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 RARA VEZ = 1 IMPROBABLE = 2 POSIBLE = 3 PROBABLE = 4 CASI SEGURO = 5	IMPACTO ESCALA INSIGNIFICANTE = 3 MENOR = 6 MODERADO = 9 MAYOR = 12 CATASTROFICO = 15	EVALUACION DEL RIESGO INHERENTE (PROBABILIDAD X IMPACTO)	NIVEL DE RIESGO INHERENTE (RIESGOS PROPIOS DEL PROCESO O ACTIVIDAD)	CONTROLES EXISTENTES (SE DETALLAN LOS CONTROLES EXISTENTE)	CANT. DE CONTROLES EXISTENTES (SE SUMAN LOS # DE CONTROLES EXISTENTES REFIERE COLUMNA N)	TIPO DE CONTROL 1= INEXISTENTE 2= DETECTIVO 3= CORRECTIVO 4= PREVENTIVO	PERIODICIDAD DEL CONTROL 1= OCASIONAL 2= PERIÓDICO 3= PERMANENTE	PRODUCTO (TIPO DE CONTROL X PERIODICIDAD DEL CONTROL)	EFICACIA DEL CONTROL	VALORACION DEL CONTROL (EFICACIA DEL CONTROL EN TÉRMINOS CUALITATIVOS)	NIVEL DE RIESGO RESIDUAL ESCALA EXTREMO ALTO MODERADO BAJO	OPCIÓN DE TRATAMIENTO (MITIGAR /ASUMIR /EVITAR / /TRASNFERIR)	ACCIONES (CONTROL EFECTIVO FUTURO A IMPLEMENTAR) (DETALLAR PLAN DE ACCIÓN EN TÉRMINOS DEL CICLO PVHA)	RESPONSABLE (DEL TRATAMIENTO DEL RIESGO)	CRONOGRAMA DEL PLAN DE ACCIÓN FECHA INICIO (dd/mm/aaaa)	CRONOGRAMA DEL PLAN DE ACCIÓN FECHA FIN (dd/mm/aaaa)
Sistema de Gestión de Seguridad de Información (SGSI)	Proceso_Misional	Gestión Evaluación del Riesgo	Generar los parámetros y lineamientos institucionales para la gestión y trámite de las evaluaciones del riesgo tanto individual, colectivo y a instalaciones de las poblaciones objeto del Programa de Prevención y Protección de la Unidad Nacional de Protección, necesario para coadyuvar a garantizar la vida y la integridad de las personas, grupos o comunidades, de acuerdo al nivel de riesgo extraordinario o extremo que se presente mediante el análisis efectuado	**Posibilidad de comprometer la integridad de la información institucional debido a fallas técnicas y operativas en el proceso.**	* (Proceso) Asignación errada de los derechos de acceso *(Tecnología) Ausencia de mecanismos de identificación y autentificación * (Proceso) Ausencia de control de los activos que se encuentran fuera de las instalaciones * (Proceso) Exposición de datos de respaldo * (Tecnologia) Ciberataques * (Tecnologia) Mantemiento insuficiente *(Procesos) Modificar la información sin autorización Inadecuado manejo de la información causada por una indebida manipulación de los custodios *(Procesos) Acceso no autorizado la información. *(Tecnología) Inconsistencias en la información *(Personal) Errores humanos * (Tecnologia) algunos equipos de computo obsoletos *(Procesos) Errores en la definición de roles en las aplicaciones *(Procesos) Debilidad en la capacitación *(Procesos) actualización a los usuarios en el manejo de las aplicaciones, sistemas de información y herramientas *(Procesos) Debilidad en la documentación sobre el uso de los servicios tecnológicos *(Procesos) Falta de planes de sensibilización en SI *(Procesos) Inadecuado control de acceso lógico y físico a los activos de información. *(Personal) Hurto de equipos *(Procesos) Falta de divulgación de las políticas y procedimientos propios del proceso	Seguridad Digital	* Inconsistencias en la calidad de la información y reprocesos. * Afectación en la comunicación de los servicios. * Inadecuada toma de decisiones. * Perdida reputacional. * Alteración de la información para beneficio propio. * Incumplimiento normativo * Procesos administrativos y/o judiciales	4	12	48	EXTREMO	Acceso a los servicios tecnolgicos con usuario validos. Roles y privilegios Acuerdo de confidencialidad Politicas de segurida de la informacion log de alerta para la eliminacion de la informaicon en el sharepoint Indentifcacion y clasificacion de los activos	6	4	3	12	4	ALTO	MODERADO	Mitigar el Riesgo	**fortalecer las capacidades en el uso y apropiacion de las herramientas tecnologicas a traves de charlas la interior de la entidsd. Implementar una estrategia de comunicacion adecauada para TODOS los servidores publicos y colaboradores conozcan y las cumplan. Cumplir con las politicas de seguridad y privacidad de la informacion. Informar al proceso de Generar la necesidad de proyectos de renovacion tecnologica. P: Se Pleanea realizar reunion con partes interesadas. H: Se toman decisiones mediante un plan de sensibilización para los servidores publicos y contratista referente al cumplimiento de politicas. Elabore un instrumento de evaluación frente a los**		P: H: V: A:	P: H: V: A:
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 o de mantenimiento no supervisado. *(Procesos) Carencia de procedimientos adecuados de reutilización 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) Equipos de cómputo desatendidos *(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 la información *(Procesos) Falta de divulgación de las políticas, normas y procedimientos de seguridad de la información. *(Tecnología) Solución de antivirus y código malicioso desactualizada (ataque 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. Controles de acceso debiles	Seguridad Digital					#N/D	1. Politícas de Seguridad. 2. Politicas TI. 3. Documentacion (Procedimientos-formatos-instructivos). 4. Segmentación de RED. 5. Areas Seguras definidas. 6. Usuarios con acceso logico.				0	#N/D						P: H: V: A:	P: H: V: A:
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 eventualidades, urgencias, incidencias y requerimientos por parte de TICS *(Procesos) Debilidad en la socialización de las actualizaciones a los sistemas *(Financieros) Limitada asignación de recursos presupuestales para la ejecución de los planes asociados al proceso	Seguridad Digital					#N/D					0	#N/D						P: H: V: A:	P: H: V: A:
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 productos adquiridos**	*(Tecnología) Los proveedores son los dueños del código fuente de los aplicativos, y del conocimiento de los mismos; si para continuidad del negocio necesariamente se les debe contratar porque son los únicos que pueden dar soporte y mantenimiento por fallos 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 las capacidades para atenderlos adecuadamente, por lo que se tercerizan *(Tecnología) Contratación de productos TICS con especificaciones generales frente a las necesidades puntuales de la entidad, evidenciado en el momento de entrega de los mismos.	Seguridad Digital					#N/D					0	#N/D						P: H: V: A:	P: H: V: A:
Sistema de Gestión de Seguridad de Información (SGSI)				**Posibilidad de tener Sistemas de información desatendidos o sin soporte debido a la imposibilidad de continuidad a los contratos de soporte y mantenimiento**	*(Tecnología) El fabricante del sistema de información está sancionado para contratar con entidades del Estado *(Financieros) Falta de recurso para dar continuidad a contratos de soporte y mantenimiento	Seguridad Digital					#N/D					0	#N/D						P: H: V: A:	P: H: V: A:
Sistema de Gestión de Seguridad de Información (SGSI)				**Posibilidad de tener afectacion de integridad, confidencilaid y/o disponibilidad de la informacion por errores humanos**	Desconocimiento de los lineamientos del SGSI (políticas, normas y procedimientos). Ausencia de personal que cumpla con los Roles establecidos en la guía de roles de Servicios Tecnológicos de la Estrategia de gobierno en Linea. Falta de uso y apropiacion en cultura organizacional en seguridad de la informacion. 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 custodios Abuso de derechos Copia no autorizada de información Modiifcación no aupotrizada de informacion. Ausencia de personal. Uso no autorizado de equipos Servidor publico insatisfecho Exceso de confianza	Seguridad Digital					#N/D					0	#N/D						P: H: V: A:	P: H: V: A: