Superservicios
Superintendencia de Servicios Públicos Domiciliarios

CÓDIGO DE ÉTICA Y BUEN GOBIERNO

SIGME

Proceso Direccionamiento Estratégico
Código DE-D-001, Versión 8
SEPTIEMBRE, 2017

PRESENTACIÓN

En el presente documento se expresa el compromiso directivo de la Superintendencia de Servicios Públicos Domiciliarios con la gestión estratégica institucional en atención a las orientaciones del Gobierno a las entidades del sector público nacional, y al papel de Entidad rectora en materia de inspección, vigilancia y control a la prestación de los servicios públicos domiciliarios.

Es así como en este “Código de ética y buen gobierno” se consolidan los referentes éticos y las distintas políticas temáticas, que, implementadas mediante estrategias soportadas en la ética, integridad, transparencia y eficiencia, facilitan y comprometen las actuaciones de los servidores de la entidad hacia el cumplimiento de los fines misionales y propósitos del Gobierno, en beneficio del bienestar de los ciudadanos.

CONTENIDO

1. OBJETIVO

Establecer las disposiciones de autorregulación para la Superservicios que, en términos de compromiso de los Directivos y demás servidores de la Entidad, promueven y fortalecen una gestión eficiente, íntegra y transparente, orientada al cumplimiento de su misión y visión y al logro de sus objetivos.

2. ALCANCE

El Código de Ética y Buen Gobierno contiene las normas de conducta y las políticas de dirección y gestión adoptadas por las instancias de dirección, administración y gestión de la Superservicios, y debe ser atendido en sus decisiones y acciones, por todos los miembros de la Superintendencia.

3. PRINCIPIOS ÉTICOS

La Superservicios es la Entidad rectora del Gobierno Nacional en materia de control, inspección y vigilancia a las empresas prestadoras de servicios públicos domiciliarios. Los servidores públicos de la entidad tienen disposición de servicio y actitud positiva en el cumplimiento de las responsabilidades, para lo cual están comprometidos con:

- **LA VERDAD.** Es la conformidad de pensar y comunicar de acuerdo a la realidad de los hechos.
- **EL CUMPLIMIENTO.** Se manifiesta en la atención y ejecución de los compromisos, normas, procedimientos y demás orientaciones establecidas.
- **EL APRENDIZAJE EN EQUIPO.** Cada día se promueve y fortalece la capacidad de la creación y construcción colectiva orientada a la producción de resultados que contribuyan a incrementar el bienestar social. Se construye sobre la visión compartida y el dominio personal.
- **LA CORDIALIDAD.** Símbolo de respeto por los demás, nos permite entablar y mantener buenas relaciones con terceros.

4. VALORES ÉTICOS

- **RESPETO.** Consideración y reconocimiento del derecho de los demás a ser, sentir, pensar y actuar diferente. El respeto en la Superservicios está presente en el reconocimiento de los derechos de la comunidad, de sus servidores y de sus clientes**.**
- **INTEGRIDAD.** Es hacer visible la gestión de la Superservicios a través de la relación directa entre los servidores públicos con los usuarios. Entregar información adecuada y oportuna que facilite la participación de los ciudadanos, conforme a lo establecido en el artículo 2 de la Constitución Política.
- **HONESTIDAD.** Es la conciencia clara ante sí mismo y ante los demás de lo que está bien y es apropiado en nuestras acciones, conducta y relaciones, sin contradicciones ni discrepancias, entre los pensamientos palabras o acciones, obrando correctamente con respeto por sí mismo y por los demás.

- **JUSTICIA.** Comportamiento equitativo en todas las acciones. La justicia se evidencia en la Superservicios cuando se construyen relaciones sólidas sobre la base del respeto y la equidad en procura de satisfacer y alcanzar un alto nivel de bienestar.
- **RESPONSABILIDAD.** Capacidad para asumir las responsabilidades y compromisos contraídos y las consecuencias de nuestros actos. Los Servidores Públicos asumimos los deberes que impone el servicio público, las consecuencias de las acciones ejecutadas en la búsqueda del cumplimiento misional de la entidad, y somos reservados y cautelosos en el manejo de la información y de los recursos.
- **TRANSPARENCIA.** Es actuar con claridad haciendo evidentes las decisiones y acciones. La Superintendencia, es una entidad transparente que rinde cuentas de la gestión encomendada y está abierta al ejercicio del control social. Los Servidores Públicos producimos y entregamos información veraz y oportuna para la entidad y nuestros clientes, comunidad y grupos de interés.
- **LEALTAD.** Los servidores de la Superintendencia atienden con devoción los compromisos que se derivan de sus funciones y sus propósitos constitucionales y legales. Los Servidores Públicos somos fieles a la misión de nuestra entidad y al servicio público.
- **DEDICACIÓN Y ESFUERZO.** Los Servidores Públicos de la Superintendencia nos comprometemos a realizar las labores encomendadas con la dedicación y esfuerzo necesarios para cumplir con los parámetros de calidad establecidos en la entidad, de igual manera estamos en la obligación de dar lo mejor de sí para el cumplimiento de las funciones y de los objetivos, metas establecidas individualmente.
- **PROFESIONALISMO.** Los Servidores Públicos de la Superintendencia adquirimos la obligación de actuar en todo momento de manera profesional y de aplicar estándares de calidad en la realización de nuestro trabajo, con el objetivo de cumplir las responsabilidades de manera competente e imparcial.
- **SERVICIO.** Disposición permanente para el cumplimiento de las funciones asignadas en procura de la satisfacción de las necesidades de los clientes. Los Servidores Públicos atendemos cálida, oportuna y eficientemente a nuestros clientes, la comunidad y los grupos de interés.

5. CONTENIDO

5.1 POLÍTICA GENERAL DE GESTIÓN DE LA ENTIDAD

La Superservicios orienta su gestión hacia la protección y promoción de los derechos y deberes de los usuarios y prestadores de los servicios públicos domiciliarios, mediante el ejercicio de sus funciones de inspección, vigilancia y control a la prestación de dichos servicios, gestionando información de manera oportuna y con calidad y fortaleciendo e incrementando la presencia institucional y promoviendo la participación ciudadana en todo el territorio nacional.

5.2 POLÍTICA DE CONTROL INTERNO

La Superintendencia asume el control interno como un elemento estratégico esencial para asegurar el logro de los objetivos institucionales y contribuir a los fines esenciales del Estado. El Equipo Directivo promueve el acatamiento, respeto y ejercicio del control interno con el fin de garantizar y propiciar el mejoramiento de la función institucional, así como la autogestión, la autorregulación y el autocontrol, mediante la adopción, implementación, difusión, mantenimiento y mejora del Modelo Estándar de Control Interno.

5.3 POLÍTICA DE CALIDAD

La Superintendencia vigila, inspecciona y controla la prestación a los servicios públicos domiciliarios atendiendo las necesidades y expectativas de sus clientes y grupos de interés, soportando su gestión en la eficiencia, eficacia y efectividad del desempeño de su sistema de calidad, mediante el mejoramiento continuo de sus procesos, con la participación activa de un equipo humano capaz, dinámico e innovador.

5.4 POLÍTICA DE GESTIÓN DE RIESGOS

La Alta Dirección de la Superintendencia de Servicios Públicos Domiciliarios, se compromete a la administración integral de los riesgos de gestión y de corrupción, a través de la implementación de estrategias que permitan su identificación, análisis, valoración, consulta, divulgación, monitoreo, revisión y seguimiento, con el fin de prevenir su ocurrencia, minimizar su impacto y garantizar la transparencia institucional en el desarrollo de la planeación estratégica. La Entidad determina el nivel de exposición a los riesgos de gestión y de corrupción, así como sus impactos para priorizar su tratamiento y estructurar criterios orientadores en la toma de decisiones respecto a los efectos de los mismos.

5.5 POLITICA DE PARTICIPACIÓN Y SERVICIO AL CIUDADANO

La Superintendencia de Servicios Públicos Domiciliarios en el marco de la corresponsabilidad Estado – Ciudadano, está comprometida con el fortalecimiento de los espacios y mecanismos de participación ciudadana y comunicación entre los diferentes actores del sector y la implementación de estrategias orientadas a facilitar el control social a la prestación de los servicios públicos domiciliarios, así como con la atención a los lineamientos de gestión sectorial e institucional en materia de eficiencia administrativa y actitud de servicio frente al ciudadano.

5.6 POLÍTICA DE RELACIÓN CON LOS ÓRGANOS DE CONTROL EXTERNO

La Superservicios se compromete a mantener relaciones armónicas con los órganos de control externos y a suministrar la información requerida, en forma oportuna, completa y veraz. Se compromete a implementar las acciones de mejoramiento que dichos órganos de control recomienden en sus respectivos informes, previa evaluación de las mismas.

5.7 POLÍTICA DE GESTIÓN DEL TALENTO HUMANO

La Superintendencia promueve el desarrollo y cualificación de los servidores públicos buscando la observancia del principio de mérito para la provisión de los empleos, el desarrollo de competencias, vocación del servicio, la aplicación de estímulos y una gerencia pública enfocada a la consecución de resultados. Incluye, principalmente la Planeación Estratégica de Recursos Humanos como herramienta que integra el Plan Anual de Vacantes, el Plan Institucional de Capacitación-PIC-, el Programa de Bienestar e Incentivos y los temas relacionados con Clima Organizacional.

5.8 POLITICA DE SEGURIDAD Y SALUD EN EL TRABAJO

La Superintendencia vigila, inspecciona y controla la prestación de los servicios públicos Domiciliarios atendiendo las necesidades de clientes y grupos de interés.

La alta dirección se compromete a mantener el bienestar de sus servidores públicos, desarrollando actividades enfocadas a la prevención de las lesiones, accidentes, riesgos y enfermedades laborales, proporcionando los recursos necesarios para el mejoramiento continuo de su Sistema de Gestión de Seguridad y Salud en el Trabajo, cumpliendo los requisitos legales y otros requisitos que la entidad suscriba, contando con la participación activa de funcionarios, contratistas, subcontratistas y demás grupos de interés.

5.9 POLÍTICA AMBIENTAL

La Superintendencia de Servicios Públicos Domiciliarios, está comprometida con la protección y preservación del ambiente en el marco de sus programas, proyectos y procesos, a través de la implementación de buenas prácticas ambientales, que minimicen, mitiguen y controlen la generación de impactos ambientales, dando cumplimiento a la legislación ambiental vigente, a través del mejoramiento continuo y con el propósito de contribuir al desarrollo sostenible del país.

5.10 POLITICA DE CERO PAPEL

La Superservicios se compromete con la implementación de buenas prácticas orientadas a reducir el uso del papel, a través de la utilización de electrónicos apoyados en la aplicación de tecnologías de la información y de las comunicaciones.

5.11 POLITICA DE GESTIÓN DOCUMENTAL

La Superservicios está comprometida con la gestión documental y para ello realiza actividades enfocadas a la correcta administración física y electrónica de los documentos durante su creación, uso, mantenimiento, retención, acceso y preservación, sirviendo de base para la toma de decisiones y como mecanismo de prueba del desarrollo de los objetivos misionales. Para ello cuenta con un grupo humano interdisciplinario que aporta las mejores prácticas en la administración de documentos, priorizando la transparencia de nuestros actos y la atención oportuna a los requerimientos de la ciudadanía.

5.12 POLÍTICA DE COMUNICACIÓN E INFORMACIÓN

La Superintendencia de Servicios Públicos Domiciliarios se compromete a considerar la gestión de comunicación como un componente estratégico, orientado a la creación, divulgación, retroalimentación, seguimiento y control de la información institucional divulgada en desarrollo de sus planes, programas y proyectos hacia los diferentes públicos de interés.

5.13 POLÍTICA DE ALTO NIVEL DE SEGURIDAD DE LA INFORMACIÓN

La Superintendencia de Servicios Públicos Domiciliarios en el marco de su Sistema de Gestión de seguridad de la información, asegura el cumplimiento de los requisitos normativos, legales y regulatorios. Asimismo, establece directrices y gestiona los riesgos en pro de mantener la confidencialidad, integridad y disponibilidad de la información que es procesada mediante la vigilancia, inspección y control de los servicios públicos domiciliarios; mejorando continuamente sus procesos, con el apoyo de un talento humano dispuesto a contribuir a la cultura de seguridad de la información.

Política de Uso aceptable de los activos

Dominio A.8 - Responsabilidad por los activos

Objetivo: Establecer lineamientos para el uso aceptable de los activos, con el fin de identificar los activos de información de la entidad, sus propietarios y las responsabilidades de protección apropiadas.

La política se compone de los siguientes lineamientos, aplicables a los roles de seguridad de la información adoptados por la entidad:

Lineamientos:

1. El Líder de seguridad de la información es el responsable de dirigir las actividades para la identificación de activos de información en cada proceso, asegurando que el inventario sea exacto, consistente y esté alineado con los criterios establecidos por la entidad para la valoración y calificación de los activos, cumpliendo que:
   - Toda la información contenida en los activos debe ser clasificada por su criticidad, valor, y requisitos legales determinados por los propietarios y por la Superservicios.
   - Cada activo debe tener un etiquetado en donde se identifique el nivel de clasificación asignado. El etiquetado de la información debe ser utilizado en la información física o magnética.
   - Toda la información contenida en el inventario y clasificación de activos de información es reservada y de propiedad de la entidad.
   - El inventario y clasificación de activos de información debe permanecer en un repositorio seguro con acceso restringido.
   - Cualquier modificación, inclusión o exclusión que se realice en el inventario y clasificación de activos de información debe ser debidamente documentado y controlado en el historial de cambios.

- El inventario y clasificación de activos de información debe ser actualizado por lo menos una vez al año y cuando se presenten retiros, adquisiciones o reemplazos en los activos identificados.

2. Los propietarios de los activos deben asegurar que éstos cuenten con los niveles de seguridad pertinentes para su protección y cumplan con las políticas determinadas por el SGSI.
3. El líder se seguridad de la información debe asegurar que sobre todo activo o repositorio de información que vaya a ser reutilizado, se ejecute un borrado seguro a fin de evitar la recuperación de la información.
4. El líder de seguridad de la información debe asegurar que los medios removibles no queden desatendidos debido a que pueden ser susceptibles de pérdida o robo de la información, considerando que:
    - La información contenida en los medios es reservada o sensible para la Superservicios, se debe usar un cifrado que asegure la integridad y confidencialidad de la información.
    - Se debe llevar un registro de la información contenida dentro de los medios removibles, con el objetivo de que no afecte la confidencialidad, integridad y disponibilidad de la información.
5. Cuando se termine el contrato de algún contratista o funcionario, por cualquier razón, el jefe inmediato debe asegurar la devolución del activo que estaba bajo la responsabilidad del contratista o funcionario.
6. Para cualquier activo que sea retirado o desvinculado del inventario de los activos de la Superservicios, el líder de seguridad de la información debe garantizar que la información sea eliminada de forma segura.
7. Todo contratista o funcionario, custodio de un activo, debe hacer un uso adecuado de los activos teniendo en cuenta los requisitos de seguridad de la información establecidos por la Superservicios.
8. Los propietarios de los activos de información identificados para la Superservicios, deben cumplir con las políticas de seguridad de la información establecidas en el marco del Sistema de Gestión de Seguridad de la Información.

Política de Control de acceso

Dominio A.9 - Control de acceso

Requisitos del negocio para control de acceso

Objetivo: Establecer lineamientos para limitar el acceso a la información y a instalaciones de procesamiento de información.

La política se compone de los siguientes lineamientos, aplicables a los roles de seguridad de la información adoptados por la entidad:

Lineamientos:

1. El líder de seguridad de la información debe desarrollar los lineamientos y los procedimientos de acceso a los recursos tecnológicos necesarios para que los usuarios, funcionarios y/o contratistas puedan desempeñar las funciones.
2. El líder de seguridad de la información debe definir los lineamientos y las respectivas responsabilidades que deben asumir, los jefes de las dependencias y los supervisores de contrato.
3. El líder de seguridad de la información debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de la Superservicios.
4. El líder de seguridad de la información debe establecer la periodicidad con la cual debe verificar los controles de acceso a la información, de los funcionarios y contratistas de la Superservicios, y cerciorarse que los usuarios han sido eliminados o deshabilitados, una vez que los funcionarios y/o contratistas dejen de pertenecer a la Entidad.
5. Es responsabilidad de los funcionarios y contratistas el manejo y uso de los recursos, así como de las claves, contraseñas y/o usuarios asignados.
6. Cada administrador de un recurso informático o dispositivo tecnológico, debe garantizar que el acceso a este recurso, cuente con métodos de autenticación que eviten accesos no autorizados.

Gestión de acceso de usuarios

Objetivo: Establecer lineamientos para asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.

La política se compone de los siguientes lineamientos, aplicables a los roles de seguridad de la información adoptados por la entidad:

Lineamientos:

La Superservicios a través de la Oficina de Informática, debe desarrollar los lineamientos para el acceso de usuarios teniendo en cuenta las siguientes directrices:

1. El administrador del control de acceso lógico debe implementar controles para asegurar que solo los usuarios autorizados puedan ingresar a los sistemas, datos y servicios de información.
2. El administrador del control de acceso lógico debe activar las claves de acceso a los diferentes activos de información cuando es un usuario nuevo; o cuando un usuario actual haya sido trasladado de dependencia al interior de la Superservicios; o cuando a un usuario actual le hayan sido modificadas sus funciones, actividades y/u obligaciones.
3. El Administrador del control de acceso lógico debe inactivar las claves de acceso a los diferentes activos de información cuando un usuario ha sido desvinculado o ya no desarrolle contrato o convenio alguno con la Superservicios; o cuando hayan sido suspendidas sus funciones y/u obligaciones; o cuando haya sido trasladado de dependencia en el interior de la Superservicios.

4. Los jefes de las dependencias, deben definir los usuarios que puedan utilizar los recursos informáticos, así como los perfiles que se les asignan (consultar, ingresar o modificar información, etc.). Para cada uno de estos perfiles se deben generar cláusulas de confidencialidad entre los empleados que lo utilizan y la Superservicios, por otra parte, los jefes de las dependencias deben monitorear periódicamente que los perfiles definidos por ellos, cuenten los privilegios designados.
5. Cualquier cambio en las funciones de los usuarios, deben ser notificados por el jefe de la dependencia a la Oficina de Informática.
6. El administrador del control de acceso lógico debe revisar los derechos de acceso de los usuarios a intervalos regulares.
7. Las contraseñas deben cambiarse obligatoriamente cuando lo establezca la Oficina de Informática.
8. Después de un número determinado de intentos no exitosos de ingreso de la contraseña, el usuario será bloqueado de manera inmediata y deberá solicitar el desbloqueo a través de la Oficina de Informática.

Responsabilidad de los usuarios

Objetivo: Establecer lineamientos para asegurar que los usuarios se responsabilicen por la salvaguarda de su información de autenticación.

La política se compone de los siguientes lineamientos, aplicables a los roles de seguridad de la información adoptados por la entidad:

Lineamientos:

Todos los usuarios deben seguir los siguientes lineamientos para el uso de contraseñas:

1. Cada usuario tiene que autenticarse antes de acceder a un recurso de tecnología sobre el cual está autorizado, por medio de un usuario y una contraseña.
2. La contraseña es de carácter personal e intransferible. Por lo tanto, se presume que toda la acción realizada bajo la cuenta del usuario asociada, fueron ejecutadas por el usuario responsable de la cuenta.
3. Es responsabilidad de cada usuario la salvaguarda de las contraseñas que le fueron entregadas o establecidas por el mismo.
4. En el caso que la aplicación o sistema no permita el uso de contraseñas seguras, el usuario debe definir una contraseña.
5. En el caso que la aplicación o sistema no obligue al cambio periódico de la contraseña, el usuario debe cambiarla periódicamente.
6. Los administradores de cada sistema, aplicativo o dispositivo de infraestructura tecnológica, deben entregar al Jefe de la dependencia, sus contraseñas, en intervalos planificados o cuando éstas sean cambiadas. Dicha entrega debe formalizase en sobres sellados. Lo anterior aplica también para administradores externos.
7. Las contraseñas deben poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal.

8. Las contraseñas no deben ser reveladas ni compartidas con ninguna persona.
9. Las contraseñas no se deben registrar en papel, correo electrónico ni archivos digitales.
10. La contraseña debe cumplir con los siguientes parámetros de seguridad:
    - Mínimo de ocho (8) caracteres alfanuméricos. o No debe contener el nombre de usuario, el nombre real o nombre de la empresa. o No debe contener nombre de hijo, esposo, mascotas, etc. o No debe contener fechas de aniversarios ni cumpleaños. o Debe ser diferente de otras contraseñas anteriores proporcionadas.
    - Debe estar compuestas por: letras en mayúsculas, letras en minúsculas, números, símbolos especiales y espacios en cualquier orden.

Control de acceso a sistemas y aplicaciones

Objetivo: Establecer lineamientos para evitar el acceso no autorizado a sistemas y aplicaciones.

La política se compone de los siguientes lineamientos, aplicables a los roles de seguridad de la información adoptados por la entidad:

Lineamientos:

1. El propietario de la aplicación y de la información, debe identificar y documentar explícitamente la sensibilidad o confidencialidad de la información.
2. Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos.
3. No está permitido para ningún usuario acceder a la información y a las aplicaciones de un sistema de información para el cual no haya sido autorizado.
4. El líder de seguridad de la información debe establecer los lineamientos para garantizar la seguridad en ambientes separados a nivel físico y lógico para desarrollo, pruebas y producción.
5. El líder de seguridad de la información, debe asegurar que los usuarios utilicen diferentes perfiles de acceso para los ambientes de desarrollo, pruebas y producción.
6. El líder de seguridad de la información, debe establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información.
7. El administrador del control de acceso lógico, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
8. Los desarrolladores deben verificar que los controles de autenticación sean confiables.
9. Los desarrolladores deben validar periódicamente la autorización de los usuarios en los aplicativos.
10. El administrador de recursos informáticos debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
11. El líder de seguridad de la información debe determinar el tiempo de inactividad del sistema para el bloqueo automático de sesión.

12. El líder del equipo de desarrollo debe designar al personal que considere adecuado como el responsable para cumplir el rol de “Administrador de Programas Fuentes”, quien tendrá en custodia los programas fuentes, sin embargo, no debe pertenecer al grupo de desarrollo.
13. El administrador de Programas Fuentes debe llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador, analista responsable que autorizó, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).
14. El administrador de Programas Fuentes debe restringir el acceso a los códigos fuente de los programas, solamente los ingenieros desarrolladores tendrán acceso.
15. El administrador de Programas Fuentes debe mantener los códigos fuentes de los programas en el servidor o repositorio de fuentes.
16. El administrador de Programas Fuentes debe asegurar que el código fuente del programa y las bibliotecas de fuentes del programa sean manejados de acuerdo al Instructivo Principios de Ingeniería para Sistemas Seguros (SI-I-003).
17. El administrador de Programas Fuentes debe limitar el acceso a las bibliotecas de fuentes del programa.
18. La actualización de las bibliotecas de fuentes del programa, así como la emisión de las fuentes del programa para los programadores sólo se realizan después de haber recibido la apropiada autorización del líder del equipo de desarrollo.
19. El administrador de Programas Fuentes debe mantener un registro de auditoría de todos los accesos a las bibliotecas de fuentes del programa.
20. El administrador de Programas Fuentes debe desarrollar un procedimiento que garantice que toda vez que se migre a producción el módulo fuente, se cree el código ejecutable correspondiente en forma automática.
21. El administrador de Programas Fuentes debe realizar copias de respaldo de los programas fuentes.

Política para los procedimientos de gestión de TI

Dominio A.12 - Seguridad de las operaciones

Objetivo: Establecer lineamientos en cuanto a los procedimientos de gestión de TI, para asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

La política se compone de los siguientes lineamientos, aplicables a los roles de seguridad de la información adoptados por la entidad:

Lineamientos:

La Oficina de Informática debe documentar todos sus procedimientos operativos y ponerlos a disposición de la entidad.
Se deben preparar procedimientos documentados para las actividades operacionales asociadas con las instalaciones de procesamiento y comunicación, tales como los procedimientos de encendido y

apagado, copias de respaldo, mantenimiento de equipos, manejo de medios, salas de cómputo y gestión, y seguridad del manejo de correo.
Los procedimientos especificarán instrucciones operacionales, incluyendo:

1. Instalación y configuración de sistemas.
2. Procesamiento y manejo de la información.
3. Copias de respaldo
4. Requisitos de programación, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.
5. Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.
6. Restricciones en el uso de utilitarios del sistema.
7. Contactos de apoyo y personas de soporte a contactar en caso de dificultades operativas o técnicas inesperadas.
8. Instrucciones especiales para el manejo de “salidas”, como el uso de papelería especial o la gestión de elementos de salida confidenciales, incluyendo procedimientos para la eliminación segura de salidas fallidas de tareas.
9. Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.
10. Gestión de rastros de auditoría y de la información de registro del sistema.
11. Procedimientos de seguimiento.

Política para la construcción de sistemas seguros

Dominio A.14 - Adquisición, desarrollo y mantenimiento de sistemas

Objetivo: Establecer lineamientos para garantizar que la seguridad de la información este incluida dentro del ciclo de desarrollo de los sistemas de información.

La política se compone de los siguientes lineamientos, aplicables a los roles de seguridad de la información adoptados por la entidad:

Lineamientos:

1. La Oficina de Informática debe documentar y aplicar procedimientos de construcción de sistemas de información seguros basados en principios de construcción de seguridad y las debe incluir en el diseño de todas las capas de arquitectura.
2. El líder de Seguridad de la Información, debe verificar los lineamientos expuestos en el Instructivo Principios de Ingeniería para Sistemas Seguros (SI-I-003), para garantizar que cumpla con los estándares de seguridad en el ciclo de vida del desarrollo.
3. La Oficina de Informática debe aplicar los principios de construcción de sistema seguros a todos los nuevos desarrollos o cambios en los paquetes de software para garantizar la seguridad de la información.

4. La Oficina de Informática debe verificar que cada nuevo desarrollo se evalúe y se identifiquen los riesgos de seguridad de la información.
5. Para la adquisición de software con terceros, se debe cumplir con los siguientes requerimientos: - Los acuerdos de licenciamiento, propiedad de los códigos y propiedad intelectual.
   - Los ensayos de aceptación para determinar la calidad y exactitud de los entregables.
   - El suministro de evidencia que garantiza que el software no incluye contenido malicioso y cumple con niveles aceptables de seguridad.

Política para la gestión de incidentes

Dominio A.16 - Gestión de incidentes de seguridad de la información

Objetivo: Establecer lineamientos para asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

La política se compone de los siguientes lineamientos, aplicables a los roles de seguridad de la información adoptados por la entidad:

Lineamientos:

1. La entidad debe definir:
   - Los medios dispuestos por la entidad para el reporte de los incidentes de seguridad de la información.
   - Los mecanismos y métodos para la recolección de evidencias de los incidentes de seguridad de la información.

2. La gestión de incidentes debe compartirse con todos los colaboradores, lo cual permite que puedan identificar y reportar todos los incidentes que afecten uno o varios de los pilares de seguridad de la información (confidencialidad, integridad y disponibilidad).
3. La gestión de incidentes debe contar con mecanismos o herramientas que permitan cumplir con los tiempos de respuesta antes los incidentes que se presenten.
4. A partir de los incidentes presentados, el líder de seguridad de la información debe proporcionar los mecanismos para el aprendizaje que permitan reducir la probabilidad de ocurrencia de incidentes semejantes.

Política para la continuidad de seguridad de la información

Dominio A.17 - Aspectos de seguridad de la información de la gestión de continuidad del negocio

Continuidad de seguridad de la información

Objetivo: Establecer lineamientos para incluir la continuidad de seguridad de la información en los sistemas de gestión de la continuidad de negocio de la entidad.

La política se compone de los siguientes lineamientos, aplicables a los roles de seguridad de la información adoptados por la entidad:

Lineamientos:

1. El líder de seguridad de la información debe determinar los requisitos de seguridad de la información que deben mantenerse durante una crisis o desastre. Para ello debe tener en cuenta inicialmente el inventario y clasificación de activos de información (SGSI-F-002) y el procedimiento gestión del riesgo (MC-P-003).
2. El líder de seguridad de la información debe realizar el análisis de impacto al negocio (BIA) en el formato establecido por la entidad, para determinar, principalmente, los activos críticos y controles que soportan los requisitos de seguridad de la información.
3. El líder de seguridad de la información debe asegurar la gestión adecuada de los incidentes de seguridad a través del **INSTRUCTIVO PARA LA GESTIÓN DE INCIDENTES (GT-I-003).**
4. El líder de seguridad de la información debe identificar los escenarios más probables para el diseño de las estrategias de continuidad, de acuerdo con los resultados de la Valoración de Riesgos y el Análisis de Impacto al Negocio.
5. El Comité Interinstitucional de Desarrollo Administrativo debe evaluar y aprobar las estrategias de continuidad viables en términos de recursos, tiempo e impacto, presentadas por el líder de seguridad de la información.
6. Ante toda estrategia aprobada, el líder de seguridad de la información en conjunto con el responsable de la estrategia seleccionada, debe diseñar el plan de continuidad, el cual como mínimo debe contener:
    - Roles y responsabilidades definidos para la respuesta
    - Proceso de activación de la respuesta
    - Acciones inmediatas
    - Como recuperar las actividades en los tiempos definidos
    - Proceso para finalizar el incidente y volver a la operación normal
    - El árbol de llamadas (contiene los datos de los equipos que conforman el plan).
7. El Comité Interinstitucional de Desarrollo Administrativo debe aprobar el cronograma de ejercicios (pruebas) periódicas para cada uno de los planes de continuidad presentados. El cronograma debe indicar como mínimo, quiénes son los responsables de llevar a cabo cada una de las pruebas y de elevar el resultado obtenido al Comité Interinstitucional de Desarrollo Administrativo.
8. El líder de seguridad de la información debe asegurar que cada líder de proceso realice los ejercicios (pruebas) de los planes de continuidad de acuerdo al cronograma establecido. Así mismo, se deben generar informes una vez se ejecute cada prueba y/o ejercicio, que incluya recomendaciones y acciones para mejorar el plan.
9. Los planes de continuidad se deben revisar mínimo una vez al año o cuando se presenten cambios significativos que puedan afectar la continuidad de seguridad de la información, dejando registro de la aprobación y revisión de los mismos.
10. Los ejercicios (pruebas) deben ejecutarse de manera que se simule las condiciones de un desastre y no se afecte la operación.
11. El Plan de Continuidad debe ser socializado y comunicado al interior de la Superservicios.

12. Los líderes responsables del plan de continuidad, deben asegurarse de que el personal con responsabilidades en los planes, esté capacitado y entrenado en los procedimientos y planes definidos para la continuidad de seguridad de la información.

Redundancias

Objetivo: Establecer lineamientos para asegurar la disponibilidad de las instalaciones de procesamiento de información de la entidad.

La política se compone de los siguientes lineamientos, aplicables a los roles de seguridad de la información adoptados por la entidad:

Lineamientos:

1. Ante la ocurrencia de un incidente o desastre que inhabilite el centro de datos, la entidad a través de la Oficina de Informática, debe contar con un plan documentado para implementar la estrategia de continuidad, que permita dar continuidad a las aplicaciones de los procesos misionales, hasta el momento del retorno a la operación normal.

2. La alta dirección debe proveer a la Oficina de Informática, los recursos necesarios para mantener la continuidad de las aplicaciones de los procesos misionales, tales como: recurso humano, proveedores y los necesarios para implementar planes de continuidad tecnológicos actualizados y aprobados.

Política de seguridad para las relaciones con proveedores

Dominio A.15 - Relaciones con los proveedores

Objetivo: Establecer lineamientos para asegurar la protección de los activos de información de la entidad, que sean accesibles a los proveedores.

La política se compone de los siguientes lineamientos, aplicables a los roles de seguridad de la información adoptados por la entidad:

Lineamientos:

1. Antes del proceso de contratación, durante la fase de planeación, el comité evaluador debe identificar sí el objeto de la propuesta u oferta evaluada, requiere del acceso de los proveedores a la información, sistemas de información y/o áreas seguras de la entidad. De acuerdo al tipo de acceso que se requiera, el comité evaluador debe contar con la participación del líder de seguridad de la información a fin de determinar los requisitos mínimos de seguridad y los controles necesarios por parte del proveedor para ejecutar dicho contrato. En cualquiera de los casos, se debe dar a conocer a los proveedores las políticas complementarias de seguridad de la información.

2. Así mismo, la identificación de los riesgos de seguridad de la información debe ser parte de la estimación y cobertura de los riesgos del proceso de contratación, los cuales se deben incluir en los documentos de estudios previos según corresponda. De acuerdo con lo anterior, el análisis de riesgos de seguridad de la información debe incluir la identificación de los mismos en la respectiva contratación, su clasificación, probabilidad de ocurrencia estimada, su impacto, la determinación de la parte que debe asumirlos, el tratamiento que se les debe dar para eliminarlos o mitigarlos y las características del monitoreo más adecuado para administrarlos.
3. En medio de la etapa pre contractual, se debe asegurar la inclusión de la cláusula de confidencialidad, protección de datos, derechos de propiedad intelectual y derechos de autor, en la suscripción y perfeccionamiento del contrato que se celebre entre la entidad y aquellos proveedores que tendrán acceso a la información de la Superservicios.
4. Durante la ejecución del contrato, es función del supervisor y/o interventoría asignada, monitorear y hacer seguimiento a los controles pactados para asegurar la confidencialidad, integridad y disponibilidad de la información, frente a los riesgos previamente identificados.
5. Como parte de la supervisión a la ejecución del contrato, se debe contemplar procesos de auditoria a proveedores cuyo objetivo sea validar el cumplimiento de los requisitos de seguridad de la información estipulados desde la fase de planeación de la contratación, dichos resultados deben quedar consignados también en los informes presentados por el supervisor del contrato.
6. Para los servicios de tecnología y de comunicaciones contratados externamente, se debe exigir que los proveedores divulguen los requisitos y prácticas de seguridad de la entidad, a lo largo de la cadena de suministro.
7. Toda gestión que represente una modificación, mantenimiento, revisión al servicio de tecnología de la información, comunicaciones o equipos de suministros, debe pasar por el Procedimiento para la Gestión de Cambios de Seguridad de la Información (SGSI-P-004) y seguir las directrices del líder de seguridad de la información, antes de su ejecución.
8. Para la contratación de servicios o componentes de la infraestructura de TI y/o áreas seguras, se debe exigir a los proveedores la presentación de los planes de contingencia que aseguren la disponibilidad de la información, suministrada y procesada entre las partes.
9. Antes de iniciar la ejecución del contrato, el supervisor debe socializar a los proveedores el Instructivo para la Gestión de Incidentes de Seguridad de la Información (GT-I-003) y acordar el canal para su debido reporte.
10. Los demás lineamientos deben aplicarse de acuerdo al Manual de Contratación y el Manual de supervisión e interventoría definidos por la entidad.

Política de procedimientos operativos para la gestión de la tecnología y las comunicaciones

Dominio A.12 – Seguridad de las Operaciones

Objetivo: Establecer lineamientos para asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

La política se compone de los siguientes lineamientos, aplicables a los roles de seguridad de la información adoptados por la entidad:

Lineamientos:

1. La Oficina de Tecnologías de la Información, debe documentar todos los procedimientos operacionales asociados con la gestión de la infraestructura tecnológica y las comunicaciones, tales como, copias de respaldo, mantenimiento de equipos, gestión del correo electrónico y demás procesos que se lleven a cabo para garantizar la confidencialidad, integridad y disponibilidad de los dispositivos tecnológicos a cargo de esta oficina.
2. Todos los instructivos, guías o manuales que involucren lineamientos para la gestión de las operaciones de tecnología y las comunicaciones deben ser avalados y aprobados en el SIGME.
3. Cada documento que se desarrolle para la operación y gestión de la tecnología y las comunicaciones, debe seguir los lineamientos del *Instructivo para la elaboración y control de la documentación MC-I-001.*

SANCIONES

Todo funcionario, contratista y/o parte externa está en la obligación de cumplir a cabalidad cada lineamiento, de lo contrario, se verá expuesto inicialmente a los procesos disciplinarios que la entidad determine.

El incumplimiento puede llegar a sanciones administrativas, disciplinarias y hasta penales como lo establece la Ley 1273 de 2009, respecto a los Delitos Informáticos.

5.14 POLÍTICA EDITORIAL

La Superintendencia de Servicios Públicos Domiciliarios cumple todos los lineamientos establecidos en el Manual para la implementación de la Estrategia de Gobierno en línea en las entidades del orden nacional de la República de Colombia, para la cual se compromete a que toda la información de interés para la ciudadanía sea oportuna, clara y verazmente publicada en el portal WEB de la entidad.
La información disponible es de carácter público y se caracterizará por las siguientes consideraciones:

1. Administración y producción de contenido

- Los documentos son elaborados y están bajo responsabilidad de las diferentes dependencias de la entidad, conforme a sus funciones y competencias, y los lineamientos de la estrategia “Gobierno en Línea”.
- La publicación de contenidos y control de actualizaciones del portal institucional está a cargo del Grupo de Comunicaciones de la superintendencia.
- Cada área cuenta con un enlace que interactúa con el Grupo de Comunicaciones para el envío y solicitud de publicación de contenidos.
- La administración de otros sitios web enlazados en el portal institucional está a cargo y son responsabilidad del área competente. Deben atender los lineamientos de imagen y estilo de la superintendencia.

- La administración de los foros virtuales está a cargo del Grupo de Comunicaciones.
- La apertura y cierre de foros debe ser solicitada por el área que lo requiera al Grupo de Comunicaciones. El área solicitante está a cargo de la moderación, seguimiento y control del foro.

2. Periodicidad y responsabilidad de producción de contenidos

MENÚ	SUBMENÚS	RESPONSABLE	PERIODICIDAD PUBLICACIÓN
Institucional	Superintendente	Despacho / Grupo de Comunicaciones	Conforme a necesidades
	Misión y Visión	Oficina Asesora de Planeación	
	Objetivos		
	Funciones		
	Política de calidad		
	Organigrama		
	SIGME		
	Oficina de control interno	Oficina de Control Interno	Permanente
	Gestión financiera	Dirección Financiera	Mensual
	Planeación	Oficina Asesora de Planeación	
	Talento Humano	Dirección Administrativa / Grupo Talento Humano	Permanente
	Rendición de cuentas	Oficina Asesora de Planeación / Dirección General Territorial	
	Sitios de interés	Todas las dependencias	Conforme a necesidades
	Notificaciones	Secretaría General / Grupo de Notificaciones	Permanente
	Gestión Documental	Secretaría General / Grupo de Gestión Documental	Conforme a necesidades
Acueducto, Alcantarillado y Aseo	Acueducto y alcantarillado	Dirección Técnica de Gestión de AA	Permanente
	Aseo	Dirección Técnica de Gestión de Aseo	
	Pequeños prestadores	Grupo Pequeños Prestadores	
	Certificaciones	Delegada / Grupo de Certificaciones	
Energía y gas	Energía	Dirección Técnica de Gestión de Energía	Permanente
	Gas	Dirección Técnica de Gestión de Gas	
	Gas Licuado de Petróleo	Dirección Técnica de Gestión de Gas	
Intervenidas	Administración		

MENÚ	SUBMENÚS	RESPONSABLE	PERIODICIDAD PUBLICACIÓN
	Liquidación	Dirección de Entidades Intervenidas y en Liquidación	Conforme a necesidades
	Normatividad intervenidas		
	Gestión		Anual
Participación ciudadana	Eventos	Dirección General Territorial y territoriales	Conforme a necesidades
	Vocales de control	Dirección General Territorial	
Servicio al ciudadano	Calendario	Todas las dependencias	Conforme a necesidades
	Tramite su solicitud	Dirección General Territorial	
	Direcciones territoriales	Dirección General Territorial	
	Estadísticas		Anual
	Servicio al ciudadano		Permanente
	Preguntas frecuentes		Permanente
	Chat con el ciudadano		Permanente
	Foros	Grupo de Comunicaciones / área solicitante	Conforme a necesidades
	Formulario de Contacto		Conforme a necesidades
Servicio a empresas	Proceso NIIF	Grupo NIIF	Conforme a necesidades
	RUPS		Conforme a necesidades
	Formatos de pago	Dirección Financiera	Conforme a necesidades
	Preguntas NIIF	Grupo NIIF	Conforme a necesidades
	Distintivo vigilado Superservicios	Despacho / Grupo de Comunicaciones	Conforme a necesidades
	SUI	Grupo SUI	Permanente
	Correo electrónico	Secretaría General / Grupo Gestión Documental	NA
	Formulario de Contacto		Conforme a necesidades
Sala de Prensa	Comunicados	Despacho / Grupo de Comunicaciones	Conforme a necesidades
	Noticias		
	Red de Apoyo Informativo		
	Videos institucionales		
	Audios institucionales		
Publicaciones	A.A.A	Oficina Asesora de Planeación	Conforme al Plan Anual de Publicaciones
	Contratación		
	El Observador		
	Energía		
	Entidades territoriales		

MENÚ	SUBMENÚS	RESPONSABLE	PERIODICIDAD PUBLICACIÓN
	Guías de uso		
	Información institucional		
	NIIF		
	Planeación		
	SUI		
Contratación	Contratación	Secretaría General/ Dir. Administrativa	Conforme a necesidades

3. Características del contenido

- Los contenidos son de carácter institucional, por ello, no reflejan posiciones políticas, religiosas, económicas o de otra índole.
- Los contenidos no incluyen calificativos ofensivos ni discriminatorios en relación con la raza, credo político o religioso, de género, discapacidad, ubicación geográfica, apariencia física o estrato social, ni refleja los intereses, gustos, o tendencias particulares.
- Los contenidos mantienen la privacidad. No se publican contenidos que revelen aspectos confidenciales de las personas o la entidad, que afecten el buen nombre o que puedan generar efectos legales adversos por su publicación.
- Los contenidos corresponden a las competencias de la entidad. En caso de publicar contenidos tomados de un tercero, se referencia la fuente de donde se obtuvieron.
- No se publican procesos sancionatorios en trámite, para no afectar la reserva de ley.
- En los casos en que se solicite información de los particulares, se aclarará que la misma sólo será utilizada para los fines para los cuales fue solicitada y que no será divulgada a terceros sin consentimiento de quien suministra la información, salvo en los casos previstos por la ley.
- Los contenidos que correspondan a archivos para descargar indican la fecha de publicación o de su última actualización.
- Los comunicados de prensa que señalen posición institucional en temas críticos son publicados previa revisión del Despacho o área autorizada por el mismo.
- Las fotografías que se carguen en el sitio web están en formato jpg o pgn.
- Las imágenes publicadas deben ser etiquetadas.
- Los enlaces externos publicados en el sitio web tienen relación con entidades públicas o privadas, en concordancia con las necesidades propias de la entidad o de directrices de Gobierno.

4. Uso del lenguaje y estilo

- La redacción de las publicaciones cumple los lineamientos del manual de estilo de la SSPD.
- Se utiliza un lenguaje objetivo, claro, sencillo, sin exceso de adjetivos.

- Se deben seguir las reglas sintácticas, gramáticas y ortográficas del idioma español, de acuerdo con la Real Academia de la Lengua Española.
- Se debe evitar el uso de términos en idiomas extranjeros. Cuando sea necesario utilizarlos, se explicará su equivalencia en idioma español.
- Cuando sea necesario utilizar siglas, tecnicismos y abreviaturas, se especificará el significado en el propio documento o información publicada.
- No se deben utilizar regionalismos o frases coloquiales que son de uso común en algún lugar del país pero que en otras regiones pueden ser consideradas ofensivas.
- Al referenciar fechas, el nombre de los meses no se debe abreviar.
- Las imágenes, dibujos, fotos y cualquier otro material gráfico deben estar acorde con los textos. Cuando este tipo de material sufra algún tipo de tratamiento técnico (por ejemplo: montajes, composición, transparencias, etc.), se indicará claramente en el pie del material que éste ha sido tratado y ha sufrido modificaciones de su versión original.

5. Derechos de autor

- Las obras protegidas por el derecho de autor que se encuentren dentro del sitio web hacen parte del patrimonio de la entidad; y por lo tanto son considerados bienes fiscales. Por ello, su utilización debe estar autorizada expresamente indicando que se puede hacer con el material.
- El uso (reproducción, transformación, o puesta a disposición) de contenidos de terceros protegidos por el derecho de autor, deben contar con la debida autorización del titular de los derechos.
- El uso de textos, elementos gráficos, audios, videos, bases de datos, entre otros materiales tomados de fuentes externas y sujetos a derechos de autor deben ser referenciados como tal. En caso de textos, se utilizará entre comillas (“”) incluyendo, como mínimo nombre del autor, libro o documento origen.

5.15 POLITICA DE PRIVACIDAD, TERMINOS DE USO Y PROTECCIÓN DE DATOS PERSONALES

El sitio WEB de la Superintendencia de Servicios Públicos Domiciliarios se compromete a publicar los temas y actividades relacionados con su referente estratégico, funciones, trámites, servicios y en general toda la información que establece el Manual para la implementación de la estrategia de Gobierno en línea en las entidades del orden nacional de la República de Colombia.

La Superintendencia de Servicios Públicos Domiciliarios solicita al visitante y al usuario de la página, que lean detalladamente las condiciones y la política de privacidad, antes de iniciar su exploración o utilización. Si alguno de los dos, no está de acuerdo con las condiciones o con cualquier disposición de la política de privacidad, le sugerimos que se abstenga de acceder o navegar por la página WEB de la entidad.

Aceptación de Términos

Cuando un usuario accede al sitio WEB de la Superintendencia de Servicios Públicos Domiciliarios lo hace bajo su total responsabilidad y por tanto acepta plenamente y sin reservas el contenido de los términos y condiciones de uso del sitio WEB de la entidad. La Superintendencia de Servicios Públicos

Domiciliarios se reserva, en todos los sentidos, el derecho de actualizar y modificar en cualquier momento y, de cualquier forma, de manera unilateral y sin previo aviso, las presentes condiciones de uso y los contenidos de la página.

La página WEB de la entidad tiene enlaces a otros sitios de interés o a documentos localizados en otras páginas WEB de propiedad de otras entidades, personas u organizaciones diferentes a la Superintendencia de Servicios Públicos Domiciliarios. Solamente por el hecho de que el usuario acceda a otro sitio WEB o a un documento individual localizado en otra página, a través de un link o un vínculo establecido en el sitio WEB de la Superintendencia de Servicios Públicos Domiciliarios, el usuario debe someterse a las condiciones de uso y a la política de privacidad de la página WEB a la que envía el link.

La prestación del servicio del sitio WEB de la Superintendencia de Servicios Públicos Domiciliarios es de carácter libre y gratuito para los usuarios y se rige por los términos y condiciones que se incluyen a continuación, los cuales se entienden como conocidos y aceptados por los (las) usuarios (as) del sitio:

1. Propiedad del contenido de la Página - Copyright

El sitio de Internet y el contenido son de propiedad de la Superintendencia de Servicios Públicos Domiciliarios. Está prohibida su reproducción total o parcial, su traducción, inclusión, transmisión, almacenamiento o acceso a través de medios analógicos, digitales o de cualquier otro sistema o tecnología creada, sin autorización previa y escrita de la Superintendencia de Servicios Públicos Domiciliarios.

Sin embargo, es posible descargar material de www.superservicios.gov.co para uso personal y no comercial, siempre y cuando se haga expresa mención de la propiedad en cabeza de la Superintendencia de Servicios Públicos Domiciliarios.

Con respecto a los contenidos que aparecen en el sitio WEB de la Superintendencia de Servicios Públicos Domiciliarios, el usuario se obliga a:

- Usar los contenidos de forma diligente, correcta y lícita.
- No suprimir, eludir, o manipular el copyright (derechos de autor) y demás datos que identifican los derechos de la Superintendencia de Servicios Públicos Domiciliarios.
- No emplear los contenidos y, en particular, la información de cualquier otra clase obtenida a través de la Superintendencia de Servicios Públicos Domiciliarios o de los servicios, para emitir publicidad.
- La Superintendencia de Servicios Públicos Domiciliarios no será responsable por el uso indebido que hagan los usuarios del contenido de su sitio WEB.
- El usuario del sitio WEB se hará responsable por cualquier uso indebido, ilícito o normal que haga de los contenidos, información o servicios del sitio WEB de la Superservicios.
- El usuario del sitio WEB de la Superintendencia de Servicios Públicos Domiciliarios, no incurrirá en y desde el mismo, en conductas ilícitas como daños o ataques informáticos, interceptación de

comunicaciones, infracciones al derecho de autor, uso no autorizado de terminales, usurpación de identidad, revelación de secretos o falsedad en los documentos.

2. Protección de la información principal

Privacidad

La información personal es aquella suministrada por el Usuario para el registro, incluye datos como nombre, identificación, edad, género, dirección, correo electrónico y teléfono. Para salvaguardad la privacidad de la información personal del Usuario obtenida a través de la página WEB de la entidad, se cumplen los principios de protección de datos personales de acuerdo a la ley 1581 de 2012. Los lineamientos de la entidad para el acceso a la información pública y el tratamiento de datos personales, se encuentran definidos por la entidad en el Manual de divulgación de información y política de protección de datos personales que se encuentra en el proceso de Gestión de Conocimiento SIGME.

La entidad ha adoptado niveles de seguridad de protección de los datos personales, instalando medidas técnicas necesarias para evitar la pérdida, mal uso, alteración, accesos no autorizados y robo de los datos facilitados. La información personal proporcionada por el Usuario está asegurada por una clave de acceso que sólo él conoce. Por tanto, es el único responsable de mantener en secreto su clave. La Superintendencia de Servicios Públicos Domiciliarios se compromete a no acceder ni pretender conocer dicha clave. Debido a que ninguna transmisión por Internet es absolutamente segura ni puede garantizarse dicho extremo, el Usuario asume el hipotético riesgo que ello implica, el cual acepta y conoce.

La Superintendencia de Servicios Públicos Domiciliarios protege la infraestructura que involucra la página WEB desde sus servidores hasta la salida a Internet, sin embargo, ninguna transmisión por Internet puede garantizar su seguridad al 100%. Por tal motivo el sitio de La Superintendencia de Servicios Públicos Domiciliarios no puede garantizar que la información ingresada a su sitio WEB o transmitida utilizando su servicio, sea completamente segura, con lo cual el usuario corre su propio riesgo.

La Superintendencia de Servicios Públicos Domiciliarios podrá utilizar cookies durante la prestación de servicios en nuestro Sitio WEB.

Finalidad y tratamiento de los datos

El Usuario de manera voluntaria ingresa información personal para realizar un trámite, presentar una queja o reclamo, o para acceder a los mecanismos interactivos que la página de la Superintendencia de Servicios Públicos Domiciliarios contiene. El usuario tiene conocimiento que los datos por él consignados harán parte de un archivo y/o base de datos que podrá ser usado por la entidad para efectos de surtir el proceso solicitado por el Usuario.

3. Duración y terminación

La prestación del servicio del sitio WEB de la Superintendencia de Servicios Públicos Domiciliarios tiene una duración indefinida. Sin embargo, la entidad podrá dar por terminada o suspender la prestación de

este servicio en cualquier momento. En caso de que se llegue a presentar esta situación, la Superintendencia de Servicios Públicos Domiciliarios informará previamente sobre el hecho, para evitar mayores traumatismos.

Igualmente, la Superintendencia de Servicios Públicos Domiciliarios no podrá garantizar la disponibilidad de los servicios en línea y de la información que los usuarios requieran en determinado momento. Tampoco incurrirá en responsabilidad con el usuario o terceros, cuando su sitio WEB no se encuentre disponible