MAPA DE RIESGOS POR PROCESO Y SEGUIMIENTO A LOS RIESGOS			
METODO ESTANDARIZADO DE FORMULACIÓN Y GESTIÓN			
CODIGO:	FDE-01-F01	VERS:	FECHA: 21/05/2019

PROCESO: GESTIÓN DE LA INFORMACIÓN Y LA COMUNICACIÓN

OBJETIVO DEL PROCESO: Gestionar la información y la comunicación de la Agencia Nacional de Infraestructura, a partir de la identificación de las necesidades de información y comunicación de los grupos de interés, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.

FASE 1 – IDENTIFICACIÓN DE RIESGOS

PROCESO/ÁREA/PROYECTO	PLANES ESTRATÉGICOS	PLANES OPERACIONALES	PUNTOS FRENTE	FACTORES DE RIESGO INTERNOS	FACTORES DE RIESGO EXTERNOS	CAUSAS DE RIESGO	PATRONES DE CAUSA	ID	RIESGO	RESPONSABLE DEL PROCESO/ÁREA/PROYECTO
Gestionar la información y la comunicación de la Agencia Nacional de Infraestructura, a partir de la identificación de las necesidades de información y comunicación de los grupos de interés, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional. Objetivos y políticas del proceso: Objetivos: Gestionar la información y la comunicación de la Agencia de Infraestructura. Políticas: Gestionar la información y la comunicación de la Agencia de Infraestructura. Alineación a Planes estratégicos institucionales: Gestionar PMI Agencia.	Gestionar la información y la comunicación de la Agencia de Infraestructura.	Gestionar la información y la comunicación de la Agencia de Infraestructura.	Grupo de gestión	Procesos	Ataques cibernéticos (Hackeo, Ciberataques, Amenaza cyber, Ciberataque, Ciberataque a la Agencia de Infraestructura, Ciberataque a la Agencia de Infraestructura)	Ciberataques	Procesos	R1-G-GIC-01	Posibilidad de pérdida reputacional y económica por ataques de hacker, desplazamiento de datos, ciberataques y/o ciberataque a la Agencia de Infraestructura, debido a la falta de capacidad de ciberataque.
			Grupo de gestión	Sistemas	Ataques Ciberataques	Operacional	Procesos	R2-G-GIC-02	Posibilidad de pérdida reputacional y económica por sanciones de la Nación, desplazamiento de datos, ciberataques y/o ciberataque a la Agencia de Infraestructura, debido a la falta de capacidad de ciberataque.	Operadores y administrativos de Procesos
Alineación Plan Estratégico Institucional: Fortalecer la gestión administrativa y financiera de la Agencia de Infraestructura. Alineación con Planes Sectoriales: Fortalecer la gestión administrativa y financiera de la Agencia de Infraestructura, con el fin de mantener el presupuesto de la Agencia de Infraestructura y ejecutar los recursos de manera eficiente y eficaz para cumplir con la misión institucional. Alineación a Planes Operativos: Gestionar PMI Agencia.	Fortalecer la gestión administrativa y financiera.	Gestionar la información y la comunicación de la Agencia de Infraestructura.	Grupo de gestión	Procesos	Ataques cibernéticos (Hackeo, Ciberataques, Amenaza cyber, Ciberataque, Ciberataque a la Agencia de Infraestructura, Ciberataque a la Agencia de Infraestructura)	Ciberataques	Procesos	R3-G-GIC-03	Posibilidad de pérdida reputacional y económica por sanciones de la Nación, desplazamiento de datos, ciberataques y/o ciberataque a la Agencia de Infraestructura, debido a la falta de capacidad de ciberataque.	Operadores y administrativos de Procesos
Alineación Plan Estratégico Institucional: Fortalecer la gestión administrativa y financiera de la Agencia de Infraestructura. Alineación con Planes Sectoriales: Fortalecer la gestión administrativa y financiera de la Agencia de Infraestructura, con el fin de mantener el presupuesto de la Agencia de Infraestructura y ejecutar los recursos de manera eficiente y eficaz para cumplir con la misión institucional. Alineación a Planes Operativos: Gestionar PMI Agencia.	Fortalecer la gestión administrativa y financiera.	Gestionar la información y la comunicación de la Agencia de Infraestructura.	Grupo interno	Grupo Finanzas (Ser. carnes)	Ambiental, ambiental cambio, cambiario, Financiero	Económico	Grupo Información optica	R4-G-GIC-04	Posibilidad de pérdida económica por sanciones de la Nación, debido a la ejecución ineficiente del presupuesto de la Agencia de Infraestructura.	Grupo Finanzas (Ser. carnes)
Alineación Plan Estratégico Institucional: Fortalecer la gestión administrativa y financiera de la Agencia de Infraestructura. Alineación con Planes Sectoriales: Fortalecer la gestión administrativa y financiera de la Agencia de Infraestructura, con el fin de mantener el presupuesto de la Agencia de Infraestructura y ejecutar los recursos de manera eficiente y eficaz para cumplir con la misión institucional. Alineación a Planes Operativos: Gestionar PMI Agencia.	Fortalecer la gestión administrativa y financiera.	Gestionar la información y la comunicación de la Agencia de Infraestructura.	Grupo de gestión	Procesos	Ambiental, ambiental cambio, cambiario, Financiero	Económico	Procesos	R5-G-GIC-05	Posibilidad de pérdida económica y/o reputacional por incumplimiento a la ejecución del presupuesto de la Agencia de Infraestructura, debido a la falta de capacidad de ejecución.	Operadores y administrativos de Procesos
Alineación Plan Estratégico Institucional: Fortalecer la gestión administrativa y financiera de la Agencia de Infraestructura. Alineación con Planes Sectoriales: Fortalecer la gestión administrativa y financiera de la Agencia de Infraestructura, con el fin de mantener el presupuesto de la Agencia de Infraestructura y ejecutar los recursos de manera eficiente y eficaz para cumplir con la misión institucional. Alineación a Planes Operativos: Gestionar PMI Agencia.	Fortalecer la gestión administrativa y financiera.	Gestionar la información y la comunicación de la Agencia de Infraestructura.	Grupo de gestión	Procesos	Ambiental, ambiental cambio, cambiario, Financiero	Económico	Procesos	R6-G-GIC-06	Posibilidad de pérdida económica y/o reputacional por sanciones de la Nación, desplazamiento de datos, ciberataques y/o ciberataque a la Agencia de Infraestructura, debido a la falta de capacidad de ejecución.	Operadores y administrativos de Procesos
			Grupo inicial	Interfaces	Grupo Grupo (Ser. carnes)	Operacional	Procesos	R7-G-GIC-07	Posibilidad de pérdida reputacional por incumplimiento a pagos de bienes y servicios, debido a la falta de capacidad de pagos.	Usuarios, Proveedores y Partes Interesadas
	Fortalecer la gestión administrativa y financiera.	Gestionar la información y la comunicación de la Agencia de Infraestructura.	Grupo inicial	Grupo Finanzas (Ser. carnes)	Ambiental, ambiental cambio, cambiario, Financiero	Económico	Grupo Información optica	R8-G-GIC-08	Posibilidad de pérdida económica por sanciones ante la Nación, debido a la falta de capacidad de pagos.	Grupo Finanzas (Ser. carnes)
Alineación Plan Estratégico Institucional: Fortalecer la gestión administrativa y financiera de la Agencia de Infraestructura. Alineación con Planes Sectoriales: Fortalecer la gestión administrativa y financiera de la Agencia de Infraestructura, con el fin de mantener el presupuesto de la Agencia de Infraestructura y ejecutar los recursos de manera eficiente y eficaz para cumplir con la misión institucional. Alineación a Planes Operativos: Gestionar PMI Agencia.	Fortalecer la gestión administrativa y financiera.	Gestionar la información y la comunicación de la Agencia de Infraestructura.	Grupo de gestión	Procesos	Ambiental, ambiental cambio, cambiario, Financiero	Económico	Talento Humano	R9-G-GIC-09	Posibilidad de pérdida económica y/o reputacional por pérdida de información, debido a la falta de capacidad de información.	Usuarios, Contratistas, Partes Interesadas
Gestionar la información y la comunicación de la Agencia de Infraestructura, a partir de la identificación de las necesidades de información y comunicación de los grupos de interés, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional. Objetivos y políticas del proceso: Objetivos: Gestionar la información y la comunicación de la Agencia de Infraestructura. Políticas: Gestionar la información y la comunicación de la Agencia de Infraestructura. Alineación a Planes estratégicos institucionales: Gestionar PMI Agencia.	Fortalecer la gestión administrativa y financiera.	Gestionar la información y la comunicación de la Agencia de Infraestructura.	Grupo inicial	Grupo Finanzas (Ser. carnes)	Ambiental, ambiental cambio, cambiario, Financiero	Económico	Grupo Información optica	R10-G-GIC-10	Posibilidad de pérdida económica y/o reputacional por sanciones ante la Nación, desplazamiento de datos, ciberataques y/o ciberataque a la Agencia de Infraestructura, debido a la falta de capacidad de información.	Grupo Finanzas (Ser. carnes)
	Fortalecer la gestión administrativa y financiera.	Gestionar la información y la comunicación de la Agencia de Infraestructura.	Grupo inicial	Grupo Finanzas (Ser. carnes)	Ambiental, ambiental cambio, cambiario, Financiero	Económico	Grupo Información optica	R11-G-GIC-11	Posibilidad de pérdida económica y/o reputacional por sanciones ante la Nación, desplazamiento de datos, ciberataques y/o ciberataque a la Agencia de Infraestructura, debido a la falta de capacidad de información.	Grupo Finanzas (Ser. carnes)
	Fortalecer la gestión administrativa y financiera.	Gestionar la información y la comunicación de la Agencia de Infraestructura.	Grupo inicial	Grupo Finanzas (Ser. carnes)	Ambiental, ambiental cambio, cambiario, Financiero	Económico	Grupo Información optica	R12-G-GIC-12	Posibilidad de pérdida económica y/o reputacional por sanciones ante la Nación, desplazamiento de datos, ciberataques y/o ciberataque a la Agencia de Infraestructura, debido a la falta de capacidad de información.	Grupo Finanzas (Ser. carnes)

FASE 2 – VALORACIÓN DE RIESGOS

PROCESO/ÁREA/PROYECTO	VALORACIÓN DEL RIESGO INHERENTE			No.	CONTROL	VALORACIÓN DEL CONTROL			VALORACIÓN DEL RIESGO RESIDUAL			OPCIÓN DE TRATAMIENTO	VALORACIÓN DEL RIESGO RESIDUAL		
	PROBABILIDAD	IMPACTO	ZONA DE RIESGO INHERENTE			TIPO DE CONTROL	IMPLEMENTACIÓN	CALIFICACIÓN	PROBABILIDAD	IMPACTO	ZONA DE RIESGO RESIDUAL		PROBABILIDAD	IMPACTO	ZONA DE RIESGO RESIDUAL
Gestionar la información y la comunicación de la Agencia Nacional de Infraestructura, a partir de la identificación de las necesidades de información y comunicación de los grupos de interés, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional. Objetivos y políticas del proceso: Objetivos: Gestionar la información y la comunicación de la Agencia de Infraestructura. Políticas: Gestionar la información y la comunicación de la Agencia de Infraestructura. Alineación a Planes estratégicos institucionales: Gestionar PMI Agencia.	4 - Casi seguro (100%)	4 - Mayor (100%)	ALTO	1	Cada vez que ocurra un ataque cibernético, el responsable de la ciberseguridad de la ANI, el 1 de enero de cada año, actualiza el mapa de riesgos de ciberseguridad, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Preventivo	Así es	Probabilidad	4 - Casi seguro (100%)	4 - Mayor (100%)	ALTO
				2	Cada vez que ocurra un ataque cibernético, presente un ciberataque, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad							
	3 - Probable (80%)	4 - Mayor (100%)	ALTO	3	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad	2 - Improbable (20%)	4 - Mayor (100%)	ALTO	Reducir (mitigar)	1 - Improbable (20%)	4 - Mayor (100%)	ALTO
				4	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad							
	4 - Casi seguro (100%)	4 - Mayor (100%)	EXTREMO	5	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad	4 - Casi seguro (100%)	4 - Mayor (100%)	EXTREMO	Reducir (mitigar)	3 - Probable (80%)	4 - Mayor (100%)	EXTREMO
				6	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad							
	3 - Probable (80%)	4 - Mayor (100%)	ALTO	7	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad	2 - Improbable (20%)	4 - Mayor (100%)	ALTO	Reducir (mitigar)	1 - Improbable (20%)	4 - Mayor (100%)	ALTO
				8	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad							
	4 - Casi seguro (100%)	4 - Mayor (100%)	EXTREMO	9	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad	4 - Casi seguro (100%)	4 - Mayor (100%)	EXTREMO	Reducir (mitigar)	3 - Probable (80%)	4 - Mayor (100%)	ALTO
				10	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad							
	3 - Probable (80%)	4 - Mayor (100%)	ALTO	11	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad	2 - Improbable (20%)	4 - Mayor (100%)	ALTO	Reducir (mitigar)	1 - Improbable (20%)	4 - Mayor (100%)	ALTO
				12	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad							
	4 - Casi seguro (100%)	4 - Mayor (100%)	EXTREMO	13	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad	4 - Casi seguro (100%)	4 - Mayor (100%)	EXTREMO	Reducir (mitigar)	3 - Probable (80%)	4 - Mayor (100%)	ALTO
				14	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad							
	3 - Probable (80%)	4 - Mayor (100%)	ALTO	15	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad	2 - Improbable (20%)	4 - Mayor (100%)	ALTO	Reducir (mitigar)	1 - Improbable (20%)	4 - Mayor (100%)	ALTO
				16	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad							
	4 - Casi seguro (100%)	4 - Mayor (100%)	EXTREMO	17	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad	4 - Casi seguro (100%)	4 - Mayor (100%)	EXTREMO	Reducir (mitigar)	3 - Probable (80%)	4 - Mayor (100%)	ALTO
				18	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad							
	3 - Probable (80%)	4 - Mayor (100%)	ALTO	19	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad	2 - Improbable (20%)	4 - Mayor (100%)	ALTO	Reducir (mitigar)	1 - Improbable (20%)	4 - Mayor (100%)	ALTO
				20	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad							
	4 - Casi seguro (100%)	4 - Mayor (100%)	EXTREMO	21	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad	4 - Casi seguro (100%)	4 - Mayor (100%)	EXTREMO	Reducir (mitigar)	3 - Probable (80%)	4 - Mayor (100%)	ALTO
				22	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad							
	3 - Probable (80%)	4 - Mayor (100%)	ALTO	23	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad	2 - Improbable (20%)	4 - Mayor (100%)	ALTO	Reducir (mitigar)	1 - Improbable (20%)	4 - Mayor (100%)	ALTO
				24	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad							
	4 - Casi seguro (100%)	4 - Mayor (100%)	EXTREMO	25	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad	4 - Casi seguro (100%)	4 - Mayor (100%)	EXTREMO	Reducir (mitigar)	3 - Probable (80%)	4 - Mayor (100%)	ALTO
				26	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad							
	3 - Probable (80%)	4 - Mayor (100%)	ALTO	27	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad	2 - Improbable (20%)	4 - Mayor (100%)	ALTO	Reducir (mitigar)	1 - Improbable (20%)	4 - Mayor (100%)	ALTO
				28	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad							
	4 - Casi seguro (100%)	4 - Mayor (100%)	EXTREMO	29	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad	4 - Casi seguro (100%)	4 - Mayor (100%)	EXTREMO	Reducir (mitigar)	3 - Probable (80%)	4 - Mayor (100%)	ALTO
				30	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad							
	3 - Probable (80%)	4 - Mayor (100%)	ALTO	31	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad	2 - Improbable (20%)	4 - Mayor (100%)	ALTO	Reducir (mitigar)	1 - Improbable (20%)	4 - Mayor (100%)	ALTO
				32	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad							
	4 - Casi seguro (100%)	4 - Mayor (100%)	EXTREMO	33	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad	4 - Casi seguro (100%)	4 - Mayor (100%)	EXTREMO	Reducir (mitigar)	3 - Probable (80%)	4 - Mayor (100%)	ALTO
				34	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad							
	3 - Probable (80%)	4 - Mayor (100%)	ALTO	35	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad	2 - Improbable (20%)	4 - Mayor (100%)	ALTO	Reducir (mitigar)	1 - Improbable (20%)	4 - Mayor (100%)	ALTO
				36	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad							
	4 - Casi seguro (100%)	4 - Mayor (100%)	EXTREMO	37	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad	4 - Casi seguro (100%)	4 - Mayor (100%)	EXTREMO	Reducir (mitigar)	3 - Probable (80%)	4 - Mayor (100%)	ALTO
