

CRITERIO DE CLASIFICACIÓN Y ACCESO A LA INFORMACIÓN SENSIBLE

1. OBJETO Y ALCANCE DEL CONCEPTO

El presente documento tiene por objeto definir los criterios jurídicos aplicables para la clasificación, tratamiento, protección y acceso a la información en la Empresa de Servicios Públicos de Sabaneta EAPSA E.S.P., en atención a su naturaleza como Empresa Industrial y Comercial del Estado y a las particularidades derivadas de su actuación en ámbitos administrativos, contractuales, jurídicos y negociales.

En este sentido, el documento establece lineamientos orientados a:

- i) Determinar las categorías de información en función del régimen de acceso a la información pública, la protección de datos personales y la salvaguarda de los intereses institucionales;
- ii) Precisar los criterios para la identificación de información sujeta a restricciones de acceso, incluyendo aquella que, por su contenido o contexto, requiera un nivel de protección reforzada;
- iii) Definir parámetros para el acceso y uso de la información por parte de servidores públicos, contratistas, particulares y entes de control; y
- iv) Integrar el análisis jurídico de la información en escenarios, contractuales, jurídicos y de gestión negocial, en los cuales su divulgación pueda incidir en la posición institucional de la entidad.

El presente documento es aplicable a todas las dependencias de EAPSA, así como a los servidores públicos y contratistas que, en desarrollo de sus funciones u obligaciones, administren, accedan, produzcan o custodien información de la entidad, sin perjuicio de las disposiciones específicas contenidas en la normativa vigente y en los instrumentos internos de gestión de la información.

2. PROBLEMA JURÍDICO

Corresponde determinar cómo debe la Empresa de Servicios Públicos de Sabaneta EAPSA E.S.P. clasificar, gestionar y controlar el acceso a la información bajo su custodia, de manera que se garantice, de forma armónica:

- i) El derecho fundamental de acceso a la información pública;
- ii) La protección de los datos personales y, en especial, de los datos sensibles; y

iii) La salvaguarda de la información estratégica, contractual, jurídica y negocial de la entidad, cuya divulgación pueda afectar su posición institucional, económica o jurídica en el desarrollo de sus actividades.

Lo anterior, teniendo en cuenta la naturaleza jurídica de EAPSA como Empresa Industrial y Comercial del Estado, que actúa en escenarios de derecho público y de derecho privado, y que, en consecuencia, administra información que no solo se enmarca en el principio de transparencia, sino también en dinámicas propias de la contratación estatal, la gestión empresarial y la interacción en entornos de mercado.

En este contexto, el problema jurídico se concreta en establecer cuáles son los criterios jurídicos y operativos que permiten diferenciar los niveles de acceso y protección de la información, evitando tanto la restricción injustificada del acceso a la información pública, como la divulgación indebida de información protegida por reserva legal, por el régimen de protección de datos personales o por su carácter estratégico para la entidad.

3. MARCO CONSTITUCIONAL Y LEGAL APLICABLE

La determinación de los criterios de clasificación, tratamiento y acceso a la información en EAPSA debe abordarse desde un marco normativo integral que articule el derecho de acceso a la información pública, la protección de los datos personales y la naturaleza jurídica de la entidad como Empresa Industrial y Comercial del Estado.

3.1. Derecho de acceso a la información pública y principio de transparencia

El artículo 74 de la Constitución Política consagra el derecho de todas las personas a acceder a los documentos públicos, estableciendo como regla general la publicidad de la información en poder de las entidades estatales, salvo las excepciones previstas en la ley.

En desarrollo de este mandato, la Ley 1712 de 2014 define el régimen de acceso a la información pública, bajo el principio de máxima divulgación, conforme al cual toda información en posesión de los sujetos obligados es pública, salvo que se encuentre sometida a clasificación o reserva en los términos previstos por la ley.

Así mismo, dicha normativa establece que las restricciones al acceso deben ser de interpretación restrictiva, estar expresamente consagradas y responder a fines constitucionalmente legítimos, lo que impide la adopción de criterios discrecionales o indeterminados para limitar el acceso a la información.

3.2. Protección de datos personales como límite al acceso a la información

El derecho de acceso a la información no es absoluto y encuentra uno de sus principales límites en la protección de los datos personales, derivada del artículo 15 de la Constitución Política.

En este sentido, la Ley 1581 de 2012 establece el régimen general de protección de datos personales, definiendo las condiciones para su tratamiento y consagrando una categoría especial de protección para los denominados datos sensibles, cuya utilización indebida puede afectar la intimidad del titular o generar discriminación.

En consecuencia, la información que contenga datos personales no puede ser objeto de divulgación irrestricta, debiendo armonizarse el principio de transparencia con los principios de legalidad, finalidad, necesidad y seguridad en el tratamiento de la información.

3.3. Naturaleza jurídica de EAPSA y protección de la información estratégica

De conformidad con lo dispuesto en la Ley 489 de 1998, las Empresas Industriales y Comerciales del Estado desarrollan actividades de naturaleza industrial o comercial y, en dicho ámbito, se rigen por las reglas del derecho privado.

Esta particularidad implica que EAPSA no solo ejerce funciones administrativas, sino que también participa en escenarios de contratación, estructuración de negocios, ejecución de proyectos y, en general, en dinámicas propias de la gestión empresarial.

En este contexto, la información que produce y administra la entidad no se limita a documentos administrativos sujetos al principio de publicidad, sino que incluye información de carácter estratégico, técnico, financiero, contractual y jurídico, cuya divulgación puede:

- Afectar procesos de selección o negociación en curso;
- Comprometer la posición jurídica de la entidad en litigios o controversias;
- Generar desventajas en escenarios de competencia o gestión empresarial;
- Impactar la sostenibilidad financiera o la ejecución de proyectos.

Por lo anterior, la aplicación del principio de transparencia debe realizarse de manera armónica con la necesidad de proteger la información que, aun cuando repose en una entidad pública, está vinculada a su actividad industrial, comercial o negocial.

3.4. Articulación de los regímenes aplicables

De lo expuesto se concluye que la gestión de la información en EAPSA no puede analizarse desde un único régimen normativo, sino que exige la articulación de:

- El régimen de acceso a la información pública, que impone la publicidad como regla general;
- El régimen de protección de datos personales, que limita el acceso cuando se afecten derechos fundamentales; y
- El régimen propio de las Empresas Industriales y Comerciales del Estado, que impone la necesidad de proteger la información estratégica y negocial.

En consecuencia, la clasificación y acceso a la información debe responder a un análisis integral que permita equilibrar dichos regímenes, evitando tanto la restricción injustificada del acceso como la divulgación indebida de información protegida.

4. NATURALEZA DE LA INFORMACIÓN EN LA EMPRESA DE SERVICIOS PÚBLICOS DE SABANETA E.S.P. EAPSA

En atención a las funciones, competencias y actividades desarrolladas por la Empresa de Servicios Públicos de Sabaneta EAPSA E.S.P., la información que esta produce, administra o custodia responde a distintas finalidades y procedimientos jurídicos.

En este sentido, para efectos de su adecuada clasificación, tratamiento y control de acceso, la información en EAPSA puede agruparse en las siguientes categorías funcionales:

4.1. Información administrativa y de gestión pública

Corresponde a aquella generada en desarrollo de la función administrativa y de la gestión institucional, vinculada al cumplimiento de los fines del Estado y al principio de transparencia.

Incluye, entre otros:

- Plan Anual de Adquisiciones
- Informes de gestión
- Ejecución presupuestal
- Actos administrativos
- Documentos de planeación institucional

Esta información, por regla general, tiene carácter público, sin perjuicio de las excepciones legales

4.2. Información personal

Comprende la información asociada a personas naturales identificadas o identificables, cuyo tratamiento se encuentra regulado por el régimen de protección de datos personales.

Incluye entre otros:

- Información de usuarios de los servicios públicos
- Datos de empleados y ex empleados
- Información de contratistas y proveedores

El acceso y tratamiento de esta información deberá sujetarse a los principios y condiciones establecidos en la normativa aplicable, especialmente en lo relacionado con autorización, finalidad, necesidad y seguridad.

4.3. Información técnica y operativa

Corresponde a aquella relacionada con la operación de los servicios públicos y la infraestructura administrada por la entidad.

Incluye, entre otros:

- Planos y diseños técnicos.
- Información de redes, sistemas e infraestructura.
- Protocolos operativos
- Información sobre mantenimiento y operación de activos

Esta información puede tener restricciones de acceso cuando su divulgación comprometa la seguridad de la infraestructura, la continuidad del servicio o la integridad de los sistemas.

4.4. Información contractual y precontractual

Comprende aquella generada en el marco de los procesos de contratación adelantados por la entidad, tanto en su etapa de estructuración como de ejecución.

Incluye entre otros:

- Estudios y documentos previos
- Invitaciones
- Ofertas presentadas
- Informes de evaluación
- Contrato
- Actas de inicio
- Informes de gestión e informes de supervisión.

Si bien en principio esta información se encuentra sujeta a publicidad, su acceso debe analizarse de manera diferenciada según la modalidad contractual, etapa del proceso y el impacto que su divulgación pueda generar en la transparencia, la selección objetiva y la adecuada ejecución contractual vs la estrategia comercial de la empresa, teniendo en cuenta que los secretos comerciales están sujetos a reserva, por lo que antes de proceder a publicar o difundir la información debe validarse esta situación.

4.5. Información jurídica

Corresponde a aquella relacionada con la gestión jurídica de la entidad y la defensa de sus intereses.

Incluye entre otros:

- Conceptos jurídicos
- Estrategias de defensa judicial
- Documentos asociados a procesos litigiosos
- Actuaciones administrativas con implicaciones jurídicas

Esta información puede estar sujeta a reserva cuando su divulgación comprometa la posición jurídica de la entidad.

4.6. Información estratégica y negocial

Comprende aquella vinculada a la toma de decisiones estratégicas y a la participación de la entidad en escenarios de estructuración de proyectos, alianzas, contratos o modelos de negocio.

Incluye:

- Modelos financieros
- Estructuración de proyectos
- Estrategias de negociación
- Análisis de viabilidad
- Información comercial o competitiva
- Know-how institucional

La divulgación de esta información puede afectar la posición institucional, económica o contractual de la entidad, por lo que su tratamiento exige un nivel especial de protección, particularmente en atención a la naturaleza de EAPSA como Empresa Industrial y Comercial del Estado.

5. PRECISIÓN CONCEPTUAL SOBRE LAS CATEGORÍAS DE INFORMACIÓN

Para efectos del presente concepto, resulta necesario precisar el alcance de las distintas categorías jurídicas aplicables a la información en poder de la entidad, con el fin de evitar confusiones conceptuales que puedan derivar en restricciones indebidas de acceso o en la divulgación no autorizada de información protegida.

5.1. Información pública

Corresponde a toda información en posesión, bajo control o custodia de la entidad, que no se encuentra sometida a reserva o clasificación legal.

En virtud del principio de máxima divulgación, esta constituye la regla general, y su acceso debe garantizarse de manera efectiva, oportuna y completa.

5.2. Información clasificada

Es aquella información que, aun estando en poder de la entidad, se encuentra protegida en razón de los derechos fundamentales de las personas, en particular el derecho a la intimidad.

En esta categoría se ubica, principalmente, la información que contiene datos personales, cuyo acceso está limitado en los términos de la normativa de protección de datos personales.

5.3. Información reservada

Corresponde a aquella información cuya divulgación puede afectar intereses públicos o institucionales legítimos, y que por disposición legal puede ser sustraída del acceso público.

En esta categoría se incluyen, entre otros:

- Estrategias jurídicas
- Información relacionada con la defensa judicial
- Información técnica crítica
- Información que comprometa la seguridad o funcionamiento de la entidad

La reserva debe estar debidamente justificada y no puede extenderse más allá de lo estrictamente necesario.

5.4. Datos sensibles

En los términos de la Ley 1581 de 2012, los datos sensibles son aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación, tales como:

- Datos biométricos
- Información sobre salud
- Convicciones políticas o religiosas

Estos datos cuentan con una protección reforzada y su tratamiento está sujeto a condiciones estrictas.

5.5. Alcance del concepto de “información sensible” en EAPSA

En el ordenamiento jurídico colombiano, la expresión “información sensible” no constituye una categoría autónoma de clasificación de la información en el marco del derecho de acceso a la información pública.

En consecuencia, su uso debe entenderse como un criterio material de análisis, orientado a identificar aquellos casos en los cuales la información requiere un nivel de protección reforzada.

Para efectos de EAPSA, se considerará que una información reviste carácter sensible cuando:

- i) Contiene datos sensibles en los términos de la normativa de protección de datos personales;
- ii) Se encuentra amparada por una causal de clasificación o reserva legal; o
- iii) Su divulgación tiene la potencialidad de afectar de manera significativa la posición jurídica, contractual, económica o estratégica de la entidad.

En este sentido, el carácter sensible de la información deriva del riesgo asociado a su acceso, uso o divulgación, lo cual exige un análisis contextual en cada caso concreto.

6. CRITERIOS DE CLASIFICACIÓN DE LA INFORMACIÓN

La clasificación de la información en la Empresa de Servicios Públicos de Sabaneta EAPSA E.S.P. obedece a un ejercicio de análisis jurídico y funcional que debe considerar tanto el régimen normativo aplicable como el riesgo asociado a su acceso, uso o divulgación.

En este sentido, la clasificación deberá realizarse de manera caso a caso, atendiendo los criterios que se desarrollan a continuación:

6.1. Criterio de naturaleza jurídica de la información

La información deberá clasificarse inicialmente en función del régimen jurídico que le resulte aplicable, así:

- Información pública: Aquella que no se encuentra sujeta a restricciones legales y cuyo acceso constituye la regla general.
- Información clasificada: Aquella protegida por involucrar datos personales o derechos fundamentales de terceros.
- Información reservada: Aquella cuya divulgación puede afectar intereses públicos o institucionales y que se encuentra amparada por una causal legal de reserva.

6.2. Criterio de contenido de la información

Se deberá analizar el contenido material de la información, en particular si:

- Contiene datos personales o datos sensibles;
- Incorpora información técnica crítica;
- Incluye elementos de carácter jurídico, estratégico o financiero;
- Hace parte de procesos contractuales o decisiones institucionales en curso.

6.3. Criterio de finalidad y contexto de la información

La clasificación deberá considerar el contexto en el cual se produce y utiliza la información, especialmente cuando esta se encuentra vinculada a:

- Procesos precontractuales o contractuales en curso;
- Actuaciones administrativas en etapa de decisión;
- Estrategias jurídicas o de defensa institucional;
- Procesos de estructuración de proyectos o negocios.

En estos casos, la divulgación anticipada o indiscriminada puede afectar la transparencia del proceso o la posición institucional de la entidad.

6.4. Criterio de riesgo por divulgación

Se deberá evaluar el impacto potencial que tendría el acceso o divulgación de la información, considerando, entre otros, los siguientes riesgos:

- Afectación de derechos fundamentales de terceros;
- Compromiso de la seguridad o continuidad del servicio;
- Alteración de procesos contractuales o de selección;
- Pérdida de ventaja en escenarios de negociación;
- Debilitamiento de la posición jurídica de la entidad;
- Impacto económico o reputacional.

A mayor nivel de riesgo, mayor deberá ser el nivel de restricción o control en el acceso.

6.5. Criterio de temporalidad

La clasificación de la información no es estática, por lo que deberá evaluarse si:

- La información está asociada a procesos en curso;
- Existen condiciones que justifican una reserva temporal;
- La información puede ser divulgada una vez finalizado el proceso correspondiente.

6.6. Criterio de función y rol del solicitante

En el caso de acceso interno, deberá considerarse:

- Las funciones del servidor público o contratista;
- El nivel de responsabilidad dentro del proceso;
- La necesidad real de acceso para el cumplimiento de sus obligaciones.

6.7. Integración de los criterios de clasificación

La clasificación de la información en EAPSA deberá resultar de la evaluación conjunta de los criterios anteriormente señalados, evitando decisiones automáticas o basadas exclusivamente en la denominación del documento.

En consecuencia, una misma tipología documental podrá tener distintos niveles de acceso dependiendo de su contenido, contexto, finalidad y riesgo asociado.

7. CRITERIOS PARA DETERMINAR EL NIVEL DE SENSIBILIDAD DE LA INFORMACIÓN

Sin perjuicio de la clasificación jurídica de la información, en la Empresa de Servicios Públicos de Sabaneta EAPSA E.S.P. deberá realizarse un análisis adicional orientado a determinar el nivel de sensibilidad de la información, entendido como el grado de riesgo asociado a su acceso, uso o divulgación.

Este análisis permite establecer medidas de protección diferenciadas y justificar restricciones de acceso en aquellos casos en que, aun tratándose de información no sometida expresamente a reserva legal, su divulgación pueda generar impactos relevantes para la entidad o para terceros.

7.1. Criterio de afectación de derechos fundamentales

Se considerará de alta sensibilidad la información que:

- Contenga datos personales, especialmente datos sensibles;
- Permita la identificación directa o indirecta de personas;
- Pueda afectar la intimidad, seguridad o dignidad de los titulares.

7.2. Criterio de impacto jurídico

Se considerará de alta sensibilidad la información cuya divulgación pueda:

- Comprometer la defensa jurídica de la entidad;
- Revelar estrategias litigiosas o posiciones jurídicas;

- Incidir en actuaciones administrativas en curso;
- Generar riesgos de responsabilidad para la entidad.

7.3. Criterio de impacto contractual

Se considerará de alta sensibilidad la información que:

- Haga parte de procesos precontractuales o contractuales en curso;
- Revele criterios de evaluación, análisis comparativos o decisiones internas;
- Pueda afectar la transparencia, la selección objetiva o la igualdad entre proponentes;
- Incida en la ejecución o equilibrio económico de los contratos.

7.4. Criterio de impacto económico y financiero

Se considerará de alta sensibilidad la información que:

- Contenga modelos financieros, proyecciones o estructuras de costos;
- Revele condiciones económicas de negociación;
- Permita inferir estrategias de inversión o sostenibilidad financiera;
- Pueda generar afectación patrimonial directa o indirecta a la entidad.

7.5. Criterio de impacto estratégico y negocial

Se considerará de alta sensibilidad la información que:

- Esté asociada a la estructuración de proyectos o alianzas;
- Revele estrategias de negociación o toma de decisiones;
- Contenga información comercial o competitiva;
- Constituya know-how institucional o ventaja operativa.

7.6. Criterio de impacto operativo y de seguridad

Se considerará de alta sensibilidad la información cuya divulgación pueda:

- Comprometer la seguridad de la infraestructura o de los sistemas;
- Afectar la continuidad o calidad del servicio público;
- Exponer vulnerabilidades operativas o técnicas.

7.7. Criterio de impacto reputacional

Se considerará de alta sensibilidad la información que, en caso de uso indebido o descontextualización, pueda:

- Generar afectaciones a la confianza institucional;
- Impactar la imagen de la entidad;
- Desencadenar riesgos comunicacionales o de percepción pública.

7.8. Determinación del nivel de sensibilidad

El nivel de sensibilidad de la información deberá establecerse a partir de la evaluación integral de los criterios anteriormente señalados, pudiendo clasificarse, para efectos operativos, en:

- Sensibilidad baja: Información cuya divulgación no genera impactos relevantes.
- Sensibilidad media: Información que requiere control en su acceso, sin implicar restricción absoluta.
- Sensibilidad alta: Información cuya divulgación puede generar impactos significativos jurídicos, económicos, contractuales o institucionales, y que exige medidas reforzadas de protección.

7.9. Carácter dinámico de la sensibilidad

El nivel de sensibilidad de la información no es estático, por lo que deberá ser revisado periódicamente, en especial cuando:

- Finalicen procesos contractuales o administrativos;
- Se modifique el contexto en el cual fue generada la información;
- Desaparezcan las condiciones que justificaban su restricción.

• 8. CRITERIOS PARA EL ACCESO A LA INFORMACIÓN

El acceso a la información en la Empresa de Servicios Públicos de Sabaneta EAPSA E.S.P. deberá garantizar, de manera armónica, el principio de transparencia y el derecho de acceso a la información pública, con la protección de los datos personales y la salvaguarda de la información estratégica, contractual y negocial de la entidad.

En consecuencia, el acceso a la información no es absoluto y deberá analizarse en cada caso concreto, atendiendo a los criterios que se desarrollan a continuación.

8.1. Acceso externo a la información

El acceso por parte de ciudadanos, entes de control u otras entidades deberá regirse por las siguientes reglas:

8.1.1. Regla general de acceso

Toda información en poder de la entidad se presume pública y deberá ser suministrada, salvo que se encuentre sometida a clasificación o reserva legal debidamente justificada.

8.1.2. Límites al acceso

El acceso podrá restringirse cuando:

- La información tenga carácter clasificado por contener datos personales;
- Se encuentre amparada por reserva legal;
- Su divulgación afecte procesos contractuales en curso;
- Comprometa la defensa jurídica de la entidad;
- Revele información estratégica, económica o negocial.

En estos casos, la restricción deberá ser proporcional, motivada y limitada a lo estrictamente necesario.

8.1.3. Acceso parcial y anonimización

Cuando la información solicitada contenga elementos públicos y protegidos, la entidad deberá:

- Suministrar la información pública;
- Restringir o suprimir la información protegida;
- Aplicar técnicas de anonimización o disociación cuando sea procedente.

8.1.4. Temporalidad del acceso

En materia contractual, jurídica y negocial, la restricción de acceso podrá tener carácter temporal, de manera que la información pueda ser divulgada una vez desaparezcan las condiciones que justificaban su reserva.

8.2. Acceso interno a la información

El acceso por parte de servidores públicos y contratistas deberá regirse por criterios funcionales y de control.

8.2.1. Principio de finalidad

El acceso a la información deberá responder a una finalidad legítima relacionada con el ejercicio de funciones o el cumplimiento de obligaciones contractuales.

8.2.2. Principio de necesidad

Los usuarios internos solo podrán acceder a la información estrictamente necesaria para el desarrollo de sus actividades.

8.2.3. Principio de rol y competencia

El acceso deberá estar determinado por:

- El rol dentro del proceso;
- El nivel de responsabilidad;
- Las funciones asignadas.

No todo servidor o contratista puede acceder a toda la información.

8.2.4. Principio de confidencialidad

Los servidores públicos y contratistas deberán garantizar la reserva de la información a la que acceden, especialmente cuando esta tenga carácter clasificado, reservado o sensible.

8.2.5. Principio de trazabilidad

El acceso a información de nivel medio o alto de sensibilidad deberá permitir:

- Identificar quién accede;
- Cuándo accede;
- Para qué accede.

8.3. Reglas especiales de acceso en escenarios contractuales y negociales

En atención a la naturaleza de EAPSA como Empresa Industrial y Comercial del Estado, el acceso a la información en escenarios contractuales y negociales deberá sujetarse a reglas especiales:

8.3.1. Protección de procesos en curso

No se deberá divulgar información que:

- Afecte la igualdad entre proponentes;
- Revele evaluaciones internas antes de su consolidación;
- Incida en decisiones aún no adoptadas formalmente.

8.3.2. Protección de estrategias y negociación

Se deberá restringir el acceso a información que:

- Revele estrategias de negociación;
- Contenga modelos financieros o estructuras económicas;
- Permita anticipar decisiones institucionales.

8.3.3. Publicidad condicionada

La información podrá hacerse pública una vez:

- Finalicen los procesos correspondientes;
- Se adopten las decisiones institucionales;
- Desaparezcan las condiciones que justificaban su restricción.

8.4. Deber de motivación

Toda decisión de restricción, limitación o denegación de acceso a la información deberá:

- Estar debidamente motivada;
- Fundarse en una causal legal o en un criterio de protección debidamente justificado;
- Ser proporcional al riesgo que se pretende evitar.

• 9. REGLAS ESPECIALES PARA LA GESTIÓN DE INFORMACIÓN CONTRACTUAL Y NEGOCIAL

En atención a la naturaleza de la Empresa de Servicios Públicos de Sabaneta EAPSA E.S.P. como Empresa Industrial y Comercial del Estado, y a su participación en escenarios de contratación, estructuración de proyectos y gestión negocial, la información generada en estos ámbitos deberá ser objeto de un tratamiento diferenciado.

Lo anterior, en la medida en que su divulgación puede incidir directamente en la transparencia de los procesos, la selección objetiva, la adecuada ejecución contractual y la protección de los intereses institucionales.

9.1. Información en etapa precontractual

Durante la etapa de estructuración y planeación de los procesos contractuales, la información deberá gestionarse bajo criterios de reserva funcional, especialmente cuando se trate de:

- Estudios y análisis previos en construcción;

- Estructuración técnica, jurídica y financiera;
- Modelos de negocio o esquemas de operación;
- Análisis de mercado o de viabilidad;
- Borradores de documentos del proceso.

La divulgación de esta información antes de su consolidación puede afectar la objetividad del proceso, inducir comportamientos estratégicos de los interesados o comprometer la adecuada estructuración contractual.

9.2. Información en etapa de selección

Durante los procesos de selección, el acceso a la información deberá garantizar la transparencia, pero sin afectar la igualdad entre proponentes ni la imparcialidad de la evaluación.

En consecuencia:

- Las ofertas tendrán el tratamiento previsto en la normativa aplicable, garantizando su integridad y confidencialidad cuando corresponda;
- Los informes de evaluación tendrán carácter reservado hasta tanto no sean consolidados y publicados oficialmente;
- No se deberá divulgar información que permita inferir anticipadamente el sentido de la decisión o que genere ventajas indebidas para alguno de los proponentes.

9.3. Información en etapa contractual (ejecución)

Durante la ejecución del contrato, la información deberá gestionarse de manera diferenciada según su naturaleza:

- Será pública aquella relacionada con la ejecución general del contrato, en los términos de la normativa aplicable;
- Tendrá acceso restringido aquella que contenga información técnica, financiera o estratégica que pueda afectar la ejecución, el equilibrio económico o los intereses de las partes;
- Deberá protegerse la información que constituya know-how, condiciones económicas específicas o información sensible del contratista o de la entidad.

9.4. Información en procesos de negociación y estructuración de proyectos

En escenarios de estructuración de proyectos, alianzas estratégicas, convenios o esquemas de colaboración, la información deberá ser tratada con un nivel reforzado de protección, en particular cuando:

- Se estén definiendo condiciones económicas o técnicas;

- Existan intercambios de información con potenciales aliados;
- Se adelanten análisis de viabilidad o estructuración financiera;
- Se construyan modelos de operación o distribución de riesgos.

La divulgación de esta información puede afectar la posición negociadora de la entidad y comprometer el resultado del proceso.

9.5. Publicidad diferida de la información

En los casos en que la divulgación de la información contractual o comercial pueda afectar el desarrollo de los procesos, la entidad podrá aplicar criterios de publicidad diferida, de manera que:

- La información se haga pública una vez finalice la etapa correspondiente;
- Se adopten las decisiones institucionales;
- Desaparezcan las condiciones que justificaban su restricción.

Este criterio resulta especialmente aplicable en etapas de evaluación, negociación o estructuración.

9.6. Protección de información estratégica y confidencial

La entidad deberá adoptar medidas para proteger la información que:

- Constituya ventaja competitiva o estratégica;
- Haya sido entregada bajo acuerdos de confidencialidad;
- Corresponda a secretos empresariales o comerciales;
- Haga parte de modelos técnicos o financieros propios o de terceros.

En estos casos, el acceso deberá restringirse y su uso limitarse a los fines para los cuales fue suministrada.

9.7. Articulación con los deberes de transparencia

Las reglas aquí previstas no implican la eliminación del principio de publicidad, sino su aplicación razonada y proporcional, de manera que:

- Se garantice el acceso a la información pública;
- Se protejan los procesos contractuales y comerciales;
- Se eviten riesgos jurídicos, económicos y operativos para la entidad.

• 10. RESPONSABILIDAD DERIVADA DEL MANEJO DE LA INFORMACIÓN

El manejo inadecuado de la información por parte de los servidores públicos y contratistas de la Empresa de Servicios Públicos de Sabaneta EAPSA E.S.P. puede generar diferentes tipos de responsabilidad, en función de la naturaleza de la conducta y del daño ocasionado.

En este sentido, la clasificación, tratamiento y acceso a la información constituyen una actuación sujeta a deberes legales y funcionales cuyo incumplimiento puede acarrear consecuencias jurídicas.

10.1. Responsabilidad administrativa y sancionatoria

El tratamiento indebido de datos personales puede dar lugar a investigaciones y sanciones por parte de la autoridad competente, en particular cuando se presenten conductas como:

- Acceso no autorizado a información personal;
- Uso de datos para finalidades distintas a las autorizadas;
- Falta de implementación de medidas de seguridad;
- Divulgación indebida de datos sensibles.

Estas conductas pueden derivar en sanciones administrativas, incluidas multas, órdenes de suspensión de actividades y demás medidas previstas en la normativa aplicable.

10.2. Responsabilidad disciplinaria

Los servidores públicos que incumplan los deberes relacionados con el manejo de la información podrán incurrir en falta disciplinaria, especialmente cuando:

- Divulguen información sometida a reserva;
- Permitan el acceso indebido a información clasificada o sensible;
- Omitan los controles necesarios para la protección de la información;
- Utilicen la información en beneficio propio o de terceros.

10.3. Responsabilidad fiscal

Cuando el manejo inadecuado de la información genere un daño al patrimonio público, podrá configurarse responsabilidad fiscal, en particular en aquellos casos en que:

- La divulgación de información afecte procesos contractuales o negociaciones;
- Se generen perjuicios económicos derivados de la pérdida de ventajas estratégicas;
- Se comprometa la adecuada ejecución de recursos públicos.

10.4. Responsabilidad contractual

Los contratistas que accedan a información de la entidad estarán sujetos a deberes de confidencialidad y uso adecuado de la información, cuyo incumplimiento puede dar lugar a:

- Imposición de cláusulas penales;
- Declaratorias de incumplimiento;
- Terminación contractual;
- Indemnización de perjuicios.

10.5. Responsabilidad penal

En casos graves, el uso indebido de la información puede configurar conductas punibles, especialmente cuando:

- Se acceda de manera ilícita a sistemas de información;
- Se revele información reservada con ánimo de causar daño o beneficio indebido;
- Se utilice la información para la comisión de delitos contra la administración pública.

10.6. Deber reforzado de diligencia

En atención a los riesgos asociados al manejo de la información, los servidores públicos y contratistas de EAPSA deberán actuar con un deber reforzado de diligencia, que implica:

- Aplicar los criterios de clasificación y acceso definidos por la entidad;
- Verificar la naturaleza de la información antes de su divulgación;
- Adoptar medidas de seguridad y control;
- Abstenerse de utilizar la información para fines distintos a los autorizados.

• 11. CONCLUSIONES

1. La gestión de la información en la Empresa de Servicios Públicos de Sabaneta EAPSA E.S.P. no puede abordarse exclusivamente desde el principio de transparencia ni desde el régimen de protección de datos personales, sino que exige un análisis integral que articule dichos regímenes con la naturaleza jurídica de la entidad como Empresa Industrial y Comercial del Estado.
2. La clasificación de la información es un ejercicio reglado que debe sustentarse en criterios jurídicos, funcionales y de riesgo, orientados a garantizar tanto el acceso a la información pública como la protección de los derechos fundamentales y de los intereses institucionales.
3. El concepto de “información sensible” constituye un criterio material que permite identificar aquellos casos en los cuales la información requiere un nivel de protección reforzada, en función del impacto que su divulgación pueda generar.

4. En el contexto de EAPSA, resulta especialmente relevante la protección de la información de carácter contractual, jurídico y negocial, cuya divulgación puede afectar la transparencia de los procesos, la selección objetiva, la posición jurídica de la entidad y su sostenibilidad económica.
5. El acceso a la información debe analizarse de manera caso a caso, atendiendo su naturaleza, contenido, contexto y nivel de riesgo, evitando tanto la restricción injustificada del acceso como la divulgación indebida de información protegida.

- **12. RECOMENDACIONES**

1. **Adopción de un Índice de Información Clasificada y Reservada:** Se recomienda a la entidad estructurar, actualizar y adoptar formalmente un índice de información Clasificada y Reservada, en el cual se identifiquen las tipologías de información que, en el contexto de EAPSA, se encuentran sujetas a restricciones de acceso, incluyendo aquellas de carácter contractual, jurídico y negocial. Este instrumento deberá ser dinámico y revisado periódicamente.
2. **Definición de un procedimiento interno de clasificación de la información.** Se recomienda establecer un procedimiento institucional que permita a los líderes de proceso clasificar la información bajo criterios jurídicos, funcionales y de riesgo, conforme a lo desarrollado en el presente concepto.

Dicho procedimiento deberá incluir:

- Responsables de la clasificación;
 - Momentos de revisión (creación, uso, archivo);
 - Criterios de actualización de la clasificación;
 - Mecanismos de control y validación.
3. **Incorporación del manejo de la información en la matriz de riesgos institucional**
Se recomienda incluir el manejo, acceso y divulgación de la información como un riesgo institucional, particularmente en las categorías de:
 - Riesgo operativo;
 - Riesgo jurídico;
 - Riesgo de cumplimiento;
 - Riesgo reputacional.

Lo anterior permitirá implementar controles preventivos y correctivos asociados al tratamiento de la información.

4. **Definición de lineamientos para la publicación de información en plataformas como SECOP**

Se recomienda establecer criterios claros sobre:

- Qué información debe publicarse;
- En qué momento debe publicarse;
- Qué información debe ser objeto de reserva o publicidad diferida;
- Cómo debe aplicarse la anonimización de datos personales.

Estos lineamientos deberán armonizar el principio de transparencia con la protección de la información estratégica y contractual.

5. Implementación de protocolos de acceso y control de la información

Se recomienda adoptar mecanismos que permitan:

- Controlar el acceso a la información según el rol del usuario;
- Garantizar la trazabilidad de los accesos;
- Definir niveles de acceso según la sensibilidad de la información;
- Establecer medidas de seguridad para la protección de la información.

6. Fortalecimiento de cláusulas contractuales de confidencialidad

Se recomienda incorporar en los contratos suscritos por la entidad cláusulas específicas que regulen:

- El acceso a la información por parte del contratista;
- El uso limitado de la información;
- Las obligaciones de confidencialidad;
- Las consecuencias del uso indebido de la información.

7. Capacitación a servidores públicos y contratistas

Se recomienda adelantar procesos de capacitación orientados a:

- La correcta clasificación de la información;
- El manejo de datos personales;
- La identificación de información sensible;
- Los riesgos asociados a la divulgación indebida.

8. Revisión periódica de la clasificación y nivel de sensibilidad de la información

Se recomienda establecer mecanismos de revisión periódica de la clasificación de la información, especialmente en aquellos casos en que:

- Finalicen procesos contractuales o administrativos;
- Cambien las condiciones que justificaban su reserva;
- Se requiera ajustar su nivel de protección.

• **13. LINEAMIENTOS OPERATIVOS PARA LA CLASIFICACIÓN, ACCESO Y CONTROL DE LA INFORMACIÓN**

Con el fin de garantizar la adecuada aplicación de los criterios definidos en el presente concepto, se establecen los siguientes lineamientos operativos para la gestión de la información en la Empresa de Servicios Públicos de Sabaneta EAPSA E.S.P.

13.1. Responsables del proceso de clasificación de la información

La clasificación de la información será responsabilidad de:

- **Primera Línea de Defensa (líderes de proceso):** Encargados de identificar, clasificar y aplicar los criterios de acceso a la información generada o administrada en el marco de sus funciones.
- **Segunda Línea de Defensa (gestión jurídica):** Encargada de definir lineamientos, asesorar en la clasificación y validar criterios en casos complejos o de alto impacto.
- **Tercera Línea de Defensa (control interno):** Encargada de evaluar la efectividad de los controles asociados a la gestión de la información.

13.2. Momento de la clasificación de la información

La clasificación deberá realizarse en los siguientes momentos:

- Al momento de la creación o recepción de la información
- Durante su utilización en procesos administrativos, contractuales o jurídicos
- Al momento de su archivo o disposición final

La clasificación podrá ser ajustada cuando cambien las condiciones que dieron lugar a su determinación.

13.3. Procedimiento básico de clasificación

Para clasificar la información, el responsable deberá:

1. Identificar la naturaleza de la información
2. Determinar el régimen jurídico aplicable: (pública, clasificada o reservada)
3. Evaluar el nivel de sensibilidad conforme a los criterios de riesgo definidos en el presente concepto
4. Definir el nivel de acceso (libre, restringido, controlado o reservado)

5. Documentar la decisión de clasificación, cuando se trate de información de nivel medio o alto de sensibilidad

13.4. Niveles operativos de acceso

Para efectos de gestión interna, se establecen los siguientes niveles de acceso:

- **Acceso libre:** Información pública sin restricciones.
- **Acceso controlado:** Información accesible a usuarios autorizados según su rol.
- **Acceso restringido:** Información de sensibilidad media o alta, cuyo acceso requiere validación previa.
- **Acceso reservado:** Información de alta sensibilidad o con reserva legal, con acceso limitado a personal autorizado.

13.5. Control de acceso a la información

La entidad deberá implementar mecanismos que permitan:

- Asignar accesos conforme al rol del usuario;
- Restringir el acceso a información sensible;
- Garantizar la trazabilidad de los accesos;
- Prevenir el acceso no autorizado o el uso indebido de la información.

13.6. Gestión de la información en procesos contractuales

En los procesos contractuales, los responsables deberán:

- Verificar el nivel de clasificación de la información antes de su publicación;
- Aplicar criterios de anonimización cuando sea necesario;
- Evaluar la procedencia de la publicidad diferida;
- Evitar la divulgación de información que afecte la selección objetiva o la negociación.

13.7. Manejo de información por parte de contratistas

Los contratistas que accedan a información de la entidad deberán:

- Utilizarla exclusivamente para los fines contractuales;
- Garantizar su confidencialidad;
- Abstenerse de divulgarla sin autorización;
- Adoptar medidas de seguridad adecuadas para su protección.

13.8. Revisión y actualización de la clasificación

La clasificación de la información deberá ser objeto de revisión:

- Cuando finalicen procesos contractuales o administrativos;
- Cuando cambien las condiciones de riesgo;
- Cuando se requiera su divulgación posterior;
- De manera periódica, conforme a los lineamientos institucionales.

13.9. Registro y soporte de decisiones

Las decisiones relacionadas con la clasificación, restricción o limitación del acceso a la información deberán:

- Estar debidamente soportadas;
- Basarse en criterios jurídicos y de riesgo;
- Ser verificables en caso de auditoría o requerimiento de autoridad competente.