Plan de Seguridad y Privacidad de la Informacion

AGUAS DE BARRANCABERMEJA S.A. E.S.P.

Datos de Contacto:

Empresa	AGUAS DE BARRANCABERMEJA SA ESP
NIT	900045408-1
Representante Legal	Sergio Jesus Amaris Fernandez
Documento preparado por	Rafael Andres Lastre Gomez
Conmutador	+57 6216504 +57 6102491
Fax	+57 8 5121350
Correo Notificaciones Judiciales	notificaciones@aguasdebarrancabermeja.gov.co
Correo contacto y PQRD	atenciónalciudadano@aguasdebarrancabermeja.gov.co
Sitio Web	www.aguasdebarrancabermeja.gov.co
Horario de Atención al Público	lunes a Jueves 7:00 am a 12:00 pm y de 2:00 pm a 6:00 pm y Viernes de 7:00 am a 03:00 pm
Dirección	Planta de Tratamiento de Aguas de Barrancabermeja Vía Carretera Nacional Barrio el Boston

INTRODUCCIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la Empresa Aguas de Barrancabermeja SA ESP con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan el Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.
Aguas de Barrancabermeja SA ESP, para asegurar el direccionamiento estratégico de la Entidad, establece la compatibilidad de la política y de los objetivos de seguridad de la información, estos últimos correspondientes a:

a) Mitigar los riesgos de la entidad.
b) Cumplir con los principios de seguridad de la información.
c) Cumplir con los principios de la función administrativa.
d) Mantener la confianza de los funcionarios, contratistas y terceros.
e) Apoyar la innovación tecnológica.
f) Implementar el sistema de gestión de seguridad de la información.
g) Proteger los activos de información.
h) Establecer las políticas, procedimientos e instructivos en materia de
i) seguridad de la información.
j) Fortalecer la cultura de seguridad de la información en los funcionarios y clientes externos de Aguas de Barrancabermeja SA ESP
k) Garantizar la continuidad del servicio frente a incidentes.

ALCANCE

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de la Empresa Aguas de Barrancabermeja SA.

NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento a esta política.
A continuación se establecen las políticas que soportan el plan de seguridad y privacidad de la información de Aguas de Barrancabermeja SA ESP.

a) La Empresa Aguas de Barrancabermeja SA ESP ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, amparado en lineamientos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios que le aplican a su naturaleza.
b) Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
c) La Empresa Aguas de Barrancabermeja SA ESP protege la información generada, procesada o resguardada por los procesos de la entidad y activos de información que hacen parte de los mismos.
d) La Empresa Aguas de Barrancabermeja SA ESP protege la información creada, procesada, transmitida o resguardada por sus procesos de la entidad, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
e) Aguas de Barrancabermeja SA ESP protege su información de las amenazas originadas por parte del personal.
f) Aguas de Barrancabermeja SA ESP protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
g) Aguas de Barrancabermeja SA ESP controla la operación de sus procesos de la entidad garantizando la seguridad de los recursos tecnológicos y las redes de datos.
h) Aguas de Barrancabermeja SA ESP implementa controles de acceso a la información, sistemas y recursos de red.
i) Aguas de Barrancabermeja SA ESP garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
j) Aguas de Barrancabermeja SA ESP garantiza a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
k) Aguas de Barrancabermeja SA ESP garantiza la disponibilidad de sus procesos de la entidad y la continuidad de su operación basada en el impacto que pueden generar los eventos.
l) Aguas de Barrancabermeja garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Justificación

La Empresa Aguas de Barrancabermeja SA ESP con el propósito de salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la misma, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos.
La seguridad de la información se entiende como la preservación de las siguientes características:
a) Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
b) Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
c) Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, debe considerarse los conceptos de:
a) Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
b) Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
c) No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
d) Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
e) Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación del presente Plan, se realizan las siguientes definiciones:

a) Información: se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

b) Sistema de Información: se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
c) Tecnología de la Información: se refiere al hardware y software operados la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

OBJETIVO

Definir los mecanismos y todas las medidas necesarias por parte de la Empresa Aguas de Barrancabermeja SA ESP, tanto técnica, lógica, física, legal y ambiental para la protección de los activos de información, los recursos y la tecnología de la entidad, con el propósito de evitar accesos no autorizados, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir de forma intencional o accidental, frente a amenazas internas o externas, asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

ALCANCE

Este Plan de Seguridad y Privacidad de la Información y su política, son aplicables a todos los funcionarios de Aguas de Barrancabermeja SA ESP, a sus recursos, procesos y procedimientos tanto internos como externos, así mismo al personal vinculado a la entidad y terceras partes, que usen activos de información que sean propiedad de la entidad.

ROLES Y RESPONSABILIDADES

Es responsabilidad del Comité de Seguridad de la Información de Aguas de Barrancabermeja SA ESP, la implementación, aplicación, seguimiento y autorizaciones de la política del Plan de Seguridad y Privacidad de la información en las diferentes áreas y procesos de la entidad, además garantiza el apoyo y el uso de la Política de Seguridad de la Información como parte de su herramienta de gestión, la cual debe ser aplicada de forma obligatoria por todos los funcionarios para el cumplimiento de los objetivos.

Comité de Seguridad de la Información. El comité está encargado de recomendar la formulación y actualización periódica de las políticas relativas a los recursos informáticos y a la seguridad de la información. La Gerencia, Subgerentes y Profesional de recursos informáticos de la Empresa. Es responsable de clasificar y proteger la información utilizada por ellos; cuando ocurra un incidente grave que refleje alguna debilidad, deberán tomar las acciones para reducir los riesgos.
Control de Gestión. Debe velar por el cumplimiento de las políticas, normas y procedimientos de seguridad de la información en la Empresa. Igualmente, advertir acerca de las vulnerabilidades detectadas.
Profesional III Adscrito a la Subgerencia Administrativa y Financiera. Responsable de implantar las políticas, normas y procedimientos de seguridad en la empresa; evaluar, proponer la adquisición e implantar productos de seguridad informática; acordar el análisis de riesgos, planes de contingencia y realizar las demás actividades necesarias para garantizar un ambiente informático seguro.

El Administrador del sistema. Es responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y llevar a cabo las tareas de seguridad relativas a los sistemas que administra.
Usuario. Todo servidor público o persona que asuma funciones públicas, es responsable de cumplir con todas las políticas informáticas y de seguridad de la Empresa.

CUMPLIMIENTO

El cumplimiento de la Política de Seguridad y Privacidad de la Información es obligatorio. Si los funcionarios de la entidad o terceros violan este plan, Aguas de Barrancabermeja SA ESP se reserva el derecho de tomar las medidas correspondientes.

COMUNICACIÓN

Mediante socialización a todos los funcionarios de la Empresa Aguas de Barrancabermeja SA ESP se dará a conocer el contenido del documento de las políticas de seguridad, así mismo se deberá informar a los contratistas y/o terceros en el momento que se requiera con el propósito de realizar los ajustes y la retroalimentación necesaria para dar cumplimiento efectivo al plan.
Todos los funcionarios, contratistas y/o terceros de la entidad deben conocer la existencia de las políticas, la obligatoriedad de su cumplimiento, la ubicación física del documento estará a cargo del Sistema de Gestión Integrado para que sean consultados en el momento que se requieran, igualmente estarán alojados en la página de la entidad www.aguasdebarrancabermeja.gov.co.

MONITOREO

Se crearán los mecanismos y los indicadores correspondientes a la política de seguridad con el fin de determinar el cumplimiento de las mismas para establecer qué modificaciones o adiciones deben hacerse, este monitoreo debe realizarse como mínimo una vez al año o cuando sea necesario.

DESCRIPCIÓN DE LAS POLÍTICAS

Generalidades

La Empresa Aguas de Barrancabermeja SA ESP en todas sus áreas y procesos cuenta con información, reservada, relevante, privilegiada e importantante, es decir que esta información es el principal activo de la entidad para el desarrollo de todas sus actividades por lo que se hace necesario y se debe proteger conforme a los criterios y principios de los sistemas de información, como son integridad, disponibilidad y confidencialidad de la información.

De acuerdo a esta Política se divulgan los objetivos y alcances de seguridad de la información de la entidad, que se logran por medio de la aplicación de controles de seguridad, con el fin de mantener y gestionar el riesgo como lo establece la política de riesgos institucional. Este documento tiene el objetivo de garantizar la continuidad de los servicios, minimizar la probabilidad de explotar las amenazas, y asegurar el eficiente cumplimiento de los objetivos institucionales y de las obligaciones legales conforme al ordenamiento jurídico vigente y los requisitos de seguridad destinados a impedir infracciones y violaciones de seguridad.

DERECHOS MORALES Y PATRIMONIALES

Los usuarios son responsables de la custodia y la confidencialidad de los datos y la información a la cual tengan acceso en forma directa e indirecta.
La empresa es propietaria de todos los datos e información que circule o se genere al interior de la misma o que esté disponible a través de sus sistemas de información y/o computadores.
En este sentido, el Gerente y Servidores públicos de nivel directivo clasificaran los datos y la información generados o utilizados por su Subgerencia solicitando a sus colaboradores y contratistas seguir los procedimientos establecidos por la Subgerencia Administrativa y Financiera para el resguardo de los mismos a través de copias de seguridad (Backup).

DIVULGACION DE LA INFORMACION

La información entregada a los medios de comunicación debe hacerse a través del funcionario encargado del manejo de la comunicación empresarial.
La empresa no se hace responsable por las consecuencias que se deriven de la utilización inadecuada por parte de terceros. Igualmente, se abstiene de suministrar la información que haya recibido de terceros para su uso interno y confidencial.

INFORMACIÓN CONFIDENCIAL

Exigir a los usuarios la protección de la información clasificada como confidencial o de uso restringido.
Incluir una cláusula de confidencialidad en los contratos u órdenes, cuando el contratista requiera acceder de manera directa o indirecta a los datos o información de la Empresa.
Todo empleado que participe en proyectos de la Empresa, o tenga acceso a su información, debe guardar confidencialidad sobre la misma. El responsable del proyecto debe solicitar a los participantes, como parte de los términos, compromiso y condiciones iniciales de su participación, que firmen un acuerdo de confidencialidad de la información.

RECURSOS INFORMÁTICOS

Establecer el cambio periódico de los recursos informáticos, dependiendo de la obsolescencia, la vida útil, el estado de los mismos y las necesidades de la Empresa.
Se dará de baja a los equipos teniendo en cuenta el procedimiento establecido para tal fin.
Exigir a los usuarios la utilización responsable y razonable de los recursos informáticos. Igualmente, el acatamiento de las medidas de control establecidas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde con la importancia de los datos y la naturaleza de los riesgos.

ADMINISTRACIÓN Y CONTROL

La conexión a la red debe ser autorizada por el Profesional de Recursos Informáticos con las directrices emitidas por la Subgerencia Administrativa y Financiera. No pueden conectarse computadores, servidores, hubs, switches, routers, o cualquier otro hardware a la red sin la autorización correspondiente.

WEBSITE E INTRANET

Adoptar el Website http://www.aguasdebarrancabermeja.gov.co y la intranet como los sitios electrónicos oficiales de la empresa, para la publicación de información externa e interna.
Realizar la publicación de información en la Website e intranet con la autorización de la Subgerencia Administrativa y Financiera y ejecutado por el administrador de la Web o quien haga sus veces, pero tratándose de información sobre la actividad contractual de la empresa. Cuando la información a publicar sea inherente a alguna Subgerencia específica, deberá el Subgerente o la Gerencia enviar dicha autorización. Una vez publicada, la actualización es responsabilidad del funcionario solicitante.

DERECHOS DE AUTOR LICENCIAS DE SOFTWARE

Proteger el Derecho de Autor y Derechos Conexos, de acuerdo con lo consagrado en la constitución política, los ordenamientos legales y acuerdos regionales.
Emplear, en lo posible, las últimas versiones del software disponible en el mercado, para disminuir los problemas ocasionados por las diferencia de versiones.
Todos los programas utilizados en los computadores de la empresa deben contar con sus respectivas licencias de uso vigentes y condiciones exigidas

CORREO ELECTRONICO

La empresa suministrara el acceso al correo electrónico y a internet, como herramientas para la realización de las labores, dependiendo de las responsabilidades y naturaleza del trabajo contratado, conforme a lo previsto en el manual de funciones.
El uso inadecuado de internet constituirá una falta grave, que se clasificara como tal por la magnitud del hecho o por no atender los requerimientos de la empresa para que se cese la utilización indebida. La comprobación y las sanciones disciplinarias se realizaran conforme lo establecido en la legislación aplicable.

GESTIÓN DOCUMENTAL

Propender porque las circulares y en general comunicaciones informáticas enviadas entre los servidores de la Empresa Aguas de Barrancabermeja S.A E.S.P, se realice por medios electrónicos.
Responsabilizar al funcionario de mantener consultando permanente la cuenta habilitada en el Sistema de Gestión Documental Mercurio y atender los compromisos definidos por este medio.
Cualquier comunicación registrada por otro medio, no será considerada como oficial y el funcionario responderá por las consecuencias derivadas de ello, todo documento será reconocido una vez haya sido enviado a su destinatario, el radicado de por sí solo no implica oficialización del documento y se entenderá por no tramitado, el funcionario que a sabiendas radique y no envié la comunicación responderá por las consecuencias que se deriven de dicho acto.
Solamente se exceptuarán situaciones que por dificultades del sistema o fallos en las redes no permita hacer en debido registro con el sistema de gestión documental, lo que sí requeriría un registro manual y ser certificado por la persona competente.
La radicación de correspondencia interna y externa que requiera imprimirse es responsabilidad de cada dirección y la oficina de gestión documental únicamente se encargara del envío local y/o nacional.

