COPNIA

MAPA DE RIESGOS

PROCESO	**TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES**																		
																	FECHA DE REVISIÓN: ENERO 2019 **VERSIÓN: 7**		
CAUSAS	**RIESGO**	**DESCRIPCIÓN**	**CONSECUENCIAS**	**RIESGO INHERENTE**				**NIVEL RIESGO INHERENTE**	**CONTROLES**	**RIESGO RESIDUAL**				**NIVEL RIESGO RESIDUAL**	**ACCIONES**	**RESPONSABLE**	**REGISTROS**
				PROBABILIDAD		**IMPACTO**				**PROBABILIDAD**		**IMPACTO**					
				NIVEL	**DESCRIPTOR**	**NIVEL**	**DESCRIPTOR**			**NIVEL**	**DESCRIPTOR**	**NIVEL**	**DESCRIPTOR**				
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.	Pérdida o alteración de la información	Riesgo de seguridad de la información: cuando hay ocurrencia no autorizada de: Sustracción de información Eliminación de Información Modificación de la información Pérdida de información. Indisponibilidad de información. Divulgación de información sensible.	Consecuencias de tipo legal. Afectación en la prestación del servicio	1	Rara vez	4	Mayor	ZONA RIESGO ALTA	*Subcomité de seguridad de la información que vela por el cumplimiento de las políticas de seguridad de la información de la entidad, en cuyas 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 evento que atente a la seguridad, integridad o disponibilidad de la información. *Alertas a través de informes proactivos y	1	Rara vez	4	Mayor	Alta	* 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 *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 *Contingencia: Restaurar backups enmarcados en los RPO y RTO pactados contractualmente	Profesional de gestión del área TIC	*Manual de seguridad de la información *Ítems técnicos de seguridad de la información en contratos *Ítems técnicos de backup en contratos
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.	Desarticulación de la estretegia de tecnología con la estrategia institucional.	Riesgo de estrategia TI y Gobierno TI:La definición de PETIC, proyecta el camino a seguir para la organización en materia de TI, lo cual alimenta directamente a la estrategia organizacional general, donde se proyectan recursos para la sostenibilidad de los mismos y la alineación con el plan estratégico del COPNIA , si esta estrategia consignada en el PETIC se ve seriamente modificada por lineamientos organizacionales, puede desarticular todos los proyectos tecnológicos y los recursos programados.	Inconsistencias e incompatibilidades en las tecnologías implementadas Sub utilización de los proyectos TI implementados	1	Rara vez	3	Moderado	ZONA RIESGO MODERADA	*Seguimientos en comité de desarrollo administrativo trimestral a la estrategia organizacional *Indicador de PETIC del área TIC	1	Rara vez	3	Moderado	Moderada	*Para reducir el riesgo: Se debe realizar seguimientos a cada uno de los procesos en los comités de desarrollo administrativo para verificar que la ejecución de sus planes de acción están encaminadas a la estrategia organizacional *Contingencia: en caso de cambio de direccionamiento estratégico, se debe realizar un estudio de arquitectura empresarial TOGAF para diseñar la nueva ruta de proyectos	Profesional de gestión del área TIC	*Comités de desarrollo administrativo trimestrales *Seguimiento a indicador del PETIC
Falta de controles para la calidad, seguridad, conservación, integridad y disponibilidad de la información.	Alteración premeditada en las bases de datos para favorecer un tercero.	Riesgo de gestión de la Información: El riesgo de gestión de la información se presenta cuando hay inconsistencias en la información, generadas de forms premeditada, que reposa en las bases de datos de la entidad ya que esta se comporta como un bien público	Información errónea presentada a la ciudadanía que desencadena un mal ejercicio de la ingeniería en la sociedad colombiana.	1	Rara vez	4	Mayor	ZONA RIESGO ALTA	*Manejo de matriz de roles y perfiles en los sistemas de información y las bases de datos	1	Rara vez	4	Mayor	Alta	*Contingencia: restaurar backups de acuerdo a los RPO y RTO contractuales *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 *Para eliminar las causas: designación acertada de los líderes funcionales encargados de vigilar la data	Profesional de gestión del área TIC	*Matriz de roles y perfiles
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.	Indisponibilidad del servicio a usuarios interno o externos por fallas u obsolescencia de los sitemas de información	Riesgo de sistemas de información: se presenta cuando hay una obsolescencia tecnológica o una carencia de soporte y mantenimiento adecuado en el mercado, generando un impacto para los procesos organizacionales que estén implementados en dicho sistema de información.	Consecuencias legales. Insatisfacción de los usuarios Costos de migraciones.	2	Improbable	3	Moderado	ZONA RIESGO MODERADA	*Contratos de soporte, mantenimiento y actualización de sistemas de información y servicios TIC	1	Rara vez	3	Moderado	Moderada	*Para reducir el riesgo: Gestión contractual por parte del supervisión de contratos con respecto a los ítems de seguridad de la información, disponibilidad, eficiencia, eficacia, integridad, mantenimiento y actualización. *Contingencia: migración de la data al sistema que se encuentre en operación.	Profesional de gestión del área TIC	*Supervisión de contratos
Fallas en la capacidad operativa del área de TI. Portafolio de servicios de TI insuficiente. Incorrecto manejo del ciclo de vida de los servicios TI.	Portafolio de servicios de tecnología insuficiente para los incidentes y/o requerimientos de la Entidad.	Riesgo de Servicios Tecnológicos: se presenta cuando el portafolio de servicios de tecnología no cubre todas las necesidades de la entidad y la capacidad operativa para sustentarlos es insuficiente.	La entidad no contaría con un soporte sobre los servicios TI	2	Improbable	2	Menor	ZONA RIESGO BAJA	*Procedimiento del área TIC alineado a ÚTIL V3, definiendo niveles de escalamiento y ANS	1	Rara vez	2	Menor	Baja	*Contingencia: utilizar el ultimo portafolio de servicios vigente para el área TIC	Profesional de gestión del área TIC	*procedimientos y portafolio de servicios del área de TIC

Inadecuadas sensibilizaciones o capacitaciones para incentivar el uso y la apropiación de TIC	Brecha entre el usuario y la tecnología	Riesgo de uso y apropiación: El riesgo de uso y apropiación de TIC se presenta cuando la entrega de proyectos de tecnología no se hace de una forma adecuada a las necesidades de la organización, creando brechas entre el usuario y la tecnología, donde no se realizo una efectiva capacitación, sensibilización y una retroalimentación continua conforme evoluciona el portafolio TIC.	Sub utilización de los sistemas de información y servicios TIC. Falta de entendimiento por parte de los usuarios de la interacción con los servicios TI del COPNIA.	2	Improbable	2	Menor	ZONA RIESGO BAJA	*Planes de capacitación de proyectos en los cronogramas de los contratos	1	Rara vez	2	Menor	Baja	Reducir el riesgo: Adecuadas capacitaciones y sensibilizaciones en la entrada a producción de servicios TIC Contingencia: Ejecutar presupuesto adicional de capacitaciones a grupos focales que tengan dificultades con el uso y apropiación de herramientas TIC	Profesional de gestión del área TIC	Capacitaciones coordinadas entre GH o proveedores y TIC en cuanto al uso y apropiación de tecnologías de la información.

CONTROL DE CAMBIOS

VERSIÓN Y FECHA	DESCRIPCIÓN
Versión 3 Julio 2017	Se hizo revisión del mapa de riesgos, teniendo en cuenta el conocimiento del proceso y las observaciones realizadas por la Oficina de control Interno. Se eliminó el riesgo que se tenía de Incumplimiento del PETIC y se determinó relacionar un solo riesgo relacionado con la pérdida de la información.
Versión 4 Octubre 2017	Se modifica las causas de los riesgos, ampliando los temas detectados en el análisis de TIC en arquitectura empresarial, se actualizan las consecuencias, generando un lineamiento claro en el índice de disponibilidad de los sistemas de información y se adjuntan acciones encaminadas al cumplimiento del PETIC.
Versión 5 Enero 2018	Del riesgo "Perdida o indisponibilidad de la operación" se elimino la causa Falta de plan estrategico de tecnologia de la información, se incluyó la causa: Riesgos emergentes de la seguridad de la información y de las comunicaciones, se elimino la acción: Elaborar PETIC (Plan estrategico de tecnologia) para tener un direccionamiento claro de los proyectos a implementarse y tener un crecimiento ordenado y dinámico y se incluyó la acción implementar los proyectos de inversión que ayudan a mitigar sustancialmente la ocurrencia y el impacto de incidentes de seguridad de la información y las comunicaciones planteados en el PETIC.
Versión 6 Octubre 2018	Se hizo un replanteamiento total del mapa de riesgos, definiendo un riesgo por cada categoría: de seguridad de la información, de estrategia TI y gobierno TI, de gestión de la información, de sistemas de información y de uso y apropiación.
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"

ELABORADO POR:

IVÁN TORRES

Profesional de gestión del área de Tecnología de la Información y de las Comunicaciones

APROBADO POR:

RUBEN DARÍO OCHOA ARBELÁEZ

Director General