1. OBJETIVO

Establecer la metodología para el registro y el almacenamiento seguro de la información generada en el laboratorio, incluyendo resultados de pruebas, datos de control de calidad y notificaciones, garantizando su integridad, confidencialidad y trazabilidad.

2. ALCANCE

Este procedimiento aplica a toda la información generada por el personal del laboratorio durante la ejecución de las pruebas y los procesos de control de calidad, desde su creación hasta su archivo final.

3. RESPONSABLES

Responsable de la Información	• Identificar, clasificar y custodiar la información a su cargo conforme a su nivel de confidencialidad, clasificación o reserva. • Atender de manera inmediata los eventos de fuga o exposición de información relacionados con los documentos o datos bajo su responsabilidad. • Definir, implementar y documentar los controles de mitigación y corrección cuando se materialice un riesgo de confidencialidad. • Formular, ejecutar y hacer seguimiento al Plan de Acción correspondiente al tipo documental afectado. • Reportar oportunamente los incidentes y las acciones adoptadas a la Oficina de Control Interno y a las instancias que correspondan.
Jefe de Oficina de Control Interno	• Verificar la correcta aplicación del procedimiento y el cumplimiento de la normatividad vigente en materia de manejo de la información. • Evaluar la efectividad de los controles implementados y del Plan de Acción definido frente al incidente. • Emitir recomendaciones, requerir ajustes y realizar seguimiento a las acciones correctivas y preventivas. • Informar a la Gerencia General sobre los incidentes relevantes y los resultados del seguimiento efectuado.
Auxiliar Administrativo de Archivo	• Garantizar la adecuada custodia, organización y protección de la documentación física bajo su responsabilidad. • Implementar las medidas de control físico necesarias para la protección de la información intervenida. • Registrar y conservar las evidencias documentales relacionadas con el incidente y las acciones adoptadas.
Profesional del Sistema Integrado de Gestión (SIG)	• Asesorar técnicamente la aplicación del procedimiento y su alineación con el Sistema Integrado de Gestión. • Apoyar la identificación, clasificación y valoración del riesgo asociado al incidente de confidencialidad. • Verificar la correcta formulación y seguimiento del Plan de Acción dentro del ciclo de mejora continua. • Mantener actualizados los registros, matrices y documentos del SIG relacionados con el manejo de la información.
Líder del Proceso y Responsables	• Garantizar la aplicación del procedimiento dentro del proceso a su cargo.

	• Reportar de manera inmediata cualquier evento de fuga o exposición de información. • Colaborar en la implementación de los controles de mitigación y las acciones definidas en el Plan de Acción. • Velar por el cumplimiento de las políticas de confidencialidad y manejo seguro de la información por parte del personal del proceso.
4. DEFINICIONES / TERMINOLOGÍA	
Acceso a la Información	Facultad otorgada a una persona natural o jurídica para consultar, usar o tratar información institucional, de acuerdo con su rol, funciones, nivel de autorización y el principio de necesidad de conocer.
Archivo Central	Unidad responsable de la custodia, organización, conservación, control y préstamo de la documentación transferida desde los archivos de gestión, conforme a la Ley General de Archivos y las Tablas de Retención Documental vigentes.
Clasificación de la Información	Proceso mediante el cual la Entidad determina el nivel de protección aplicable a la información institucional (confidencial, clasificada, reservada o pública), atendiendo su naturaleza, contenido, sensibilidad, riesgos asociados y marco normativo vigente.
Confidencialidad	Principio mediante el cual se garantiza que la información solo sea conocida, consultada o utilizada por personas debidamente autorizadas, evitando accesos, usos, divulgaciones o tratamientos no autorizados.
Datos Personales	Cualquier información vinculada o que pueda asociarse a una persona natural determinada o determinable, de conformidad con la Ley 1581 de 2012.
Excepción al Acceso a la Información	Limitación legal, total o parcial, al derecho de acceso a la información pública, fundamentada en causales constitucionales o legales, que impide su divulgación por razones de confidencialidad, reserva o clasificación.
Fuga o Exposición de Información	Evento mediante el cual la información confidencial, clasificada o reservada es divulgada, accedida, utilizada o transmitida sin autorización, ya sea de manera accidental o intencional.
Incidente de Confidencialidad	Cualquier evento real o potencial que comprometa la confidencialidad, integridad o disponibilidad de la información institucional.
Seguridad de la Información	Conjunto de políticas, controles y medidas orientadas a proteger la confidencialidad, integridad y disponibilidad de la información institucional.
Trazabilidad de la Información	Capacidad de identificar y seguir el historial de creación, acceso, uso, modificación, transferencia y disposición de la información.
5. POLÍTICAS DE OPERACIÓN	
PRINCIPIO GENERAL DE CONFIDENCIALIDAD Toda la información generada, tratada, almacenada o transmitida por la Entidad se considera confidencial, salvo aquella que, por disposición legal o autorización expresa de la Gerencia General, tenga carácter público.	

El personal y demás terceros autorizados deberán proteger dicha información frente a accesos, usos, divulgaciones, alteraciones, pérdidas o destrucciones no autorizadas, garantizando en todo momento su confidencialidad, integridad y disponibilidad.

CUSTODIA DE LA INFORMACIÓN

Toda la documentación e información generada, recibida o administrada por la Entidad deberá ser registrada, identificada y etiquetada de manera completa, veraz y oportuna desde el momento de su recepción o creación, garantizando su trazabilidad y control institucional.

La documentación e información deberá ser almacenada en medios físicos y/o digitales seguros, protegidos contra daño, pérdida, alteración, uso indebido, robo o acceso no autorizado, mediante la aplicación de controles técnicos, administrativos y físicos definidos por la Entidad.

El acceso a la documentación e información estará estrictamente limitado al personal debidamente autorizado, de acuerdo con su rol, cargo y nivel de responsabilidad, asegurando en todo momento la confidencialidad, integridad y disponibilidad de la información institucional.

La entrega, consulta o divulgación de documentación e información a personas naturales o jurídicas externas a la Entidad solo podrá realizarse previa autorización expresa de la instancia competente y deberá quedar debidamente documentada, dejando constancia de la información suministrada, el destinatario y el motivo de la entrega.

CONTROL DE ACCESO Y MANEJO DE LA INFORMACIÓN

La Entidad cuenta con la Matriz de Índice de Información Clasificada y Reservada, mediante la cual se identifican, clasifican y controlan los distintos tipos de información institucional. El acceso a dicha información será estrictamente restringido y se otorgará únicamente al personal debidamente autorizado, de acuerdo con su rol, cargo, funciones y nivel de accesibilidad definido.

La asignación, modificación o revocatoria de accesos deberá ser autorizada por la instancia competente de la Entidad y documentada formalmente, garantizando el principio de necesidad de conocer, así como la confidencialidad, integridad y uso adecuado de la información.

El personal autorizado será responsable del manejo seguro de la información a la que tenga acceso y deberá cumplir las políticas, procedimientos y lineamientos institucionales establecidos para su protección, custodia y confidencialidad.

CLASIFICACIÓN DE LA INFORMACIÓN

La información institucional se clasifica, para efectos de control y acceso, de la siguiente manera:

Información Confidencial

Es toda información institucional cuyo acceso está restringido para proteger derechos, procesos internos o intereses de la Entidad. Su divulgación no autorizada puede generar riesgos administrativos, legales, reputacionales o técnicos.

Información Clasificada

Es la información que, por su naturaleza o por mandato legal, cuenta con una protección especial, debido a que su divulgación puede afectar derechos fundamentales, la seguridad de la información o el adecuado cumplimiento de la función pública. Su acceso es altamente restringido y se encuentra respaldado por disposiciones legales específicas.

Información Reservada

Es la información que, aunque en principio es de carácter público, se encuentra temporalmente sujeta a restricción por razones legales, estratégicas o administrativas. La reserva se mantendrá vigente durante el tiempo definido o hasta que desaparezcan las causas que la originaron.

DEBER DE RESERVA Y COMPROMISO DE CONFIDENCIALIDAD

Para el acceso y manejo de información confidencial, la Entidad cuenta con la Declaración de Confidencialidad (Global) y, cuando aplique, con el Acta de Confidencialidad correspondiente, las cuales deberán ser suscritas por el personal de la Entidad, contratistas, proveedores, consultores, auditores y particulares ajenos a la Entidad que, por razón de sus funciones, actividades o autorizaciones, tengan acceso a información institucional, antes de acceder a la misma.

El deber de reserva sobre la información a la que se tenga acceso será obligatorio para todos los anteriores y se mantendrá vigente incluso después de finalizada la relación laboral, contractual, funcional o la autorización otorgada, de conformidad con la normatividad vigente.

Apartado Especial –Informes de Resultados de Laboratorio

Los Informes de Resultados de Laboratorio, por su naturaleza técnica, impacto sanitario, regulatorio y reputacional, tendrán un régimen reforzado de control de acceso, adicional a los controles generales del Archivo Central.

Para estos documentos se deberán aplicar, como mínimo, las siguientes medidas:

El acceso estará limitado exclusivamente al personal expresamente autorizado, conforme a su rol, funciones y nivel de accesabilidad definido en la **PM-LAB-MT-02 MATRIZ DE ROLES Y RESPONSABILIDADES DE MANEJO DE INFORMACIÓN LAB**.

Todo acceso, consulta, reproducción, préstamo o remisión deberá contar con autorización previa del Responsable de la Información, la cual deberá quedar documentada y asociada al registro de acceso.

El registro de accesos deberá especificar de manera obligatoria:

- Tipo de informe (físico-químico, microbiológico u otro).
- Código o identificación del informe.
- Fecha de emisión y estado del informe (preliminar, validado, publicado).
- Finalidad específica del acceso.

Los informes en estado preliminar o no validados tendrán acceso altamente restringido, prohibiéndose su reproducción, digitalización o divulgación por cualquier medio no autorizado.

La entrega a terceros (entes de control, autoridades sanitarias, usuarios u otros) solo podrá realizarse una vez el informe se encuentre oficialmente validado, mediante canales institucionales, dejando constancia documental de la entrega, receptor, fecha y finalidad.

Así mismo, el personal relacionado en la Matriz **PM-LAB-MT-02 MATRIZ DE ROLES Y RESPONSABILIDADES DE MANEJO DE INFORMACIÓN LAB** deberá abstenerse de divulgar, compartir o transmitir información institucional por medios no autorizados, tales como correos electrónicos personales, aplicaciones de mensajería instantánea, dispositivos externos no institucionales u otros canales que no cuenten con autorización expresa de la Entidad.

ATENCIÓN DE EVENTOS DE FUGA O EXPOSICIÓN DE INFORMACIÓN CONFIDENCIAL, CLASIFICADA O RESERVADA

Notificar de manera inmediata y formal al Responsable de la Información que el riesgo asociado al tipo documental afectado se ha materializado, informando las circunstancias generales del evento, el tipo de información comprometida y el impacto preliminar identificado.

Como resultado de esta notificación, se deberán activar de forma inmediata las acciones de mitigación y corrección, orientadas a contener el incidente, limitar su alcance y evitar la continuidad de la fuga o exposición de la información. Para tal efecto, se solicitará al Responsable de la Información la definición, implementación y remisión de los nuevos controles técnicos, administrativos y documentales que resulten necesarios, en concordancia con la normatividad vigente y los lineamientos institucionales de manejo, custodia y confidencialidad de la información.

FORMULACIÓN Y EJECUCIÓN DEL PLAN DE ACCIÓN PARA EL TIPO DOCUMENTAL INTERVENIDO

El Responsable de la Información deberá formular un Plan de Acción específico para el tipo de documento o información intervenida, en el cual se identifiquen claramente las acciones correctivas y preventivas a implementar, los responsables, los plazos de ejecución y los mecanismos de seguimiento, con el fin de subsanar las causas del incidente, fortalecer los controles existentes y prevenir su recurrencia.

El Plan de Acción deberá considerar, como mínimo:

- El nivel de clasificación de la información (confidencial, clasificada o reservada).
- El medio afectado (físico, digital o mixto).
- Los riesgos asociados al tipo documental.

La ejecución y seguimiento del Plan de Acción deberá quedar debidamente documentada, y su efectividad será evaluada por la instancia competente, conforme a los procedimientos institucionales de control y mejora continua.

6. DESARROLLO DEL PROCEDIMIENTO

No	ACTIVIDAD (QUE)	DESCRIPCIÓN (COMO)	RESPONSABLE (QUIEN)	REGISTRO / DOCUMENTO
1	Identificación y Clasificación de la Información	Toda información generada, recibida, procesada o administrada por la Entidad deberá ser identificada y clasificada desde el momento de su creación o recepción, determinando si corresponde a información confidencial, clasificada, reservada o pública, de conformidad con la Ley 1712 de 2014, la Ley 142 de 1994, la	Responsable de la Información Jefe Oficina de Control Interno	PV-CI-MC-MT-02 Matriz de Índice de Información Clasificada y Reservada

		normatividad de protección de datos personales y los lineamientos institucionales vigentes. La clasificación se realizará mediante la verificación del tipo documental, la finalidad de uso, la presencia de datos personales, datos sensibles, información estratégica, técnica, jurídica o económica, y los riesgos asociados a su divulgación. La información identificada como confidencial, clasificada o reservada deberá registrarse indicando el tipo de excepción (total o parcial) y la vigencia de la restricción (temporal o permanente).		
2	Recepción y Verificación de Documentación	Verificar que toda la documentación e información recibida por la Entidad se encuentre completa, correcta, legible y debidamente autorizada, garantizando su confidencialidad desde el momento de la recepción. Cualquier inconsistencia deberá ser reportada de manera inmediata a la instancia competente.	Auxiliar Administrativo Archivo	PA-ID-GD-FO-02 Registro Recepción de Documentos
3	Almacenamiento y custodia de la información	Almacenar la información física y digital en medios seguros, protegidos contra pérdida, daño, alteración o acceso no autorizado. Los documentos físicos se archivarán en espacios con acceso restringido y los archivos digitales en repositorios institucionales seguros con copias de seguridad periódicas.	Auxiliar Administrativo Archivo	PA-ID-GD-FO-01 Formulario Único de Inventario Documental
4	Identificación del Personal Autorizado	Definir, actualizar y documentar la lista de personas autorizadas para acceder a la información institucional, especificando cargo, rol y nivel de acceso, conforme a las políticas de	Responsable de la Información	PE-SIG-SGC-MT-06 Matriz de Roles Y Responsabilidades de Manejo De Información

		confidencialidad y control de la información.		PM-LAB-MT-02 Matriz de Roles Y Responsabilidades de Manejo De Información De Laboratorio
5	Capacitación en confidencialidad y manejo de la información	Garantizar que todo el personal autorizado reciba capacitación inicial y periódica sobre las políticas de confidencialidad, deber de reserva, uso seguro de la información y prohibición de compartir accesos o utilizar medios no autorizados. *NOTA: Para el Laboratorio de Agua Potable se tiene uso exclusivo el Acta de Confidencialidad, dando cumplimiento a la Política de Confidencialidad, como se establece en el Manual de Calidad de Laboratorio de Agua Potable PM-LAB-MA-01.*	Profesional SIG Líder del Proceso y Responsables	PE-SIG-SGC-FO-21 Declaración de confidencialidad PM-LAB-FO-01 Acta de Confidencialidad PE-SIG-SGC-FO-08 Registro de Asistencia
6	Control y acceso de la información	**Para el Archivo Central** El acceso a la documentación del Archivo Central estará restringido exclusivamente al personal autorizado, conforme a la Matriz de Roles y Responsabilidades y a la Matriz de Índice de Información Clasificada y Reservada. No se permitirá el retiro, reproducción, digitalización o divulgación de documentos sin autorización expresa y registrada. El Auxiliar Administrativo de Archivo será responsable de la verificación previa de la autorización, del diligenciamiento correcto de los registros y del control de los tiempos de préstamo y devolución, mientras que el Responsable de la Información deberá validar y autorizar los accesos según el nivel de clasificación de la información.	Responsable de la Información Auxiliar Administrativo Archivo Líder del Proceso y Responsables	Libros Radicadores PA-DD-GD-FO-02 Registro Préstamo de Documentos PV-CI-MC-MT-02 Matriz de Índice de Información Clasificada y Reservada PE-SIG-SGC-MT-06 Matriz de Roles Y Responsabilidades De Manejo De Información PM-LAB-MT-02 Matriz de Roles Y Responsabilidades De Manejo De Información De Laboratorio

		Para el Archivo de Gestión (Físico / Digital) El acceso a la documentación del Archivo de Gestión de los Líderes y Responsables de procesos estará restringido exclusivamente al personal autorizado, conforme a la Matriz de Roles y Responsabilidades y a la Matriz de Índice de Información Clasificada y Reservada. No se permitirá el retiro, reproducción, digitalización o divulgación de documentos sin autorización expresa y registrada. (*Ver Políticas de Operación / Apartado Especial –Informes de Resultados de Laboratorio)*		
7	Entrega de Información a Terceros	Toda solicitud de información por parte de personas o entidades externas (como auditores, entidades de salud, etc.) debe ser presentada por escrito. El Responsable a cargo de la custodia de la información revisará la solicitud y determinará si se autoriza la entrega. Esta decisión debe basarse en el rol del solicitante y la necesidad de la información. Si se autoriza, se entregará una copia de la información solicitada. Se debe dejar constancia de esta entrega, incluyendo la fecha, la información entregada, el nombre del receptor y la firma de recibido.	Responsable de la Información	Soportes Documentales Externos
8	Monitoreo y auditoría del manejo de la información	Realizar auditorías internas periódicas para verificar el cumplimiento de las políticas de confidencialidad, custodia y control de acceso a la información. Los hallazgos y	Jefe Oficina de Control Interno	PV-CI-AI-FO-03 Informe de Auditorías Internas

		recomendaciones deberán documentarse y comunicarse para su seguimiento y mejora continua.		

PUNTO DE CONTROL

Todas las actividades con puntos de control establecidos.

7. DOCUMENTOS DE REFERENCIA

Constitución Política de Colombia
Ley 87 de 1993. Sistema de Control Interno
Ley 594 de 2000. Ley General de Archivos
Ley 1581 de 2012. Protección de Datos Personales
Ley 1712 de 2014. Transparencia y del Derecho de Acceso a la Información Pública Nacional
Decreto 103 de 2015. Reglamentación parcial de la Ley 1712 de 2014
Decreto 1377 de 2013. Reglamentación parcial de la Ley 1581 de 2012
Decreto 1074 de 2015. Decreto Único Reglamentario del Sector Comercio, Industria y Turismo
Decreto 1078 de 2015. Decreto Único Reglamentario del Sector Tecnologías de la Información y las Comunicaciones
Decreto 648 de 2017. Modificación y adición del Decreto 1083 de 2015 en materia de control interno
Acuerdo 006 de 2014. Criterios básicos para clasificación, ordenación y descripción documental
Acuerdo 007 de 2014. Lineamientos para reconstrucción de expedientes
NTC-ISO 9001:2015. Sistema de gestión de la calidad – Requisitos
NTC-ISO/IEC 17025:2017. Requisitos generales para la competencia de los laboratorios de ensayo y calibración
ISO/IEC 27001. Sistemas de gestión de la seguridad de la información – Requisitos
ISO/IEC 27002. Código de prácticas para controles de seguridad de la información

8. ANEXOS

PV-CI-MC-MT-02 Matriz de Índice de Información Clasificada y Reservada
PE-SIG-SGC-MT-06 Matriz de Roles y Responsabilidades de Manejo de Información
PM-LAB-MT-02 Matriz de Roles y Responsabilidades de Manejo de Información de Laboratorio
PE-SIG-SGC-FO-21 Declaración de confidencialidad
PM-LAB-FO-01 Acta de Confidencialidad
PE-SIG-SGC-FO-08 Registro de Asistencia
PV-CI-AI-FO-03 Informe de Auditorías Internas
Soportes Documentales Externos

ELABORÓ	NATURALEZA DEL CAMBIO	VERSIÓN	FECHA DE APROBACIÓN
Andrew Masami Asakura Garcia	Procedimiento inicial	01	09/01/2025
Andrew Masami Asakura Garcia	Actualización del Correo Corporativo	02	01/04/2025
Andrew Masami Asakura Garcia	Fortalecimiento de las Políticas de Operación, en cuanto a Atención de Eventos de Fuga o Exposición de Información Confidencial, Clasificada o Reservada	03	08/01/2026

ELABORÓ	REVISÓ	APROBÓ

Nombre: Andrew Masami Asakura Garcia	Nombre: Yeison Rokney Torres Suarez	Nombre: Yeison Rokney Torres Suarez
Cargo: Profesional SIG	Cargo: Gerente General	Cargo: Gerente General
Firma:	Firma:	Firma: