GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

IDENTIFICACIÓN								CALIFICACIÓN				VALORACIÓN								PLAN DE
COMPONENTE DEL GIS	TIPO DE PROCESO	PROCESO	OBJETIVO DEL PROCESO	RIESGO	CAUSAS O EVENTOS	TIPO DE RIESGO	CONSECUENCIAS (RESULTADOS DEL EVENTO)	PROBABILIDAD INHERENTE [NUMERO DE VECES QUE SE PASA POR EL PUNTO DE RIESGO EN EL TIEMPO QUE DURA EL DESARROLLO DEL PROCESO] 5= CASI SEGURO – >5 4=PROBABLE – 4 3=MODERADO – 3 2=RARO – 2 1=CASI IMPOSIBLE – <1	IMPACTO INHERENTE [CONSECUENCIAS ECONÓMICAS O REPUTACIONALES] 5=CATASTRÓFICO – 5 4=MAYOR – 4 3=MODERADO – 3 2=MENOR – 2 1=INSIGNIFICANTE – 1	EVALUACIÓN DEL RIESGO INHERENTE [PROBABILIDAD X IMPACTO]	NIVEL DE RIESGO INHERENTE [RESULTADO DE LA EVALUACIÓN DEL RIESGO INHERENTE]	CONTROLES EXISTENTES DE CADA UNA DE LAS CAUSAS O EVENTOS CONTROLES EXISTENTES	CANT. DE CONTROLES EXISTENTES [CANTIDAD DE CONTROLES EXISTENTES PARA CADA CAUSA O EVENTO]	TIPO DE CONTROL 1= INCORRECTIVO 2= CORRECTIVO 3= PREVENTIVO	FRECUENCIA DEL CONTROL 1= OCASIONAL 2= PERIÓDICO 3= PERMANENTE	PRODUCTO (TIPO DE CONTROL X FRECUENCIAS DEL CONTROL)	EFICACIA DEL CONTROL	CALIFICACIÓN DEL CONTROL [RESULTADO DE LA EVALUACIÓN DEL CONTROL]	NIVEL DE RIESGO RESIDUAL [RESULTADO DE LA EVALUACIÓN DEL RIESGO RESIDUAL] Bajo Moderado Alto	OPCIÓN DE TRATAMIENTO [OPCIÓN: CANCELAR, MITIGAR, TRANSFERIR]	ACCIONES [ACTIVIDAD DE CONTROL, RESPONSABLE, FECHA IMPLEMENTACIÓN, FECHA SEGUIMIENTO, EVIDENCIA DE LA ACTIVIDAD DE CONTROL]
Sistema de Gestión de Seguridad de Información (SGSI)	Proceso_Estratégico	Direccionamiento Estratégico	Dirigir estratégicamente a la Unidad Nacional de Protección -UNP- a través de la definición de lineamientos generales, políticas, estrategias y del modelo de operación, armonizando los planes, programas y proyectos de carácter estratégico para dar cumplimiento a la misión, objetivos institucionales, sectoriales y metas de gobierno.	**Posibilidad de comprometer la integridad de la información institucional debido a fallas técnicas y operativas en el proceso.**	[Tecnología] Mantenimiento insuficiente [Personal] Errores humanos [Procesos] adaptación a los usuarios en el manejo de las aplicaciones, sistemas de información y herramientas	Seguridad Digital	* Inconsistencias en la calidad de la información y proporcionar información errónea a los usuarios de los servicios. * Inoportunidad toma de decisiones por parte de la alta dirección * Incumplimiento normativo * Reprocesos administrativos y/o judiciales	3	9	27	ALTO	GESTION DE ACTIVOS	1	4	2	8	3	MEDIO	MODERADO	Mitigar el Riesgo	**Participar en las sesiones de inducción y reinducción Realizar charlas relacionadas con uso y apropiación de las herramientas tecnológicas.**
Sistema de Gestión de Seguridad de Información (SGSI)	Proceso_Estratégico	Direccionamiento Estratégico	Dirigir estratégicamente a la Unidad Nacional de Protección -UNP- a través de la definición de lineamientos generales, políticas, estrategias y del modelo de operación, armonizando los planes, programas y proyectos de carácter estratégico para dar cumplimiento a la misión, objetivos institucionales, sectoriales y metas de gobierno.	**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 de mantenimiento de medios. [Procesos] Ausencia de Plan de mantenimiento de equipos de digital. [Procesos] Desconocimiento activo de responsabilidades en seguridad de la información [Procesos] Falta de capacitación de los usuarios de acuerdo con su rol. [Procesos] Falta de seguimiento a los sistemas de acceso a la información. [Procesos] Ausencia de políticas y código de conducta documentado (aplicar por horas extensas) [Procesos] Falta de renovación de los derechos de acceso al activo de información una vez finalizado el contrato o cambio de rol o retiro de la organización. Sistemas de acceso débiles	Seguridad Digital	Llamados de atención	2	9	18	MODERADO	1. Políticas de Seguridad. 2. SEGURIDAD DE LOS RECURSOS HUMANOS. 3. CONTROL DE ACCESO. 4. SEGURIDAD FÍSICA Y DEL ENTORNO 5. SEGURIDAD DE LAS OPERACIONES. 6. SEGURIDAD DE LAS COMUNICACIONES.	6	4	2	8	3	MEDIO	BAJO	Mitigar el Riesgo	**ASEGURAR LA VIGILANCIA DE CONTRATISTAS Y SEGUROS DE ACUERDO AL ROL.**
Sistema de Gestión de Seguridad de Información (SGSI)	Proceso_Estratégico	Direccionamiento Estratégico	Dirigir estratégicamente a la Unidad Nacional de Protección -UNP- a través de la definición de lineamientos generales, políticas, estrategias y del modelo de operación, armonizando los planes, programas y proyectos de carácter estratégico para dar cumplimiento a la misión, objetivos institucionales, sectoriales y metas de gobierno.	**Posibilidad de comprometer la disponibilidad por dependencia (parcial o total) tecnológica de los procesos de carácter TIC**	[Tecnología] Dependencia tecnológica de los proveedores de las herramientas. [Tecnología] Ausencia de planes de mantenimiento a maquinarias, equipos, herramientas y computadoras por parte de TIC. [Procesos] Debilidad en la sensibilización de las actualizaciones a los sistemas [Procesos] Ausencia de planes de contingencia de procesos presupuestales para la ejecución de los planes anualizados en planeación	Seguridad Digital	Reprocesos	3	9	27	ALTO	1. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	1	4	1	4	2	BAJO	MODERADO	Mitigar el Riesgo	**ASEGURAR LA DISPONIBILIDAD DE EQUIPOS**
Sistema de Gestión de Seguridad de Información (SGSI)	Proceso_Estratégico	Direccionamiento Estratégico	Dirigir estratégicamente a la Unidad Nacional de Protección -UNP- a través de la definición de lineamientos generales, políticas, estrategias y del modelo de operación, armonizando los planes, programas y proyectos de carácter estratégico para dar cumplimiento a la misión, objetivos institucionales, sectoriales y metas de gobierno.	**Posibilidad de no atender las necesidades de automatización de requerimientos de la entidad, debido a la escasez de los productos adquiridos**	desconocimiento de los riesgos; y; para continuidad del negocio mancomunamente se les debe establecer acuerdos, planes que permitan el soporte y mantenimiento por falta del mantenimiento de los equipos de cómputo. [Tecnología] Algunos sistemas Tic que soportan la operación de la entidad son heredados y no se cuenta con las capacidades para atenderlos adecuadamente, por lo que se tiene: [Tecnología] Contratación de productos TIC con especificaciones genéricas frente a los necesidades puntuales de la entidad, evidenciado en el momento de entrega de los productos	Seguridad Digital	Interrupción de la Operación o del Servicio	3	9	27	ALTO	1. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	1	4	1	4	2	BAJO	MODERADO	Mitigar el Riesgo	**ASEGURAR LA DISPONIBILIDAD DE EQUIPOS**
Sistema de Gestión de Seguridad de Información (SGSI)	Proceso_Estratégico	Direccionamiento Estratégico	Dirigir estratégicamente a la Unidad Nacional de Protección -UNP- a través de la definición de lineamientos generales, políticas, estrategias y del modelo de operación, armonizando los planes, programas y proyectos de carácter estratégico para dar cumplimiento a la misión,	**Posibilidad de tener Sistemas de Información desatendidos con soporte debido a la inopetividad de continuidad a los contratos de soporte y mantenimiento.**	[Tecnologia] Falta de recurso para dar continuidad a contratos de soporte y mantenimiento	Seguridad Digital	Interrupción de la Operación o del Servicio	3	6	6	BAJO	1. SEGURIDAD DE LOS RECURSOS HUMANOS.	1	4	2	8	3	MEDIO	BAJO	Mitigar el Riesgo	**ASEGURAR LA CONTRATACIÓN DEL PERSONAL ESTRATEGIA ENCAMINADOS DEL MANTENIMIENTO DE LOS EQUIPOS**
Sistema de Gestión de Seguridad de Información (SGSI)	Proceso_Estratégico	Direccionamiento Estratégico	Dirigir estratégicamente a la Unidad Nacional de Protección -UNP- a través de la definición de lineamientos generales, políticas, estrategias y del modelo de operación, armonizando los planes, programas y proyectos de carácter estratégico para dar cumplimiento a la misión, objetivos institucionales, sectoriales y metas de gobierno.	**Posibilidad de tener afectación de integridad, confidencialidad y disponibilidad de la información por errores humanos**	Desconocimiento de las Lineamientos del SGSI (políticas, normas y procedimientos) Ausencia de personal que cumpla con los Roles establecidos en la guía de roles de seguridad de la información. Falta de Cultura de Seguridad Falta de una apropiación en activos organizacional en seguridad de la información. Incumplimiento y/o desactualización de los Procesos y procedimientos relacionados con el SGSI Inadecuada manejo de la información ocasiona por una indebida manipulación de los ususarios Falta de directivas Alerta no oportunidad de información Modificación no oportunidad de información. Perdida de información Uso no autorizado de equipos Sensibles perdidas insuficiente Errores de modificación	Seguridad Digital	Reprocesos	3	6	6	BAJO	1. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN. 2. SEGURIDAD DE LOS RECURSOS HUMANOS 3. CONTROL DE ACCESO 4. SEGURIDAD FÍSICA Y DEL ENTORNO 5. SEGURIDAD DE LAS OPERACIONES. 6. SEGURIDAD DE LAS COMUNICACIONES.	6	4	2	8	3	MEDIO	BAJO	Mitigar el Riesgo	**ASEGURAR LA EXPERIENCIA, HABILIDADES Y CONOCIMIENTO DEL PERSONAL TÉCNICO**

E TRATAMIENTO		
RESPONSABLE (Nombre, Apellidos y cargo)	CRONOGRAMA DEL PLAN DE ACCIÓN	
	FECHA INICIO (dd/mm/aaaa)	FECHA FIN (dd/mm/aaaa)
TECNOLOGICA		
TECNOLOGICA		
TECNOLOGICA		
TECNOLOGICA		
TECNOLOGICA		
TECNOLOGICA		