento a 5 equipos diarios durante dos semanas. Se hace por medio del formato de calidad SPFO-14V-01. 2.Se tiene implementado el FORTINET para seguridad perimetral hace 22 meses. 3.Se hace mantenimiento preventivo cada 3 meses.	Verificación del procedimiento por parte de la oficina de Control Interno	Se evidencian los formatos que permiten el seguimiento al apoyo que se brinda a los funcionarios, cuando algún equipo falla o requiere mantenimiento. Técnico en sistemas / Contratista apoyo de sistemas.
Riesgo de Informática y Tecnología	1.Falta de capacitación del personal en la realización de copias y manejo de datos 2.No se cuenta con servidor con capacidad para almacenamiento de copias de la información 3.Equipos sin mantenimiento. 4. Falta de seguir el procedimiento diseñado, para la salvaguarda de la información, por parte de los funcionarios.	**Pérdida de la información**	1. Reprocesos 2.Retraso en las actividades y procesos 3.Posibles sanciones legales	1.Instalación de Carpetas en cada equipo para copias de seguridad en nuevo servidor 2.Capacitación a cada uno de los usuarios de equipos de computo, para el almacenamiento de las copias de seguridad 3.Programación y ejeución de mantenimientos preventivos y correctivos de equipos .	2	4	ALTA	A: Zona de riesgo Alta: Reducir el riesgo, Evitar, Compartir o Transferir	1.Monitoreso permanentes de los equipos. 2. Hacer copias de seguridad 3- Mantenimientos preventivos y actualización de programas 4. Revisión y restricción de programas piratas con el fin de evitar instalación de virus. 5. Capacitación al personal en general sobre el manejo de la unidad de Red que contiene la información importante de la Empresa.	1. Crearon unidad de red para cada persona con copias automáticas incrementales. 2. Personal capacitado en el manejo de la Unidad de Red.	Verificación del procedimiento por parte de la oficina de Control Interno	Se evidencian los formatos que permiten el seguimiento al apoyo que se brinda a los funcionarios cuando algún equipo falla o requiere mantenimiento. Técnico en sistemas / Contratista apoyo de sistemas.
Riesgo de Informática y Tecnología	1. Falta de Software que mejore los procesos de la Entidad. 2.Mala programación y disponibilidad al momento de ejecutar el proceso. 3. Dependencia de un tercero que no realice las actualiciones o implementaciones requeridas, oportunamente, de acuerdo a las necesidades de los procesos. 4. Falta de una planeación adecuada en el momento de definir las necesidades tecnológicas de la Entidad 5. Infraestructura o plataforma tecnológica insuficiente o que no cuenta con los requerimientos necesarios para satisfacer las necesidades de la Entidad	**Ausencia de optimización de los procesos (Falta de gestión de los procesos y debilidades de cumplimientos a tiempo)**	1. Procesos poco optimos que afectan el cumplimiento de los objetivos estratégicos. 2. Retraso en el cumplimiento de las funciones de los ejecutores de los procesos y procedimientos institucionales. 3. Incumplimiento en la oportunidad de los reportes de información	1. Acercamiento e Identificación oportuna con los dueños de los procesos y procedimientos institucionales de las necesidades tecnológicas que permitan la opimización de sus actividades. 2. Oportunidad en los requerimientos de actualización de software y hardware. 3. Presentación de Planes de inversión en tecnología e informática.	2	4	ALTA	A: Zona de riesgo Alta: Reducir el riesgo, Evitar, Compartir o Transferir	1. Identificación oportuna de las necesidades tecnológicas de los procesos y procedimientos institucionales. 2. Solicitudes de requerimientos de actualización de software y hardware de manera oportuna. 3. Planeación de inversiones tecnologicas necesarias para poder tenerlas en cuenta en el momento de la proyección presupuestal y disponibilidad de recursos.	1. Falta de recursos para inversión tecnológica. 2. Falta de identificación oportuna de necesidades de actualización de software. 3. Dependencia de un tercero externo proveedor de software.	1. Identificación inicial de las necesidades en materia de actualizaciones informáticas. 2. Evaluación de la efectividad de los controles existentes y recomendación de la implementación de nuevos controles.	Formatos que permitan el seguimiento a los requerimientos de los funcionarios de acuerdo con sus necesidades que debe ser implementado.

SERVICIUDAD	**Serviciudad E.S.P.**	**Código CIFO -01**	**Versión 03**
	Mapa de Riesgos	**Página 1 de 1**	

PROCESO: Mantenimiento de Equipo Tecnológico

OBJETIVO: Garantizar el adecuado mantenimiento y calibraciòn de los equipos tecnológicos que inciden en la calidad de la prestación de los servicios que presta la empresa.

ALCANCE: El proceso abarca desde la planificaciòn del mantenimiento correctivo y preventivo de los equipos hasta la puesta en funcionamiento de los mismos.

RESPONSABLE: Subgerente de Planeaciòn /Profesional en sistemas

CLASIFICACIÓN	CAUSAS	RIESGO	EFECTOS	CONTROLES	CALIFICACION		Evaluación	OPCIONES DE MANEJO	ACCIONES	SEGUIMIENTO		
					PROBABILIDAD	IMPACTO				AUTOEVALUACIÓN DEL PROCESO (Lider de Proceso)	OFICINA DE CONTROL INTERNO	REGISTRO EVIDENCIA DEL SEGUIMIENTO
Riesgo de Informática y Tecnología	1. Ausencia de controles efectivos y seguimientos a los mismos. 2. Daños o ataques a los sistemas informáticos ocasionados intencionalmente por incumplimiento de las politicas de seguridad de la información (Copias de seguridad, trazabilidad a modificaciones y control de asignación a permisos de acceso a la información)	**Seguridad Informática**	1. Perdidas económicas. 2. Pérdida de información vital para la Entidad.	1. Actualización de controles. 2. Restricciones en los permisos de acceso a información neurálgica de la Entidad. 3. Sistemas de seguridad efectivos. 4. Copias de seguridad confiables y debidamente custodiadas y salvaguardadas.	2	4	ALTA	A: Zona de riesgo Alta: Reducir el riesgo, Evitar, Compartir o Transferir	1. Seguimiento permanente a la efectividad de los controles existentes y actualización e implementación oportuna de nuevos controles de ser necesario. 2. Permisos de accesos de acuerdo a los requerimientos propios de cada actividad operativa, sin exceder dichos permisos a información susceptible a modificaciones o alteraciones no permitidas en determinados procedimientos. 3. Actualización permanente de los sistemas de seguridad y antivirus. 4. Definición de procedimientos para la salvaguarda y custodia de las copias de seguridad que garantizan su efectividad de respaldo de información.	1. Monitoreo permanente a la efectividad de los controles en seguridad informatica. 2. Cambios periodicos de claves y permisos de acceso 3. Seguimiento y control a los vencimientos de los antivirus. 4. contol a los respaldos de la información (copias de seguridad)	1. Evaluación de la efectividad de los controles existentes y recomendación de la implementación de nuevos controles con el apoyo de los expertos en informática. 2. Seguimiento al procedimiento de respaldo, custodia y salvaguarda de la información neurálgica de la Entidad. 3. Verificación del cumplimiento de los controles de seguridad en materia informática.	1. Formatos que permiten el seguimiento a los controles de seguridad informatica y respaldo de la información. 2. Copias de seguridad automatizadas.

	PROBABILIDAD	IMPACTO				
		Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrofico (5)
	Raro (1)	B	B	M	A	A
	Improbable (2)	B	B	M	A	E
	Posible (3)	B	M	A	E	E
	Probable (4)	M	A	A	E	E
	Casi Seguro (5)	A	A	E	E	E
BAJA	B: Zona de riesgo Baja: Asumir el riesgo					
MODERADA	M: Zona de riesgo Moderada: Asumir el riesgo, Reducir el riesgo					
ALTA	A: Zona de riesgo Alta: Reducir el riesgo, Evitar, Compartir o Transferir					
EXTREMA	E: Zona de riesgo Extrema: Reducir el riesgo, Evitar, Compartir o Transferir					