IDENTIFICACIÓN									**CALIFICACIÓN**				**VALORACIÓN**										**OPCIÓN DE TRATAMIENTO**
COMPONENTE DEL SIG	**TIPO DE PROCESO**	**PROCESO**	**ACTIVO AFECTADO**	**TIPO DE AMENAZA**	**AMENAZA**	**RIESGO**	**CAUSAS O EVENTOS**	**CONSECUENCIAS (EFECTOS DEL EVENTO)**	**PROBABILIDAD (Escala 1)**	**IMPACTO (Escala 1) (SEGURIDAD: 1 a 5; CALIDAD: 1 a 5; AMBIENTAL: 1 a 5)**	**EVALUACIÓN DEL RIESGO INHERENTE** (PROBABILIDAD*IMPACTO)	**NIVEL DE RIESGO INHERENTE** (ZONA RIESGO EN LA MATRIZ)	**CONTROLES EXISTENTES** (SE DETALLAN LOS CONTROLES EXISTENTES)	**CANT. DE CONTROLES EXISTENTES** (SE TOMARÁ EN CUENTA LA CANTIDAD DE CONTROLES EXISTENTE COLUMNA N)	**TIPO DE CONTROL**	**DETERMINACIÓN DEL CONTROL**	**PROBABILIDAD** (PROBABILIDAD DEL CONTROL)	**IMPACTO** (IMPACTO DEL CONTROL)	**VALORACIÓN DEL CONTROL** (APLICACIÓN DEL CONTROL PARA CADA RIESGO)	**NIVEL DE RIESGO RESIDUAL** (Después de aplicar Controles)	**OPCIÓN DE TRATAMIENTO** (ACEPTAR, EVITAR, REDUCIR, COMPARTIR)
															1= PREVENTIVO 2= CORRECTIVO 3= DETECTIVO	**1= PERSONAL 2= TECNOLÓGICO 3= DOCUMENTAL**						
SGSI	Tercear_Informal	Gestión Movilidad de Protección	Hardware	4. HARDWARE	4.1 Deficiencias los componentes de hardware	**Facilidad de comprometer la disponibilidad de la información deliberadamente debido a fallas técnicas y operativas en el proceso.**	* Procesos Degradación amplia de los electrónicos simple * Procesos Degradación amplia de los electrónicos complejo (ensamblaje) * Procesos Degradación de los medios de soporte de información (cintas magnéticas, discos ópticos) * Procesos Evolución de la cadena de suministro * Tecnología Obsolescencia * Procesos Vulnerabilidad ante el medioambiente Inadecuado manejo de la información cometido por una indebida manipulación de los medios * Procesos Acceso no autorizado a la información * Procesos Pérdida de confidencialidad de la información * Procesos Errores humanos * Procesos Pérdidas en la distribución de datos en las aplicaciones * Procesos Errores en el uso de las aplicaciones, sistemas de información y herramientas * Procesos Errores humanos * Procesos Falta de conocimiento adecuado sobre el uso de la seguridad tecnológica * Procesos Falta de planes de rehabilitación en TI * Procesos Falta de conocimiento adecuado sobre el uso de la seguridad tecnológica * Procesos Fuerte de equipos * Procesos Fuerte de equipos de hardware * Procesos Inadecuada mantenimiento de hardware * Procesos Inadecuada mantenimiento/ falta de mantenimiento de hardware * Procesos Inadecuada mantenimiento/ falta de mantenimiento de red * Procesos Ausencia de esquemas de reemplazo y mantenimiento de los periféricos para la reducción de fiabilidad y copias de seguridad	* Desmotivación en la calidad de la información (decisiones, estimaciones y objetivos) por la comunicación de los errores * Incertidumbre en las decisiones. * Pérdida reputacional * Pérdida de la información, para nuevos proyectos * Pérdida económica * Pérdida administrativa/no jurídicas	5	4	75	EXTREMO	A.11.1 Establecimiento de Seguridad de la Información A.8.1.1 Inventario de Activos Propiedad y Responsabilidades A.7.1.1 Antes de asumir el empleo A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información A.8.1 Responsabilidad por los activos A.8.2.3 Manejo de Activos A.8.3.2 Eliminación de Soportes A.9.4.1 Restricción del acceso a la información A.9.4.2 Procedimiento de Ingreso Seguro A.9.4.3 Sistema de Gestión de Contraseñas A.10.1 Criptografía A.11.1.4 Protección contra amenazas externas y ambientales A.11.2 Equipos A.11.2.1 Ubicación y Protección de Equipos A.11.2.4 Mantenimiento de equipos A.11.2.5 Retiro de Activos Propiedad de la Empresa A.12.1.2 Gestión de Riesgos A.18.1 Cumplimiento de requisitos legales y contractuales	20	4	2	4	3	MEDIO	ALTO	Mitigar el Riesgo

Definiciones	**Tratamiento de los riesgos para la seguridad de la información**	**Opción**
-	Proceso de selección de las medidas de tratamiento de riesgos para la seguridad de la información, para modificar, retener, evitar o compartir los riesgos identificados, preparando así un plan de tratamiento de riesgos, para que los responsables de los activos de información implementen estas medidas.	aceptar
-	Acciones de carácter técnico-jurídico y social, dirigidas a disminuir el riesgo de seguridad de la información, para que la materialización de dicho riesgo no afecte a los activos de la información.	mitigar

PLAN DE TRATAMIENTO DE RIESGOS

ACCIONES (ACCIÓN O CONJUNTO DE ACCIONES PARA MITIGAR [UN] RIESGO) [DEBE CORRESPONDER CON LA(S) ACCIÓN(ES) REGISTRADA(S) EN EL PLAN DE ACCIÓN]	RESPONSABLE (ÁREA O PERSONA RESPONSABLE DE LA ACCIÓN)	CRONOGRAMA DEL PLAN DE ACCIÓN		SEÑALE/DESCRIBA LA ACCIÓN OBJETIVA (Evidencias o soportes)
		Fecha Inicio (DD/mm/aaaa)	Fecha Fin (DD/mm/aaaa)	
Fortalecer las capacidades en el uso y apropiación de las herramientas tecnológicas mesa de ayuda de la Unión de la entidad. Implementar una estrategia de concientización sobre el uso seguro de la información y el cibercomportamiento humano y tecnológico. Cumplir con las políticasde seguridad y privacidad de la información. Fortalecer el interior del proceso la toma de conciencia en el uso y apropiación de las buenas prácticas de seguridad de la información dentro del proceso.	Gestión Medidas de Prevención	05/04/2024 08/04/2024 02/09/2024	31/12/2024 31/12/2024 30/09/2024	Area de nuevo Presentaciones Capacitaciones Listado de asistencias Evaluación de tema de conciencia

	OBSERVACIÓN
	-
	-