GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

	IDENTIFICACIÓN								CALIFICACIÓN				VALORACIÓN								PLAN DE TRATAMIENTO				
									PROBABILIDAD ESCALA	IMPACTO ESCALA				TIPO DE CONTROL	NUMERO DIAS DEL CONTROL								CRONOGRAMA DEL PLAN DE ACCIÓN	
COMPONENTE DEL SIG	TIPO DE PROCESO	PROCESO	OBJETIVO DEL PROCESO	RIESGO	CAUSAS O EVENTOS	TIPO DE RIESGO	CONSECUENCIAS (RESULTADO DEL EVENTO)		BAJA 10 = 1 IMPROBABLE = 2 POSIBLE = 3 PROBABLE = 4 CASI SEGURO = 5	INSIGNIFICANTE = 1 MENOR = 2 MODERADO = 4 MAYOR = 12 CATASTROFICO = 20	EVALUACIÓN DEL RIESGO INHERENTE (PROBABILIDAD X IMPACTO)	NIVEL DE RIESGO INHERENTE (REFERIRSE TABLA DE ZONAS DE RIESGO INHERENTE)	CONTROLES EXISTENTES (DE DETALLAR LOS CONTROLES EXISTENTES)	CANT. DE CONTROLES EXISTENTES (DEBE TENER CLARIDAD EN LOS CONTROLES REFERIR SOLO LOS QUE SE ASOCIAN AL RIESGO)	1= INEXISTENTE 2= DETECTIVO 3= CORRECTIVO 4= PREVENTIVO	1= OCASIONAL 2= PERIÓDICO 3= PERMANENTE	PRODUCTO (TIPO DE CONTROL X PERIODICIDAD DEL CONTROL)	EFICACIA DEL CONTROL	VALORACIÓN DEL CONTROL (EFICACIA DEL CONTROL X PRODUCTO DEL CONTROL)	NIVEL DE RIESGO RESIDUAL ESCALA EXTREMO ALTO MODERADO BAJO	OPCIÓN DE TRATAMIENTO (REFERIRSE TABLA DE ZONAS DE RIESGO INHERENTE)	ACCIONES (ACTIVIDADES ASOCIADAS A LA OPCIÓN DE TRATAMIENTO DEL RIESGO FINAL)	RESPONSABLE (DEL TRATAMIENTO DEL RIESGO)	FECHA INICIO (DD/MM/AAAA)	FECHA FIN (DD/MM/AAAA)
Sistema de Gestión de Seguridad de Información (SGSI)	Proceso_Estratégico	Gestión Estratégica del Talento Humano	Gestionar, simular y promover el desarrollo y bienestar del talento humano que permita contribuir al logro de la misionalidad de la entidad, en el marco de la integridad y del servicio público.	Posibilidad de comprometer la integridad de la información institucional debido a fallas técnicas y operativas en el proceso.	* [Proceso] Implementación de soluciones tecnológicas sin la validación y autorización del proceso de gestión tecnológica * [Proceso] Asignación errada de los derechos de acceso *[Proceso] Modificar la información en automatización *Inadecuado manejo de la información causada por una indebida manipulación de los cuidados. *[Tecnología] Inconsistencias en la información *[Personal] Errores humanos *[Proceso] Errores en la definición de roles en las aplicaciones	Seguridad Digital	* Inconsistencias en la calidad de la información y reprocesos. * Inadecuada toma de decisiones. * Posible requisicional. * Procesos administrativos y/o judiciales		4	12	48	EXTREMO	*Politicas para la seguridad de la información *Roles de responsabilidades *Seguridad de la información roles y responsabilidades *Gestión de información de autenticación secreta de usuarios.	4	4	3	12	4	ALTO	MODERADO	Evitar el Riesgo	P. Planear reuniones con los equipo de trabajo para tener una sola fuente de información. H. Evaluar y revisar las fuentes de información que utilizamos. V. Realizar seguimiento y muestras aleatorias de la información. A. Se realiza memorando a todo el personal del área indicando las fuentes de información que deben ser utilizadas.	Servidores públicos y/o contratistas de la Subdirección de Talento Humano	P: 01/01/2022 H: 01/02/2022 V: 01/05/2022 A: 01/05/2022	P: 30/06/2022 H: 30/03/2022 V: 30/12/2022 A: 30/12/2022
Sistema de Gestión de Seguridad de Información (SGSI)		Gestión Estratégica del Talento Humano	Gestionar, simular y promover el desarrollo y bienestar del talento humano que permita contribuir al logro de la misionalidad de la entidad, en el marco de la integridad y del servicio público.	Posibilidad de comprometer la confidencialidad de la información institucional debido a fallas técnicas y operativas en el proceso.	* [Proceso] Desconocimiento y/o incumplimiento de las politicas de seguridad y privacidad de la información. *[Personal] Trabajo de personal externo sin el entrenamiento no supervisado. *[Personal] Falta de seguimiento a los controles de acceso a la información *[Personal] Accesos autorizado a la información.	Seguridad Digital	*Fuga de información * Imagen y reputación de la entidad * Incumplimiento normativo. * Afectación en la credibilidad hacia la entidad.		3	9	27	ALTO	*Clasificación de la información *Gestión de Accesos a usuarios *Control de acceso a sistemas y aplicaciones *Capacitación especial para quienes tienen acceso a documentos reservados.	4	4	3	12	4	ALTO	BAJO	Evitar el Riesgo	P. Planear reunión con el equipo de trabajo H. Informar sobre la importancia de la confidencialidad de la información. V. Realizar seguimiento a la información confidencial del área y los personas que tienen acceso. A. se realiza memorando al personal que incumpla con las disposiciones dadas.	Servidores públicos y/o contratistas de la Subdirección de Talento Humano	P: 01/01/2022 H: 01/02/2022 V: 01/05/2022 A: 01/05/2022	P: 30/06/2022 H: 30/03/2022 V: 30/12/2022 A: 30/12/2022
Sistema de Gestión de Seguridad de Información (SGSI)		Gestión Estratégica del Talento Humano	Gestionar, simular y promover el desarrollo y bienestar del talento humano que permita contribuir al logro de la misionalidad de la entidad, en el marco de la integridad y del servicio público.	Posibilidad de comprometer la disponibilidad por dependencia (parcial o total) tecnologica de los procedimientos 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	Seguridad Digital	*No poder responder oportuna y eficazmente a las solicitudes que presentan los usuarios internos de la entidad. *Repercusiones en la gestión *Dificultad en el acceso a la información por indisponibilidad del servicio.		3	9	27	ALTO	*Politica para dispositivos moviles *Requisitos del negocio para control de acceso *Gestión de acceso de usuarios *Cadena de suministro de tecnologia de información y comunicación	4	4	3	12	4	ALTO	BAJO	Evitar el Riesgo	P. Planear reunión con partes interesadas. H. Realizar listado de la información sensible del área y otros backup en caso de no tener acceso al sistema de información. H. Realizar seguimiento a los backup realizados. A. Se realiza comunicación a las partes interesadas información de la sucursales.	Servidores públicos y/o contratistas de la Subdirección de Talento Humano	P: 01/01/2022 H: 01/02/2022 V: 01/05/2022 A: 01/05/2022	P: 30/06/2022 H: 30/03/2022 V: 30/12/2022 A: 30/12/2022
Sistema de Gestión de Seguridad de Información (SGSI)	Proceso_Estratégico	Gestión Estratégica del Talento Humano	Gestionar, simular y promover el desarrollo y bienestar del talento humano que permita contribuir al logro de la misionalidad de la entidad, en el marco de la integridad y del servicio público.	**Posibilidad de no atender la necesidades de automatización de los procesos de la entidad, debido a capacidad limitada de los proveedores adquiridos**	* [Proceso] Implementación de soluciones tecnológicas sin la validación y autorización del proceso de gestión tecnológica * [Proceso] Desconocimiento y/o incumplimiento de las politicas de seguridad y privacidad de la información. *[Tecnología] Los proveedores son los dueños del código fuente de las aplicativos, y del conocimiento de los mismos, si para continuidad del negocio internamente no les 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 organizaciones y no se cuenta con el personal idóneo para el mantenimiento y/o actualización de los mismos. *[Tecnología] Caracterización de productos TICS no específicos, para que se ajuste a las necesidades y/o actividades de la entidad, mediante el uso de herramientas ofimáticas.	Seguridad Digital						#N/D					0	#N/D				**P. Se Planean realizar reuniones con partes interesadas H. Se toman decisiones mediante un plan de sensibilización para los servidores publicos y contratistas referente al cumplimiento de politicas. V. Se realizan encuestas de evaluación frente a las temas sensibilizados. V. aplica instrumento y evalua mediante indicadores de sensibilizacion. A. Se realizan memorando a todo el personal indicando que se tiene las politicas y los aplique porque el resultado de la evaluacion no fue optimo y se evidencia que hay falencias en la apropiacion de los temas.**		P: H: V: A:		P: H: V: A:
Sistema de Gestión de Seguridad de Información (SGSI)	Proceso_Estratégico	Gestión Estratégica del Talento Humano	Gestionar, simular y promover el desarrollo y bienestar del talento humano que permita contribuir al logro de la misionalidad de la entidad, en el marco de la integridad y del servicio público.	**Posibilidad de tener Sistemas de información obsoletos que no ofrezcan 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	*Incumplimiento normativo. *Sanciones por los entes de control. *Afectación en las finanzas de la entidad		3			#N/D					0	#N/D					P: H: V: A:		P: H: V: A:
Sistema de Gestión de Seguridad de Información (SGSI)	Proceso_Estratégico	Gestión Estratégica del Talento Humano	Gestionar, simular y promover el desarrollo y bienestar del talento humano que permita contribuir al logro de la misionalidad de la entidad, en el marco de la integridad y del servicio público.	Posibilidad de tener afectaciones de integridad, confidencialidad y/o disponibilidad de la información por errores humanos	* [Proceso] Desconocimiento y/o incumplimiento de las politicas de seguridad y privacidad de la información. Desconocimiento de los lineamientos del SGSI (politicas, normas y procedimientos). *Inadecuado manejo de la información causada por una indebida manipulación de los cuidados. *Deterior publico inestable/ne	Seguridad Digital	* Afectación en la comunicación de los servicios. * Inadecuada toma de decisiones. * Posible requisicional. * Alteración de la información para beneficio propio. * Incumplimiento normativo * Procesos administrativos y/o judiciales		3	9	27	ALTO	*Politicas para seguridad de la información *Roles de responsabilidades *Clasificación de la información *Gestión de medios de soporte y removibles *Gestión de accesos a usuarios *Control de acceso a sistemas y aplicaciones	6	4	3	12	4	ALTO	BAJO	Evitar el Riesgo	P. Planear reuniones con los equipos de trabajo para tener una sola fuente de información. H. Evaluar y revisar las fuentes de información que utilizamos. V. Realizar seguimiento y muestras aleatorias de la información. A. Se realiza memorando a todo el personal del área indicando las fuentes de información que deben ser utilizadas.	Servidores públicos y/o contratistas de la Subdirección de Talento Humano	P: 01/01/2022 H: 01/02/2022 V: 01/05/2022 A: 01/05/2022	P: 30/06/2022 H: 30/03/2022 V: 30/12/2022 A: 30/12/2022