Alcaldía de Medellín
Cuenta con vos
ISVIMED
Instituto Social de Vivienda y Hábitat de Medellín

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

**PL-GT-04**

| ELABORADO POR | REVISADO POR | APROBADO POR |
|---|---|---|
| Carlos Gómez V.<br>Carolina Martinez<br>Contratistas | Jorge Iván Velásquez<br>Subdirector Administrativo y Financiero | Jorge Iván Velásquez<br>Subdirector Administrativo y Financiero |

# 1 OBJETIVOS

## 1.1 Objetivo general

Implementar el plan de gestión de seguridad y privacidad para minimizar el riesgo de pérdida de activos de la información a los que puede estar expuesto el Instituto de Vivienda y Hábitat de Medellín, partiendo de la identificación, análisis, valoración, acciones y seguimiento de riesgos potenciales que tengan un efecto adverso en la integridad, confiablidad y disponibilidad de la información.

## 1.2 Objetivos específicos

- Comunicar al interior de instituto, a través de las diferentes herramientas, la importancia de gestionar de una forma adecuada el flujo de la información para disminuir el riesgo inherente a ella.

- Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional.

# 2 Alcance

Las políticas documentadas en el presente documento aplican a todos los empleados del ISVIMED tanto empleados directos, como contratistas

# 3 Definiciones :

- **Activo**

  En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- **Amenazas**

  Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Análisis de Riesgo**

  Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Auditoría**

  Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

- **Ciberseguridad**

  Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

- **Ciberespacio**

  Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua Española).

- **Control**

  Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Declaración de aplicabilidad**

  Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así

como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

- **Gestión de incidentes de seguridad de la información**

  Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **Plan de continuidad del negocio**

  Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- **Plan de tratamiento de riesgos**

  Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- **Riesgo**

  Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información**

  Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Sistema de Gestión de Seguridad de la Información SGSI**

  Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

- **Trazabilidad**

  Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

- **Vulnerabilidad**

  Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

- **Materialización del Riesgo**

  Cuando los riesgos identificados se hacen realidad.

## 4 Justificación

La gestión de riesgos de seguridad y privacidad de la información son los procesos por medio de los cuales se busca eliminar las pérdidas de información, facilitando el conocer las fortalezas y debilidades a los que está expuesto el servicio durante todo su ciclo de vida.

Por esto es muy importante para las organizaciones contar con un plan de tratamiento de riesgos de seguridad y privacidad de la información, para generar confianza a los usuarios, empleados y entidades con las cuales se relacionan. Por

esta razón el Instituto de vivienda y hábitat de Medellín – ISVIMED, basado en una Mapa de riesgos desarrolla este plan, buscando dar respuesta a las necesidades actuales y proteger la confianza depositada en ella con los datos almacenados por sus diferentes procesos.

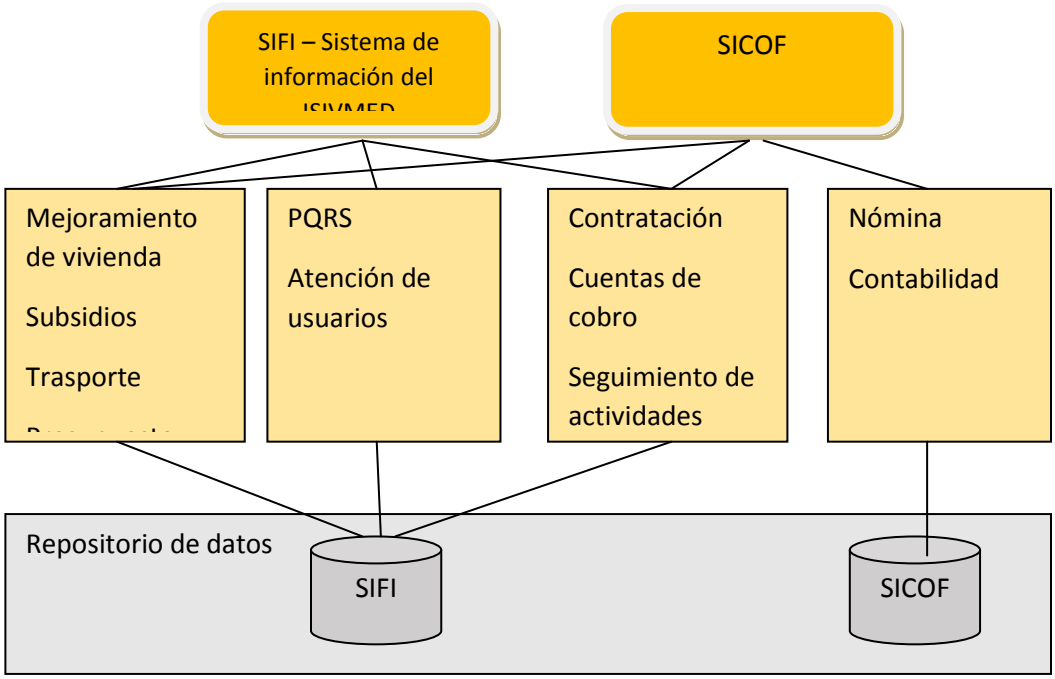
## 5 Riesgos de seguridad y privacidad de la información

ISVIMED consiente que los riegos de seguridad y privacidad de la información pueden afectar al continuidad del negocio y que a través de los diferentes procesos de la organización pueden afectar la confiabilidad, integridad y disponibilidad de la información, tiene identificado sus riesgos y establecidas las barreras que mitigan su ocurrencia y disminuyan su impacto, es de anotar que los riesgos inherentes a la seguridad y privacidad de la información pueden ser derivados de factores internos y externos.

## 6 Identificación de Activos

Se presentan los activos de información por medio de los cuales se gestiona la información del ISVIMED.

Sistemas de información del ISIVMED




**Grafica 1: Sistemas de información del ISIVMED**

A continuación de describe con mayor detalle las características del Sistema de información.

### 6.1 El Sistema de Información SIFI

Se constituye en la única herramienta tecnológica para el ingreso de la información relacionada con la gestión misional y de apoyo del Instituto Social de Vivienda y Hábitat del Municipio de Medellín, en lo relacionado con su objeto "Gerenciar la vivienda de interés social en el Municipio de Medellín, conduciendo a la solución de necesidades habitacionales; especialmente de los asentamientos humanos y grupos familiares en situación de pobreza y vulnerabilidad; involucrando a los diferentes actores públicos, privados y comunitarios en la gestión y ejecución de proyectos de construcción de vivienda nueva, titulación y legalización, mejoramiento de vivienda, mejoramiento de entorno, reasentamiento, acompañamiento social, gestión inmobiliaria y demás actuaciones integrales de vivienda y hábitat en el contexto urbano y rural Municipal y regional."

SIFI se encuentra diseñado de manera modular, donde cada subdirección administra de forma independiente el ingreso de la información, de acuerdo con las actividades asociadas a cada uno de los procesos establecidos al interior del Instituto, constituyéndose dicha información como fuente primaria de datos para los demás procesos para la toma de decisiones. El sistema permite integrar todos los módulos de tal manera que tanto el nivel directivo y operativo logren acceder a la información en cualquier momento con reportes en línea y en tiempo real.

El sistema de información está estructurado por módulos los cuales fueron diseñados dando respuesta a los programas y proyectos que lidera el instituto. Así mismo contiene otros módulos que apoyan a la gestión tal como se observa en la siguiente figura:

**Gráfica 2:Sistema de Información del ISVIMED - SIFI**

Actualmente el SIFI se encuentra en versión 9.0, administrada directamente por el líder de TICS. El licenciamiento de este sistema es propio al ser un desarrollo hecho en casa, y los derechos de autor sobre el software y la estructura de datos se encuentran debidamente registrados a nombre del Instituto Social de Vivienda y hábitat de Medellín.

Tanto el *front-end* como el *back-end* de la aplicación están desarrollados en el lenguaje de programación Ruby on Rails, mientras que la base de datos funciona sobre ORACLE 11G. Actualmente, el sistema se encuentra instalado localmente en un servidor, cuyo sistema operativo es Windows server 2008.

Los funcionarios del instituto tienen gran aceptación del sistema, cabe anotar que es el único sistema de información con el que cuenta entidad, es decir, se convierte en la herramienta básica de trabajo para gestión.

A continuación, se detalla las fortalezas, debilidades, iniciativas y/o proyectos en marcha, así mismo como las recomendaciones que se tienen visionadas para su perfeccionamiento:

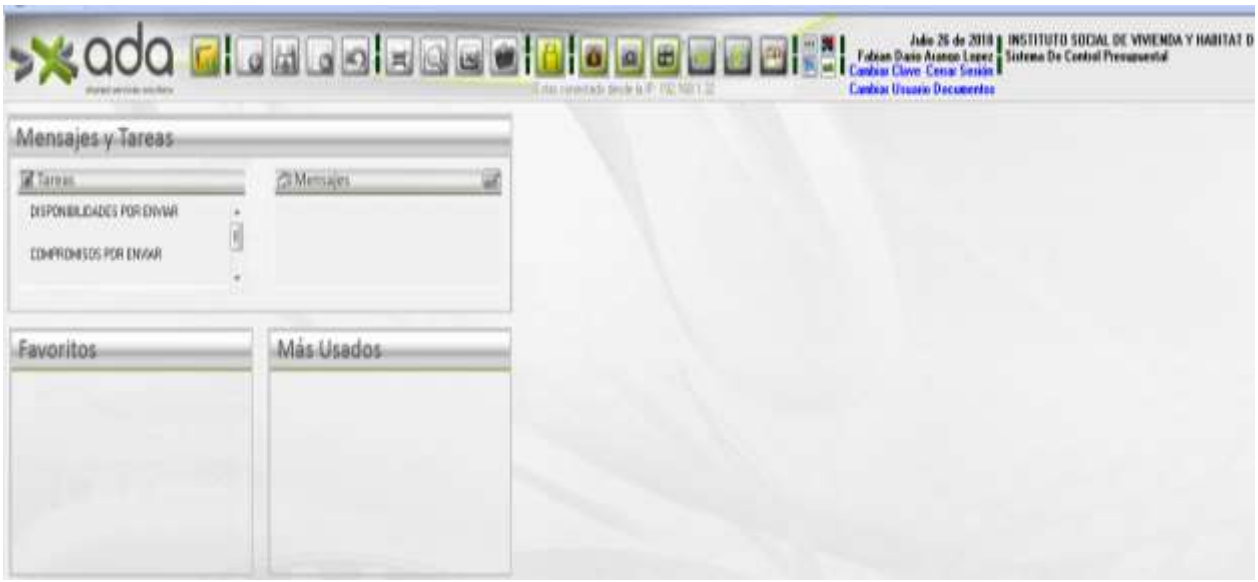
## 6.2 **Sistema SICOF**

El instituto para gestionar el tema financiero y contable, se soporta en un sistema de información denominado SICOF, dicho sistema está estructurado por módulos que integran la información financiera. Los módulos se describen a continuación:

- Tesorería
- Presupuesto.
- Contabilidad.

Éste sistema de información es suministrado y administrado por un tercero, sin embargo las licencias son propias, el pago se realiza por soporte y mantenimiento del mismo.

Como parte de la estrategia enmarcada en el PETIC, se pretende migrar a una integración tanto del SIFI como del SICOF, de tal manera que se integren actividades administrativa y financieras que tienen un impacto directo en el tema presupuestal del instituto, así mismo disminuir los riesgos en la seguridad de la información evitando gestiones paralelas y garantizando un blindaje desde el acceso y administración a la información institucional.




**Grafica 3: Sistema de Información-SICOF**

## 7 Acceso a la Información:

Todos los funcionarios que laboran para el ISVIMED tanto en calidad de vinculados como contratistas cuentan con dos tipos de perfiles:

- **Administrador:** tiene la potestad de realizar ajustes al sistema y asignar permisos de acceso.
- **Usuario:** persona que hace uso del sistema. (consulta, indexa y corregir información)

Todos los vinculados dentro de las obligaciones como funcionarios públicos están obligados a realizar un adecuado uso de la información institucional en el marco de la ley de transparencia y anticorrupción. El instituto debe garantizar a futuro que todos los contratistas independientemente del rol que desempeñen, tengan claramente descritos en sus contratos las responsabilidades inherentes al uso adecuado de la información. Así mismo garantizar que al momento de no continuar prestando servicios al instituto, se realice una entrega formal de la información derivada de su rol.

Como parte de las barreras implementadas para garantizar la accesibilidad de los colaboradores después de haber terminado su contrato por prestación de servicios, desde la subdirección jurídica para el caso de contratistas se garantiza indexar en el SIFI, la terminación de dichos contratos, lo que de manera transparente deshabilita el ingreso al mismo.

Lo anterior se debe aplicar a los vinculados, de tal manera que el líder de Gestión Humana informe al Líder de TIC´s los retiros del personal para proceder a validarlo en el directorio activo del instituto.

## 8 Seguridad

### 8.1 Seguridad de la Información

Los funcionarios públicos, contratistas y practicantes del Instituto Social de Vivienda y Hábitat de Medellín son responsables de la información que administran y cumplen los lineamientos generales y especiales dados por el Instituto en la materia, lo

anterior dando cumplimiento a la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma. No obstante y consientes que tenemos identificadas brechas en ese sentido, se deberá ajustar e implementar un protocolo que garantice que ningún funcionario público, contratistas y practicantes pueden suministrar información de la entidad a ningún ente externo sin las autorizaciones respectivas.

Como regla general, la información a publicar en términos de políticas, normas y procedimientos de seguridad se entregarán en el marco de la normatividad aplicable vigente y a entes externos que por su competencia así lo requieran.

## 8.2 Seguridad para Servicios Informáticos

En ISVIMED se cuenta con los siguientes servicios informáticos:

- SIFI- Sistema de Información de Isvimed.
- SICOF- Sistema de Información Contable y Financiero
- Correo electrónico.

Cada uno de los usuarios cuenta con su respectivo acceso el cual es personal e intransferible. Para el caso de vinculados el tema es trabajo directamente con gestión humana, para el cas o de contratista el supervisor debe solicitar a TIC´s, los accesos requeridos según su rol a desempeñar, quedando así la evidencia de la seguridad en el acceso a dichos sistemas informáticos Todos los anteriores son de uso únicamente para el ejercicio de las funciones de competencia de cada funcionario y de las actividades contratadas en el caso de los contratistas y practicantes.

Con el fin de mejorar la solicitud de los accesos a usuarios, se ajustará el documento que delimite lo siguiente: Toda persona nueva o que requiera acceso a otros módulos, el jefe directo o supervisor de contrato debe realizar la solicitud a TIC´s mediante el Módulo de Solicitud de soporte

### 8.3 Seguridad en recursos informáticos

Los recursos informáticos deben cumplir como mínimo con lo siguiente:

- **Gestión de claves:** Establece como deben ser utilizadas las claves de ingreso a los recursos informáticos, parámetros sobre la longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiar su contraseña y los períodos de vigencia de las mismas, entre otras. Las palabras claves o contraseñas de acceso a los recursos informáticos, que designen los funcionarios públicos, contratista y practicantes del instituto son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.

- **Las puertas traseras:** Las puertas traseras son entradas no convencionales a los sistemas operacionales, bases de datos y aplicativos. Es de suma importancia aceptar la existencia de las mismas en la mayoría de los sistemas operacionales, bases de datos, aplicativos y efectuar las tareas necesarias para contrarrestar la vulnerabilidad que ellas generan.

- El control de acceso a todos los sistemas de computación de la entidad debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicos para cada usuario.

- Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.

- Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a él.

- Cuando el ISVIMED cuente con desarrollos propios, deberá garantizar ecosistemas separados para el desarrollo, pruebas y producción, con el fin de garantizar una adecuada administración, operación, control y seguridad.

## 9 LA INFORMACIÓN

La Información es un recurso vital producido por los Sistemas de la institución, esta debe ser protegida apropiadamente contra accesos no autorizados, alteración, modificación, propagación, perdida o destrucción, independientemente de los medios de almacenamiento donde esta reside. Cabe anotar que la información del instituto desde su generación hasta su custodia debe cumplir con los lineamientos definidos por el ARG- Archivo General de la Nación.

La información que se genera y administra en el ISVIMED se evidencia en medio físico y electrónico, según la dinámica de cada actividad.

La información física se consolida mediante la TRD- Tablas de Retención Documental, las cuales describen la especificidad de la serie documental generada desde cada área del instituto.

**Parte de la información física generada:**

- Expedientes de beneficiarios.
- Expedientes de contratos.
- Expedientes de convenios.
- Expedientes de proyectos.
- Hojas de vida de funcionarios.
- Entre otros

**Parte de la Información electrónica:**

- Ejecución derivado de los programas y proyectos del instituto.
- Caracterización de población.
- Trazabilidad de la gestión realizada a cada hogar.
- Información de funcionarios y contratistas.
- Solicitudes de soportes.
- El SGC- Sistema de Gestión de Calidad.

- SMO- Sistema de Medición Organizacional

Lo anterior almacenado de manera lógica en una sola base de datos, en el SIFI- Sistema de información de ISVIMED.

### 9.1 Instaurar clasificación de la información

La calificación asignada a la categoría de información se ciñe a la clasificación que determina el ARG- Archivo General de la Nación, de ésta manera se instauran los controles requeridos de seguridad y privacidad contemplando los siguientes aspectos:

- **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. (Artículo 5 Ley 1712 de 2014)
- **Información clasificada**: Es toda aquella que al ser divulgada puede llegar a causar daño a algunos derechos individuales de personas naturales o jurídicas por contener información relacionada con la intimidad y privacidad de éstas. (Artículo 18 Ley 1712 de 2014)
- **Información reservada:** Información reservada: Su divulgación indebida puede afectar bienes o intereses públicos. (Artículo 19 Ley 1712 de 2014). Es necesario establecer el plazo para la clasificación de la reserva, es decir el tiempo en que se considera debe limitarse el acceso a la información el cual según la Ley solo puede durar un máximo de 15 años desde la creación del documento.

Todo lo anterior reposa en las TRD- Tablas de Retención Documental previamente elaboradas en el marco del SGD- Sistema de Gestión Documental del Instituto. (ver TRD).

Con el fin de cerrar algunas brechas identificas en términos de controles requeridos de seguridad y privacidad según la clasificación de información anterior, se revisará y ajustarán las herramientas hoy existentes en la materia, de tal manera que sean transversales a la normatividad aplicable vigente.

## 10 IDENTIFICACIÓN, ANÁLISIS Y CONTROL DEL RIESGO

En ISVIMED el riesgo se trabaja acorde a los lineamientos definidos por el DAFP-Departamento Administrativo de la Función Pública, para ello contamos con un Mapa de riegos en el cual se tipifican, se analizan y se establecen los controles correspondientes para eliminar su ocurrencia o mitigar su impacto en caso que se materialicen. Este ejercicio es liderado por la Subdirección de planeación en conjunto con los responsables de los procesos. Se cuenta con un Mapa de riesgos anual y se realizar seguimiento evaluativo cada tres meses dando cumplimiento al MECI-Modelo Estándar de Control Interno.

Para entender mejor el control que se tiene implementado actualmente, se describe cada una de las etapas, desde la identificación hasta su evaluación y seguimiento:

**Matriz de Calificación, Evaluación y Respuesta al Riesgo**

| Probabilidad de Ocurrencia | | | | | | |
|---|---|---|---|---|---|---|
| | **Casi seguro 5** | | | | | |
| | **Probable 4** | | | | | |
| | **Posible 3** | | | | | |
| | **Improbable 2** | | | | | |
| | **Rara vez 1** | | | | | |
| | | **Insignificante 1** | **Menor 2** | **Moderado 3** | **Mayor 4** | **Catastrófico 5** |
| | | **Impacto** | | | | |

**Convenciones De Evaluación Del Riesgo**

| | |
|---|---|
| | **Zona Riesgo Extrema** |
| | **Zona Riesgo Alta** |
| | **Zona Riesgo Moderada** |
| | **Zona Riesgo Baja** |

## 10.1 Identificación: Contexto interno y externo:

| CONTEXTO ESTRATÉGICO E IDENTIFICACIÓN DEL RIESGO | | | | | | |
|---|---|---|---|---|---|---|
| N° | RIESGO IDENTIFICADO | CONTEXTO INTERNO Y EXTERNO | | CLASIFICACION | CAUSAS | CONSECUENCIAS |
| | | INTERNO | EXTERNO | | | |
| 1 | Falta o vencimiento de licencias | x | | Cumplimiento. | Falta de seguimiento y control frente a los contratos.<br>Falta de control operativo por parte del responsable de verificar información en el sifi.<br>Inadecuada compra del servicio | Perdida económica.<br>Sanción.<br>Suspensión de la operación.<br>Activación de garantias contractuales por ambas partes (ISVIMED-CONTRATISTA) |

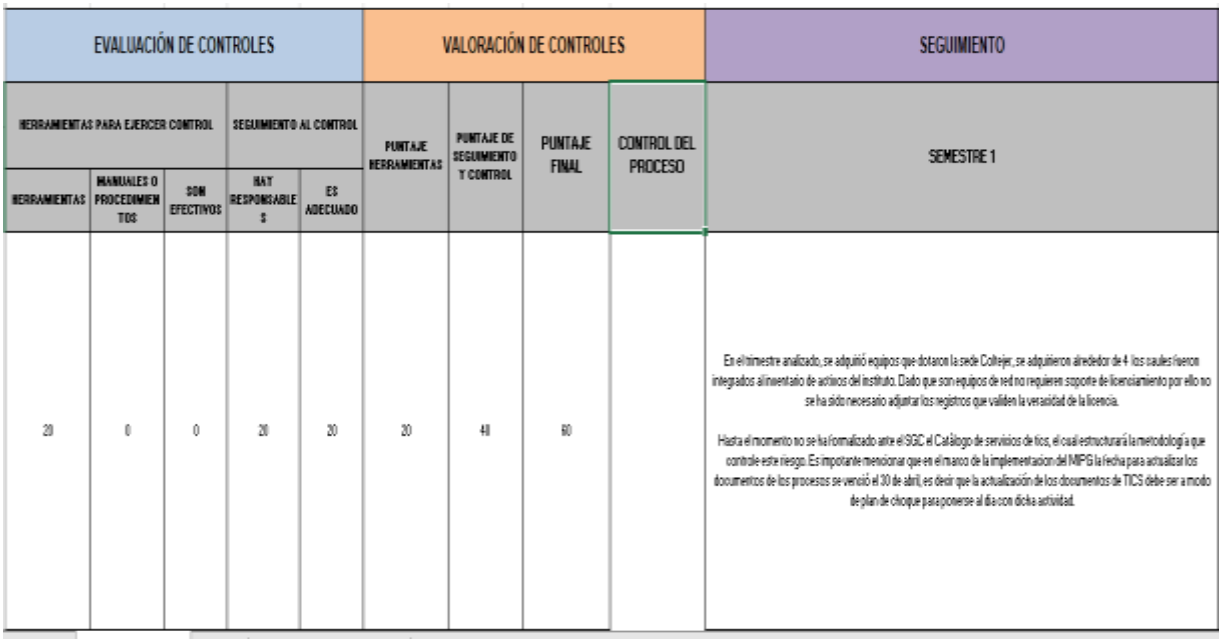
## 10.2 Análisis del Riesgo

Con base a los riesgos identificados se analiza realizando la calificación y estableciendo las acciones de mejora, como se muestra en la siguiente tabla:

| ANÁLISIS DEL RIESGO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| TIPO DE IMPACTO | RIESGO INHERENTE | | | MEDIDAS DE RESPUESTA | | RIESGO RESIDUAL | | |
| | PROBABILIDAD (1-5) | IMPACTO (1-5) | EVALUACIÓN | MEDIDA | ACCIONES | PROBABILIDAD (1-5) | IMPACTO (1-5) | EVALUACIÓN |
| Legal | 2 | 2 | Zona de riesgo baja | Evitar | .Cada que se vaya a adquirir un equipo hadware o software debe pasar por el concepto técnico de sistemas.<br>.Asegurar que los equipos adquiridos sean indexados en el invetario. Esta labor debe ser ejecutada por el responsable de inventarios.<br>.Verificación de la legalidad de las licencias adquiridas en la página del proveedor.<br>.Incluir como obligación contractual que el proveedor de licencias aporte el registro que evidencia su legalidad.<br>.Generar sinergia con el responsable de inventarios de tal manera que semestralmente se verifique su vigencia de las licencias.<br>.Documentar en el proceso lo anteriormente descrito. | 1 | 1 | Zona de riesgo baja |

### 10.3 Evaluación, valoración de controles y Seguimiento

Posterior al análisis y a la definición de acciones hacia la mejora, en una frecuencia trimestral, se realiza seguimiento a los riesgos previamente identificados y se registran en la herramienta de Mapa de Riesgos del proceso como se ilustra en la siguiente imagen.



| EVALUACIÓN DE CONTROLES | | | | | VALORACIÓN DE CONTROLES | | | | SEGUIMIENTO |
|---|---|---|---|---|---|---|---|---|---|
| HERRAMIENTAS PARA EJERCER CONTROL | | | SEGUIMIENTO AL CONTROL | | PUNTAJE HERRAMIENTAS | PUNTAJE DE SEGUIMIENTO Y CONTROL | PUNTAJE FINAL | CONTROL DEL PROCESO | SEMESTRE 1 |
| HERRAMIENTAS | MANUALES O PROCEDIMIENTOS | SON EFECTIVOS | HAY RESPONSABLES | ES ADECUADO | | | | | |
| 20 | 0 | 0 | 20 | 20 | 20 | 40 | 60 | | En el trimestre analizado, se adquirió equipos que dotaron la sede Coltejer, se adquirieron alrededor de 4 los cuales fueron integrados al inventario de activos del instituto. Dado que son equipos de red no requieren soporte de licenciamiento por ello no se ha sido necesario adjuntar los registros que validen la vera sidad de la licencia.<br><br>Hasta el momento no se ha formalizado ante el SGC el Catálogo de servicios de tics, el cual estructurará la metodología que controle este riesgo. Es importante mencionar que en el marco de la implementacion del MIPG la fecha para actualizar los documentos de los procesos se venció el 30 de abril, es decir que la actualización de los documentos de TICS debe ser a modo de plan de choque para ponerse al dia con dicha actividad. |

Somos conscientes que el análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo. Por lo anterior nuestra metodología la ajustaremos a los parámetros tal como lo propone la Guía de gestión de riesgos, Seguridad y privacidad de la información de MINTIC, la cual se hace de manera cualitativa generando una comparación en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, obteniendo al final la matriz denominada “Matriz de Calificación, Evaluación y respuesta a los Riesgos”.