



**UNIDAD NACIONAL PROTECCIÓN  
MAPA DE RIESGOS POR PROCESOS  
OFICINA ASESORA DE PLANEACIÓN E INFORMACIÓN**

FECHA DE ELABORACIÓN: 09/03/2018

**CONSOLIDACIÓN MAPA DE RIESGO**

**GESTIÓN TECNOLÓGICA**

**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

No. DEL RIESGO	DESCRIPCIÓN DEL RIESGO	CAUSAS	CONSECUENCIAS	ANÁLISIS DEL RIESGO			CONTROLES	CONTROL PARA MITIGAR	VALORACIÓN DEL RIESGO			TRATAMIENTO	ACCIONES PARA ADMINISTRAR EL RIESGO	INDICADOR (Mide el cumplimiento de las acciones)	RESPONSABLE
				PROBABILIDAD	IMPACTO	ZONA DE RIESGO			PROBABILIDAD	IMPACTO	NUEVA EVALUACIÓN				
R1	Afectación de la custodia de la información digital de la Entidad	1. Falta de mecanismos de protección y seguridad física y lógica de la infraestructura tecnológica. 2. Falta de mantenimiento preventivo y correctivo de la plataforma tecnológica e informática. 3. Ausencia de políticas y procedimientos para la custodia de la información digital. 4. Inefectivos procesos de generación de respaldos de la información, y falta de protocolos para su restauración. 5. Falta de Sistemas de Información integrados que incorporen controles automáticos de acceso y manipulación. 6. Falta de planes formales frente a la exposición a Desastres Naturales. 7. Limitada disponibilidad de recursos presupuestales para el fortalecimiento de la infraestructura tecnológica e informática de la Entidad. 8. Elevados costos de los elementos de seguridad y servicios tecnológicos para la gestión de los riesgos de seguridad de la información digital para proteger los datos de la Entidad.	1. Pérdida de información. 2. Retrasos y reprocesos. 3. Fallas de operación que impacta los servicios misionales. 4. Interrupción de los procesos institucionales con Afectación en la continuidad de la operación. 5. Afectación de la reputación Institucional. 6. Problemas de Seguridad Nacional. 7. Pérdidas humanas por falta de información requerida para el proceso. 8. Imposición de sanciones administrativas.	5	20	ZONA RIESGO EXTREMA	Controles para mantener la integridad, disponibilidad y confidencialidad de la información. Plan de mantenimiento preventivo y correctivo de la infraestructura tecnológica de la UNP. Estrategia de implementación del plan de recuperación de desastres - DRP.	PROBABILIDAD	5	20	ZONA RIESGO EXTREMA	Reducir Ocurrencia	1. Identificación de activos de información clave. 2. Definición de estrategias, políticas y procedimientos para la custodia y protección de la información digital de la entidad en servicios, aplicaciones y repositorios de TI. 3. Implementación de mecanismos de control de acceso físico a equipos que manejan información de la entidad. 4. Definición e implementación de políticas de backup y recuperación. 5. Proyección de necesidades de productos y servicios de tecnología. 6. Solicitud de presupuesto para la adquisición de bienes y servicios de tecnología. 7. Ejecución del plan de mantenimiento preventivo y correctivo de TI. 8. Definir la metodología para desarrollar el plan de recuperación de desastres - DRP.	1 Documento con la estrategia, y estado de implementación de controles para la protección de activos de TI. 1 Documento de seguimiento a la ejecución del plan de mantenimiento de la infraestructura tecnológica. 1 Documento del plan de recuperación de desastres - DRP.	LIDER DE TECNOLOGÍA
R2	Falta de alineación entre la gestión de tecnologías de información y las líneas estratégicas de la Entidad	1. Desconocimiento del contexto de las líneas estratégicas de la entidad alineando la gestión de tecnología para lograr el cumplimiento de los objetivos y metas institucionales. 2. Falta de análisis y definición de la estrategia de tecnología alineado con las necesidades estratégicas de la entidad. 3. Falta de participación estratégica del líder de tecnología en la formulación de los planes institucionales con el apoyo de la alta gerencia. 4. Falta de definición, ejecución y seguimiento del Plan Estratégico de Tecnologías de Información PETI actualizado. 5. Inadecuada gestión de los procesos de TI para diseñar, ejecutar y prestar productos y servicios tecnológicos. 6. Disponibilidad de suministros, productos o servicios por obsolescencia o incompatibilidad de la plataforma tecnológica debido a una	1. Incumplimiento de requerimientos y expectativas respecto al apoyo que tecnología genera a los procesos estratégicos y misionales de la entidad. 2. Sanciones disciplinarias por formular y ejecutar proyectos que no apoyen o soporten el cumplimiento de los objetivos institucionales. 3. Imposición de sanciones administrativas por la falta de un plan estratégico de tecnología actualizado. 4. Afectación a la imagen institucional por incumplimientos normativos.	3	20	ZONA RIESGO EXTREMA	Definición del Plan Estratégico de Tecnologías de Información - PETI actualizado. Seguimiento a la implementación y cumplimiento del Plan Estratégico de Tecnologías de Información - PETI.	PROBABILIDAD	3	20	ZONA RIESGO EXTREMA	Reducir Ocurrencia	1. Análisis del contexto estratégico y normativo de la entidad. 2. Levantamiento y actualización del proceso de gestión tecnológica. 3. Establecimiento del G-CIO al interior de la entidad con el apoyo de las altas directivas. 4. Definición y formalización del Plan Estratégico de Tecnologías de Información - PETI. 1. Definición y ejecución del mecanismo de monitoreo al cumplimiento del Plan Estratégico de Tecnologías de Información - PETI.	1 Documento con el Plan Estratégico de Tecnologías de Información - PETI. 1 Informe de seguimiento a la implementación del Plan Estratégico de Tecnologías de Información - PETI.	LIDER DE TECNOLOGÍA
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					