COMPUTADORES, SERVIDORES Y REDES

Prohibir a los usuarios la modificación de la configuración de hardware y software establecida por el funcionario encargado de administrar el sistema.
La Subgerencia administrativa y financiera será responsable que los equipos se protejan para disminuir el riesgo de hurto, destrucción, fluctuaciones de energía, incendio y medio ambiente (por ejemplo: agua), utilizando instalaciones en condiciones adecuadas, cerraduras, vigilantes, protectores contra transitorios de energía eléctrica y, para los servidores, fuentes de poder interrumpibles (UPS).
Prohibir el uso de módems en computadores que tengan conexión a la red local (LAN), para prevenir la intrusión de hackers a través de las puertas traseras. Todas las comunicaciones de datos deben efectuarse a través de la red LAN de la empresa.

CUENTAS DE LOS USUARIOS

Exigir que la solicitud de una nueva cuenta o el cambio de privilegios se haga a través del funcionario encargado de la Subgerencia.
Cuando la empresa vincula a un respectivo funcionario este debe firmar un documento donde declara conocer las políticas informáticas y de seguridad de la información y acepta las responsabilidades.
No debe concederse una cuenta a personas que no sean empleados de la empresa, a menos que estén debidamente autorizados por la Subgerencia correspondiente. En este caso, la persona debe firmar un documento donde declare conocer las políticas informáticas y de seguridad de la información y acepta sus responsabilidades.

IDENTIFICACION, CONTRASEÑAS Y AUTORIZACIONES

Todos los usuarios que acceden a los sistemas de información requieren de un único e intransferible identificador, el cual será proporcionado como parte del proceso de autorización.
Los identificadores concedidos deberán eliminarse o deshabilitarse, por solicitud de la Subgerencia, cuando cese la vinculación del usuario con la empresa en forma permanente o temporal, o cuando se presente un uso indebido.
De esta manera, todas las acciones realizadas con un identificador de usuario son responsabilidad del titular del mismo.

SEGURIDAD FISICA Y DEL ENTORNO

Implantar los controles de seguridad apropiados para el ingreso a las instalaciones de la empresa de funcionarios, contratistas y terceros.
El acceso de personal contratista, se debe autorizar una vez se haya formalizado el contrato y de acuerdo con los controles de seguridad definidos.
Se debe exigir al personal contratista, cumplir igualmente con las políticas, procesos procedimientos establecidos en la empresa.
Esta guía, proporciona la metodología establecida por la Entidad para la administración y gestión de los riesgos a nivel de procesos; orienta sobre las actividades a desarrollar desde la definición del contexto estratégico, la identificación de los riesgos, su análisis, valoración y la definición de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

ACTIVIDADES

1. Revisión de la Política de Seguridad y Privacidad de la Informacion
2. Creación de Comité de Seguridad y Privacidad de la Informacion
3. Implementacion de las Políticas de la Seguridad de la Informacion.
    3.1. Entrevistar con los líderes de los Procesos.
4. Aprobación y adopción de las políticas de seguridad y privacidad de la información.
6. Aspectos de seguridad y privacidad de la información en la gestión de continuidad del negocio
5. Seguimiento y Control de las políticas

CRONOGRAMA

CRONOGRAMA DE ACTIVIDADES PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION																							
ACTIVIDAD	2018												2019										
	Octubre				Noviembre				Diciembre				Enero -Abril				Mayo -Agosto				Septiembre- Diciembre		
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3
Revision de las Politicas de Seguridad y Privacidad de la Informacion																							
Creacion del Comité de Seguridad de la Informacion																							
Implementacion de las Policitas de Seguridad y Privacidad de la Informacion																							
Entrevista con los lideres del Proceso																							
Aspectos de Seguridad Aspectos de seguridad y privacidad de la información en la gestión de continuidad del negocio																							
Seguimiento y Control																							

ENTREGABLES

- Acta de Reunión.
- Plan de Seguridad y Privacidad de la Informacion
- Manuales y procedimientos de la Implementacion de las Políticas de Seguridad y Privacidad de la Informacion.
- Productos de cada etapa