GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

	IDENTIFICACIÓN								CALIFICACIÓN				VALORACIÓN								PLAN DE TRATAMIENTO				
COMPONENTE DEL SIG	TIPO DE PROCESO	PROCESO	OBJETIVO DEL PROCESO	RIESGO	CAUSAS O EVENTOS	TIPO DE RIESGO	CONSECUENCIAS (RESULTADO DEL EVENTO)	PROBABILIDAD ESCALA ZONA DE RIESGO BAJA = 1 - 2 ZONA DE RIESGO MODERADA = 3 - 6 ZONA DE RIESGO ALTA = 8 - 12 ZONA DE RIESGO EXTREMA = 16	IMPACTO ESCALA ZONA DE RIESGO BAJA = 1 - 2 ZONA DE RIESGO MODERADA = 3 - 6 ZONA DE RIESGO ALTA = 8 - 12 ZONA DE RIESGO EXTREMA = 16	EVALUACIÓN DEL RIESGO INHERENTE (PROBABILIDAD X IMPACTO)	NIVEL DE RIESGO INHERENTE (ZONA DE RIESGO BAJA, ZONA DE RIESGO MODERADA, ZONA DE RIESGO ALTA, ZONA DE RIESGO EXTREMA)	CONTROLES EXISTENTES (DE DETALLAN LOS CONTROLES EXISTENTE)	CANT. DE CONTROLES EXISTENTES (DESCRIBIR CADA UNO DE LOS CONTROLES EXISTENTES, NO PUEDE DEJARSE EN BLANCO)	TIPO DE CONTROL 1= INEXISTENTE 2= DETECTIVO 3= CORRECTIVO 4= PREVENTIVO	FRECUENCIA DEL CONTROL 1= OCASIONAL 2= PERIÓDICO 3= PERMANENTE	PRODUCTO (TIPO DE CONTROL X FRECUENCIA DEL CONTROL)	EFICACIA DEL CONTROL	VALORACIÓN DEL CONTROL (EFICACIA DEL CONTROL X PRODUCTO) (VALORACIÓN FINAL)	NIVEL DE RIESGO RESIDUAL FINAL ZONA DE RIESGO BAJA ZONA DE RIESGO MODERADA ZONA DE RIESGO ALTA ZONA DE RIESGO EXTREMA	OPCIÓN DE TRATAMIENTO (REDUCIR EL RIESGO, EVITAR EL RIESGO, COMPARTIR EL RIESGO, ACEPTAR EL RIESGO)	ACCIONES (ACCIONES ADICIONALES PARA EL TRATAMIENTO DEL RIESGO, ACCIÓN PREVENTIVA O CORRECTIVA PARA EVITAR LA CAUSA RAÍZ DEL RIESGO)	RESPONSABLE (DEL TRATAMIENTO DE LA ACCIÓN)	CRONOGRAMA DEL PLAN DE ACCIÓN FECHA INICIO (MM/YY-DD.mm)	FECHA FIN (MM/YY-DD.mm)
Sistema de Gestión de Seguridad de Información (SGSI)	Proceso_Estratégico	Planeación Institucional	Planeación	**Posibilidad de comprometer la integridad de la información institucional debido a fallas técnicas y operativas en el proceso.**	* [Tecnología] Ausencia de manuales de uso * [Tecnología] Obsolescencia * [Tecnología] Ausencia de mantenimiento adecuado *[Personal] Errores no autorizado a la información. *[Personal] Errores humanos	Seguridad Digital	* Inconsistencias en la calidad de la información y reprocesos. * Dificultades en la comunicación de los procesos. * Inadecuada toma de decisiones. * Perdida reputacional. * Incumplimiento normativo * Procesos administrativos y/o judiciales	3	12	36	ALTO	Acceso a la información con usuarios y claves. Roles y privilegios Identificación de los activos de información Políticas de control de acceso Política de seguridad de la información	5	4	3	12	4	ALTO	MODERADO	Mitigar el Riesgo	**P. Solicitar charla de socialización de las políticas de seguridad de la información para que toda el personal del proceso las conozcan y las cumplan.** **Participar en las sesiones de inducción y reinducción** **Solicitar charlas relacionadas con uso y apropiación de las herramientas tecnológicas.**	R/personas: Comunicaciones.	F: 01/01/24 R: 31/12/24 E:	F: 01/01/24 R: 31/12/24 E:
Sistema de Gestión de Seguridad de Información (SGSI)				**Posibilidad de comprometer la confidencialidad de la información institucional debido a fallas técnicas y operativas en el proceso.**	*[Personal] Trabajo de personal externo sin mantenimiento no supervisado. *[Procesos] Carencia de procedimientos adecuados de eliminación de medios, computadores y disposición final de medio de almacenamiento (Físico y digital). *[Procesos] Desconocimiento o falta de capacitación en seguridad de la información *[Procesos] Ausencia de mantenimiento. *[Procesos] Errores en la definición de roles en las aplicaciones. *[Tecnología] Falta de aplicación de buenas prácticas en la configuración de aplicaciones. *[Procesos] Falta de capacitación de los usuarios de acuerdo con su rol. *[Procesos] Falta de capacitación para las funciones asignadas. *[Procesos] Falta de seguimiento a los controles de acceso a información *[Procesos] Falta de divulgación de las políticas, normas y procedimientos de seguridad de la información. *[Tecnología] Infección de antivirus y código malicioso desactualizada (alojar por nuevas amenazas) *[Procesos] Falta de revocación de los derechos de acceso al activo de información una vez el funcionario cambie de rol o se retire de la organización. *[Personal] Errores humanos	Seguridad Digital					#N/D					0	#N/D						F: 01/01/24 R: 31/12/24 E:	F: 01/01/24 R: 31/12/24 E:
Sistema de Gestión de Seguridad de Información (SGSI)				**Posibilidad de comprometer la disponibilidad por dependencia (parcial o total) tecnológica de los proveedores de servicios TICs**	*[Tecnología] Dependencia tecnológica de los proveedores de las herramientas. *[Tecnología] Limitada capacidad de respuesta frente a mantenibilidad, urgencias, incidencias y requerimientos por parte de TICS *[Procesos] Debilidad en la socialización de las actualizaciones a los sistemas *[Procesos] Limitada asignación de recursos presupuestales para la ejecución de los planes asociados a procesos	Seguridad Digital					#N/D					0	#N/D						F: 01/01/24 R: 31/12/24 E:	F: 01/01/24 R: 31/12/24 E:
Sistema de Gestión de Seguridad de Información (SGSI)				**Posibilidad de no atender las necesidades de automatización de los procesos de la entidad, debido a capacidad limitada de los proveedores adquiridos**	*[Tecnología] Los proveedores son los dueños del código fuente de las aplicativos, y del conocimiento de los mismos, lo para continuidad del negocio necesariamente se debe contratar porque son los únicos que pueden dar soporte y mantenimiento por fallas del mismo, y/o actualizaciones requeridas al producto *[Tecnología] Algunos servicios TIC que soportan la operación de la entidad son especializados y no se cuenta con personal interno con conocimiento suficiente para realizar el soporte de forma interna *[Tecnología] Contratación de productos TICS extemporáneos para generar la mejora a las necesidades actuales de la entidad, evidenciado en el incremento de mesas de ayuda.	Seguridad Digital					#N/D					0	#N/D						F: 01/01/24 R: 31/12/24 E:	F: 01/01/24 R: 31/12/24 E:
Sistema de Gestión de Seguridad de Información (SGSI)				**Posibilidad de tener Sistemas de información obsoletos que no cuenten con soporte debido a la imposibilidad de continuidad a los contratos de soporte y mantenimiento**	*[Tecnología] El fabricante del sistema de información está caducando para contratar con entidades del Estado *[Financieros] falta de recursos para dar continuidad a contratos de soporte y mantenimiento	Seguridad Digital					#N/D					0	#N/D						F: 01/01/24 R: 31/12/24 E:	F: 01/01/24 R: 31/12/24 E:
Sistema de Gestión de Seguridad de Información (SGSI)				**Posibilidad de tener afectación de integridad, confidencialidad y/o disponibilidad de la información por errores humanos**	Desconocimiento de los lineamientos del SGSI (políticas, normas y procedimientos). Falta de aplicación de buenas prácticas de seguridad. Falta establecerlas en la guía de roles de Servicios Tecnológicos de la Estrategia de gobierno en línea. Falta de uso y apropiación en cultura organizacional en seguridad de la información. Incumplimiento y/o desactualización de los Procesos y procedimientos relacionados con Gestión de TICS. Inadecuado manejo de la información causada por una indebida manipulación de los sistemas. Perdida de datos. Copia no autorizada de información. Modificación no aceptó/autorizó de información. Ausencia de personal. Uso no autorizado de equipos. Servidor público inadecuado. Errores de confianza	Seguridad Digital					#N/D					0	#N/D						F: 01/01/24 R: 31/12/24 E:	F: 01/01/24 R: 31/12/24 E: