



CIG.13.31.01 - 00163

Armenia, 9 de mayo de 2022

Doctor:

JHON MARIO LIEVANO FERNADEZ

Secretario de las Tecnologías de la Información y la Comunicación

Gobernación del Quindío

La Ciudad

ASUNTO: Remisión de Informe Mapa de Riesgos Institucionales, correspondiente al segundo semestre de la vigencia 2021.

Cordial saludo

De manera respetuosa me permito remitir el Informe Mapa de Riesgos Institucionales de la Secretaría TIC, correspondiente al segundo semestre de la vigencia 2021, en la que se mide el grado de avance para alcanzar la eficiencia y/o eficacia de dichos indicadores. Este seguimiento se ejecutó a través de la revisión de las evidencias suministradas por la dependencia a su cargo.

Del mismo modo se informa que la Oficina Privada, dispone de cinco (5) días hábiles, contados a partir del recibido de la presente comunicación, para realizar el análisis de la evaluación efectuada por la Oficina de Control Interno de Gestión y remitir, si se considera pertinente, las observaciones a que haya lugar, debidamente justificadas y acompañadas de las evidencias del caso, con el fin de que sean analizadas por el equipo auditor y si procede, realizar los ajustes pertinentes.

Atentamente,

JOSE DUVAN LIZARAZO CUBILLOS

Jefe Oficina de Control Interno de Gestión

Anexo: Mapa de Riesgos Institucionales Folios seis (6) folios
Elaboró: Andrea Chacón Mellizo. – Auditor Contratista OCIG
Revisó: Dr. José Duvan Lizarazo Cubillos

*Recebo
Remisión
May 12/2022
11:25 am*



FORMATO

Código: F-PLA-15

**Informe auditoría interna
de calidad**

Versión: 04

Fecha: 20/12/2012

Página 1 de 11

Coordinador de Calidad:	SECRETARÍA TIC
Auditor Líder:	José Duván Lizarazo Cubillos – Jefe de Oficina de Control Interno de Gestión
Equipo Auditor:	Andrea Chacón Mellizo – Auditor Contratista OCIG
Objetivo:	Realizar seguimiento y evaluación a los controles y acciones formuladas, para mitigar las causas de los riesgos a través de la metodología del Mapa de riesgo Institucionales por la Secretaría TIC y de las acciones propuestas para mitigar los riesgos dentro de la entidad.
Alcance:	Verificar el cumplimiento de las acciones establecidas por la Secretaría TIC para la definición y tratamiento del Mapa de riesgos Institucionales identificados en los procesos, en el periodo comprendido de julio a diciembre de 2021. Tomando como base: <ul style="list-style-type: none">- La información reportada en el Mapa de riesgos correspondientes a este periodo.- La publicación de la documentación en la Plataforma de Intranet a través del formato MR-GER-01.- El diligenciamiento del formato MECI- F-PLA-25 “Gestión y monitoreo del Riesgo”.
Documentos de referencia:	Documentación del Modelo Integrado de planeación y gestión, Mapa de riesgos, Gestión Gerencial – MR – GER-01
Fecha de apertura:	22 de abril de 2022
Fecha de cierre:	9 de abril de 2022
Proceso:	La Oficina de Control Interno de Gestión a través de la solicitud emitida con la circular No. S.A 60.07.01-00067 de enero 25 de 2022; se cerciora de los hechos y circunstancias relacionadas con las acciones y actividades presentadas para el diagnóstico hacia la Secretaría TIC. Lo evidenciado y observado por parte de la OCIG queda soportado en el presente informe, así como las observaciones y recomendaciones.

Conclusiones del equipo auditor

1. Anotaciones iniciales

La Oficina de control interno de gestión mediante circular No. circular No. S.A 60.07.01-00067 de 25 de enero de 2022, la solicitud de evidencias a la secretaría TIC para el cumplimiento del Mapa de Riesgos Institucionales correspondientes al segundo semestre de 2021.

El equipo auditor procede a realizar el Monitoreo y evaluación de los riesgos descritos por la Secretaría TIC, teniendo en cuenta las evidencias presentadas y entregadas mediante CD y oficio S.TIC 62.217.00 - 0257 del 11 de febrero de 2022 radicado en la Oficina de Control Interno de Gestión y el formato MECI -F-PLA-25.



FORMATO

Código: F-PLA-15

**Informe auditoría interna
de calidad**

Versión: 04

Fecha: 20/12/2012

Página 2 de 11

2. Aspectos relevantes

Para realizar el presente informe, la metodología adoptada consistió en realizar seguimiento al mapa de riesgos Institucional, con el fin de evaluar el cumplimiento de las acciones de control propuestas; así como el diseño conceptual en la formulación de los controles, para este efecto se trabajó sobre la información que fue suministrada por la Secretaría TIC para segundo semestre de la vigencia 2021, la cual consta de los mapas de riesgos y las evidencias de las acciones adelantadas en cada uno de los controles:

GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES

Fortalecer el uso, la innovación y la apropiación de las Tecnologías de la Información y las Comunicaciones y la gestión de la información, con el fin de propiciar el cumplimiento de los objetivos de la institucionalidad gubernamental; promoviendo, aplicando y gestionando el ecosistema digital departamental, contribuyendo en el acercamiento permanente de la Administración Central Departamental con los ciudadanos mediante la implementación de la Política de Gobierno Digital. Lo cuales son:

- **R1. Hurto de sistemas de información en custodia de la secretaría TIC.**
- **R2. Equipos susceptibles a fallos electrónicos que se encuentren en el edificio de la gobernación del Quindío.**
- **R3. Ineficiencia administrativa por desconocimiento o falta de información TI**
- **R4 adulterar, modificar, sustraer o eliminar datos o información sensible, confidencial, critica en beneficio propio de terceros.**
- **R5. Copias de seguridad sistemas de información**
- **R6. Política de gobierno digital con baja implementación.**

RIESGO 1. HURTO DE SISTEMAS DE INFORMACIÓN EN CUSTODIA DE LA SECRETARÍA TIC.

- El tipo de Riesgo: de Imagen o reputacional.
- improbabilidad: 2
- Impacto: 2 (Menor).
- Zona de Riesgo: Bajo.

✓ **Descripción:**

Hace referencia al hurto de la información, de los mismos equipos de cómputo o equipos de red con los que cuenta la gobernación del Quindío.

✓ **Causas:** falta de controles de seguridad apoyados en la tecnología que garanticen la seguridad de los bienes tecnológicos del edificio de la Gobernación del Quindío.

✓ **Control:** para reducir el riesgo de robo la Gobernación del Quindío cuenta con un inventario de los sistemas de información con el que cuenta la entidad, indicando así, si se ha perpetrado algún hurto. ...

✦ **Indicador:** $\frac{\text{Numero de inventarios realizados}}{\text{Numero de inventarios programados}} * 100$

✦ **Aplicación:** $\frac{(1) \text{ inventarios realizados}}{(1) \text{ inventarios programados}} * 100\% = 100\%$



FORMATO

Código: F-PLA-15

**Informe auditoría interna
de calidad**

Versión: 04

Fecha: 20/12/2012

Página 3 de 11

• **Evidencias:**

La Secretaría TIC, cuenta con un sistema de monitoreo de inventario para garantizar los bienes tecnológicos con que cuenta la Entidad. El software OCS Inventory, permite reportar diariamente el inventario con que cuenta la Gobernación del Quindío. El reporte fue generado para el segundo periodo auditado para los meses de julio a diciembre de 2021 encontrando 476 equipos de computo.

ID	Descripción	Estado
001	Equipo de computo	Activo
002	Equipo de computo	Activo
003	Equipo de computo	Activo
004	Equipo de computo	Activo
005	Equipo de computo	Activo
006	Equipo de computo	Activo
007	Equipo de computo	Activo
008	Equipo de computo	Activo
009	Equipo de computo	Activo
010	Equipo de computo	Activo

✓ **Observaciones:**

Se recomienda a la Secretaria que si bien el software brinda una información constante de los equipos con que cuenta la gobernación, no es suficiente para mantener un control de inventarios, por tal motivo es importante establecer un cronograma o estrategias donde se especifique a través de visitas a las diferentes secretarias, sobre el estado de cada equipos.

La información que brinda la secretaria TIC a través del software OCS Inventory no evidencia y no registra el total de servidores con que cuenta la Gobernación.

El reporte que emite la secretaria no es organizado, ya que no permite clasificar la información correspondiente, si bien el reporte me informa sobre los equipos con que cuenta la gobernación no evidencia el número de inventarios realizados a la Gobernación.



FORMATO

Código: F-PLA-15

**Informe auditoría interna
de calidad**

Versión: 04

Fecha: 20/12/2012

Página 4 de 11

RIESGO 2: EQUIPOS SUSCEPTIBLES A FALLOS ELECTRÓNICOS QUE SE ENCUENTREN EN EL EDIFICIO DE LA GOBERNACIÓN DEL QUINDÍO.

- El tipo de Riesgo: Operativo
- Probabilidad: 4 (Probable)
- Impacto: 2 (Menor)
- Zona de Riesgo: Alto

✓ **Descripción:**

Los factores como traumatismos en los diferentes procesos informáticos de la administración Central Departamental por daño, falta de mantenimiento o virus en los equipos electrónicos de la entidad, ocasiona equipos susceptibles a fallos electrónicos que se encuentran en el edificio de la Gobernación del Quindío.

✓ **Causas:**

Traumatismos en los diferentes procesos informáticos de la administración Central Departamental por daño, falta de mantenimiento o virus en los equipos electrónicos de la entidad

✓ **Control**

El Director de Sistemas verifica periódicamente que los equipos se encuentren con el anti-virus instalado y licenciado correctamente, a través de la consola del aplicativo instalado en uno de los servidores de la entidad, además de esto se realiza mantenimiento preventivo anualmente a los equipos tecnológicos de la gobernación del Quindío; en caso de encontrar fallas en algún equipo o algún anti-virus no licenciado se procede a realizar el mantenimiento correctivo que se requiere y se deja como evidencia los informes presentados por el director de sistemas y el mantenimiento en el aplicativo en la mesa de ayuda

✚ **Indicador:**

a.
$$\frac{\text{Numero de equipos con antivirus licenciado}}{\text{Numero total de equipos de la gobernación del Quindío}} * 100$$

b.
$$\frac{\text{Numero de mantenimiento preventivo realizado}}{\text{Numero de mantenimientos preventivos programados}} * 100$$

✚ **Aplicación:**

a.
$$\frac{(433) \text{ de equipos con antivirus licenciado}}{(476) \text{ total de equipos de la gobernación del Quindío}} * 100 = 91\%$$

b.
$$\frac{(0) \text{ mantenimiento preventivo realizado}}{(416) \text{ de mantenimientos preventivos programados}} * 100 = 0$$



FORMATO

Código: F-PLA-15

**Informe auditoría interna
de calidad**

Versión: 04

Fecha: 20/12/2012

Página 5 de 11

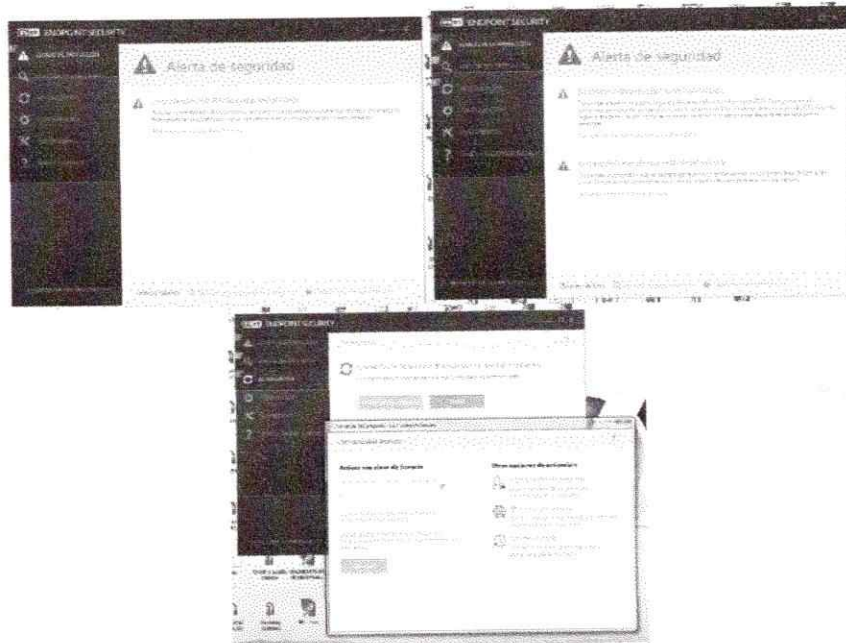
• **Evidencias:**

- a. Para este indicador la Secretaría TIC reporta mediante el software Eset PROTECT que tiene 433 anti-virus instalados y licenciados.


• **Observaciones:**

Se sugiere a la secretaria TIC, establecer mayor control sobre la cantidad de los antivirus instalados, ya que debería de corresponder con el numero de equipos con que cuenta la secretaria el cual no se ve reflejado

en las evidencias reportadas. El equipo auditor realizo una verificación del antivirus instalado en los pc's de la OCIG y la OCID, donde quedo registrado que las licencias se encuentran vencidas y hay un pc donde el software Eset Protect, no carga al cliquer sobre el icono, lo que refleja la falta de mantenimientos preventivos.



- b. Para el segundo indicador se reporta a través de un archivo en Excel de 409 mesas de ayuda donde la información suministrada por la secretaria TIC, no le permite al equipo auditor realizar una trazabilidad a cada mantenimiento realizado. Ya que el archivo en Excel que reporta la TIC no identifica el tipo de mantenimiento preventivo que se realiza a cada uno de los equipos. También se presentan 7 equipos en estado pendientes pero la OCIG no puede emitir un concepto acertado sobre esta categoría. Por tal motivo a este indicador no se le pueda establecer un porcentaje.

	FORMATO	Código: F-PLA-15
	Informe auditoría interna de calidad	Versión: 04 Fecha: 20/12/2012
		Página 6 de 11

RIESGO 3. INEFICIENCIA ADMINISTRATIVA POR DESCONOCIMIENTO O FALTA DE INFORMACIÓN TI

- El tipo de Riesgo: Operativo
- Probabilidad: 4 (Probable)
- Impacto: 2 (Menor)
- Zona de riesgo: Alto.

✓ **Descripción:**

Riesgo asociado a la falta de actualización y capacitación de los conocimientos en sistemas de información e implementación de la estrategia de gobierno digital en la gobernación del Quindío

✓ **Causa 1:**

Falta de difusión planes y políticas asociadas a la administración y el manejo de la infraestructura tecnológica

✓ **Causa 2:**

Falta de capacitación para la administración y actualización de la infraestructura tecnológica

✓ **Control:**

El Director de Gobierno Digital semestralmente, realizara verificación del Plan de difusión de Planes y políticas de la Secretaria TIC, a través de informe estadístico de consolidación de capacitaciones y/o difusiones. En caso de que encuentre el no cumplimiento del Plan de sensibilización, se realizara reajuste del cronograma establecido. Como evidencia se tendrá el Plan de difusión y cronograma, informes estadísticos y listados de asistencia.

✚ **Indicador:**


a.
$$\frac{\text{Numero de estrategias de difusión implementadas}}{\text{Numero de estrategias programadas en el plan}} * 100$$

b.
$$\frac{\text{Numero de capacitaciones realizadas}}{\text{Numero de capacitaciones programadas en el plan}} * 100$$

✚ **Aplicación:**

a.
$$\frac{(1) \text{ de estrategias de difusión implementadas}}{(1) \text{ de estrategias programadas en el plan}} * 100 = 100\%$$

b.
$$\frac{(3) \text{ capacitaciones realizadas}}{(3) \text{ de capacitaciones programadas en el plan}} * 100 = 100\%$$

	FORMATO	Código: F-PLA-15
	Informe auditoría interna de calidad	Versión: 04
		Fecha: 20/12/2012
		Página 7 de 11

• **Evidencias:**

- a. Para la causa 1. La dirección de gobierno digital de las TIC ejecuta estrategias a través de capacitaciones sobre temas acerca de: Datos Abiertos, Seguridad de la Información y la socialización de estrategia de gobierno digital.
- b. En el segundo indicador la secretaria TIC realiza capacitaciones en los meses de julio, septiembre y noviembre a 40 funcionarios de la gobernación del Quindío en los temas implementados para la estrategia de difusión

RIESGO 4 ADULTERAR, MODIFICAR, SUSTRAR O ELIMINAR DATOS O INFORMACIÓN SENSIBLE, CONFIDENCIAL, CRITICA EN BENEFICIO PROPIO DE TERCEROS.

- El tipo de Riesgo: Corrupción
- Probabilidad: 2 (Improbable)
- Impacto: 5 (Catastrófico)
- Zona de Riesgo: Externo

✓ **Descripción:**

Hace referencia a accesos a las bases de datos no autorizados de los diferentes aplicativos misionales de la entidad y de computadores que manejen información confidencial de la misma.

✓ **Causa 1:**

Ofrecimiento de dadas o presión por parte de un externo o superior para el acceso no autorizado a información

✓ **Causa 2:**


Baja capacitación en los lineamientos de seguridad y privacidad de la información, y las consecuencias de la violación de la ley.

✓ **Control:**

El Director de Gobierno Digital cuatrimestralmente, realizara una capacitación a los funcionarios en el Plan de Seguridad y Privacidad de la Información, así como en las implicaciones legales como sanciones y multas en caso de propiciar vulneración a los sistemas de información de la entidad. En caso de evidenciar que no son suficientes las capacitaciones, se ajustara la periodicidad de las mismas. Como evidencia quedan listados de asistencia, el Plan de Seguridad y Privacidad de la Información y cronograma

✦ **Aplicación:**

$$\frac{\text{No. de capacitaciones realizadas}}{\text{No. de capacitaciones programadas en el plan}} * 100 = 0\%$$

	FORMATO	Código: F-PLA-15
	Informe auditoría interna de calidad	Versión: 04
		Fecha: 20/12/2012
		Página 8 de 11

- **Evidencias:**

La secretaria TIC informa que para el RIESGO 4 ADULTERAR, MODIFICAR, SUSTRAR O ELIMINAR DATOS O INFORMACIÓN SENSIBLE, CONFIDENCIAL, CRITICA EN BENEFICIO PROPIO DE TERCEROS y el RIESGO 5. COPIAS DE SEGURIDAD SISTEMAS DE INFORMACIÓN, luego de realizar mesa de trabajo y socialización con la oficina de Gobierno digital, manifiestan que se procede a unificar estos dos riesgos ya que presenta duplicidad en la entrega de información.

Se aclara que para el primer periodo comprendido entre los meses de primero de enero a treinta de junio de vigencia 2021 se realiza el seguimiento al Riesgo 4.

La OCIG no evidencia de parte de la Secretaría TIC constancia de mesas de trabajo y socializaciones realizadas entre la secretaria de Planeación o Gobierno digital evidenciando cambios en el Mapa de Riesgos Institucionales.

RIESGO 5. COPIAS DE SEGURIDAD SISTEMAS DE INFORMACIÓN

- El tipo de Riesgo: Operativo
- Probabilidad: 3 (Posible)
- Impacto: 3 (Moderado)
- Zona de Riesgo: Alto.

- ✓ **Descripción:**

Riesgo asociado a la falta de copias de seguridad de las bases de datos de los sistemas de información con los que cuenta la entidad, dichas copias se deben realizar diariamente y por la Secretaría TIC.

- ✓ **Causa:**

Falta de capacitación en el manejo y realización diaria a diferentes funcionarios de la secretaria TIC de las copias de seguridad de las bases de datos.

- ✓ **Control:**

La Secretaría TIC, cuenta con una política de respaldo de la información de los servidores de la gobernación, este respaldo se realiza todos los días en discos duros externos que se encuentran en el data center y se replican a la unidad de almacenamiento NAS que se encuentra en el centro de convenciones

✚ **Indicador:**

$$\frac{\text{No. de copias de seguridad de las bases de dato (PCT, HUMANO, SEVENET, SISCAR) realizadas} * 100}{\text{No. de copias de seguridad a las bases de dato (PCT, HUMANO, SEVENET, SISCAR) programadas}}$$

✚ **Aplicación:**

$$\frac{(540) \text{ de copias de seguridad de las bases de dato (PCT, HUMANO, SEVENET, SISCAR) realizadas} * 100}{(648) \text{ de copias de seguridad a las bases de dato (PCT, HUMANO, SEVENET, SISCAR) programadas}} = 83.33\%$$



FORMATO

Código: F-PLA-15

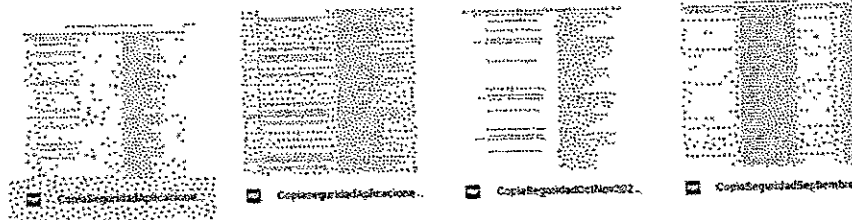
Informe auditoría interna de calidad

Versión: 04

Fecha: 20/12/2012

Página 9 de 11

• Evidencias:



Para el cálculo del indicador se tiene en cuenta que cada mes se debería de reportar 27 copias de seguridad de cada una de las bases de datos. Para el segundo semestre de 2021 se deberían tener 648 copias de seguridad ($4 * 27 * 6 = 648$).

La secretaria TIC reporte listado de inventarios realizados a cada uno de los aplicativos (PCT, HUMANO, SEVENET, SISCAR), donde se evidencia un total de 540 copias de seguridad. Donde se verifica que en todo el mes de Julio no se evidencian Backus de los aplicativos en mención, es de recordar a la secretaria la importancia de ser constantes en la realización de la actividad.

RIESGO 6. POLÍTICA DE GOBIERNO DIGITAL CON BAJA IMPLEMENTACIÓN.

- El tipo de Riesgo: Operativo
- Probabilidad: 4 (Probable)
- Impacto: 3 (Moderado)
- Zona de Riesgo: Alto

✓ **Descripción:**

Riesgo asociado a la política de gobierno digital, como requisito legal bajo el decreto 2008 de 2018 para todas las entidades públicas del país.

✓ **Causa 1:**

Falta de implementación del eje transversal a la política Llamado Arquitectura TI.

✓ **Causa 2:**


Falta de implementación del eje transversal a la política Llamado Seguridad de la información.

✓ **Causa 3:**

Falta de implementación del eje transversal a la política Llamado servicios ciudadanos digitales

✓ **Control:**

A través de la dirección de gobierno digital se pretende dar seguimiento a la implementación de la política de gobierno digital en la Gobernación del Quindío a través de la creación y/o actualización de planes y/o políticas correspondientes a la estrategia

	FORMATO	Código: F-PLA-15
	Informe auditoría interna de calidad	Versión: 04
		Fecha: 20/12/2012
		Página 10 de 11

± **Indicador:**

Índice de implementación de la política de gobierno digital en la entidad*100

± **Aplicación:**

Índice de implementación de la política de gobierno digital en la entidad*100 . = 94.8%

• **Evidencias:**

Se evidencia el cumplimiento y progreso de las estrategias implementadas en las políticas de gobierno digital de la gobernación del Quindío, donde se evidencia un porcentaje muy alto.

3. HALLAZGOS DE AUDITORIA:

- ✓ La secretaria Tic cuenta con un excelente grupo de profesionales idóneos para el cumplimiento de sus funciones, para el seguimiento del segundo periodo se presentan algunos hallazgos que deben estar en consideración para el posterior seguimiento.

Tipo	Requisito	Descripción
Observación N.1	RIESGO 1. HURTO DE SISTEMAS DE INFORMACIÓN EN CUSTODIA DE LA SECRETARÍA TIC	Se presenta debilidades en el RIESGO 1. , ya que el software OCS Inventory, omite el inventario de los servidores con que cuenta la gobernación y se deben realizar controles físicos para evidenciar el estado de los equipos e implementar medidas que eviten el suceso de pérdida o hurto de los equipos tecnológicos con que cuenta la gobernación del Quindío.
Observación N.2	RIESGO 2: EQUIPOS SUSCEPTIBLES A FALLOS ELECTRÓNICOS QUE SE ENCUENTREN EN EL EDIFICIO DE LA GOBERNACIÓN DEL QUINDÍO	Se le sugiere a la Secretaría TIC plantear mesas de trabajo y reprogramar, replantear estrategias que le permitan, brindar soluciones de mejora continua para el cumplimiento del RIESGO 2 , donde la OCIG evidencia debilidades con el monitoreo del software Eset Protect para el antivirus y mantenimiento preventivo que se debe realizar a los equipos. Donde el segundo indicador recibe un porcentaje en cero ya que la información suministrada no por permite emitir una conclusión.



FORMATO

Código: F-PLA-15

**Informe auditoría interna
de calidad**

Versión: 04

Fecha: 20/12/2012

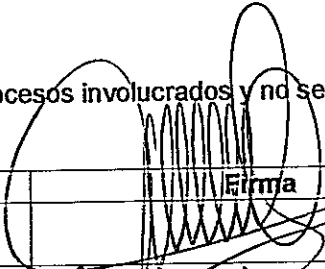
Página 11 de 11

4. Recomendaciones para auditorías posteriores

- ✓ Es necesario que cada responsable de proceso revise su caso particular, las causas que lo ocasionaron y establezca las acciones para prevenir su ocurrencia en el 2022, tanto en la gestión de sus riesgos durante la vigencia, como al momento de entregar la información anual, para la evaluación del mapa de riesgos institucional.
- ✓ Formular un procedimiento que establezca responsables, tiempos, que permita tener un inventario actualizado y que permita la articulación oportuna entre los os procesos.
- ✓ Todas las observaciones y recomendaciones plasmadas en el presente informe hacen parte de las oportunidades de mejora, teniendo en cuenta las situaciones encontradas, para que se realicen los ajustes que se consideren pertinentes para el mejoramiento del proceso de gestión del Mapa de riesgos Institucional.

AUTORIZACIÓN PARA COMUNICAR ESTE INFORME:

Este informe se comunicará después de la auditoría únicamente a los procesos involucrados y no será divulgado a terceros sin su autorización.

Nombre completo	Responsabilidad	Firma
	Coordinador de Calidad	
	Auditor Líder	