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 (MAYOR VALOR ENTRE 1 Y 5) 5= SIEMPRE, 4 = ALTA PROBABILIDAD, 3 = MEDIA PROBABILIDAD, 2 = BAJA PROBABILIDAD, 1 = RARA VEZ	IMPACTO ESCALA (MAYOR VALOR ENTRE 1 Y 5) 5= DESASTRE, 4 = GRAVE, 3 = MODERADO, 2 = MENOR, 1 = INSIGNIFICANTE	EVALUACIÓN DEL RIESGO INHERENTE (PROBABILIDAD X IMPACTO)	NIVEL DE RIESGO INHERENTE (ALTO, MODERADO, BAJO, EXTREMO)	CONTROLES EXISTENTES (DE DETALLAN LOS CONTROLES EXISTENTES)	CANT. DE CONTROLES EXISTENTES (DESCRIBIR LAS ACCIONES DESCRITAS EN LOS CONTROLES)	TIPO DE CONTROL 1= INHERENTE 2= DETECTIVO 3= CORRECTIVO 4= PREVENTIVO	FREC DE EJECUCIÓN DEL CONTROL 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) (MAYOR VALOR ENTRE 0 Y 1)	NIVEL DE RIESGO RESIDUAL FINAL (ALTO, MODERADO, BAJO)	OPCIÓN DE TRATAMIENTO (MITIGAR EL RIESGO, ACEPTAR EL RIESGO, TRANSFERIR EL RIESGO)	ACCIONES (ACTIVIDADES ASOCIADAS A LA ACCIÓN DE MEJORA) (ACTIVIDAD PLANTEADA DESDE EL PROCESO PARA EVITAR LA CAUSA RAÍZ)	RESPONSABLE (Dos. Responsables de cada actividad)	CRONOGRAMA DEL PLAN DE ACCIÓN	
																							FECHA INICIO (MM/YY/dd/aa)	FECHA FIN (MM/YY/dd/aa)
Sistema de Gestión de Seguridad de Información (SGSI)	Proceso_Apoyo	Gestión de Servicio al Ciudadano	Facilitar el acceso de la ciudadanía a los trámites y servicios de la UNP cuando así lo requieran atender las peticiones, quejas, reclamos, sugerencias y felicitaciones elevadas ante la entidad, a través de los diferentes canales establecidos, y en el marco de la normatividad vigente, tendente promover las necesidades, inclusión y especialmente el ejercicio de los derechos de la población objeto y grupo de interés, verificando su generación de satisfacción	**Posibilidad de comprometer la integridad de la información institucional debido a fallas técnicas y operativas en el proceso.**	*(Procesos)Modificar la información no autorizada. *(Personas)Errores humanos. * (Tecnología)Plataforma tecnológica obsoleta	Seguridad Digital	* Inconsistencias en la calidad de la información y responsabilidad. * Incumplimiento normativo * Procesos administrativos y/o judiciales	1	6	6	BAJO	Cumplimiento con las políticas y normas de seguridad.	3	4	2	8	3	MEDIO	BAJO	Mitigar el Riesgo	**P. Mesas de trabajo al interior del GSC para socializar la Política de Seguridad de la Información.** **Q. Mesas de trabajo al interior del GSC con los temas de seguridad de la información cuando haya lugar a ello.** **R. Participar en las socializaciones de la Política de Seguridad de la Información de acuerdo a cronograma del GSC.** **S. Asistencia obligatoria de funcionarios y colaboradores del GSC a socializaciones Política de Seguridad de la Información** **Revisión de documentos internos remitidos por Coordinador GSC activos a funcionarios y colaboradores la apropiación y aplicación estricta de la Política de Seguridad de la Información.**	Grupo de Servicio al Ciudadano.	P. 01/02/2022 Q. 01/02/2022 R. 01/02/2022 S. 01/02/2022	P. 31/12/2022 Q. 31/12/2022 R. 31/12/2022 S. 31/12/2022
											#N/D					0	#N/D							
											#N/D					0	#N/D							
											#N/D					0	#N/D							
											#N/D					0	#N/D							
											#N/D					0	#N/D							