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)	FECHA FIN (dd/mm/aaaa)
Sistema de Gestión de Seguridad de Información (SGSI)	Proceso_Misional	Gestión Medidas de Protección	Gestionar la implementación, el seguimiento y control de las medidas de prevención y protección tendientes a salvaguardar la vida de los beneficiarios del programa de protección, así como realizar el desmonte de medidas, de acuerdo con la normativa vigente y procedimientos establecidos	**Posibilidad de comprometer la integridad de la información institucional debido a fallas técnicas y operativas en el proceso.**	*(Procesos) Modificar la información sin autorización *(Procesos) Inadecuado manejo de la información causada por una indebida manipulación de los custodios *(Tecnología) Inconsistencias en la información *(Personal) Errores humanos *(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. *(Procesos) Debilidades en la divulgación y cumplimiento de las políticas para la realización de BackUp y copias de seguridad. * (Proceso) Posibilidad de extravió, pérdida, deterioro o daño del dispositivo * (Tecnología) Ciberataques	Seguridad Digital	* Inconsistencias en la calidad de la información y reprocesos. * Inadecuada toma de decisiones. * Perdida reputacional. * Alteración de la información para beneficio propio. * Reprocesos en la gestión. * Incumplimiento normativo. * Procesos administrativos y/o judiciales. * Afectación en las finanzas de la entidad.	3	9	27	ALTO	1. Políticas de Seguridad. 2. Políticas TI. 3. Documentacion (Procedimientos-formatos-instructivos). 4. Autenticación de Usuarios. 5. Permisos de Acceso a los servicios asignados. 6. Monitoreo de acceso de bienes y personas. 7. Copias de respaldo. 8. Registro de eventos.	8	4	3	12	4	ALTO	BAJO	Mitigar el Riesgo	**P: Se planea una reunión con las partes interesadas: Talento Humano (Capacitación), Oficina Asesora de Planeación e información (Gestión de Tecnologías de la Información) y Subdirección de Protección; con el fin de determinar el plan de capacitación necesario para el personal asociado a los procesos que permita cubrir y reforzar los conocimientos sobre los temas requeridos. H: Se ejecuta el plan de capacitación de acuerdo con lo definido. V: Al final de cada sesión se deberá hacer la correspondiente verificación de la eficacia de la capacitación. Para el personal que se identifique que no alcanzó los objetivos de la capacitación deberá volver a tomarla. A: Para el personal que se identifique que no alcanzó los objetivos de la capacitación deberá volver a tomarla. P: Se planea una reunión con las partes interesadas: Seguridad de la Información, Tecnología y Subdirección de Protección; con el fin de determinar**	Talento Humano (Capacitación), Oficina Asesora de Planeación e información (Gestión de Tecnologías de la Información) y Subdirección de Protección	P: H: De acuerdo a cronograma definido para 2022 V: De acuerdo a cronograma definido para 2022 A: De acuerdo a cronograma definido para 2022 P: H: De acuerdo a cronograma definido para 2022 V: De acuerdo a cronograma definido para 2022 A: De acuerdo a cronograma definido para 2022	P: H: De acuerdo a cronograma definido para 2022 V: De acuerdo a cronograma definido para 2022 A: De acuerdo a cronograma definido para 2022 P: H: De acuerdo a cronograma definido para 2022 V: De acuerdo a cronograma definido para 2022 A: De acuerdo a cronograma definido para 2022
Sistema de Gestión de Seguridad de Información (SGSI)	Proceso_Misional	Gestión Medidas de Protección	Gestionar la implementación, el seguimiento y control de las medidas de prevención y protección tendientes a salvaguardar la vida de los beneficiarios del programa de protección, así como realizar el desmonte de medidas, de acuerdo con la normativa vigente y procedimientos establecidos	**Posibilidad de comprometer la confidencialidad de la información institucional debido a fallas técnicas y operativas en el proceso.**	*(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) Falta de capacitación de los usuarios de acuerdo con su rol. *(Procesos) Falta de seguimiento a los controles de acceso a la información. *(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. *No se cuenta con un lineamiento que establezca los criterios o condiciones para el almacenamiento de información en nubes externas de carácter interinstitucional * (Proceso) Posibilidad de extravió, pérdida, deterioro o daño del dispositivo * (Tecnología) Ciberataques	Seguridad Digital	*Fuga de información. * Imagen y reputación de la entidad. * Incumplimiento normativo. * Procesos administrativos y/o judiciales. * Afectación en las finanzas de la entidad.	3	9	27	ALTO	1. Políticas de Seguridad. 2. Políticas TI. 3. Documentacion (Procedimientos-formatos-instructivos). 4. Autenticación de Usuarios. 5. Permisos de Acceso a los servicios asignados. 6. Monitoreo de acceso de bienes y personas. 7. Copias de respaldo. 8. Registro de eventos.	8	4	3	12	4	ALTO	BAJO	Mitigar el Riesgo	**P: Se planea una reunión con las partes interesadas: Talento Humano (Capacitación), Oficina Asesora de Planeación e información (Gestión de Tecnologías de la Información) y Subdirección de Protección; con el fin de determinar el plan de capacitación necesario para el personal asociado a los procesos que permita cubrir y reforzar los conocimientos sobre los temas requeridos. H: Se ejecuta el plan de capacitación de acuerdo con lo definido. V: Al final de cada sesión se deberá hacer la correspondiente verificación de la eficacia de la capacitación. Para el personal que se identifique que no alcanzó los objetivos de la capacitación deberá volver a tomarla. A: Para el personal que se identifique que no alcanzó los objetivos de la capacitación deberá volver a tomarla.**	Talento Humano (Capacitación), Oficina Asesora de Planeación e información (Gestión de Tecnologías de la Información) y Subdirección de Protección	P: H: De acuerdo a cronograma definido para 2022 V: De acuerdo a cronograma definido para 2022 A: De acuerdo a cronograma definido para 2022 P: H: De acuerdo a cronograma definido para 2022 V: De acuerdo a cronograma definido para 2022 A: De acuerdo a cronograma definido para 2022	P: H: De acuerdo a cronograma definido para 2022 V: De acuerdo a cronograma definido para 2022 A: De acuerdo a cronograma definido para 2022 P: H: De acuerdo a cronograma definido para 2022 V: De acuerdo a cronograma definido para 2022 A: De acuerdo a cronograma definido para 2022
Sistema de Gestión de Seguridad de Información (SGSI)	Proceso_Misional	Gestión Medidas de Protección	Gestionar la implementación, el seguimiento y control de las medidas de prevención y protección tendientes a salvaguardar la vida de los beneficiarios del programa de protección, así como realizar el desmonte de medidas, de acuerdo con la normativa vigente y procedimientos establecidos	**Posibilidad de comprometer la disponibilidad por dependencia (parcial o total) tecnológica de los proveedores de servicios TICS**	requerimientos por parte de TICS * (Proceso) Posibilidad de pérdida de los registros documentales que no están en los repositorios institucionales, o en los PC´s de los funcionarios *(Tecnología) No contar con el acceso al aplicativo o sitio web, por eventos o incidentes. *(Tecnología) No contar con el acceso al servicios del correo institucional, por eventos o incidentes. * (Persona) Posibilidad de extravío, pérdida o daño de la información, por agente externo (Humano o ambiental). *(Procesos) Debilidades en la divulgación y cumplimiento de las políticas para la realización de BackUp y copias de seguridad. * (Proceso) Posibilidad de extravió, pérdida, deterioro o daño del dispositivo * (Tecnología) Ciberataques	Seguridad Digital	*No poder responder oportuna y eficazmente a las solicitudes que presentan las partes interesadas de la entidad. *Reprocesos en la gestión.{ * Imagen y reputación de la entidad. * Incumplimiento normativo. * Procesos administrativos y/o judiciales. * Afectación en las finanzas de la entidad.	3	9	27	ALTO	1. Políticas de Seguridad. 2. Políticas TI. 3. Documentacion (Procedimientos-formatos-instructivos). 4. Autenticación de Usuarios. 5. Permisos de Acceso a los servicios asignados. 6. Monitoreo de acceso de bienes y personas. 7. Copias de respaldo. 8. Registro de eventos.	8	4	3	12	4	ALTO	BAJO	Mitigar el Riesgo	**P: Se planea una reunión con las partes interesadas: Talento Humano (Capacitación), Oficina Asesora de Planeación e información (Gestión de Tecnologías de la Información) y Subdirección de Protección; con el fin de determinar el plan de capacitación necesario para el personal asociado a los procesos que permita cubrir y reforzar los conocimientos sobre los temas requeridos. H: Se ejecuta el plan de capacitación de acuerdo con lo definido. V: Al final de cada sesión se deberá hacer la**	Talento Humano (Capacitación), Oficina Asesora de Planeación e información (Gestión de Tecnologías de la Información) y Subdirección de Protección	P: H: De acuerdo a cronograma definido para 2022 V: De acuerdo a cronograma definido para 2022 A: De acuerdo a cronograma definido para 2022 P: H: De acuerdo a cronograma definido para 2022	P: H: De acuerdo a cronograma definido para 2022 V: De acuerdo a cronograma definido para 2022 A: De acuerdo a cronograma definido para 2022 P: H: De acuerdo a cronograma definido para 2022
Sistema de Gestión de Seguridad de Información (SGSI)	Proceso_Misional	Gestión Medidas de Protección	Gestionar la implementación, el seguimiento y control de las medidas de prevención y protección tendientes a salvaguardar la vida de los beneficiarios del programa de protección, así como realizar el desmonte de medidas, de acuerdo con la normativa vigente y procedimientos establecidos	**Posibilidad de no atender las necesidades de automatización de los procesos de la entidad, debido a capacidad limitada de los productos adquiridos**	N/A - Hace parte de los tres riesgos identificados anteriormente.						#N/D					0	#N/D						P: H: V: A:	P: H: V: A:
Sistema de Gestión de Seguridad de Información (SGSI)	Proceso_Misional	Gestión Medidas de Protección	Gestionar la implementación, el seguimiento y control de las medidas de prevención y protección tendientes a salvaguardar la vida de los beneficiarios del programa de protección, así como realizar el desmonte de medidas, de acuerdo con la normativa vigente y procedimientos establecidos	**Posibilidad de tener Sistemas de información desatendidos o sin soporte debido a la imposibilidad de continuidad a los contratos de soporte y mantenimiento**	N/A - Hace parte de los tres riesgos identificados anteriormente.						#N/D					0	#N/D						P: H: V: A:	P: H: V: A:
Sistema de Gestión de Seguridad de Información (SGSI)	Proceso_Misional	Gestión Medidas de Protección	Gestionar la implementación, el seguimiento y control de las medidas de prevención y protección tendientes a salvaguardar la vida de los beneficiarios del programa de protección, así como realizar el desmonte de medidas, de acuerdo con la normativa vigente y procedimientos establecidos	**Posibilidad de tener afectacion de integridad, confidencilaid y/o disponibilidad de la informacion por errores humanos**	N/A - Hace parte de los tres riesgos identificados anteriormente.						#N/D					0	#N/D						P: H: V: A:	P: H: V: A: