IMVIYUMBO	SISTEMA INTEGRADO DE GESTIÓN INSTITUCIONAL "SIGI" **MAPA DE RIESGOS** **(GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN)**	Código: FO-GPS-11 Versión: 3 Fecha: 15/12/2022

IDENTIFICACIÓN DEL RIESGO							VALORACIÓN DEL RIESGO											
							ANALISIS DEL RIESGO			EVALUACIÓN DEL RIESGO					TRATAMIENTO DEL RIESGO			
							RIESGO INHERENTE			CONTROLES		RIESGO RESIDUAL						
PROCESO Y SU OBJETIVO	**ACTIVIDAD(ES) ASOCIADA AL PROCESO (Preferiblemente la(s) Actividad(es) descrita(s) en la Caracterización)**	**RIESGO** *Evitar iniciar con palabras negativas como: "No…", "Que no…", o tales como: "ausencia de", "falta de", "poco(a)", "escaso(a)", "insuficiente", "deficiente", "debilidades en…"*			**CAUSAS** Factores o fallas que originan o pueden originar la materialización del riesgo	**CONSECUENCIA** **¿Qué impactos puede generar el riesgo identificado?** *- Intervenciones, Sanciones, Quejas* *- Perdida de información crítica* *- Afectación a los procesos* *- Afectación de la imagen (Perdida de credibilidad)* *- Afectación a las personas*	**de materialización (Muy Baja, Baja, Media, Alta o Muy Alta**	**VALORACIÓN DEL IMPACTO**	**ZONA DE RIESGO**	**SOLIDEZ DEL CONTROL (Fuerte, Moderado o Leve)**	**CONTROLES EXISTENTES Y SU FRECUENCIA**	**PROBABILIDAD RESIDUAL**	**IMPACTO RESIDUAL**	**ZONA DE RIESGO**	**OPCIÓN DE TRATAMIENTO (Acepta, Reduce, Comparte Evita)**	**ACCIONES PARA MITIGAR Y FECHA PROPUESTA** ***Nota 1. Todos los controles existentes deberán ser considerados como acciones, que se deben implementar según la frecuencia definida)*** ***Nota 2. La acción mantener los controles es la sumatoria de los controles existentes cuantificados como acciones a realizar durante la vigencia*** **Nota 3. Las acciones deben incluir la fecha o el periodo de tiempo en el cual se estima realizar**	**RESPONSABLE(S) DE LA(S) ACCION(ES)**	**FECHA PROPUESTA PARA TERMINAR TODAS LAS ACCIONES**
Objetivo Estratégico: *Proceso:* *Objetivo del Proceso:* **Contribuir con el fortalecimiento administrativo, tecnológico y el mejoramiento de MIVIYUMBO en torno a la gestión del conocimiento, que permitan la implementación y mantenimiento de políticas de seguridad, disponibilidad, actualización, integridad y confidencialidad de la información que procesa y/o genera la entidad, hardware y software que procesa y/o genera la entidad, y la información que se genera en los procesos misionales**	Gestionar la seguridad informática de la entidad Implementación de políticas de seguridad. Control de accesos a las plataformas informáticas Creación, modificación o cancelación de usuarios y privilegios Copias de respaldo backup Reportes y gestión de incidentes de seguridad informática Recuperación en caso de interrupción del servicio.	1	**SEGURIDAD DE LA INFO.**	Posibilidad de perdida economica y reputacional por Modificación no autorizada de la información (Uso indebido)	1.Carencia de controles de seguridad 2.Ausencia de un respaldo seguro de datos 3. Usuarios no capacitados en temas de seguridad digital 4. Manejo inadecuado de los correos institucionales	Hallazgos (de tipo administrativo, Fiscal, Penal y/o Disciplinario) - Afectación a los procesos - Perdida de credibilidad (imagen) - Afectación de personas	Media	Mayor	ALTA	Fuerte	Aplicar lo establecido en: 1. Plan de seguridad y privacidad de la informacion PL-GTI-01. 2. Política de seguridad digital OD-GTI-04.	Muy Baja	Mayor	ALTA	REDUCIR	1. Aplicar los controles de seguridad disponibles en la entidad. 2. Capacitar en la NAG 3. Socializar política de seguridad digital	Gestión de Planeación Contratista profesional TIC.	dic-24
Objetivo Estratégico: *Proceso:* *Objetivo del Proceso:*	Gestionar la seguridad informática de la entidad Implementación de políticas de seguridad. Control de accesos a las plataformas informáticas Creación, modificación o cancelación de usuarios y privilegios Copias de respaldo backup Reportes y gestión de incidentes de seguridad informática Recuperación en caso de interrupción del servicio.	2	**SEGURIDAD DE LA INFO.**	Posibilidad de perdida economica y reputacional por Pérdida/Destrucción de información	Ataques externos Errores humanos. Desastres naturales Carencia de utilizacion de contraseñas	Afectacion en los procesos y perdida de credibilidad	Baja	Mayor	ALTA	Fuerte	Aplicar lo establecido en: 1. Plan de seguridad y privacidad de la informacion PL-GTI-01. 2. Plan de tratamiento de riesgos de seguridad y privacidad de la informacion PL-GTI-02. 3. Política de seguridad digital OD-GTI-04	Muy Baja	Mayor	ALTA	REDUCIR	1. Aplicar los planes de emergencia que establezca la entidad. 2. Sensibilizar a los responsables de los correos sobre la importancia de utilizar contraseñas. 3. Socializar la política de seguridad digital.	Gestión de Planeación Contratista profesional TIC.	dic-24
Objetivo Estratégico: *Proceso:* *Objetivo del Proceso:*	Coordinar servicios de mantenimiento y desarrollo de TIC Administrar la infraestructura tecnológica sobre la cual se soportan los sistemas de información de la Entidad. (Servidores, Redes y Bases de Datos)	3	**GESTIÓN**	Posibilidad de perdida reputacional por incumplimiento al mantenimiento de equipos e infraestura tecnologica.	Que no se haya programado o atendido las necesidades de mantenimiento segun cronograma o solicitud	1. - Perdida de credibilidad (imagen) - reduccion de la vida util de los equipos tecnologiccos - baja productividad - incrementos de los costos de las operaciones y mantenimiento de los equipos	Baja	Moderado	MODERADA	Fuerte	1. Dar Soporte tecnico PR-GTI-01 2. Aplicar lo establecido en el procedimiento Mantenimiento de equipos de computo PR-GTI-02. . PETI	Muy Baja	Moderado	MODERADA	EVITAR	1. Mantener los controles. 2. Seguimiento al cronograma de mantenimiento preventivo de equipos de computo.	Gestión de Planeación Contratista profesional TIC.	dic-24
Objetivo Estratégico: *Proceso:* *Objetivo del Proceso:*		4		Riesgo 4	Causas 4	1. 2. 3. 4.				**	++++++					1. 2. 3. 4.		
Objetivo Estratégico: *Proceso:* *Objetivo del Proceso:*		5		Riesgo 5	Causas 5	1. 2. 3. 4.				**	++++++					1. 2. 3. 4.		
Objetivo Estratégico: *Proceso:* *Objetivo del Proceso:*		6		Riesgo 6	Causas 6	1. 2. 3. 4.				**	++++++					1. 2. 3. 4.		
Objetivo Estratégico: *Proceso:* *Objetivo del Proceso:*		7		Riesgo 7	Causas 7	1. 2. 3. 4.				**	++++++					1. 2. 3. 4.		
Objetivo Estratégico: *Proceso:* *Objetivo del Proceso:*		8		Riesgo 8	Causas 8	1. 2. 3. 4.				**	++++++					1. 2. 3. 4.		
Objetivo Estratégico: *Proceso:* *Objetivo del Proceso:*		9		Riesgo 9	Causas 9	1. 2. 3. 4.				**	++++++					1. 2. 3. 4.		