				38	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad							
	3 - Probable (80%)	4 - Mayor (100%)	ALTO	39	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad	2 - Improbable (20%)	4 - Mayor (100%)	ALTO	Reducir (mitigar)	1 - Improbable (20%)	4 - Mayor (100%)	ALTO
				40	Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Detectivo	Así es	Probabilidad							

FASE 3 – TRATAMIENTO DE RIESGOS

PROCESO/ÁREA/PROYECTO	OPCIÓN DE TRATAMIENTO	ACTIVIDAD DE CONTROL	FECHA INICIO	FECHA FINAL	SEGUIMIENTO	ESTADO	EVIDENCIA	RESPONSABLE	INDICADOR
Gestionar la información y la comunicación de la Agencia Nacional de Infraestructura, a partir de la identificación de las necesidades de información y comunicación de los grupos de interés, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional. Objetivos y políticas del proceso: Objetivos: Gestionar la información y la comunicación de la Agencia de Infraestructura. Políticas: Gestionar la información y la comunicación de la Agencia de Infraestructura. Alineación a Planes estratégicos institucionales: Gestionar PMI Agencia.	Reducir (mitigar)	1. Cada vez que ocurra un ataque cibernético, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Frecuencia	Así es	Probabilidad	1. ANI-ciberseguridad-Ciberataque-Informe 2. ANI-ciberseguridad-Informe	ANI-ciberseguridad-Ciberataque-Informe	1. ciberataques/ciberataques 2. informe/informe
		2. Cada vez que ocurra un ataque cibernético, presente un ciberataque, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Frecuencia	Así es	Probabilidad										
	Reducir (mitigar)	3. Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Frecuencia	Así es	Probabilidad	1. ANI-ciberseguridad-Ciberataque-Informe 2. ANI-ciberseguridad-Informe	ANI-ciberseguridad-Ciberataque-Informe	1. ciberataques/ciberataques 2. informe/informe	1. 12/01/2020 2. 01/01/2020	1. Cinco (5) ciberataques 2. Cinco (5) informes	Ciberataques/ciberataques Informe/informe	1. ciberataques/ciberataques 2. informe/informe
		4. Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Frecuencia	Así es	Probabilidad										
	Reducir (mitigar)	5. Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Frecuencia	Así es	Probabilidad	1. ANI-ciberseguridad-Informe	ANI-ciberseguridad-Informe	1. informe/informe	1. 12/01/2020	1. Cinco (5) informes	Informe/informe	1. informe/informe
		6. Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Frecuencia	Así es	Probabilidad										
	Reducir (mitigar)	7. Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Frecuencia	Así es	Probabilidad	1. ANI-ciberseguridad-Informe	ANI-ciberseguridad-Informe	1. informe/informe	1. 12/01/2020	1. Cinco (5) informes	Informe/informe	1. informe/informe
		8. Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Frecuencia	Así es	Probabilidad										
	Reducir (mitigar)	9. Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Frecuencia	Así es	Probabilidad	1. ANI-ciberseguridad-Informe	ANI-ciberseguridad-Informe	1. informe/informe	1. 12/01/2020	1. Cinco (5) informes	Informe/informe	1. informe/informe
		10. Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Frecuencia	Así es	Probabilidad										
	Reducir (mitigar)	11. Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Frecuencia	Así es	Probabilidad	1. ANI-ciberseguridad-Informe	ANI-ciberseguridad-Informe	1. informe/informe	1. 12/01/2020	1. Cinco (5) informes	Informe/informe	1. informe/informe
		12. Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Frecuencia	Así es	Probabilidad										
	Reducir (mitigar)	13. Cada vez que ocurra un ataque cyber en la Entidad, el responsable de ciberseguridad de la ANI, en un plazo de 24 horas, informa a la Agencia Nacional de Infraestructura, con el fin de mantener la información actualizada y disponible para la toma de decisiones y el cumplimiento de la misión institucional.	Frecuencia	Así es	Probabilidad	1. ANI-ciberseguridad-Informe	ANI-cibersegu