UNIDAD NACIONAL PROTECCIÓN

MAPA INTEGRAL DE RIESGOS

OFICINA ASESORA DE PLANEACIÓN E INFORMACIÓN

FECHA DE ELABORACIÓN:		12-dic-2019
NOMBRE DEL PROCESO		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 protoco los y especificaciones técnicas, según la normatividad, e strategias, objetivos y procedimientos que rigen a la Entidad, presta ndo servicios informáticos que permitan el flujo eficiente, veraz y oportun o de la información entre las dependencias internas, la ciudadanía y los entes de control.

CONSOLIDACIÓN MAPA INTEGRAL DE RIESGO

No. DEL RIESGO	NOMBRE DEL RIESGO		TIPO DE 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	PERFIL DEL RIESGO (1-100)	NUEVA EVALUACIÓN				
Riesgo 1	Afectación de la operación de la entidad por falta de ejecución de los proyectos tecnológicos definidos e n el PETI (Plan Estratégico de las Tecnologías de Información)	Falta de ejecución de los Proyectos tecnológicos del PETI (Plan Estratégico de las Tecnologías de Información) que habilitan procesos misionales generando incumplimiento del objeto misional.	Proceso	"1. . Deficiente gestión de los riesgos asociados a los proyectos tecnológicos definidos en el PETI 2. Insuficiente recurso humano para la estructuración y gestión de proyectos de TI 3. Falta de apoyo de la Alta Dirección en la implementación de proyectos tecnológicos " " "4. Cambio de Políticas Gubernamentales"	"1. Retrasos y reprocesos. 2. Fallas de operación que impacta los servicios misionales. 3. Afetación de la reputación Institucional. 4. Problemas de Seguridad de la Información 5. Pérdidas humanas por falta de información requerida para el proceso. 6. Investigaciones disciplinarias"	3	20	ZONA RIESGO EXTREMA	1. Definir líneas de seguimiento y control para la ejecución de los proyectos tecnológicos incluidos en el PETI a fin de gestionar los riesgos asociados .2. Solicitar el personal con las competencias requeridas para la estructuración y gestión de los proyectos de TI definidos en el PETI ante la instancia compartante3. Socializar a la Alta Dirección sobre la metodología de estructuración del PETI y su actualización para la vigencia 2020	PROBABILIDAD	1	20	20	ZONA RIESGO ALTA	Reducir Ocurrenc ia	1. Definir líneas de seguimiento y control para la ejecución de los proyectos tecnológicos incluidos en el PETI a fin de gestionar los riesgos asociados 2. Solicitar el personal con las competencias requeridas para la estructuración y gestión de los proyectos de TI definidos en el PETI ante la instanciacompartante 3. Socializar a la Alta Dirección sobre la metodología de estructuración del PETI y su actualizaciónpara la vigencia 2020	PETI - Ajustado y actualizado vigencia 2020 Solicitud de personal con los Estudios previos del personal con las competencias en estructuración y gestión de Proyectos de TI Soport4e de Socialización de la metodología de estructuración del PETI y su actualización vigencia 2020	CIO, Coordinador GGTI y Gestor de Arquitectura Empresarial y Proyectos de TI
Riesgo 2	Inoportunidad e inefectividad en la prestación de servicios de mesa de ayuda de TI	La combinación de factores con la inadecada aplicación de la documentación del proceso de Gestión Tecnológica y la falta de mantenimiento preventivo y correctivo de la infraestructura tecnológica e informática de la Entidad, genera afectación de la capacidad de la prestación del servicio de Mesa de Ayuda de TI. (capacidad se refiere a aspectos humanos, tecnológicos u operativos).	Proceso	"1. Inadecuada gestión del Proceso Gestión Tecnológica para incorporar los Acuerdos de Nivel de Servicios - ANS en el diseño, ejecución y control en la prestación de los servicios tecnológicos 2. Falta de mecanismo de seguimiento y control para la ejecución del mantenimiento preventivo y correctivo de la plataforma tecnológica e informática de la Entidad. 3. Desactualización del alcance de los servicios tecnologicos existentes. 4. Necesidad de incorporar nuevos servicios tecnologicos." " 5. Cambios en el marco normativo legal aplicable. "	"1. Afectación de la capacidad de la prestación del servicio de Mesa de Ayuda. (aspectos humanos, tecnológicos u operativos). 2. Retrasos y reprocesos por la falta de atención de soporte técnico oportuno 3. Afectación de la continuidad de la operación. 4. Afectación de la reputación Institucional. 5. Investigaciones disciplinarias"	4	20	ZONA RIESGO EXTREMA	1. Realizar seguimiento en la Herramienta de gestión de la mesa de ayuda de TI (Centro de Servicios), sobre atención y el cumplimiento de los ANS establecidos en el Catálogo de Servicios. 2. Ejecutar el Plan de Mantenimiento preventivo ycorrectivo de la Infraestructura Tecnológica de la Entidad de acuerdo a los términos establecidos en el mismo. .	PROBABILIDAD	2	12	24	ZONA RIESGO MODERADA	Reducir Ocurrenc ia	1. Realizar seguimiento en la "Herramienta de gestión de la mesa de ayuda de TI (Centro de Servicios), sobre atención y el cumplimiento de los ANS establecidos en el Catálogo de Servicios 2. Ejecutar el Plan de Mantenimiento preventivo y correctivo de la Infraestructura Tecnológica de la Entidad de acuerdo a los términos establecidos en el mismo. 3 y 4. Realizar periódicamente las actividades de revisión y actualización del Catálogo de Servicios Tecnológicos de la Entidad	[(NUMERO DE INCIDENTES Y/O REQUERIMIENTOS ATENDIDOS POR MEDIO DE AYUDA DE TI QUE DIERON CUMPLIMIENTO A LOS ANS) / TOTAL DE INCIDENTES Y/O REQUERIMIENTOS REGISTRADOS EN LA HERRAMIENTA TECNOLÓGICA DEL PERIODO EVALUADO= REQUERIMIENTOS E INCIDENTES PENDIENTES DE ATENCIÓN] * 100 [(NUMERO DE ACTIVIDADES DE MANTENIMIENTO PREVENTIVO EJECUTADAS)/(NUMERO TOTAL DE ACTIVIDADES DE MANTENIMIENTO PREVENTIVO DEFINIDAS ENEL PLAN DE MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLOGICA DE LA ENTIDAD)] * 100 Dos (2) soportes de la revisión del Catálogo de Servicios Tecnológicos	CIO, Coordinador GGTI, Gestor de Mesa de Ayuda y Gestor de Proveedores
Riesgo 3	Afectación de la operación de la Entidad por pérdida de disponibilidad y continuidad de los servicios de TI	Afectación de la operación de la Entidad debido a la indisponibilidad de suministros, productos y servicios tecnológicos, fallas de la infraestructura tecnológica, pérdida de capacidad de los servicios TIC, afectando la posibilidad de ejecutar procesos y acceder a la información institucional para operar.	Proceso	"1. Indisponibilidad de los servicios tecnológicos por falta de la capacidad de la plataforma tecnológica o fallas en los procesos de mantenimiento de la infraestructura que afectan los servicios tecnológicos. 2. Falta de articulación de todos los procesos con tecnología para establecer procedimientos que identifiquen los activos y servicios que deban contar con planes de contingencia y continuidad. 3. Falta de actualizaciones en laplataforma de los servicios de TI de la entidad " " 4. Avances y requerimientos tecnológicos cambiantes del entorno externo. 5. Cambios normativos en el marco de la transformación digital del Estado	"1. Indisponibilidad y pérdida de información. 2. Pérdida de oportunidad en la ejecución de los procesos. 3. Reprocesos. 4. Interrupción de los procesos institucionales 5. Afectación de la reputación Institucional. 6. Compromiso de la seguridad de la información. 7. Pérdidas humanas por falta de información requerida para el proceso. 8. Investigaciones y sanciones disciplinarias, penales y fiscales. "	3	20	ZONA RIESGO EXTREMA	1. Realizar seguimiento y monitoreo a la disponibilidad y capacidad de los servicios tecnológicos, a través de los mecanismos establecidos en la gestión de capacidad documentada. 2. Realizar actividades de operación e implementación de lineamientos sobre la habilitación tecnológica de los procesos en la gestión de activos de información y la protección de los mismos. . 3. Actualizar la plataforma de servicios de TI de la entidad de acuerdo a los lineamientos establecidos en los mapas de servicio.de TI	PROBABILIDAD	1	20	20	ZONA RIESGO ALTA	Evitar el riesgo	1. Realizar seguimiento y monitoreo a la disponibilidad y capacidad de los servicios tecnológicos, a través de los mecanismos establecidos en la gestión de capacidad documentada 2. Realizar actividades de generación e implementación de lineamientos sobre la habilitación tecnológica de los procesos en la gestión de activos de información y la protección de los mismos. 3. Actualizar la plataforma de servicios de TI de la entidad de acuerdo a los lineamientos establecidos en los mapas de servicio.de TI	[(CANTIDAD DE TIEMPO TOTAL DEL PERIODODEVALUADO– TIEMPO DE INDISPONIBILIDAD DE LOS SERVICIOS ANALIZADOS / CANTIDAD DETIEMPO TOTAL DEL PERIODODEVALUADO)]*100 Informe de generación e implementación de lineamientos sobre la habilitación tecnológica para la gestión de Activos de Información y la protección de los mismos Tres informes sobre la actualización de la Plataforma de Servicios de TI de conformid ad a los lineamientos establecidos en los Mapas de Servicio de TI	CIO, Coordinador GGTI,CIO Y Gestor de Infraestructura
Riesgo 4	Suministro, divulgación o alteraciónde información reservada, clasificada, sensible o privilegiada de la entidad, parauso indebido en beneficio propio o de un tercero. "	Suministro, divulgación o alteraciónde información reservada, clasificada, sensible o privilegiada de la entidad, parauso indebido en beneficio propio o de un tercero, a través de la concentracion de conocimiento y capacidades tecnicas y operativas, así como del incumplimiento del código de integridad y las reglas de operacion de la entidad.	Corrupción	1. Fuga de información por motivaciones personales (funcionarios y colaboradores inconformes) presión, amenazas o engaños por parte de terceros para beneficios particulares o daño institucional. "2. Mecanismos de control débiles frente la confidencialidad y acceso a la información asociados a la falta de metodologías para la identificación, clasificación y uso de activos de información. 3. No formalización de roles y responsabilidades relacionados con la seguridad y privacidad de la información de la entidad . " 4. Ataque informático con fines de extracción de información delvalor de interes.	1. Perdida de confianza en la entidad por parte de ciudadano. 2. Acceso a informacion clasificada, reservada, sensible por procesos o personas no autorizadas, afectando la seguridad y privacidad de la información de la entidad. 3. ardida y manipulación de información o fuga de información reservada o confidencial usada para vulneración de esquemas de protección, chantajes, amenazas, o beneficio de terceros. 4. roblemas de Seguridad Nacional y desprestigio Institucional. 5. Vulnerabilidades y fallas de seguridad, lo cual impacta los servicios misionales de la Entidad	4	20	ZONA RIESGO EXTREMA	1. Diseñar una estrategia de concientización sobre la responsabilidad en el manejo de la información y sus posibles consecuencias laborales y legales. 2. Implementar controles para los activos de información identificados y clasificados. 3. Definir los roles y responsabilidades relacionados con la seguridad de la información.	PROBABILIDAD	4	20	80	ZONA RIESGO EXTREMA	Evitar el riesgo	1. Diseñar una estrategia de concientización sobre la responsabilidad en el manejo de la información y sus posibles consecuencias laborales y legales. 2. Implementar controles para los activos de información identificados y clasificados. 3. Definir los roles y responsabilidades relacionados con la seguridad de la información.	Estrategia de concientización sobre la responsabilidad en el manejo de la información y sus posibles consecuencias generadas [(NUMERO DE CONTROLES IMPLEMENTADOS ENEL PERIODO EVALUADO/ NÚMERO DE CONTROLES DELMSPI DECLARADOS EN EL PERIODO EVALUADO)]*100 Estrategia de concientización sobre la responsabilidad en el manejo de la información y sus posibles consecuencias generadas	CIO, Coordinador GGTI,CISO y Gestor de Uso y Apropiación
Riesgo 5	0	0	0	.	0	0	0			PROBABILIDAD	0	0	0	ZONA RIESGO BAJA			[(CANTIDAD DE ACTIVIDADES DEL PLAN DE SENSIBILIZACIÓNDIGITAL REALIZADAE EN EL PERIDO) / CANTIDAD DEACTIVIDADES DEL PLAN DE SENSIBILIZACIÓNDIGITAL PROGRAMADAS EN EL PERIODO]*100 [(CANTIDAD DE ACTIVIDADES DEL PLAN DE SENSIBILIZACIÓNDIGITAL REALIZADAE EN EL PERIDO) / CANTIDAD DEACTIVIDADES DEL PLAN DE SENSIBILIZACIÓNDIGITAL PROGRAMADAS EN EL PERIODO]*101	CIO, Coordinador GGTI ,CISO y Gestor de Uso y Apropiación
Riesgo 6	0	0	0	.	0	0	0			IMPACTO	0	0	0	ZONA RIESGO BAJA				
Riesgo 7	0	0	0	.	0	0	0			PROBABILIDAD	0	0	0	ZONA RIESGO BAJA				
Riesgo 8	0	0	0	.	0	0	0			PROBABILIDAD	0	0	0	ZONA RIESGO BAJA				