aci Medellín

PLAN DE TRATAMIENTO

DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2026

AGENCIA DE COOPERACIÓN E INVERSIÓN DE MEDELLÍN
Y EL ÁREA METROPOLITANA
República de Colombia

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CRISTINA ZAMBRANO RESTREPO
Representante Legal

JAVIER ESTEBAN BOTERO GOMEZ
Técnico de Sistemas de Información

2026

CONTENIDO

1. INTRODUCCIÓN

La administración de los riesgos de seguridad y privacidad de la información se presenta como un enfoque lógico y sistemático, esencial para la identificación, análisis, evaluación, tratamiento, monitoreo y comunicación de los riesgos asociados a la información generada por los diversos procesos de la Agencia de Cooperación e Inversión de Medellín y el Area Metropolitana (ACI Medellín). Este método tiene como finalidad primordial permitir a la entidad minimizar las posibles pérdidas y maximizar las oportunidades de mejora.

En la búsqueda de cumplir con sus funciones, misiones y objetivos, la ACI Medellín, como entidad pública, se encuentra inmersa en una serie de riesgos que podrían comprometer la gestión de procesos e incluso afectar la integridad de la organización en su conjunto. Por lo tanto, es imperativo adoptar medidas adecuadas que permitan la identificación precisa de las causas y las posibles consecuencias que podrían derivarse de la materialización de dichos riesgos.

El presente plan es un instrumento estratégico destinado para facilitar y orientar la implementación de una gestión de riesgos eficaz, eficiente y efectiva para la Agencia. Desde la fase de identificación hasta la aplicación de medidas de mitigación máxima, se pone especial énfasis en la importancia de la administración del riesgo en la seguridad y privacidad de la información. Este documento proporcionará fundamentos técnicos sólidos y brindará lineamientos claros y sencillos para la gestión adecuada de los riesgos asociados a la información que maneja la entidad.

Para la vigencia 2026, el presente Plan de Tratamiento de Riesgos se consolida como un componente fundamental del **Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI)** de la ACI Medellín, alineado con la norma **ISO/IEC 27001**, la norma **ISO/IEC 27005**, el Modelo de Seguridad y Privacidad de la Información del MinTIC y los lineamientos de la Superintendencia de Industria y Comercio (SIC), incorporando un enfoque de mejora continua y gestión de riesgos frente a amenazas actuales

2. OBJETIVOS

2.1 Objetivo general

Establecer un marco integral y eficaz que permita identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados a la información generada por los diversos procesos de la entidad. El propósito final es salvaguardar la integridad, confidencialidad y disponibilidad de la información, minimizando pérdidas potenciales y maximizando oportunidades de mejora. Además, busca crear una cultura organizacional que reconozca la importancia de la administración del riesgo en la seguridad y privacidad de la información, promoviendo la aplicación de medidas preventivas y correctivas para garantizar la continuidad y resiliencia de la ACI Medellín frente a posibles amenazas y vulnerabilidades.

2.2 Objetivos específicos

1.2.1 Concientizar y comprometer a todos los servidores de la Agencia sobre la necesidad e importancia de gestionar de manera adecuada los sistemas de información y los recursos tecnológicos, mitigando los riesgos inherentes a los que esto conlleva.

1.2.2 Promover una cultura de prevención ante los riesgos de seguridad y privacidad de la información, creando conciencia al interior de la Agencia de los beneficios que conlleva su buen uso y aplicación, además de informar acerca de los efectos negativos que puede generar para la entidad por el desconocimiento o uso inapropiado.

2.2.3 Integrar la gestión de riesgos de seguridad y privacidad de la información al ciclo de mejora continua del SGSI.

2.2.4 Fortalecer la identificación, análisis y tratamiento de riesgos asociados a amenazas emergentes como ransomware, fuga de información, accesos no autorizados y fallas en servicios en la nube

3. ALCANCE

Este Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, suministra metodologías y conceptos para la Agencia que apalancaran la administración y gestión de los riesgos a nivel de todos los procesos; orienta sobre las actividades y buenas prácticas aplicadas a los procedimientos que tienen que ver con el uso y custodia de la información, identificando los riesgos, su valoración y la definición de opciones de manejo que pueden requerir la posible formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

4. DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización.

Activos de información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgos: uso sistemático de la información para identificar las fuentes y estimar el riesgo.

Apetito al riesgo: magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: Medida por la que se modifica el riesgo. Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. Los términos salvaguardan o contramedida son utilizados frecuentemente como sinónimos de control.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Evitación del riesgo: Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Impacto: Cambio adverso en el nivel de los objetivos del negocio logrados. NTC-ISO 27005:2008. Tecnologías de la Información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información. Términos y definiciones. P. 2.

Incidente de seguridad de la información: un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Probabilidad: se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

Reducción del riesgo: Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo: Aceptación de la pérdida o ganancia proveniente de un riesgo particular

Riesgo de corrupción: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Riesgo de seguridad digital: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles. Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 4 - Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018

Riesgo Residual: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo.

Riesgo: En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridad de la información pueden expresarse como un efecto de incertidumbre sobre los objetivos de seguridad de la información. El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.

Seguridad de la Información: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad:

Sistema de Gestión de Seguridad de la información SGSI: parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Tratamiento del Riesgo: Proceso para modificar el riesgo”

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para lograr los objetivos de la administración del riesgo en la seguridad y privacidad de la información no solo se depende del plan, también de las partes involucradas y su participación, por ello es preciso identificar los actores que intervienen.

- **Comité Directivo:** aprueban los lineamientos conceptuales y metodológicos definidos en la GI-SIG-01 guía de administración de riesgos, es responsable de fortalecer, incentivar y hacer cumplir las políticas allí definidas.
- **Proceso del Sistema Integrado de Gestión:** es el encargado de generar la metodología para la administración de riesgo; coordina, lidera, asesora y capacita en su objeto funcional.
- **Integrantes de los procesos institucionales:** identifican, analizan y valoran los riesgos del proceso o subproceso por lo menos una vez al año, si bien están apoyados por el Profesional Senior en Calidad, son los responsables de garantizar que en el proceso se definan los riesgos de la información que le competen, se establezcan los controles y se adelanten las actividades para mitigarlos.
- **Contratistas**: ejecutar en sus funciones los controles y acciones definidas en los lineamientos de la administración del riesgo, también aportan a la identificación de posibles amenazas que puedan afectar la información institucional.
- **Control Interno**: su responsabilidad es verificar y evaluar la elaboración, la visibilizarían, el seguimiento y el control del mapa de riesgos, conforme a la GI-SIG-01 guía de administración de riesgo.

6. METODOLOGÍA

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la ACI Medellín, se regirá por lo estipulado en la GI-SIG-01 Guía de Administración de Riesgos, la cual tiene como objetivo:

“Establecer disposiciones y criterios institucionales que orienten a la ACI Medellín en la correcta identificación, análisis, valoración y administración de los riesgos, con el fin de reducir la probabilidad de ocurrencia y el grado de impacto de aquellos riesgos que pueden afectar el logro de los objetivos institucionales en el marco de los procesos”.

Para ello todos los funcionarios y contratistas de la Agencia se comprometen a:

- ✓ Conocer, cumplir y apropiarse de los lineamientos en la administración del riesgo en la seguridad y privacidad de la información de acuerdo con los controles y acciones definidas en el mapa de riesgos de la Agencia.

- ✓ Aplicar a los procesos y procedimientos una permanente revisión y análisis de riesgos en la seguridad y privacidad de la información para poder tomar acciones y controles con el objetivo de mitigarlos.

- ✓ Desarrollar acciones de contingencia asegurando la disponibilidad de la información en los eventos donde pueda que se materialice un riesgo en la seguridad y privacidad de la información poniendo en peligro los objetivos y la misión de la Agencia.

- ✓ Presentar propuestas de mejora continua que permitan optimizar los proceso aumentando la eficacia y efectividad en el manejo de la información.

- ✓ Controlar permanentemente los cambios en las calificaciones de los riesgos en la seguridad y privacidad de la información para realizar ajustes pertinentes al mapa de riesgos institucional.

La gestión de riesgos de seguridad y privacidad de la información se desarrollará bajo un enfoque de **mejora continua (Planear – Hacer – Verificar – Actuar)**, permitiendo la revisión periódica de los riesgos, la efectividad de los controles implementados y la adopción de acciones correctivas y preventivas frente a cambios en el contexto organizacional y tecnológico.

7. ANALISIS DE VULNERABILIDAD

7.1 Situaciones no deseadas

- Hurto de información por robo de equipos informáticos.
- Hurto de información durante el cumplimiento de las funciones laborales, por intromisión.
- Inaccesibilidad a la información por perdida de medios de conexión.
- Incendio en las instalaciones de la entidad por desastre natural, instalaciones inadecuadas o de manera intencional.
- Alteración de claves y cuentas de acceso.
- Corte del servicio de internet por parte del ISP - Proveedor del Servicio de Internet.
- Corte del fluido eléctrico no programado.
- Daño de equipos físicos y corrupción de información.
- Retraso en asistencia técnica gestionada mediante la mesa de ayuda.
- Fuga de información al interior de la entidad, por parte de los funcionarios y contratistas.
- Manipulación indebida de información.
- Ataques de ransomware que afecten la disponibilidad de la información.
- Phishing e ingeniería social dirigida a funcionarios y contratistas.
- Uso indebido de credenciales de acceso.
- Fuga de información por error humano o uso inadecuado de herramientas colaborativas.
- Fallas de seguridad asociadas a servicios en la nube o accesos remotos.

7.2 Análisis de vulnerabilidad

A continuación, se describirán las amenazas y debilidades tecnológicas, con el fin de determinar las falencias y establecer los controles necesarios para mitigar la materialización de un posible riesgo.

- **Fortalecimiento de la conectividad a (IaaS).**

  La Agencia cuenta con sistemas de información en la nube como lo son Office 365 (correo electrónico, almacenamiento en la nube OneDrive, SharePoint intranet, Teams comunicaciones unificadas), CRM institucional ZOHO ONE, software de antivirus Cloud y una infraestructura tecnológica en nube privada (IaaS), la cual permite tener alta disponibilidad de servicio y robustos sistemas de respaldo de información, aun así no estamos protegidos ante un eventual corte de la fibra óptica que conecta las instalaciones de la ACI Medellín con su proveedor de Infraestructura.

- **Adecuaciones al centro de datos.**

  Actualmente, el centro de datos de la Agencia no cumple con las buenas prácticas de TI, debido a:

  1. El cuarto técnico no cuenta con el espacio adecuado.
  2. Se encuentran cajas de breakers sin tapa, generando riesgos como cortos circuitos.
  3. No cuenta con un aire acondicionado de precisión, no controla la humedad y no es automático.
  4. No se cuenta con un piso falso, actualmente es de madera un material combustible que puede propiciar un incendio.

  Todas estas condiciones pueden afectar la UPS, los Switches, el router y el servidor de telefonía IP físicamente al igual que el sistema de almacenamiento y cableado.

8. DESCRIPCION DE RIESGOS DE SEGURIDAD DE LA INFORMACION

Los riesgos de seguridad de la información asociados a los activos de información se encuentran en el formato FR-GSI-04 Descripción de riesgos de seguridad de la información.

No.	PROCESO ESTRATEGICO	RIESGO	ACTIVO	TIPO	AMENAZAS	VULNERABILIDADES
1	Planeación	Posible modificación no autorizada de la información causando perdida de integridad	Documento de Planeación	Información	Acto fraudulento Chantaje	Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección
			Caracterización	Información		
			Procedimientos	Información		
2	Gestión de proyectos	Posible perdida de integridad y confidencialidad de la información que pueda tener como finalidad favorecer intereses particulares o de terceros	12.9 INFORME 12.1.19 Proyectos especiales	Información	Ingeniería social Penetración del sistema Hurto de información	Líneas de comunicación sin protección Tráfico sensible sin protección Falta de conciencia en seguridad Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección
			12.9 INFORME2 Digitalización	Información		
			12.9 INFORME3 Propuestas Digitalización	Información		
			12.9 INFORME4 Propuestas de valor	Información		
			12.9 INFORME5 Digitalización-YYYY	Información		
			12.9 INFORME6 Conclusiones	Información		
		Posible divulgación intencionada de información pública clasificada	1. Cooperación 1 Desarrollo económico	Información	Crimen por computador Acto fraudulento Hurto de información Ingeniería social	Líneas de comunicación sin protección Tráfico sensible sin protección ausencia de terminación de sesión Falta de conciencia en seguridad Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección
			1. Cooperación 2 Desarrollo Social	Información		
			1. Cooperación 3 Transformación	Información		
			1. Cooperación 4 Observación y construcción de paz	Información		
			1. Cooperación 5 Ecosistemas	Información		
			1. Cooperación 6 General	Información		
			1. cooperación 7 Urbanismo y Sostenibilidad	Información		
			1. Inversión 1. Agronegocios	Información		
			1. Inversión 2. Industrias 4.0	Información		
			2. Inversión 3 Industrias Creativas	Información		
			2. Inversión 4. Infraestructura y competitividad	Información		
			1. Inversión 5. Manufactura	Información		
			2. Inversión 6 Químicos y Ciencias de la Vida	Información		
			2. Inversión 7 Territorio Verde y Sostenible	Información		
			3. Inversión 8. Comercio	Información		
			CRM	Software		

No.	PROCESO/ SUBPROCESO	RIESGO	ACTIVO	TIPO	AMENAZAS	VULNERABILIDADES
3	Procesamiento y comunicaciones	Posible pérdida de integridad que tenga como consecuencia la inexactitud de la información.	ORFEO	Software	Dimes por computador Acto fraudulento Hurto de información Ingeniería social	Líneas de comunicación sin protección Tráfico sensible sin protección Ausencia de terminación de sesión Falta de concientización en seguridad Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección
			15-4 Actas y seguimiento a controles de riesgo	Información		Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección
			15-4 Comunicaciones internas	Información		
			15-13 Planes	Información		
			15-11 Programas	Información		
			15-14 Sistema Gestión	Información		
		Posible modificación no autorizada de la información causando pérdida de integridad o suplantación de identidad	Office 365 - Onedrive	Software	Ingeniería Social Acto fraudulento Dimes por computador	Líneas de comunicación sin protección Tráfico sensible sin protección Ausencia de terminación de sesión Falta de concientización en seguridad Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección
			15-6 Contratos	Información		Líneas de comunicación sin protección Tráfico sensible sin protección Falta de concientización en seguridad
			15-4 Comunicaciones internas	Información		
			15-10 Informes	Información		
2	Relaciones sociales e internacionales	Posible indisponibilidad para consultar la información requerida del proceso de RI	14-1 Actas	Información	Ataques contra el sistema	Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección
			14-6 Convenios	Información		
			14-12 Instrumentos de control	Información		
		Posible modificación no autorizada de la información o por suplantación de identidad causando pérdida de integridad en la información del ORFEO	ORFEO	Software	Ingeniería Social Acto fraudulento Dimes por computador Ingeniería social	Líneas de comunicación sin protección Tráfico sensible sin protección Ausencia de terminación de sesión Falta de concientización en seguridad Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección
		Posible modificación no autorizada de la información o por suplantación de identidad causando pérdida de integridad en la información del proceso de RI.	14-13 Planes	Información		Líneas de comunicación sin protección Tráfico sensible sin protección Falta de concientización en seguridad
			14-11 Programas	Información		
			14-5 Informes	Información		
			14-5 Contratos	Información		Líneas de comunicación sin protección Tráfico sensible sin protección Ausencia de terminación de sesión Falta de concientización en seguridad Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección

No.	PROCESO/ SUBPROCESO	RIESGO	ACTIVO	TIPO	AMENAZAS	VULNERABILIDADES
1	Conocimiento e innovación	Posible indisponibilidad para consultar la información requerida relacionada con los documentos académicos del proceso de CI	Documentos académicos	Información	Ataques contra el sistema	Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección
		Posible divulgación de información pública clasificada relacionada con el proceso de CI	Productos CI	Información	Acto Fraudulento Chantaje	Líneas de comunicación sin protección Tráfico sensible sin protección Falta de concientización en seguridad
			Plan de trabajo Grupo primario ORFEO Subsistema	Información		
		Posible indisponibilidad para consultar oportunamente la información requerida de los redes, plataformas y documentos del proceso de CI	AZ Individual	Software De Oficina	Ataques contra el sistema Phishing Ingeniería Social	Líneas de comunicación sin protección Tráfico sensible sin protección ausencia de terminación de sesión Falta de concientización en seguridad Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección Ausencia de proceso para supresión de derechos de acceso
			Orfeo	Software De Oficina		
			Hojas de vida	Software De Oficina		
			Impacta	Software Gerencial		
			Base de Datos de usuarios	Información		
			CVLAC	Información		
			Actas comité transversal cooperación	Información		
			Actas comité transversal inversión	Información		

NO.	PROCESO / DIRECCIÓN	RIESGO	ACTIVO	TIPO	AMENAZAS	VULNERABILIDAD
7	Gestión de recursos físicos	Posible modificación no autorizada de información relacionada con los recursos físicos	Mantenimientos	Información	Acto Fraudulento	Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección
			Servicios públicos	Información		
			Arrendamiento	Información		
			Facturas bienes	Información		
			Actas	Información		
			Fotos bienes	Información		
			Plan de compras	Información		
			Bajas definitivas	Información		
			Depreciaciones	Información		
		Posible modificación no autorizada de información asociada a los bienes y activos de la entidad con o sin intención causando pérdida de integridad o suplantación de identidad	Inventarios activos	Información	Ingeniería social Acto fraudulento Ataque por computador	Líneas de comunicación sin protección Tráfico sensible sin protección Falta de conciencia en seguridad Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección
			Conciliación activos	Información		
			Convenios	Información		
			Facturación electrónica	Información		
			Activos fijos	Software		
		Posible modificación no autorizada de información relacionada con los seguros con o sin intención causando pérdida de integridad o suplantación de identidad	Seguros	Información	Ingeniería social Acto fraudulento Ataque por computador	Líneas de comunicación sin protección Tráfico sensible sin protección ausencia de terminación de sesión Falta de conciencia en seguridad Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección Ausencia de procesos para supervisión de derechos de acceso
8	Gestión presupuestal y financiera	Posible indisponibilidad para consultar oportunamente la información requerida y modificación no autorizada de la información	Documentos soporte	Información	Ataques contra el sistema Penetración del sistema	Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección
			Relación de pagos	Información		
			Liberaciones presupuestales	Información		
			Auditoría seguridad social	Información		
			Conciliación bancaria	Información		
			Manual de políticas contables	Información		
			Resoluciones	Información		
			RUB	Información		
			Análisis financiero	Información		
			DIAN	Información		
			Manual de procedimiento	Información		
			Deudores	Información		
			Plan operativo	Información		
			CDLA	Información		
		Posible modificación no autorizada de información contable y financiera con o sin intención causando pérdida de integridad o suplantación de identidad	ACDI	Información	Ataque contra el sistema Acto fraudulento cometido por computador	Líneas de comunicación sin protección Tráfico sensible sin protección Falta de conciencia en seguridad Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección
			Comunicantes	Información		
			Comunicantes contables	Información		
			Declaraciones	Información		
			Informes	Información		
			Libros contables	Información		
			Planes	Información		
			Estados financieros	Información		
			PREDIS	Información		
			Relación en la Fuente	Información		
			CDP	Información		
			Comisiones	Información		
			Certificados	Información		
			Software a fin	Software		
		Posible divulgación y notificación no autorizada de la información causando pérdida de integridad o suplantación de identidad	Base de datos de proveedores	Información	Chantaje Pérdida de información Ingeniería social	Líneas de comunicación sin protección Tráfico sensible sin protección ausencia de terminación de sesión Falta de conciencia en seguridad Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección Ausencia de procesos para supervisión de derechos de acceso
			Claves y firmas	Información		

No.	PROCESO/ SUBPROCESO	RIESGO	ACTIVO	TIPO	AMENAZAS	VULNERABILIDADES
9	Gestión documental	Posible modificación no autorizada de la información de gestión documental causando pérdida de integridad o suplantación de identidad e indisponibilidad para consultar oportunamente la información requerida	Inventario Siaserinc	Información	Ataque contra el sistema Crimen por computador Penetración contra el sistema	Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección
			Línea física tecnológica	Hardware		
			Equipo físico tecnológico	Hardware		
		Posible modificación no autorizada de la información almacenada en los equipos de GDO causando pérdida de integridad o suplantación de identidad e indisponibilidad para consultar oportunamente la información requerida	Software de Radicación	Software Servicios	Ingeniería social Ataque contra el sistema Crimen por computador Penetración contra el sistema	Líneas de comunicación sin protección Tráfico sensible sin protección Falta de conciencia en seguridad Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección
			Equipo físico tecnológico	Hardware		
			Equipo físico tecnológico	Hardware		
			Equipo físico tecnológico	Hardware		
			Inventario Medios Magneticos	Información		
		Posible divulgación de información pública clasificada, modificación no autorizada de la información causando pérdida de integridad o suplantación de identidad	Inventario Archivo Central CAD #2 Medellín	Información	Ataques contra el sistema Penetración del sistema Acto fraudulento	Líneas de comunicación sin protección Tráfico sensible sin protección ausencia de terminación de sesión Falta de conciencia en seguridad Ausencia de mecanismos de identificación y autenticación de usuarios
			Inventario Custodia Documental ACI Medellín - GRM	Información		
10	Gestión Jurídica	Posible modificación no autorizada de la información jurídica causando pérdida de integridad o suplantación de identidad e indisponibilidad para consultar oportunamente la información requerida	Circulares	Información	Ataques contra el sistema Penetración en el sistema Acto fraudulento Crimen por computador	Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección
			Resoluciones	Información		
			Normograma	Información		
			Contractual	Información		
			Procedimientos	Información		
			Formatos	Información		
		Posible divulgación de información pública clasificada, modificación no autorizada de la información causando pérdida de integridad o suplantación de identidad e indisponibilidad para consultar oportunamente la información requerida	Actas de asambleas y junta directiva	Información	Ataques contra el sistema Penetración del sistema Acto fraudulento	Líneas de comunicación sin protección Tráfico sensible sin protección ausencia de terminación de sesión Falta de conciencia en seguridad Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección Ausencia de proceso para supervisión de derechos de acceso
			Actas de comité de contratación	Información		
11	SIG	Posible indisponibilidad para consultar oportunamente la información requerida y modificación no autorizada de la información del SIG	Caracterizaciones	Información	Ataques contra el sistema Penetración del sistema	Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección
			Procedimientos	Información		
			Flujogramas	Información		
			Manuales	Información		
			Guías	Información		
			Formatos	Información		
			Registros	Información		
			Mapas de riesgos	Información		
			Actas	Información		
12	SG-SST	Posible indisponibilidad para consultar oportunamente la información requerida y modificación no autorizada de la información del SG-SST	Programas	Información	Ataques contra el sistema Penetración del sistema	Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección
			Planes	Información		
			Normograma	Información		
			Formatos	Información		
			Informes	Información		
			Actas	Información		
			Cartas	Información		
			Formato	Información		
			Fichas tecnicas	Información		

NO.	PROCESO/ SUBPROCESO	RIESGO	ACTIVO	TIPO	AMENAZAS	VULNERABILIDADES
13	Gestión de sistemas de Información	Posible pérdida de elementos y activos propiedad de la ACI Medellín por motivos de corrupción	Listado de bienes que el subproceso ha asignado a los funcionarios o estan almacenados en bodega	Información	Acto fraudulento Ingeniería social Chantaje	Ausencia de mecanismos de identificación y autenticación de usuarios Falta de conciencia en seguridad
14	Gestión de sistemas de Información	Posible Incumplimiento de actividades definidas causando perdida de control de acceso y bienes	Los procedimientos son planes por medio de los cuales se establece un método para el manejo de actividades futuras. Consisten en secuencias de las acciones requeridas.	Información	Ingeniería social Acto fraudulento Chantaje	Falta de conciencia en seguridad Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección
15	Gestión de sistemas de Información	Posible Indisponibilidad de servicios de conectividad y comunicaciones	Servidor de Telefonía IP	Servidor	Acto fraudulento ataques contra el sistema Penetración del sistema Crimen por computador	Líneas de comunicación sin protección Tráfico sensible sin protección ausencia de terminación de sesión Falta de conciencia en seguridad
16	Gestión de sistemas de Información		Sistemas de alimentación ininterrumpida para racks de comunicaciones	Hardware		
17	Gestión de sistemas de Información	Posible Indisponibilidad de hardware de la entidad	Dispositivos de impresión y escaneo	Hardware	Ataques contra el sistema Crimen por computador	Ausencia de terminación de sesión Falta de conciencia en seguridad
18	Gestión de sistemas de Información	Posible modificación no autorizada de la información o por suplantación de identidad causando pérdida de integridad en la información del proceso	Estudios previos, contratos, actas de recibo a satisfacción y liquidación generados por el subproceso	Información	Hurto de información Chantaje Crimen por computador Ingeniería social	Líneas de comunicación sin protección Tráfico sensible sin protección ausencia de terminación de sesión Falta de conciencia en seguridad
19	Gestión de sistemas de Información	Posible Indisponibilidad para consultar oportunamente la información requerida y modificación no autorizada de la información y trazabilidad de activos	Contiene los formatos de herramienta de gestion de riesgo y contexto del subproceso	Información	Ingeniería social Pretexto Acto fraudulento Chantaje	Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección Ausencia de proceso para supervision de derechos de acceso Tráfico sensible sin protección
20	Gestión de sistemas de Información		Planes de control, funcionamiento y ejecución de actividades relacionadas con el subproceso de gestion de sistemas de información	Información		
21	Gestión de sistemas de Información		Formato de registro y control de entrega de bienes de la ACI Medellín	Información		

No.	PROCESO RESPONSABLE	RIESGO	ACTIVO	TIPO	AMENAZAS	VULNERABILIDADES
22	Gestión de sistemas de información	Posible indisponibilidad de sistemas de información o.a.i. pongan en riesgo la seguridad perimetral de la infraestructura tecnológica	Portal de administración y registro de servidores	Servicios	Daño físico Hurto de información Ingeniería social Ataques contra el sistema Penetración del sistema Crimen por computador Alta fluctuación Ingreso	Línea de comunicación sin protección Tráfico sensible sin protección Ausencia de terminación de sesión Falta de conocimiento seguridad Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección Ausencia de proceso para supervisión de derechos de acceso
23	Gestión de sistemas de información		Máquinas virtuales para gestión y control de políticas de seguridad, acceso a sistemas de información y distribución de roles	Software		
24	Gestión de sistemas de información		Dispositivos de hardware que permiten la interoperabilidad y accesibilidad a los sistemas de información	Componentes de red		
25	Gestión de sistemas de información		Portal de gestión y asignación de licencias de Office 365 y buzones y políticas de correo electrónico	Servicios		
26	Gestión de sistemas de información		mecanismo de copias de seguridad y recursos de maquinas virtuales y servidores	Servicios		
27	Gestión de sistemas de información		Software de gestión del subproceso de gestión documental	Servicios		
28	Gestión de sistemas de información		Dispositivos de control y registro de acceso a las instalaciones de la ACI Medellín	Hardware		
29	Gestión de sistemas de información		Portal de administración y gestión de contratos (Contract Relationship Management)	Servicios		
30	Gestión de sistemas de información		Portal de intranet de la entidad	Servicios		
31	Gestión de sistemas de información	Posible divulgación de información pública clasificada, modificación no autorizada de la información causando pérdida de integridad o suplantación de identidad	Disco de almacenamiento que contiene la información de todos los procesos y subprocesos de la ACI Medellín	Información	Hurto de información Ingeniería social Chantaje Crimen por computador	Ausencia de mecanismos de identificación y autenticación de usuarios Contraseñas sin protección Ausencia de proceso para supervisión de derechos de acceso Falta de conciencia en seguridad
32	Gestión de sistemas de información		Información recopilada de acuerdo con las bases de datos reportadas en la superintendencia de industria y comercio	Información		

9. CRONOGRAMA

Las actividades definidas en el presente cronograma responden directamente al tratamiento de los riesgos identificados en el mapa de riesgos de seguridad y privacidad de la información, y su ejecución será objeto de seguimiento para evaluar la efectividad de los controles implementados.

OBJETIVO ESTRATÉGICO - OE	OBJETIVOS ESPECÍFICOS	ACCIÓN ANUAL
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Establecer una guía que proporcione a la entidad lineamientos, estándares y estrategias claras para la adecuada planeación e implementación de proyectos y gestión de recursos tecnológicos; y que además ayude a fortalecer el uso de la infraestructura y los sistemas de información existentes.
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Minimizar y controlar los riesgos asociados a los sistemas de información y la infraestructura tecnológica que interviene en la administración y custodia de la información de la ACI Medellín, con el fin de protegerla como el mayor activo de la Agencia.
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Asegurar el uso adecuado de los sistemas de información y los recursos tecnológicos de la Agencia por parte de todos los funcionarios, contratistas y aprendices preservando, protegiendo y administrando de forma eficiente la información y los medios utilizados para su manipulación y procesamiento, con el fin de asegurar el cumplimiento de la integridad, confidencialidad y disponibilidad.

4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Implementar sistemas de automatización que reduzcan los tiempos operativos y minimicen los riesgos en la Agencia.	Revisar las fuentes de información del subproceso de gestión de sistemas de información (TRD, SharePoint, página web, normograma)
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Implementar sistemas de automatización que reduzcan los tiempos operativos y minimicen los riesgos en la Agencia.	Realizar los cambios que solicita el equipo de sistemas de información a la herramienta CRM incluyendo los informes requeridos
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Implementar sistemas de automatización que reduzcan los tiempos operativos y minimicen los riesgos en la Agencia.	Informes de uso del CRM mensuales
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Realizar la contratación y supervisión del CRM
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Realizar la contratación y supervisión de Power BI
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Continuar con el contrato y supervisión del Datacenter en Infraestructura como servicio (IaaS)

4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Realizar un verificación de los activos de la ACI Medellín que pueden ser dados de baja y se encuentran almacenados en el centro de datos
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Atender los requerimientos reportados por los usuarios en el portal Soporte Técnico
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Establecer y ejecutar políticas de seguridad en la consola de antivirus
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Mitigar de manera oportuna los incidentes que se puedan presentar en los servidores de la ACI Medellín
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Establecer y controlar reglas de acceso a páginas web y accesos de VPN
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Administrar el panel de control del dispositivo de acceso biométrico
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Revisión e instalación de hardware y software necesario en los equipos de cómputo de la ACI Medellín
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Administrar la conectividad a nivel de red interna y acceso a internet en las instalaciones de la ACI Medellín

4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Administrar la plataforma de Microsoft Office 365 E3, lo cual incluye la asignación y control de licencias, gestión de software de ofimática, correo electrónico y buzones compartidos.
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Gestionar y verificar adecuado funcionamiento de ADConect que actualiza políticas y usuarios entre el Tenant de Office 365 y el Directorio Activo
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Implementar sistemas de automatización que reduzcan los tiempos operativos y minimicen los riesgos en la Agencia.	Administrar y garantizar la conexión y disponibilidad del servidor que aloja el software AriesNET.
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Implementar sistemas de automatización que reduzcan los tiempos operativos y minimicen los riesgos en la Agencia.	Administrar, reestablecer y desbloquear los usuarios en los sistemas de información que tiene la ACI Medellín.
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Establecer y ejecutar cronograma de trabajo para realizar los mantenimientos a los equipos de computo
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Implementar sistemas de automatización que reduzcan los tiempos operativos y minimicen los riesgos en la Agencia.	Crear y asignar los usuarios y correos en los sistemas de información que tiene la ACI Medellín.
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Realizar la contratación y supervisión de la Suite Office 365 plan E3
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Realizar la contratación y supervisión de Adobe Creative Cloud

4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Realizar la contratación y supervisión del Hosting de la ACI Medellín
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Realizar la contratación y supervisión de Mantenimientos impresoras, escáneres, UPS´s y consumibles
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Realizar la contratación y supervisión del software de gestión documental Docuware
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Revisar al corte del 30 de noviembre las facturas y saldos pendientes de los contratos a cargo del subproceso.
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Reportar la información requerida por la Dirección Nacional de Derechos de Autor
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Fortalecer la infraestructura tecnológica de la Agencia mediante la adopción de herramientas digitales innovadoras que potencien la integración y el análisis de datos.	Reportar a la superintendencia de industria y comercio la actualización de las bases de datos de la ACI Medellín
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Implementar sistemas de automatización que reduzcan los tiempos operativos y minimicen los riesgos en la Agencia.	Elaborar y hacer seguimiento al Contexto del subproceso de Gestión de Tecnologías de información - DOFA
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Implementar sistemas de automatización que reduzcan los tiempos operativos y minimicen los riesgos en la Agencia.	Elaborar y hacer seguimiento al Mapa de riesgos del subproceso de Gestión de Tecnologías de información

4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Implementar sistemas de automatización que reduzcan los tiempos operativos y minimicen los riesgos en la Agencia.	Actualizar las funciones, actividades y el alcance del subproceso de gestión de recursos tecnológicos.
4. Aumentar la eficiencia y sinergia de los procesos de la Agencia implementando herramientas de mejora continua.	Implementar sistemas de automatización que reduzcan los tiempos operativos y minimicen los riesgos en la Agencia.	Fortalecer y darle continuidad y garantía al proyecto de teletrabajo en la ACI Medellín

10. ESTRATEGIAS.

La Agencia de Cooperación en Inversión de Medellín y el Area Metropolitana (ACI), con el fin de adoptar e implementar el Modelo de Seguridad y Privacidad de la Información (MPSI), enmarcado en el Sistema de Gestión de Seguridad de la información - SGSI, tiene como objeto proteger, preservar y administrar la confidencialidad, integridad y disponibilidad de la información, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales reduciendo la probabilidad de ocurrencia de incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, propendiendo así por el acceso, uso efectivo y apropiación masiva de las Tecnologías de la Información y las Comunicaciones- TIC.

Para lograr el cumplimiento del Plan se definen las siguientes estrategias:

1. Compromiso de la alta gerencia para promover, apoyar y financiar la realización de los proyectos asociados a gestionar los riesgos de seguridad de la información.

2. Integración de los riesgos de seguridad de la información al marco de gestión de riesgos de la ACI Medellín.

3. Gestionar los riesgos de seguridad y privacidad de la información, de manera integral.

4. Mitigar los impactos y reducir la ocurrencia de posibles incidentes de Seguridad y Privacidad de la Información, de forma efectiva, eficaz y eficiente.

5. Adopción de la cultura de seguridad de la información y compromiso de todos los servidores públicos / Contratista y grupos de interés de la ACI Medellín frente los riesgos de seguridad de la información y su tratamiento.

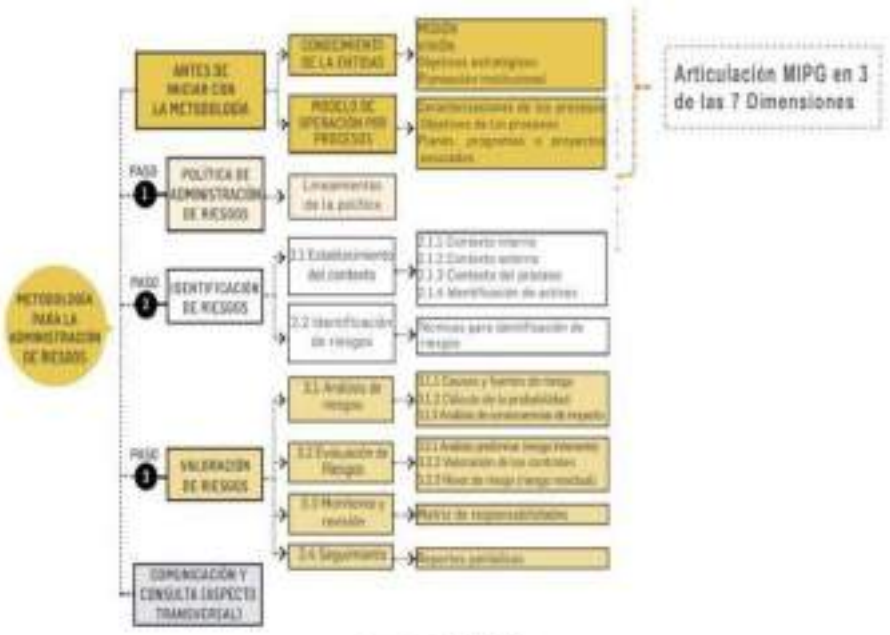
10.1 Etapas para la Gestión del Riesgo.

De acuerdo con la Guía de Gestión de Riesgos del DAFP – Departamento Administrativo de la Función Pública, las etapas generales para la gestión de riesgos adoptados por la ACI Medellín contemplan el compromiso de la dirección de la Entidad, el subproceso de gestión de Sistemas de Informacion encargado de la administración del modelo de gestión de riesgos y las capacitaciones de la metodología.

En lo que respecta a la seguridad de la información, se integrara a la gestión de riesgos adoptada por la ACI Medellín, la norma técnica NTC-ISO 27005:2009 Gestión de Riesgos en la Seguridad de la Información. Esta norma brinda soporte a los conceptos generales que se especifican en la norma NTC-ISO 27001:2013 y está diseñada para facilitar la implementación satisfactoria de la seguridad de la información con base en la gestión de Riesgos.

La guía Metodológica para la Administración del Riesgo del Departamento Administrativo de la función Pública es la carta de navegabilidad para la administración del Riesgo en las Entidades Publica, la cual actúa en concordancia con el componente de Administración del Riesgo establecido en el Manual Estándar de control Interno para el Estado Colombiano en la Identificación, Valoración, análisis y Seguimiento y Monitoreo de los mismo en una entidad.

Ilustración 1 Metodología para la Administración de Riesgos.



Fuente: DAFP (2020)

10.2 Visión general para la Administración del Riesgo.

En el marco de la implementación del Modelo de Seguridad y Privacidad de la Información MSPI, se establecer una serie de actividades relacionadas con la gestión del riesgo, las cuales se presentan a continuación.

ETAPAS DEL MSPI	PROCESO DE GESTION DEL RIESGO EN LA SEGURIDADDE LA INFORMACION
Planear	Establecer Contexto Valoración del Riesgo Planificación del Tratamiento del Riesgo Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgo
Gestionar	Monitoreo y Revisión Continuo de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

Fuente: Tomado de la Guia 7 – Gestión de Riesgos -MPSI - Mintic

10.3 Identificación de Riesgos.

De acuerdo con DAFP1 esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la organización, teniendo en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance, y el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos Es aquí donde se identifican los factores internos y externos que se han de tener en consideración para la administración del riesgo (NTC ISO31000, Numeral 2.9). Adicionalmente es requisito conocer los activos de cada proceso y realizar los análisis correspondientes frente los posibles riesgos. Amenazas y vulnerabilidades que los puedan afectar.

Fuente : Identificación de activos – DAFP1

Para el levantamiento de activos asociados a los procesos, nos apoyamos en la INSTRUMENTO DE EVALUACION MSPI que es un instrumento que permite identificar los activos de información y su tránsito a través de ciclo de vida del documento, desde su creación hasta la disposición final.

En concordancia con la metodología de riesgos adoptada por la Entidad, se incorporan los riesgos cuya tipología corresponde a “Riesgos de Seguridad Digital” conforme lo indica la guía del DAFP.

Los activos de información de acuerdo con su nivel de importancia respecto a los criterios de Confidencialidad, Integridad y Disponibilidad se clasifican en cinco

En concordancia con lo anterior, los activos de información también deben valorados y clasificados de acuerdo con su clasificación y deben estar alineados con las disposiciones legales vigentes. En la UNP existen diferentes tipos de información Altamente Confidencial (Reservada), Confidencial (Clasificada), Interna y pública, las cuales están alineados y homologados con los que define la Ley 1712 de transparencia y derecho de acceso a la información Pública. (Anexo-01- Riesgos de Seguridad de la información - Hoja VALORACIÓN).

La identificación correcta de las amenazas y vulnerabilidades es un aspecto clave del SGSI - Sistema de seguridad de la información dentro del proceso de evaluación de riesgos, razón por la cual van de la mano y deben ser consideradas en su conjunto. En este orden de ideas, se deben tomar como referencia las Amenazas y vulnerabilidades definidas en la norma NTCISO 27005, las cuales se incluyen en el presente plan.

Para la gestión de los riesgos, se tienen como documentos de referencias la norma NTC-ISO 27005, la guía de Gestión de Riesgos de DAFP y una matriz en Excel denominada Anexo-01- Riesgos de Seguridad de la Información la cual se establece como herramientas de consulta la diligenciar el instrumento de riesgos definido por la entidad.

11. INDICADORES.

Los indicadores del proceso hacen parte del seguimiento al cumplimiento de las actividades, este seguimiento se hace de manera mensual.

La medición se realiza con los indicadores de gestión que están orientados principalmente a disminuir el número de riesgos identificados con nivel alto y externo a través de la implementación y evaluación de controles.

EL subproceso de gestión de sistemas de información de la ACI Medellin lidera y ejecuta el proceso de identificación y valoración de los riesgos de seguridad de información y seguridad digital así mismo la planeación la inclusión de estos en el mapa de riesgos institucional, instrumento valoración y sus controles, en donde se registran los riesgos identificados para su seguimiento y control.

Así mismo el subproceso de gestión de sistemas de información de la ACI Medellin hará seguimiento a su implementación, con el fin, de evidenciar en el siguiente ciclo la efectividad de los controles implementados y en consecuencia la disminución del riesgo y en caso de llegar a presentar incidentes

de seguridad se validarán los riesgos identificados para determinar si obedece a un riesgo identificado y proceder a valorar recalificar e implementar nuevos controles.

El subproceso de gestión de Sistemas de Información cuenta con 5 indicadores:

11.1 Indicador Ejecución de copias de seguridad.

ASPECTOS GENERALES		
PROCESO/SUBPROCESO	**Gestión de Recursos Tecnológicos**	
NOMBRE DEL INDICADOR	**Porcentaje de ejecución de copias de seguridad**	
OBJETIVO DEL INDICADOR	**Evitar la pérdida o corrupción de la información**	
TIPO DE INDICADOR	**Cumplimiento**	
DEFINICIÓN OPERACIONAL		
NUMERADOR	Cantidad de copias exitosas	
DENOMINADOR	Cantidad de copias programadas	
UNIDAD DE MEDICIÓN	Porcentaje (%)	
INSTRUCCIÓN DE CÁLCULO	Cantidad de copias exitosas/Cantidad de copias programadas*100	
VARIABLES		
	Numerador	**Denominador**
ORIGEN DE LA INFORMACIÓN	Cantidad de copias exitosas	Cantidad de copias programadas
FUENTE PRIMARIA	Software Veritas Backup Exec	Software Veritas Backup Exec
FRECUENCIA DEL CÁLCULO Y REGISTRO	Mensual	
FRECUENCIA DE ANÁLISIS E INFORMES	Trimestral	
RESPONSABLE DEL CÁLCULO	Auxiliar administrativo de sistemas e informática	
VIGILANCIA Y CONTROL	Auxiliar administrativo de sistemas e informática y Dirección administrativa	
INTERPRETACIÓN		
0<i<49	**El indicador muestra que está lejos del cumplimiento de la meta.**	
50<i<84	**El indicador muestra que se está llegando a una situación crítica.**	
85<i<100	**El indicador muestra que se está cumpliendo la meta.**	
TENDENCIA DEL INDICADOR		

El indicador se debería comportar de manera estable

PERFIL DEL INDICADOR

Este indicador puede ser: Calculado, modificado y analizado por el Auxiliar administrativo de sistemas e informática según la cantidad de casos en relación con un tiempo determinado o cantidad de casos abiertos y cerrados según la frecuencia del indicador Consultado por Dirección de relaciones administrativas, Coordinador de Control interno y Profesional Senior calidad
Fecha de actualización del indicador: 15/10/2020

11.2 Indicador cumplimiento cronograma de contratación.

ASPECTOS GENERALES	
PROCESO/SUBPROCESO	**Gestión de recursos tecnológicos**
NOMBRE DEL INDICADOR	**Cumplimiento del cronograma de contratación del subproceso de GRT**
OBJETIVO DEL INDICADOR	Dar seguimiento al presupuesto para el control del riesgo de desactualización de la infraestructura tecnológica
TIPO DE INDICADOR	Seguimiento
DEFINICIÓN OPERACIONAL	
NUMERADOR	contratos en ejecución
DENOMINADOR	contratos planeados
UNIDAD DE MEDICIÓN	Unidades
INSTRUCCIÓN DE CÁLCULO	(contratos ejecución/contratos planeados) *100

VARIABLES		
	Numerador	**Denominador**
ORIGEN DE LA INFORMACIÓN	Cronograma de contrataciones de gestión jurídica	Cronograma de contrataciones de gestión jurídica
FUENTE PRIMARIA	Subproceso de gestión jurídica	Subproceso de gestión jurídica
FRECUENCIA DEL CÁLCULO Y REGISTRO	Mensual	
FRECUENCIA DE ANÁLISIS E INFORMES	Mensual	
RESPONSABLE DEL CÁLCULO	Auxiliar Administrativo sistemas e informática	
VIGILANCIA Y CONTROL	Profesional de Calidad - Coordinador de control interno - directora de Relaciones Administrativas	

INTERPRETACIÓN	
0%<i<50%	**El indicador muestra que está lejos del cumplimiento de la meta.**
51%<i<80%	**El indicador muestra que se está llegando a una situación crítica.**
81%<i<100%	**El indicador muestra que se está cumpliendo la meta.**

TENDENCIA DEL INDICADOR
El indicador tiene tendencia creciente

PERFIL DEL INDICADOR
Este indicador puede ser: Calculado, modificado y analizado por el Auxiliar Administrativo de Sistemas e informática Consultado por Profesional de Calidad - Coordinador de control interno - Directora de Relaciones Administrativas

11.3 Indicador mantenimientos preventivo.

ASPECTOS GENERALES		
PROCESO/SUBPROCESO	**Gestión de Recursos Tecnológicos**	
NOMBRE DEL INDICADOR	**Mantenimientos de equipos de computo**	
OBJETIVO DEL INDICADOR	**Medir el cumplimiento del indicador de mantenimiento**	
TIPO DE INDICADOR	**Cumplimiento**	
DEFINICIÓN OPERACIONAL		
NUMERADOR	Mantenimientos ejecutados	
DENOMINADOR	Mantenimientos programados	
UNIDAD DE MEDICIÓN	Porcentaje (%)	
INSTRUCCIÓN DE CÁLCULO	Mantenimientos ejecutados/Mantenimientos programados*100	
VARIABLES		
	Numerador	**Denominador**
ORIGEN DE LA INFORMACIÓN	Contrato de mantenimiento	Contrato de mantenimiento
FUENTE PRIMARIA	Actas de recibo a satisfacción	Actas de recibo a satisfacción
FRECUENCIA DEL CÁLCULO Y REGISTRO	Mensual	
FRECUENCIA DE ANÁLISIS E INFORMES	Semestral	
RESPONSABLE DEL CÁLCULO	Auxiliar administrativo de sistemas e informática	
VIGILANCIA Y CONTROL	Auxiliar administrativo de sistemas e informática y Dirección administrativa	
INTERPRETACIÓN		
0<i<49	**El indicador muestra que este lejos del cumplimiento de la meta.**	
50<i<99	**El indicador muestra que se está llegando a una situación crítica.**	
99<i<100	**El indicador muestra que se está cumpliendo la meta.**	

TENDENCIA DEL INDICADOR
El indicador no tiene tendencia dado que son actividades programadas periódicamente a demanda o consideración del Auxiliar administrativo de sistemas e informática.

PERFIL DEL INDICADOR

Este indicador puede ser:
Calculado, modificado y analizado por el Auxiliar administrativo de sistemas e informática según la cantidad de casos en relación con un tiempo determinado o cantidad de casos abiertos y cerrados según la frecuencia del indicador
Consultado por Dirección de relaciones administrativas, Coordinador de Control interno y Profesional Senior calidad

11.4 Indicador Promedio del puntaje obtenido del formato FR-GRT-02 Formato control políticas.

ASPECTOS GENERALES	
PROCESO/SUBPROCESO	**Gestión de Recursos Tecnológicos**
NOMBRE DEL INDICADOR	**Promedio del puntaje obtenido del formato FR-GRT-02 Formato control políticas**
OBJETIVO DEL INDICADOR	**Controlar el riesgo de incorporación de códigos maliciosos, intervención no autorizada a las bases de datos, ingenieria social, cibercrimen y vulnerabilidad de los sistemas**
TIPO DE INDICADOR	**Cumplimiento**

DEFINICIÓN OPERACIONAL	
NUMERADOR	Evaluaciones realizadas del formato FR-GRT-02
DENOMINADOR	Evaluaciones aprobadas
UNIDAD DE MEDICIÓN	Porcentaje (%)
INSTRUCCIÓN DE CÁLCULO	(puntaje de evaluaciones realizadas/total de evaluaciones realizadas) *100

VARIABLES		
	Numerador	**Denominador**
ORIGEN DE LA INFORMACIÓN	Evaluaciones realizadas del formato FR-GRT-02	Evaluaciones aprobadas
FUENTE PRIMARIA	Evaluaciones realizadas por el Subproceso GRT	Evaluaciones realizadas por el Subproceso GRT
FRECUENCIA DEL CÁLCULO Y REGISTRO	Al ingreso del personal nuevo. Reinducciones	
FRECUENCIA DE ANÁLISIS E INFORMES	Semestral	
RESPONSABLE DEL CÁLCULO	Auxiliar administrativo de sistemas e informática	
VIGILANCIA Y CONTROL	Auxiliar administrativo de sistemas e informática y Dirección administrativa	

INTERPRETACIÓN	
0<i<49	**El indicador muestra que está lejos del cumplimiento de la meta.**
50<i<80	**El indicador muestra que se está llegando a una situación crítica.**
81<i<100	**El indicador muestra que se está cumpliendo la meta.**

TENDENCIA DEL INDICADOR

El indicador no tiene tendencia dado que son actividades programadas periódicamente a demanda o consideración del Auxiliar administrativo de sistemas e informática.

PERFIL DEL INDICADOR
Este indicador puede ser: Calculado, modificado y analizado por el Auxiliar administrativo de sistemas e informática según la cantidad de casos en relación con un tiempo determinado o cantidad de casos abiertos y cerrados según la frecuencia del indicador Consultado por Dirección de relaciones administrativas, Coordinador de Control interno y Profesional Senior calidad

11.5 Indicador soporte técnico a usuarios.

ASPECTOS GENERALES		
PROCESO/SUBPROCESO	**Gestión de Recursos Tecnológicos**	
NOMBRE DEL INDICADOR	**Soporte técnico a usuarios**	
OBJETIVO DEL INDICADOR	**Medir la oportunidad de respuesta**	
TIPO DE INDICADOR	**Eficacia**	
DEFINICIÓN OPERACIONAL		
NUMERADOR	Casos cerrados	
DENOMINADOR	Casos creados	
UNIDAD DE MEDICIÓN	Porcentaje (%)	
INSTRUCCIÓN DE CÁLCULO	Casos cerrados/Creados*100	
VARIABLES		
	Numerador	**Denominador**
ORIGEN DE LA INFORMACIÓN	Portal soporte	Portal soporte
FUENTE PRIMARIA	Casos	Casos
FRECUENCIA DEL CÁLCULO Y REGISTRO	Mensual	
FRECUENCIA DE ANÁLISIS E INFORMES	Trimestral	
RESPONSABLE DEL CÁLCULO	Auxiliar administrativo de sistemas e informática	
VIGILANCIA Y CONTROL	Auxiliar administrativo de sistemas e informática y Dirección administrativa	
INTERPRETACIÓN		
0<i<60	**El indicador muestra que está lejos del cumplimiento de la meta.**	
61<i<80	**El indicador muestra que se está llegando a una situación crítica.**	
81<i<100	**El indicador muestra que se está cumpliendo la meta.**	
TENDENCIA DEL INDICADOR		

El indicador no tiene tendencia marcada debido a que su variación es a demanda de los funcionarios o cantidad de cargos ocupados.

PERFIL DEL INDICADOR

Este indicador puede ser:
Calculado, modificado y analizado por el técnico de sistemas de la información según la cantidad de casos en relación con un tiempo determinado o cantidad de casos abiertos y cerrados según la frecuencia del indicador
Consultado por Dirección de relaciones administrativas, Coordinador de Control interno y Profesional senior calidad

12. AREAS COMPROMETIDAS CON LA SEGURIDAD RESPONSABILIDAD

- Control Interno / Gestión del Riesgo: identificación, seguimiento y evaluación de riesgos.
- Jurídica / Cumplimiento: verificación normativa y legal.
- Áreas misionales y de apoyo: identificación de riesgos en sus procesos.
- Area TI: implementación de controles técnicos y monitoreo.
- Alta Dirección: aprobación y seguimiento.

13. RESUMEN DE CAMBIOS

FECHA	CAMBIO	VERSIÓN
2018/07/17	Se crea el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	01
2019/01/30	Se hizo revisión de todo el documento para ajustar el plan operativo	02
2020/01/16	Se realiza una revisión de todo el documento y se alinea al plan operativo	03
2021/01/30	Se realiza una revisión de todo el documento y se alinea al plan operativo	04
27/01/2022	Se realiza una revisión de todo el documento y se alinea al plan operativo	05
02/01/2023	Se realiza una revisión de todo el documento se alinea al plan operativo y se incluyen según guías de MINTIC las estrategias - los indicadores y los conceptos básicos.	06
12/01/2024	Se realiza una revisión de todo el documento, se ajusta la introducción asociada a los cambios en el plan para el 2024, se ajusta el objetivo general de acuerdo con la guía Minitic 2024. Se actualiza cronograma acorde al plan operativo para el 2024.	07
27/01/2025	Se hizo revisión de todo el documento, y se hacen ajustes al plan operativo	08
05/01/2026	Se hizo revisión de todo el documento, y se hacen ajustes al plan operativo y Se actualiza el Plan de Tratamiento de Riesgos incorporando enfoque de SGSI, amenazas emergentes, fortalecimiento de la metodología de gestión del riesgo, mejora continua y alineación con ISO/IEC 27001, ISO/IEC 27005, MSPI MinTIC y lineamientos de la SIC	09

14. RESPONSABILIDAD Y AUTORIDAD

Elaboró / Actualizó:	Revisó / Aprobó:
Nombre: Javier Esteban Botero Cargo: Técnico de Sistemas de Información	Nombre: Verónica Pupiales Giraldo Cargo: Directora de Relaciones Administrativas