Política de seguridad de la información

Aguas del Magdalena S.A. E.S.P. — Seguridad digital y protección de la información

> **En pocas palabras:** Aguas del Magdalena protege la información de la ciudadanía y de la Entidad para que solo la conozca quien debe, no se altere y esté disponible cuando se necesite. Si detecta una falla de seguridad en el portal, repórtela a **amg@aguasdelmagdalena.com**.

1. Objetivo

Establecer los lineamientos para proteger la **confidencialidad**, la **integridad** y la **disponibilidad** de la información de Aguas del Magdalena S.A. E.S.P. (en adelante, «la Entidad») y de los sistemas que la soportan.

2. Alcance

Aplica a los servidores públicos, contratistas y terceros que acceden a la información de la Entidad, y a sus sistemas, entre ellos el portal web y su panel administrativo, el correo institucional y los archivos físicos y digitales.

3. Marco de referencia

- Ley 1581 de 2012 (protección de datos personales) y Ley 1712 de 2014 (transparencia y acceso a la información pública).
- Ley 1273 de 2009 (protección de la información y de los datos, delitos informáticos).
- Resolución MinTIC 1519 de 2020, Anexo 3 (condiciones mínimas de seguridad digital de los sitios web).
- Resolución MinTIC 500 de 2021 y Modelo de Seguridad y Privacidad de la Información (MSPI), como referencia.
- Norma ISO/IEC 27001, como referencia de buenas prácticas.

4. Principios

- **Mínimo privilegio:** cada persona accede solo a lo que necesita para sus funciones.
- **Responsabilidad:** las acciones sobre la información son personales y dejan trazabilidad.
- **Protección desde el diseño:** la seguridad se tiene en cuenta desde que se crea un sistema.
- **Mejora continua:** los controles se revisan y se ajustan según los riesgos.

5. Lineamientos

Control de acceso

- Los accesos son personales e intransferibles, con usuario y contraseña, y permisos según el rol.
- Los accesos se retiran o se ajustan cuando la persona termina su vínculo o cambia de funciones.
- Las contraseñas se guardan cifradas de forma irreversible y no se comparten.
- El acceso a la infraestructura del portal se limita a personal autorizado.

Protección del portal y de los datos

- Las comunicaciones del portal van cifradas (HTTPS).
- El portal cuenta con protección de red, límites contra intentos abusivos y validación de los archivos que se reciben.
- Los anexos de las PQRSD y los documentos internos se guardan de forma privada, sin acceso público desde internet.
- Las acciones realizadas en el panel administrativo quedan en un registro de auditoría.

Copias de respaldo y continuidad

- Se hacen copias de respaldo periódicas de las bases de datos y de los archivos del portal.
- Antes de los cambios importantes en el portal se hace una copia de respaldo.

Uso de la información y de los equipos

- La información de la Entidad se usa solo para fines institucionales.
- El correo institucional y los equipos se usan con responsabilidad; se debe desconfiar de enlaces y adjuntos sospechosos.
- No se deben compartir contraseñas, documentos internos ni datos personales por canales no autorizados.

Proveedores

Los terceros que traten información de la Entidad deben protegerla y usarla solo para la finalidad acordada.

6. Incidentes de seguridad

Quien detecte un incidente, como un acceso no autorizado, una pérdida de información, un correo fraudulento o una falla en el portal, debe reportarlo de inmediato al área de Sistemas. La Entidad lo atenderá, lo documentará y tomará las medidas correctivas. Si afecta datos personales, informará a la Superintendencia de Industria y Comercio, como lo exige la ley.

Reporte responsable: si usted encuentra una vulnerabilidad en el portal, escriba a amg@aguasdelmagdalena.com con el detalle, sin explotarla ni acceder a información de terceros.

7. Responsabilidades

Quién	Qué le corresponde
Gerencia	Aprobar esta política y dar los recursos para aplicarla.
Área de Sistemas	Administrar los controles técnicos, los accesos y las copias de respaldo, y atender los incidentes.
Líderes de cada área	Autorizar los accesos de su equipo y velar por el buen uso de la información.
Servidores públicos y contratistas	Cumplir esta política, proteger sus credenciales y reportar los incidentes.

8. Incumplimiento y revisión

El incumplimiento de esta política puede dar lugar a las acciones disciplinarias, contractuales o legales que correspondan. La política se revisa al menos una vez al año, o cuando haya cambios importantes en la Entidad o en sus sistemas.

Control de versiones

Versión	Fecha	Descripción del cambio
01	Noviembre de 2026	Primera publicación en el portal.