UNIDAD NACIONAL PROTECCIÓN
MAPA DE RIESGOS DE CORRUPCIÓN
OFICINA ASESORA DE PLANEACIÓN E INFORMACIÓN

FECHA DE ELABORACIÓN:	23/01/2018

CONSOLIDACIÓN MAPA DE RIESGO

NOMBRE DEL PROCESO	GESTIÓN TECNOLOGICA
OBJETIVO DEL PROCESO	Diseñar, proponer, administrar y controlar la infraestructura tecnológica y los sistemas de información de la UNP de acuerdo a los protocolos y especificaciones técnicas, según la normatividad, estrategias, objetivos y procedimientos que rigen a la Entidad, prestando servicios informáticos que permitan el flujo eficiente, veraz y oportuno de la información entre las dependencias internas, la ciudadanía y los entes de control.

No. DEL RIESGO	DESCRIPCION DEL RIESGO	CAUSAS	CONSECUENCIAS	ANALISIS DEL RIESGO			VALORACION DEL RIESGO						ACCIONES PARA ADMINISTRAR EL RIESGO	INDICADOR (Mide el cumplimiento de las acciones)	RESPONSABLE
				PROBABILIDAD	IMPACTO	ZONA DE RIESGO	CONTROLES	CONTROL PARA MITIGAR	PROBABILIDAD	IMPACTO	NUEVA EVALUACIÓN	TRATAMIENTO			
R1	Acción de adulteración, daño, o entrega de información confidencial o crítica para beneficio de propio, de un tercero o un particular.	1. Usuarios sin cultura de seguridad informática 2. Acciones indebidas en el uso de la información y los recursos tecnológicos de la Entidad 3. Falta de control de uso y acceso a la información de la Entidad. 4. Vandalismo informático que beneficia los intereses particulares de terceros 5. Presión, amenazas por parte de particulares a un funcionario o contratista para conocer, manipular o adulterar información en beneficio de terceros interesados.'	1. Pérdida y manipulación de información o fuga de información reservada usada para chantajes, amenazas o beneficio de terceros. 2. Problemas de Seguridad Nacional y desprestigio Institucional. 3. Vulnerabilidades y fallas de seguridad, lo cual impacta los servicios misionales de la Entidad 4. Imposición de sanciones legales y económicas, investigaciones disciplinarias, y destitución del cargo 5. Pérdidas humanas por fuga de información confidencial	3	20	ZONA RIESGO EXTREMA	Política de Seguridad de la Información con los lineamientos de uso de las herramientas tecnológicas, canales y sistemas de información de la Entidad. . Estrategia de socialización de la cultura de seguridad informática en cumplimiento del Modelo de Seguridad y Privacidad de la Información - MSPI de la Entidad. Implementación de controles tecnológicos e informáticos definidos en el MSPI de la Entidad.	PROBABILIDAD	3	20	ZONA RIESGO EXTREMA	Reducir Ocurrencia	Definir los lineamientos de uso de las herramientas, canales y sistemas de información de la Entidad, orientado a la seguridad y confidencialidad de la información con su respectivo seguimiento. Definir el Programa de uso y apropiación de la cultura de Seguridad de la Información en cumplimiento del Modelo de Seguridad y Privacidad de la Información de la Entidad. Implementar controles tecnológicos orientados a la seguridad y confidencialidad de la información en los canales de comunicación, herramientas y sistemas de información de la Entidad.	Política de Seguridad de la Información aprobada por la Dirección General e Informe de seguiimento trimestral Informe de ejecución del Programa de Socialización sobre la Cultura de la Seguridad y Privacidad de la Información Informe de la implementación de los controles tecnológicos definidos en el Modelo de Seguridad y Privacidad de la Información de la Entidad	Líder Grupo de Tecnología
R2		.		0	0		. .		0	0					
R3		.		0	0		. .	0	0	0					
R4		.		0	0		. .	0	0	0					
R5		.		0	0		. .	0	0	0					
R6		.		0	0		. .	0	0	0					
R7		.		0	0		. .	0	0	0					
R8		.		0	0		. .	0	0	0					

MININTERIOR
TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN