FORMATO MAPA DE RIESGOS

Formato Mapa Riesgos

Proceso:	TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES
Objetivo:	Mantener y gestionar la plataforma tecnológica existente, implementar nuevas soluciones tecnológicas que provean en forma oportuna, eficiente y transparente la información necesaria para el cumplimiento de los fines misionales del COPNIA y formular lineamientos relacionados con estándares y buenas practicas para el manejo de la información.
Alcance:	Incluye la identificación de necesidades TIC, la administración de la plataforma tecnológica, la formulación e implementación de los proyectos, la evaluación y seguimiento de los mismos y la definición de controles que faciliten la confidencialidad, integridad y disponibilidad de la información.

Fecha de revisión	Diciembre de 2022
Versión:	9

Identificación del riesgo							Análisis del riesgo Inherente						Evaluación del riesgo - Valoración de los controles			Atributos						Evaluación del riesgo - Nivel de riesgo residual						Plan de Acción					
Referencia	Impacto	Causa Inmediata	Causa Raiz	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	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia	Probabilidad Residual Final	%	Impacto Residual Final	%	Zona de Riesgo Final	Tratamiento	Plan de Acción	Responsable	Fecha Implementación	Fecha Seguimiento	Seguimiento	Estado
1	Económico y Reputacional	Pérdida o alteración de la información	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 atentan 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	Posibilidad 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.	Ejecución y Administracion de procesos	365	Media	60%	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país	Catastrófico	100%	Extremo	1	El profesional de gestion del area tic convoca a Subcomité de seguridad de la información, que vela por el cumplimiento de las políticas de seguridad de la información de la entidad, en cuya funciones toma decisiones que generan lineamientos y reportes a entes de control en caso de ser necesario consignándose en actas.	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	Baja	36%	Catastrófico	100%	Extremo	Reducir (mitigar)	- Para eliminar las causas del riesgo: Implementar el SGSI en el COPNIA con los lineamientos de seguridad de la información para generar acciones preventivas y correctivas en la entidad.	Area TIC	31/12/2022	Trimestral	Pendiente	En curso
													2	Los supervisores de contrato del area TIC generan especificaciones técnicas exclusivas para el tema de seguridad de la información en los contratos de proyectos tecnológicos, contratos de soporte y mantenimiento.	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	Baja	22%	Catastrófico	100%	Extremo	Reducir (mitigar)	Para reducir y evitar el riesgo: generar especificaciones técnicas detalladas de seguridad de la información en los contratos donde se detalla acciones proactivas y reactivas	Area TIC	31/12/2022	Por demanda	Pendiente	En curso
													3	Los Funcionarios del area TIC reportan en bitácora de seguimiento de tickets, en caso de encontrar un evento que afente a la seguridad, integridad o disponibilidad de la información.	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	Muy Baja	13%	Catastrófico	100%	Extremo	Reducir (mitigar)	"Contingencia: Restaurar backups enmarcados en los RPO y RTO pactados contractualmente.	Area TIC				
													4	Los funcionarios del area TIC o los proveedores de contratos tecnologicos del COPNIA generan Alertas a través de informes proactivos y reactivos de los proveedores de servicios tecnológicos en caso de materialización de un incidente que afecte la seguridad de la información y acciones de remediacion o recuperacion.	Impacto	Correctivo	Manual	25%	Documentado	Continua	Con Registro	Muy Baja	13%	Mayor	75%	Alto	Reducir (mitigar)						
													5	Los funcionarios del area TIC realizan Asignación de credenciales de acceso personalizadas e intransferibles acorde a la matriz de roles y perfiles.	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	Muy Baja	8%	Mayor	75%	Alto	Reducir (mitigar)						
2	Reputacional	Desarticulación de la estrategia de tecnología con la estrategia institucional.	Estrategias de TI variables en corto plazo o mediano plazo. Marco legal y normativo variable o desactualizado. Documentos de políticas variables o desactualizados. Estructura organizacional no acorde a los procesos o proyectos TIC. Gestión inadecuada de Relaciones internas y externas.	Posibilidad de pérdida reputacional debido a la desarticulación de la estrategia de tecnología con la estrategia digital, originada 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 TI, o una gestión inadecuada de las relaciones internas y externas.	Ejecución y Administracion de procesos	365	Media	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 direccion General convoca a seguimientos de la estrategia organizacional en Comités Institucionales de Gestión y Desempeño trimestral.	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	Baja	36%	Moderado	60%	Moderado		Para reducir el riesgo: realizar seguimientos a cada uno de los procesos en los Comités Institucionales de Gestión y Desempeño para verificar que la ejecución de sus planes de acción estén encaminadas a la estrategia organizacional	Area TIC	31/12/2022	Trimestral	Pendiente	En curso
													2	El profesional de gestion TIC realiza seguimiento al indicador del Plan Estratégico de Tecnologías de la Información y las Comunicaciones. PETIC.	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	Baja	22%	Moderado	60%	Moderado		Contingencia: en caso de cambio de direccionamiento estratégico, se debe realizar un estudio de arquitectura empresarial TOGAF para diseñar la nueva ruta de proyectos.	Area TIC	31/12/2022	Trimestral	Pendiente	En curso
3	Económico y Reputacional	Alteración premeditada en las bases de datos para favorecer un tercero.	Falta de controles para la calidad, seguridad, conservación, integridad y disponibilidad de la información.	Posibilidad de pérdida económica y reputacional debido a la alteración premeditada en las bases de datos del COPNIA con el fin de favorecer un tercero, lo cual se puede propiciar por la falta de controles en la calidad, seguridad, conservación, integridad y disponibilidad de la información.	Fraude Externo	365	Media	60%	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país	Catastrófico	100%	Extremo	1	El area de Tecnologías de la Información y las Comunicaciones realiza el manejo de matriz de roles y perfiles en los sistemas de información y las bases de datos.	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	Baja	36%	Catastrófico	100%	Extremo		Contingencia: restaurar backups de acuerdo a los RPO y RTO contractuales.	Area TIC				
													2														Para eliminar las causas: designación acertada de los líderes funcionales encargados de vigilar la data.	Area TIC	31/12/2022	Por demanda	Pendiente	En curso
													3														Para reducir el riesgo: Informar a los líderes funcionales acerca de los registros de la matriz de roles y perfiles para su conocimiento y observaciones de los funcionarios que tienen acceso a la información.	Area TIC	31/12/2022	Por demanda	Pendiente	En curso

FORMATO MAPA DE RIESGOS

4	Reputacional	Indisponibilidad del servicio a usuarios internos y/o externos	Fallas u obsolescencia en la arquitectura de los sistemas de información. Inadecuado soporte y mantenimiento de los sistemas de información. Inadecuada gestión en la implementación o desarrollo de nuevos sistemas de información.	Posibilidad de pérdida reputacional por la indisponibilidad del servicio a usuarios internos y/o externos por fallas u obsolecencia 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.	Ejecucion y Administracion de procesos	365	Media	60%	El riesgo afecta la imagen de de la entidad con efectp publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal	Mayor	80%	Alto	1	El Área de tecnologias de la Información y las comunicaciones supervisa los contratos de soporte, mantenimiento y actualización de los sistemas de información y servicios, TIC.	Probabilidad	Detectivo	Manual	30%	Documentado	Continua	Con Registro	Media	42%	Mayor	80%	Alto		Para reducir el riesgo: Gestión contractual por parte del supervisor de contratos con respecto a los ítems de seguridad de la información, disponibilidad, eficiencia, eficacia, integridad, mantenimiento y actualización.	Area TIC	31/12/2022	Mensual	Pendiente	En curso
															2											Contingencia: migración de la data al sistema que se encuentre en operación.	Area TIC	31/12/2022	Por demanda	Pendiente	En curso
5	Económico y Reputacional	Portafolio de servicios de tecnología insuficiente para los incidentes y/o requerimientos de la Entidad.	Fallas en la capacidad operativa del área de TI. Incorrecto manejo del ciclo de vida de los servicios TI.	Posibilidad 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 TI.	Ejecucion y Administracion de procesos	365	Media	60%	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Moderado	60%	Moderado	1	El Área de tecnologia de la Información y las Comunicaciones ejecuta el Procedimiento del área TIC alineado a UTIL V3, definiendo niveles de escalamiento y ANS.	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	Baja	36%	Moderado	60%	Moderado		Utilizar el último portafolio de servicios vigente para el área TIC.	Area TIC	31/12/2022	Por demanda	Pendiente	En curso
6	Económico y Reputacional	Brecha entre el usuario y la tecnología	Inadecuadas sensibilizaciones o capacitaciones para incentivar el uso y la apropiación de TIC	Posibilidad de pérdida económica y reputacional por la brecha existente entre el usuario y la tecnología, debido a las inadecuadas sensibilizaciones o capacitaciones para incentivar el uso y la apropiación de TIC.	Ejecucion y Administracion de procesos	365	Media	60%	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Moderado	60%	Moderado	1	El Área de Tecnologias de la Información y las Comunicaciones con apoyo del Área de Gestión Humana ejecuta planes de capacitación de proyectos en los cronogramas de los contratos TI.	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	Baja	36%	Moderado	60%	Moderado		Reducir el riesgo: Adecuadas capacitaciones y sensibilizaciones en la entrada a producción de servicios TIC.	Area TIC	20/04/2022	Por demanda	Pendiente	En curso
															2											Contingencia: Ejecutar presupuesto adicional de capacitaciones a grupos focales que tengan dificultades con el uso y apropiación de herramientas TIC"	Area TIC				

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 2019	Cambio en el nombre del riesgo 5 antes "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 atentan 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: Consecuencias de tipo legal. Afectación en 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: *Subcomité de seguridad de la información que vela por el cumplimiento de las políticas de seguridad de la información de la entidad, en cuy as funciones toma decisiones que generan lineamientos y reportes a entes de control en caso de ser necesario consignándose en actas. *Especificaciones técnicas exclusivas para el tema de seguridad de la información en los contratos de proyectos tecnológicos, contratos de soporte y mantenimiento. *Reporte en bitácora de seguimiento de tickets en caso de encontrar un ev ento que atente a la seguridad, integridad o disponibilidad de la información. *Alertas a través de informes proactiv os y reactiv os 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 intransferibles acorde a la matriz de roles y perfiles.
Versión 9 Diciembre de 2021	Ajuste a metodología definida en procedimiento Administración de Riesgos versión 7.

ELABORADO POR:

ALVARO IVAN TORRES GONZALEZ

Firmado digitalmente por ALVARO IVAN TORRES GONZALEZ
Fecha: 2022.12.22 08:02:26 -05'00'

ÁLVARO IVÁN TORRES GONZÁLEZ

Profesional de Gestion TIC

APROBADO POR:

RUBEN DARIO OCHOA ARBELAEZ

Firmado digitalmente por RUBEN DARIO OCHOA ARBELAEZ
Fecha: 2023.01.13 18:12:36 -05'00'

RUBÉN DARÍO OCHOA ARBELÁEZ

Director General