

# FORMATO MAPA DE RIESGOS



## Formato Mapa Riesgos

**Proceso:** TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES  
**Objetivo:** Administrar, mantener y gestionar las plataformas tecnológicas existentes en el COPNIA, e implementar nuevas soluciones tecnológicas que provean en forma oportuna, eficaz, eficiente y transparente la información necesaria para el cumplimiento de la misión del COPNIA.  
**Alcance:** El proceso de Tecnologías de la Información y las Comunicaciones comprende la identificación de necesidades TIC, la administración de las plataformas tecnológicas, la formulación e implementación de los planes y proyectos, además de la evaluación y seguimiento de los mismos, alineado con la confiabilidad, la integridad y la disponibilidad de la información.

Fecha de revisión	Septiembre de 2024
Versión:	10

Referencia	Identificación del riesgo				Análisis del riesgo inherente				Evaluación del riesgo - Valoración de los controles							Plan de Acción															
	Impacto	Causa Inmediata	Causa Raíz	Descripción del Riesgo	Clasificación del Riesgo	Frecuencia con la cual se realiza la actividad	Probabilidad Inherente	%	Criterios de impacto	Impacto inherente	%	Zona de Riesgo Inherente	No. Control	Descripción del Control	Afectación	Atributos				Probabilidad Residual Final	%	Zona de Riesgo Residual Final	Tratamiento	Plan de Acción	Responsable	Fecha Implementación					
																Tipo	Maneja	Calificación	Documentación								Frecuencia	Eficacia			
1	Reputacional	Desarticulación de la estrategia de tecnología con el marco legal y normativo institucional. Documentos de políticas variables o desactualizadas. Estructura organizacional no acorde a los procesos o proyectos TIC. Gestión inadecuada de Relaciones Internas y externas.	Estrategia de TI variable en corto plazo o mediano plazo. Marco legal y normativo variable o desactualizado. Documentos de políticas variables o desactualizadas. Estructura organizacional no acorde a los procesos o proyectos TIC, o una gestión inadecuada de las relaciones internas y externas.	Probabilidad de pérdida reputacional debido a la desarticulación de la estrategia de tecnología con la estrategia digital, ordenada por estrategias de TI variables en corto o mediano plazo, marco legal y normativo, o políticas variables o desactualizadas, estructura organizacional no acorde con los procesos o proyectos TIC, o una gestión inadecuada de las relaciones internas y externas.	Ejecución y Administración de procesos	360	Medio	60%	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.	Moderado	60%	Moderado	1	La Dirección General convoca a seguimientos de la estrategia organizacional en Comités Institucionales de Gestión y Desarrollo de manera trimestral.	Probabilidad	Preventivo	Manual	Implementación	40%	Documentación	Continua	Con Regular	Eficacia	30%	20%	Moderado	Medio	Recursos (P/PP)	Para reducir el riesgo: realizar seguimientos a cada uno de los procesos en los Comités Institucionales de Gestión y Desarrollo para verificar que la ejecución de sus planes de acción estén encaminada a la estrategia organizacional.	Profesional de gestión del Área TIC	31/12/2024
2	Reputacional	Indisponibilidad del servicio de usuarios internos y/o externos por falla o disfunción en la arquitectura de los sistemas de información, por inadecuado soporte y mantenimiento de los sistemas de información, o por inadecuada gestión en la implementación o desarrollo de nuevos sistemas de información.	Fallas u obsolescencia en la arquitectura de los sistemas de información, por inadecuado soporte y mantenimiento de los sistemas de información, o por inadecuada gestión en la implementación o desarrollo de nuevos sistemas de información.	Probabilidad de pérdida reputacional por indisponibilidad del servicio a usuarios internos y/o externos por falla o disfunción en la arquitectura de los sistemas de información, por inadecuado soporte y mantenimiento de los sistemas de información, o por inadecuada gestión en la implementación o desarrollo de nuevos sistemas de información.	Ejecución y Administración de procesos	360	Medio	60%	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector público/sector nivel departamental o municipal.	Muy Alto	60%	Alto	1	Los profesionales del Área de tecnologías de la Información y las comunicaciones supervisan los contratos de soporte, mantenimiento, actualización e implementación de los sistemas de información y servicios, TIC.	Probabilidad	Detectivo	Manual	30%	Documentación	Continua	Con Regular	Eficacia	40%	20%	Muy Alto	Alto	Recursos (P/PP)	Gestionar contratos por parte del supervisor de contratos con respecto a los ítems de seguridad de la información, disponibilidad, eficiencia, integridad, mantenimiento y actualización.	Profesionales del Área TIC	31/12/2024	
																															2
4	Económico y Reputacional	Brecha entre el usuario y la tecnología que incentive el uso y la apropiación de TIC.	Falta en la capacidad operativa del área de TI, por incidentes y/o requerimientos de la Entidad, debido a fallas en la capacidad operativa del Área de TI, o al incorrecto manejo del ciclo de vida de los servicios TIC.	Probabilidad de pérdida económica y reputacional por contar con un portafolio de servicios de tecnología insuficiente para los incidentes y/o requerimientos de la Entidad, debido a fallas en la capacidad operativa del Área de TI, o al incorrecto manejo del ciclo de vida de los servicios TIC.	Ejecución y Administración de procesos	360	Medio	60%	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.	Moderado	60%	Moderado	1	Los profesionales del Área de Tecnologías de la Información y las Comunicaciones con apoyo del Área de Gestión Humana ejecutan planes de capacitación de proyectos en los congresos de los contextos TIC.	Probabilidad	Preventivo	Manual	40%	Documentación	Continua	Con Regular	Eficacia	30%	20%	Moderado	Medio	Recursos (P/PP)	Reducir el riesgo: Adequar capacidades y sensibilizaciones en el área de producción de servicios TIC.	Profesionales del Área TIC	31/12/2024	
																															2

Fuente: Adaptado de Curso Riesgo Operativo Universidad del Rosario por Dirección de Gestión y Desempeño Institucional de Función Pública. 2020.

### CONTROL DE CAMBIOS

VERSIÓN Y FECHA	DESCRIPCIÓN
Versión 7 Enero 2020	Cambio en el nombre del riesgo 5 años: "Portafolio de servicios de tecnología insuficiente para la demanda de la Entidad" ahora "Portafolio de servicios de tecnología insuficiente para los incidentes y/o requerimientos de la Entidad"
Versión 8 Octubre 2021	SE REALIZAN LOS SIGUIENTES AJUSTES: 1. RIESGO NUMERO 1, SE INCLUYE LA CAUSAL QUEDANDO DE LA SIGUIENTE FORMA: "No contar con políticas de seguridad de la información. No contar con controles adecuados para proteger la información. Amenazas Emergentes tecnológicas o de ingeniería social que atenten a la integridad, seguridad y disponibilidad de la información. No contar con matrices de roles y perfiles. Uso de credenciales de acceso a recursos tecnológicos que han sido asignadas a otros usuarios." 2. RIESGO NUMERO 1, SE MODIFICA LA CONSECUENCIA QUEDANDO DE LA SIGUIENTE FORMA: "Consecuencia de tipo legal. Afectación de la prestación del servicio, Alteración de la información de la entidad." 3. RIESGO NUMERO 1, SE MODIFICA DESCRIPTOR QUEDANDO DE LA SIGUIENTE FORMA: "Improbable." 4. RIESGO NUMERO 1, SE MODIFICA TIPO DE CONTROL EFECTUADO QUEDANDO DE LA SIGUIENTE FORMA: "Subjetivo de seguridad de la información que vela por el cumplimiento de las políticas de seguridad de la información de la entidad, en cuya función toma decisiones que generan infortinios y reportes a entes de control en caso de ser necesario consignados en actas." 5. Especificaciones técnicas incluidas para el tema de seguridad de la información en los contratos de proyectos tecnológicos, contratos de soporte y mantenimiento. 6. Reporte en bitácora de seguimiento de tickets en caso de encontrar un evento que atente a la seguridad, integridad y disponibilidad de la información. 7. Matriz de niveles de informe proactivos y reactivos de los proveedores de servicios tecnológicos en caso de materialización de un incidente que afecte la seguridad de la información. "Asignación de credenciales de acceso personalizadas e intranstrábricas acorde a la matriz de roles y perfiles"
Versión 9 Diciembre de 2022	Ajuste a metodología definida en procedimiento Administración de Riesgos versión 7.
Versión 10 Septiembre de 2024	Se ajusta el objetivo y alcance del proceso, conforme la última actualización de la caracterización del proceso. Se descriptan para el proceso de seguridad y privacidad de la información los riesgos: "Probabilidad de pérdida económica y/o reputacional debido a la pérdida o alteración de la información originada por no contar con políticas o controles adecuados para proteger la información; o por amenazas tecnológicas emergentes o de ingeniería social que atenten la integridad, seguridad y disponibilidad de la información"; y "Probabilidad de pérdida económica y reputacional debido a la alteración premeditada en las bases de datos del COPNIA con el fin de favorecer un tercero, la cual se puede producir por la falta de controles en la calidad, seguridad, conservación, integridad y disponibilidad de la información".

ELABORADO POR:

APROBADO POR:

MARLON STIVEL MARTÍNEZ MARTÍNEZ  
 Profesional especializado del Área TIC (E)

RUBÉN DARÍO OCHOA ARBELÁEZ  
 Director General