SISTEMA DE GESTION DE TECNOLOGÍAS DE LA INFORMACIÓN

1. DEFINICIÓN DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Para la Contraloría Departamental del Valle del Cauca, la seguridad de la información se fundamenta en garantizar la confidencialidad, integridad y disponibilidad de la información, estableciendo los controles suficientes que permitan cumplir plenamente la función establecida por la Constitución Política de Colombia encaminada a la inspección, la vigilancia y el control fiscal de los recursos públicos de la Nación.

La nuestra política institucional está orientada a brindar confianza a la ciudadanía, en que se está cumpliendo a cabalidad con los procesos definidos para que los recursos públicos efectúen la función asignada y de esta forma se logre el bienestar de la población en general y el desarrollo del país. Sobre esta base, la imagen de la CDVC y el buen desarrollo de los procesos internos dependen, en buena medida, de la Confidencialidad, Integridad y Disponibilidad de la información.

Para la CDVC, la seguridad de la información se debe reflejar en:

• La confidencialidad de la información, hasta que la información pasa a ser de dominio público.

• La Integridad de los datos registrados en actuaciones de los funcionarios, para que respalden a plenitud los procesos de control fiscal.

• La solidez en los sistemas de información, para que los datos solamente puedan ser accedidos y modificados por los funcionarios autorizados.

• El cumplimiento de la legislación, teniendo como base la Constitución Política de Colombia.

OBJETIVO GENERAL

Establecer los lineamientos de seguridad de la información que permitan garantizar la protección de los datos personales y los activos de información con que cuenta la Entidad.

OBJETIVOS ESPECIFICOS

1. Definir un modelo de seguridad de la información que permita minimizar el impacto en el negocio debido a la explotación de las vulnerabilidades asociadas a los activos de información.

2. Documentar y aplicar los controles y procedimientos necesarios para salvaguardar la integridad, confidencialidad y disponibilidad de los activos de información.

3. Cumplir con los lineamientos establecidos por el Gobierno Nacional y su estrategia "Prosperidad para Todos".

POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN

Considerando que la CDVC utiliza para el logro de los objetivos misionales recurso humano y tecnológico (representado en hardware, software, comunicaciones y servicios), instalaciones e información electrónica y/o física; se determinan las siguientes políticas de la seguridad que regirán a la CDVC para cumplir con los principios de confidencialidad, integridad y disponibilidad de los activos de información, así como la continuidad de los servicios que brinda la Entidad a la Nación.

1. Inventario de Activos de Información: En cabeza de la Subdirección Técnica de Informática recae la responsabilidad de definir el inventario, propiedad y responsables de los activos de información y las demás que se establezcan por parte de la Alta Dirección.

2. Gestión de activos de información: Todos los responsables de la información deben realizar la clasificación de los activos que tengan bajo su responsabilidad, de igual manera están obligados a administrar y dar uso adecuado a los mismos, teniendo en cuenta los lineamientos establecidos por la Alta Dirección.

3. Gestión de la seguridad: Como herramienta proactiva para la detección de situaciones que puedan afectar la seguridad de la información, se debe realizar el análisis de riesgos de los activos de información con una periodicidad semestral. Los resultados deben escalarse al Comité Directivo, para elaborar el plan de mitigación del riesgo que propenda por el mejoramiento continuo del sistema de seguridad de la información.

4. Uso aceptable de los recursos informáticos: Todos los funcionarios de la CDVC deben hacer uso racional de los recursos tecnológicos que les fueron asignados, asimilando que son de propósito específico para desarrollar actividades exclusivamente institucionales.

5. Seguridad física: Todos los funcionarios de la CDVC deben cumplir con los controles y procedimientos establecidos por la Entidad para el acceso a las diferentes áreas y dependencias de la CDVC.

6. Gestión de incidentes: Todos los funcionarios de la CDVC están obligados a reportar los eventos o sucesos que puedan ser incidentes de seguridad de la Información, teniendo en cuenta los lineamientos, guías y procedimientos definidos por la Entidad.

7. Detección proactiva: La CDVC implementará los mecanismos de detección requeridos para poder identificar violaciones a las políticas, normas, procedimientos y guías de seguridad de la información definidas al interior de la Entidad.

8. Cambios en la plataforma de TICs: Las decisiones que afecten los sistemas de información, como son cambios de plataforma, actualizaciones y migraciones, entre otros, deben contar con la aprobación de la Subdirección Técnica de Informática.

2. INVENTARIO DE ACTIVOS DE INFORMACIÓN

Inventario Equipos 2017						
DEPENDENCIA	**EQUIPO PC**	**PORTATILES**	**IMPRESORAS**	**ZEBRAS**	**ESCANER**	**Ptos Red**
Subdirección Técnica de Informática	4	2	1			
Sala de Servidores	4					
Oficina Asesora Jurídica	6		1		1	
Oficina de Control Disciplinario Interno	1	1	1			
Subdirección Admon Prestaciones y Nomina	3	1	1		0	
Dirección Oper Participación y Comunicaciones	6	2	1			
Prensa y Comunicaciones	2	1	1			
Subcontralora	1	1	1			
Despacho	1	2	2		1	
Cacci	3		1	2	2	
Tesorería	2	1	1		1	
Oficina de Control Interno	4		1			
Almacen	1		1	1		
Subdirección Admon Recursos Financieros	3		3			
Dirección Admon de Gestión Humana	3	2	2		1	
Procesos Sancionatorio	1				1	
Oficina Asesora de Planeación	3		1		1	
Subdirección Admon Personal y Carrera	2					
Subdirección Operativa Escuela de Capacitación	1					
Subdirección Operativa Sector Central	5	2	1			
Dirección Operativa de Control Fiscal	4	1	1		1	
Secretaria General - Incluye archivo	7		2		1	
Dirección Técnica de Infraestructura	5	1	1			
Subdirección Operativa Patrimonial	9		1			
Dirección Técnica de Recursos Naturales	6	1	1		1	
Subdirección Operativa Sector Descentralizado	2	2	1			
Subdirección Operativa de Coactiva	6		1			
Subdirección Operativa de Investigaciones	13		1		1	
Dirección Operativa de Responsabilidad Fiscal	2		1			
Sala de Audiencias	2					
Cercofis Cali	4	3	1		0	
Subtotal Cali	116	23	31	3	12	

Cercofis Tuluá	5	2	1	1	1	
Cercofis Palmira	4	4	1	1	1	
Cercofis Cartago	4	4	1	1	1	
Subtotal Cercofis	13	10	3	3	3	
TOTAL	**129**	**33**	**34**	**6**	**15**	
TOTAL GENERAL EQUIPOS (ESCRITORIO + PORTAT)	**162**					

Equipos en Comodato

Banco Occidente(2 PCS)	DELL S/N 948693	DELL S/N 929345
Bancolombia	S/N 20644428710	DELL Modelo D09U

Inventario Licencias

DETALLE	ESCRITORIO	PORTATILES	TOTAL
Microsoft Office Professional 2007	2	9	11
Microsoft Office XP Profesional 2003	8	0	8
Microsoft Office Home and Business 2010	72	15	87
TOTAL Microsoft OFFICE	**82**	**24**	**106**
Microsoft windows xp cercofis	13	8	**21**
Microsoft Windows XP Profesional	38	0	38
Microsoft Windows 7	61	16	77
Microsoft Windows 8	0	8	8
TOTAL WINDOWS	**99**	**24**	**123**
Antivirus NOD32	150	24	174
Oracle 9i	3	0	3
Linux Suse 9	2	0	2
TOTAL			**408**

Inventario de Software Interno y Externo

NUM.	DETALLE	PROCESOS / DEPENDENCIA	OBSERVACIÓN	DESARROLLO
1	SYSMAN (Presupuesto, Contabilidad, Nomina, Contratación, Gestión Documental, Indicadores, Almacen)	Recursos Financieros, Tesorería, Jurídica, Nomina, Gestión Documental, Planeación	Correcto funcionamiento	EXTERNO
2	RCL (Rendición de Cuentas en Línea)	Control Fiscal	Correcto funcionamiento	EXTERNO
3	Quejas y Denuncias	Comunicaciones y Participación	Correcto funcionamiento	INTERNO
4	Procesos de Responsabilidad Fiscal y Cobros coactivos	Responsabilidad Fiscal y Cobros coactivos	En proceso de desarrollo - Pruebas Piloto	INTERNO
5	Procesos Sancionatorios	Secretaria General / Control Fiscal	Correcto funcionamiento	INTERNO
6	Derechos de Petición	Secretaria General	Correcto funcionamiento	INTERNO
7	Observatorio	Control Fiscal	Correcto funcionamiento	INTERNO
8	Recursos Informáticos	Soporte Subdirección Técnica de Informática	Correcto funcionamiento	INTERNO

3. ANÁLISIS DEL RIESGO

El objetivo del análisis es el de establecer una valoración y priorización de los riesgos con base en la información ofrecida por los mapas elaborados en la etapa de identificación, con el fin de clasificar los riesgos y proveer información para establecer el nivel de riesgo y las acciones que se van a implementar. El análisis del riesgo dependerá de la información sobre el mismo, de su origen y la disponibilidad de los datos. Para adelantarlo es necesario diseñar escalas que pueden ser cuantitativas o cualitativas o una combinación de las dos.

Se han establecido dos aspectos para realizar el análisis de los riesgos identificados:

Probabilidad: la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia o teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya presentado nunca.

Impacto: consecuencias que puede ocasionar a la entidad la materialización del riesgo en caso de sucederse.

A continuación se presentan algunos ejemplos de las escalas que pueden implementarse para analizar los riesgos.

Análisis cualitativo: se refiere a la utilización de formas descriptivas para presentar la magnitud de consecuencias potenciales y la posibilidad de ocurrencia. Se diseñan escalas ajustadas a las circunstancias de acuerdo a las necesidades particulares o el concepto particular del riesgo evaluado.

Escala de medida cualitativa de PROBABILIDAD: se deben establecer las categorías a utilizar y la descripción de cada una de ellas, con el fin de que cada persona que aplique la escala mida a través de ella los mismos ítems, por ejemplo:

ALTA: es muy factible que el hecho se presente.
MEDIA: es factible que el hecho se presente.
BAJA: es muy poco factible que el hecho se presente.

Ese mismo diseño puede aplicarse para la escala de medida cualitativa de IMPACTO, estableciendo las categorías y la descripción, por ejemplo:

ALTO: Si el hecho llegara a presentarse, tendría alto impacto o efecto sobre la entidad.
MEDIO: Si el hecho llegara a presentarse tendría medio impacto o efecto en la entidad.
BAJO: Si el hecho llegara a presentarse tendría bajo impacto o efecto en la entidad.

Análisis cuantitativo: este análisis contempla valores numéricos; la calidad depende de lo exactas y completas que estén las cifras utilizadas. Básicamente se refiere a la construcción de indicadores que reflejen tanto la probabilidad de ocurrencia como el impacto que pueden causar. La forma en la cual la probabilidad y el impacto son expresados y las formas por las cuales ellos se combinan para proveer el nivel de riesgo puede variar de acuerdo al tipo de riesgo.

Con base en los ejemplos anteriormente expuestos, la Subdirección técnica de Informática es la encargada de establecer la metodología dentro de la cual se establecerán las probabilidades y los impactos a cada uno de los riesgos y la escala de valoración.

- **Priorización de los riesgos**

Una vez realizado el análisis de los riesgos con base en los aspectos de probabilidad e impacto, se recomienda utilizar la matriz de priorización que permite determinar cuáles requieren de un tratamiento inmediato.

Esta matriz se realiza en primera instancia al interior de cada una de las dependencias los resultados que de aquí se deriven servirán para socializarlos con el comité de mapa de riesgos.

Para su medición, se desarrollaron las siguientes escalas:

ALTA: es muy factible que el hecho se presente.

MEDIA: es factible que el hecho se presente.

BAJA: es muy poco factible que el hecho se presente.

IMPACTO: Son las consecuencias internas y externas que pueden ocasionar a la CDVC la materialización del evento adverso, afectando el logro de los objetivos propuestos.

Las escalas de medición del impacto del evento adverso son las siguientes:

ALTO: Si el hecho llegara a presentarse, tendría alto impacto o efecto sobre la entidad.

MEDIO: Si el hecho llegara a presentarse tendría medio impacto o efecto en la entidad.

BAJO: Si el hecho llegara a presentarse tendría bajo impacto o efecto en la entidad.

Contraloría Departamental del Valle del Cauca
Por un Valle mejor, control participativo en acción

Identificación de Riesgos

No.	PROCESO	RIESGO INTERNO	RIESGO EXTERNO	DESCRIPCION	CAUSAS	POSIBLES CONSECUENCIAS
1	GESTION DE INFRAESTRUCTURA	Plataforma tecnológica no satisface las necesidades de la entidad.	La infraestructura y/o plataforma tecnológica de la entidad no cuenta con los requerimientos necesarios para satisfacer las necesidades de la entidad o se encuentra desactualizada.	No se presentan proyectos para desarrollo y renovación de la plataforma tecnológica.	Atraso tecnológico de la entidad.	Renovación tecnológica descrita en el Plan de Inversión anual.
					Desgaste administrativo por gestión deficiente.	Proyectos de adquisición de tecnología.
				Falta de presupuesto y recursos escasos.	Inconformidad de los usuarios.	
					Lentitud en procesamiento de información.	Destinación presupuestal para la adquisición de tecnología.
2		Mantenimiento preventivo y correctivo de la plataforma tecnológica no se realiza.	Las tareas o actividades de mantenimiento preventivo, correctivo e inclusive predictivo, no se realizan en los diferentes equipos de sistemas que componen la plataforma tecnológica de la entidad.	Falta de personal disponible y capacitado en estas labores.	Número elevado de equipos dañados.	Cronograma de mantenimientos preventivos.
					Pérdidas económicas.	

				No existe disponibilidad de dispositivos para reemplazar.	Inconformidad de los usuarios.	Hojas de vida de equipos.
				Falta celebración de contratos para realizar las labores de mantenimiento.	Crecimiento exponencial de solicitud de soportes técnicos.	Formato de soporte técnico.
3		Fallas en el Hardware y Software de la entidad.	Defectos en los componentes, dispositivos y/o accesorios físicos, o de Sistema Operativo, programas y aplicativos de informática que impiden el correcto funcionamiento.	Falta de mantenimiento de la infraestructura de hardware y software.	Crecimiento exponencial de solicitud de soportes técnicos.	Mantenimientos preventivos y correctivos con límite de tiempo.
				Falta de coordinación y seguimiento entre los encargados de revisar el estado del hardware y software y su actualización.		
				Accidentes que dañan los equipos: sobrecargas eléctricas, caídas, mal manejo de los componentes.	Pérdida de información.	Help Desk para todos los usuarios informáticos.
					Inconformidad de los	Plan de suministro de

				Falta de divulgación y aplicación de las políticas del uso de los equipos de cómputo.	usuarios.	repuestos bajo demanda.
				Falta de capacitación del personal en el uso de los aplicativos y los equipos.	Retraso en la ejecución de las actividades de la entidad.	Garantías para los contratos de suministro de tecnología.
4		Ataques de Virus informático.	Daños o ataques a los sistemas informáticos ocasionados por programas elaborados intencionadamente por terceros.	Falta de controles en el acceso a páginas no autorizadas de internet.	Perdida de información.	Antivirus instalado y actualizado periódicamente en todos los equipos.
					Daños en el hardware y/o software.	Implementación de políticas de comunicaciones y navegación en Internet.
				Programas de antivirus no instalados o actualizados en los equipos.	Mal funcionamiento y lentitud en el procesamiento de datos a través de la red.	Activación de Firewall en la red.
						Definición de perfiles de navegación en Internet.

Identificación de Riesgos

No.	PROCESO	RIESGO INTERNO	RIESGO EXTERNO	DESCRIPCION	CAUSAS	POSIBLES CONSECUENCIAS	PROBABILIDAD	IMPACTO	NIVEL	RESPONSABLES	INDICADOR
1	GESTION DE INFRAESTRUCTURA	Plataforma tecnológica no satisface las necesidades de la entidad.	La infraestructura y/o plataforma tecnológica de la entidad no cuenta con los requerimientos necesarios para satisfacer las necesidades de la entidad o se encuentra desactualizada.	No se presentan proyectos para desarrollo y renovación de la plataforma tecnológica.	Atraso tecnológico de la entidad.	Renovación tecnológica descrita en el Plan de Inversión anual.	Baja	Alto	3	Subdirección Técnica de Informática.	Número de proyectos de desarrollo y/o renovación de la plataforma tecnológica Realizados / Número de proyectos de desarrollo y/o renovación de la plataforma tecnológica programados.
					Desgaste administrativo por gestión deficiente.						
				Falta de presupuesto y recursos escasos.	Inconformidad de los usuarios.	Proyectos de adquisición de tecnología.					
					Lentitud en procesamiento de información.	Destinación presupuestal para la adquisición de tecnología.					

2		Mantenimiento preventivo y correctivo de la plataforma tecnológica no se realiza.	Las tareas o actividades de mantenimiento preventivo, correctivo e inclusive predictivo, no se realizan en los diferentes equipos de sistemas que componen la plataforma tecnológica de la entidad.	Falta de personal disponible y capacitado en estas labores.	Número elevado de equipos dañados.	Cronograma de mantenimientos preventivos.	Baja	Alto	3	Subdirección Técnica de Informática.	Número de mantenimientos de la plataforma tecnológica Realizados / Número de mantenimientos de la plataforma tecnológica programados.
					Pérdidas económicas.						
				No existe disponibilidad de dispositivos para reemplazar.	Inconformidad de los usuarios.	Hojas de vida de equipos.					
				Falta celebración de contratos para realizar las labores de mantenimiento.	Crecimiento exponencial de solicitud de soportes técnicos.	Formato de soporte técnico.					

3		Fallas en el Hardware y Software de la entidad.	Defectos en los componentes, dispositivos y/o accesorios físicos, o de Sistema Operativo, programas y aplicativos de informática que impiden el correcto funcionamiento.	Falta de mantenimiento de la infraestructura de hardware y software.	Crecimiento exponencial de solicitud de soportes técnicos.	Mantenimientos preventivos y correctivos con límite de tiempo	Media	Medio	4	Subdirección Técnica de Informática.	Número de fallas en la plataforma tecnológica Ocurridas / Número de fallas en la plataforma tecnológica proyectadas.
				Falta de coordinación y seguimiento entre los encargados de revisar el estado del hardware y software y su actualización.							
				Accidentes que dañan los equipos: sobrecargas eléctricas, caídas, mal manejo de los componentes.	Pérdida de información.	Help Desk para todos los usuarios informáticos.					
					Inconformidad de los	Plan de suministro de					

				Falta de divulgación y aplicación de las políticas del uso de los equipos de cómputo.	usuarios.	repuestos bajo demanda.					
				Falta de capacitación del personal en el uso de los aplicativos y los equipos.	Retraso en la ejecución de las actividades de la entidad.	Garantías para los contratos de suministro de tecnología.					
4		Ataques de Virus informático.	Daños o ataques a los sistemas informáticos ocasionados por programas elaborados intencionadamente por terceros.	Falta de controles en el acceso a páginas no autorizadas de internet.	Perdida de información.	Antivirus instalado y actualizado periódicamente en todos los equipos.	Baja	Medio	2	Subdirección Técnica de Informática.	Número de ataques por virus informáticos Controlados / Número de ataques por virus informáticos
					Daños en el hardware y/o software.	Implementación de políticas de comunicaciones y navegación en Internet.					

				Programas de antivirus no instalados o actualizados en los equipos.	Mal funcionamiento y lentitud en el procesamiento de datos a través de la red.	Activación de Firewall en la red. Definición de perfiles de navegación en Internet.				Todas las Dependencias.	detectados.

4. CONTROLES A IMPLEMENTAR

Evaluación Del Riesgo

Para realizar la evolución del riesgo se debe tener en cuenta la posición del riesgo en la matriz, aplicando los siguientes criterios:

Riesgo inaceptable: Requiere acciones inmediatas

Riesgo aceptable: El riesgo se encuentra en un nivel que se puede aceptar, sin necesidad de tomar otras medidas de control diferentes a las que se poseen.

Si el riesgo se sitúa en cualquiera de las otras zonas (**Riesgo tolerable, moderado o importante**) se deben tomar medidas para llevar los riesgos a la zona Aceptable o Tolerable en lo posible.

- **Determinación del nivel del riesgo**

La determinación del nivel de riesgo es el resultado de confrontar el impacto y la probabilidad con los controles existentes al interior de los diferentes procesos y procedimientos que se realizan. Para adelantar esta etapa se deben tener muy claros los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos de tomar decisiones, estos niveles de riesgo pueden ser:

De la matriz de priorización, debe resultar el orden sistemático de los riesgos, enumerados de mayor a menor de acuerdo a su probabilidad vs. impacto.

Ahora se deben determinar los controles que existen en la institución para la eliminación o disminución del riesgo. De donde se puede obtener que:

- **Manejo del riesgo**

Cualquier esfuerzo que emprenda la entidad en torno a la valoración del riesgo llega a ser en vano, si no culmina en un adecuado manejo y control de los mismos definiendo acciones factibles y efectivas, tales como la implantación de políticas, estándares, procedimientos y cambios físicos entre otros, que hagan parte de un plan de manejo.

Para el manejo del riesgo se pueden tener en cuenta alguna de las siguientes opciones, las cuales pueden considerarse cada una de ellas independientemente, interrelacionadas o en conjunto.

Evitar el riesgo: es siempre la primera alternativa a considerar. Se logra cuando al interior de los procesos se genera cambios sustanciales de mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Un ejemplo de esto puede ser el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.

Reducir el riesgo: si el riesgo no puede ser evitado porque crea grandes dificultades operacionales, el siguiente paso es reducirlo al más bajo nivel posible. La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles. Ejemplo: Planes de contingencia.

Dispersar y atomizar el riesgo: Se logra mediante la distribución o localización del riesgo en diversos lugares. Es así como por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.

Transferir el riesgo: Hace referencia a buscar respaldo y compartir con otro parte del riesgo como por ejemplo tomar pólizas de seguros; se traslada el riesgo a otra parte o físicamente se traslada a otro lugar. Esta técnica es usada para eliminar el riesgo de un lugar y pasarlo a otro o de un grupo a otro. Así mismo, el riesgo puede ser minimizado compartiéndolo con otro grupo o dependencia.

Asumir el riesgo: Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el dueño del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

Una vez establecidos cuales de los anteriores manejos del riesgo se van a concretar, estos deben evaluarse con relación al beneficio-costo para definir, cuales son susceptibles de ser aplicadas y proceder a elaborar el plan de manejo de riesgo, teniendo en cuenta, el análisis elaborado para cada uno de los riesgos de acuerdo con su impacto, probabilidad y nivel de riesgo.

Posteriormente se definen los **responsables** de llevar a cabo las acciones especificando el grado de participación de las dependencias en el desarrollo de cada una de ellas. Así mismo, es importante construir indicadores, entendidos como los elementos que permiten determinar de forma práctica el comportamiento de las variables de riesgo, que van a permitir medir el impacto de las acciones.

5. PLAN DE TRATAMIENTO DEL RIESGO

Para elaborar el plan de manejo de riesgos es necesario tener en cuenta si las acciones propuestas reducen la materialización del riesgo y hacer una evaluación jurídica, técnica,

institucional, financiera y económica, es decir considerar la viabilidad de su adopción. La selección de las acciones más convenientes para la entidad se puede realizar con base en los siguientes factores:

- Nivel del riesgo
- Balance entre el costo de la implementación de cada acción contra el beneficio de la misma.

Una vez realizada la selección de las acciones más convenientes se debe proceder a la preparación e implementación del plan, identificando responsabilidades, programas, resultados esperados, medidas para verificar el cumplimiento y las características del monitoreo. El éxito de la implementación del plan requiere de un sistema gerencial efectivo el cual tenga claro el método que se va a aplicar.

- **Elaboración del mapa de riesgos**

El mapa de riesgos puede ser entendido como la representación o descripción de los distintos aspectos tenidos en cuenta en la valoración de los riesgos que permite visualizar todo el proceso de la valoración del riesgo y el plan de manejo de estos. El mapa de riesgos debe contener las situaciones adversas que pueden afectar el plan estratégico institucional identificando y definiendo los riesgos internos y externos que afecten su normal desarrollo, por cuanto el plan estratégico señala el camino que la entidad orientara en el cuatrienio en desarrollo de su misión.

- **Monitoreo**

Una vez diseñado y validado el plan para administrar los riesgos, es necesario monitorearlo permanentemente teniendo en cuenta que estos nunca dejan de representar una amenaza para la organización, el monitoreo es esencial para asegurar que dichos planes permanecen vigentes y que las acciones están siendo efectivas. Evaluando la eficiencia en la implementación y desarrollo de las acciones de control, es esencial adelantar revisiones sobre la marcha del plan de manejo de riesgos para evidenciar todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones preventivas.

El monitoreo debe estar a cargo de la Subdirección Técnica de Informática y la Oficina de Control Interno y su finalidad principal será la de aplicar los correctivos y ajustes necesarios para asegurar un efectivo manejo del riesgo. La Subdirección Técnica de Informática y la Oficina de Control Interno dentro de su función determinarán conjuntamente con las diferentes dependencias los aspectos que se encuentran débiles en cuanto al manejo de los riesgos y hará sugerencias para el mejoramiento y tratamiento de los riesgos detectados.

- **Autoevaluación**

La evaluación del plan de manejo de riesgos se debe realizar con base en los indicadores de gestión diseñados para tal fin y los resultados de los monitoreos aplicados en diferentes períodos. Así mismo, se evaluará como ha sido el comportamiento del riesgo y de qué manera a través del tiempo se van presentado nuevos riesgos que deban ser administrados.