AGUAS MOCOA S.A E.S.P

LO MEJOR DE NOSOTROS

EMPRESA DE SERVICIOS PÚBLICOS DE MOCOA PUTUMAYO

POLÍTICA

DE SEGURIDAD DIGITAL

CONTENIDO

1. OBJETIVO

Establecer los mecanismos corporativos que permitan salvaguardar la disponibilidad, integridad y confidencialidad de la información y comunicación de todos los procesos de la empresa y de sus colaboradores en el ejercicio de sus actividades en el entorno digital, a fin de no poner en riesgo la integridad institucional ni de las personas internas o externas.

2. ALCANCE

El alcance de la Política de seguridad digital de la empresa Aguas Mocoa S.A. E.S.P. es transversal y aplica a TODOS los procesos en razón a preservar la integridad de la información y comunicación manejada y procesada en la empresa en razón a su misión.

3. RESPONSABLES

El responsable de la adecuada implementación y ejecución de esta política institucional estará a cargo del proceso de TECNOLOGÍA DE LA INFORMACIÓN o quien haga tales funciones, esta política está encuadrada bajo las recomendaciones del Departamento Administrativo de la Función Pública DAFP en el Marco del Modelo Integrado de Planeación y Gestión MIPG.

4. TÉRMINOS ASOCIADOS[1]

- **MSPI:** Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información y las Telecomunicaciones – MINTIC.

- **Integridad:** Propiedad de la información que pretende mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

- **Disponibilidad:** Propiedad de la información que pretende garantizar el acceso y uso de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

- **Confidencialidad:** Propiedad de la información que pretende garantizar que esta sólo es accedida por personas o sistemas autorizados.

- **Información:** Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

[1] Glosario Ministerio de Tecnologías de la Información y las Telecomunicaciones – MINTIC.

- **Dato:** Es una representación simbólica (numérica, alfabética, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.

- **Copias de respaldo:** Copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. Suele conservarse en un lugar seguro, generalmente en un dispositivo distinto de aquel en el que se encuentra el original y lejos de este. De esta forma, si la información original se daña es posible reconstruirla a partir de la copia.

- **Servidor:** Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta apropiada.

- **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.

- **Vulnerabilidad:** Es una debilidad de un activo informático, o sistema de información que puede ser explotada por una o más amenazas para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

- **Amenaza:** Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en un equipo, como por ejemplo un virus.

- **Carpeta Compartida:** Carpeta cuyo contenido es accesible por todos los usuarios que pertenecen a un mismo grupo de trabajo.

5. POLÍTICAS Y ANOTACIONES RELEVANTES

5.1. GENERALIDADES EN EL MARCO DE MIPG[2]

En materia del cumplimiento de la política de Seguridad Digital, el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las entidades.

[2] Manual Operativo del Modelo Integrado de Planeación y Gestión CONSEJO PARA LA GESTIÓN Y DESEMPEÑO INSTITUCIONAL Versión 5.

Con la política se fortalecen las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta nacional en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país.

5.1.1 Ámbito de Aplicación

Manual Operativo del Modelo Integrado de Planeación y Gestión Versión 5 establece que el ámbito de aplicación corresponde a las *"Entidades que conforman la Administración Pública en los términos del artículo 39 de la Ley 489 de 1998 y los particulares que cumplen funciones administrativas. La implementación de la Política de Gobierno Digital en las Ramas Legislativa y Judicial, en los órganos de control, en los autónomos e independientes y demás organismos del Estado, se realizará bajo un esquema de coordinación y colaboración armónica en aplicación de los principios señalados en los artículos 113 y 209 de la Constitución Política (Art. 2.2.9.1.1.2. - Decreto 1078 de 2015)."*

5.1.2 Lineamientos generales para la implementación

Manual Operativo del Modelo Integrado de Planeación y Gestión Versión 5 determina que *"En el orden territorial, MinTIC definirá los lineamientos para que las entidades territoriales definan la figura del enlace de Seguridad Digital territorial para la implementación de la política de Seguridad Digital, así como las instancias respectivas para la articulación con el Coordinador Nacional de Seguridad Digital."*

5.2. RECOMENDACIONES MINTIC[3]

"El tema de seguridad es responsabilidad de todos los ciudadanos. Cada persona, empresa o entidad del Gobierno debe velar por su seguridad y proteger su información en el mundo digital. Para ello les brindamos algunas recomendaciones:

- *No descargar archivos sospechosos.*
- *Actualizar el software del sistema periódicamente.*
- *Usar antivirus y aplicaciones anti-malware.*
- *Crear mejores contraseñas y cambiarlas cada seis meses.*
- *Acostumbrar a cerrar las sesiones al terminar.*
- *Evitar operaciones privadas en redes abiertas y públicas.*
- *Desconectarse de internet cuando no se necesite.*
- *Realizar copias de seguridad.*
- *Navegar por páginas web seguras y de confianza.*
- *Comprobar la seguridad de la red WIFI.*
- *No hacer clic en enlaces raros.*
- *No dar datos personales a desconocidos.*
- *En las empresas se debe hacer una política de seguridad corporativa.*

¿Dónde puedo denunciar los delitos cibernéticos?

Si un ciudadano es víctima de delitos electrónicos financieros podrá denunciar en el CAI Virtual de la Policía Nacional. Con los soportes respectivos, los ciudadanos deben acudir a las entidades financieras, donde deben gestionar la denuncia y si considera que su solicitud no ha sido tramitada adecuadamente podrá recurrir a la Superintendencia Financiera de Colombia, donde estudiarán el caso y tendrá mayor probabilidad de recuperar el dinero hurtado.

Si el ciudadano es víctima de otros tipos de delitos informáticos, la autoridad competente en Colombia para conocer de estos casos es el Centro Cibernético Policial -CCP- de la Policía Nacional, encargado de la ciberseguridad, y de ofrecer información, apoyo y protección ante los delitos cibernéticos. Esta autoridad desarrolla labores de prevención, atención, investigación y judicialización de los delitos informáticos en el país. Puede hacer la denuncia en el CAI Virtual, en la página web www.ccp.gov.co"[4]

5.3. MARCO REGULATORIO

- **Ley 23 1982:** Derechos de Autor.

---

[3] https://mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Preguntas-frecuentes/15430:Politica-de-Seguridad-Digital

[4] https://www.mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Preguntas-frecuentes/15430:Politica-de-Seguridad-Digital#:~:text=El%20tema%20de%20seguridad%20es,de%20concientizacion%20para%20que%20los

- **Ley 527 1999**: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

- **Ley 594 2000**: Reglamentada parcialmente por los Decretos Nacionales 4124 de 2004, 1100 de 2014. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.

- **Ley 603 2000**: Esta ley se refiere a la protección de los derechos de autor en Colombia. El software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

- **Ley 962 2005**: Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas.

- **Ley 1150 2007**: Seguridad de la información electrónica en contratación en línea.

- **Ley 1266 2008:** Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- **Ley 1273 2009:** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"-y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- **Ley 1341 2009**: Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

- **Decreto 4632 de 2011**: Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.

- **Ley 1581 2012**: Por la cual se dictan disposiciones generales para la protección de datos personales.

- **Ley 1712 2014**: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- **Conpes 3854 2016**: Política Nacional de Seguridad Digital

- **Decreto 2364 2012**: Firma electrónica

- **Decreto 2693 2012**: Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones

- **Decreto 1078 2015**: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

5.4. POLÍTICA INSTITUCIONAL DE SEGURIDAD DIGITAL

La empresa Aguas Mocoa S.A. E.S.P. es consiente que la información es un activo de gran valor y de vital relevancia para la estabilidad y seguridad de la empresa. Es por ello, que se compromete en instituir mecanismos acordes a la capacidad de soporte institucional para permitan salvaguardar la disponibilidad, integridad y confidencialidad de la información y comunicación de todos los procesos de la empresa y de sus colaboradores en el ejercicio de sus actividades en el entorno digital, a fin de no poner en riesgo la integridad institucional ni de las personas internas o externas.

5.4.1 Principios

- **Integridad:** Proteger la exactitud y consistencia de los datos frente a modificaciones no autorizadas o errores.

- **Confidencialidad:** Garantizar que solo personas autorizadas accedan a la información sensible, protegiendo la privacidad de los usuarios y la empresa.

- **Disponibilidad:** Asegurar que los sistemas y la información de Aguas Mocoa estén accesibles para quienes los necesiten en el momento adecuado, garantizando la continuidad de las operaciones.

5.2.1 Plan de acción para la implementación de los lineamientos de la política

No	Actividad	Responsable (s)
1	Identificar y evaluar los riesgos de seguridad de la información.	Área de TIC
2	Implementar controles de seguridad digital.	Área de TIC
3	Desarrollar un plan de contingencia detallado que incluya acciones específicas para mitigar riesgos.	Área de TIC
4	Programar mantenimientos preventivos periódicos para equipos y sistemas.	Área de TIC
5	Realizar inspecciones regulares para detectar posibles fallos o deterioros en la infraestructura física.	Área de TIC

No	Actividad	Responsable (s)
6	Coordinar los mantenimientos preventivos internamente, y los correctivos con proveedores externos para realizar mantenimientos especializados según sea necesario.	Área de TIC
7	Establecer rutinas regulares de respaldo de datos y verificar periódicamente la integridad y la capacidad de restauración de los respaldos de información.	Área de TIC
8	Implementar un plan de respuesta a incidentes de seguridad.	Área de TIC
9	Registrar, analizar y gestionar los incidentes de seguridad reportados.	Área de TIC

5.2.2 Roles y responsabilidades

El presente documento cuenta con un componente de seguimiento y control para la verificación de la mejora continua que den mejoramiento al índice de desempeño institucional a través del aplicativo FURAG, para evaluación del cumplimiento de los objetivos trazados por la entidad.

Roles	Responsabilidades
Junta Directiva	Conocer y promover los lineamientos de la política.
Gerente General	Ejecutar la política. Liderar planes, proyectos y programas para promover la política.
Comité Institucional de Gestión y Desempeño Aguas Mocoa S.A. E.S.P.	Revisar la política y aprobarla.
Área de TIC	Presentar la política y sus actualizaciones para aprobación del Comité Institucional de Gestión y Desempeño Aguas Mocoa S.A. E.S.P. Actualizar la política cuando se considere necesario. Socializar la política al interior de la empresa.
Lideres de proceso Todos los colaboradores	Participar en las capacitaciones realizadas sobre la política. Ejercer sus labores en plena coherencia con los lineamientos de la política. Aportar en las actividades, planes, proyectos y programas que adelanten en función de la política.
Control Interno	Realizar seguimiento y controlar que se sigan los lineamientos de la política.

Nota: Los responsables de ejecutar las actividades del plan de acción corresponden a los cargos señalados en la política o a los equivalentes cuando se modifique la estructura organizacional.

5.2.3 Indicador

Indicador	Fuente
Porcentaje de cumplimiento del plan de acción de la política. (No de actividades ejecutadas/No de actividades planteadas)	• Informe de control interno sobre ejecución del plan de acción de la política.

5.2.4 Comunicación y publicación

La divulgación de la Política debe ser socializada a todas las dependencias e implementada en todos los procesos de AGUAS MOCOA S.A. E.S.P., y a través de la página web institucional y se revisará cada dos años o cada vez que la norma cambie.

5.2.5 Revisión y actualización

La política debe ser revisada permanentemente y ser actualizadas por los siguientes aspectos:

- Disposiciones normativas que generen afectación sobre los lineamientos
- Cambios disruptivos en la organización que apliquen a la política
- Recomendaciones de la alta dirección
- Ajustes y/o actualización sobre el plan de acción definido

6. DESARROLLO DE ACTIVIDADES

N/A

7. RELACIÓN DE FORMATOS UTILIZADOS

N/A

8. CONTROL DE CAMBIOS

Versión	Fecha	Ítem Modificado	No. Acta de aprobación	Responsable de la modificación
1	15/01/2025	Creación	006-2025	Comité Institucional de Gestión y Desempeño de la

				Empresa de Servicios Públicos de Mocoa – AGUAS MOCOA S.A E.S.P.

9. ANEXOS

Anexo No.1. Políticas del Modelo Integrado de Planeación y Gestión

Fuente: Construcción Propia