CONTRALORÍA MUNICIPAL DE ITAGÜÍ

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
Vigencia 2022

Itagüí, 28 enero de 2022

1. GENERALIDADES

La dirección de Contraloría Municipal de Itagüí, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para la Contraloría Municipal de Itagüí, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios. terceros, aprendices, practicantes y clientes de Contraloría Municipal de Itagüí.
- Garantizar la continuidad del negocio frente a incidentes.
- La Contraloría Municipal de Itagüí ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

  La política se seguridad y privacidad de la información al ser transversal a todos los procesos y procedimiento de la entidad, tiene en cuenta el Plan Estratégico de Tecnologías de la Información -PETIC-, el Plan de contingencia (anexo 1 de la presente resolución), la política editorial y el registro de activos de información.

En virtud de la Política de seguridad y privacidad de la Información se establecen 12 principios de seguridad que soportan el SGSI de La Contraloría Municipal de Itagüí:

- Las **responsabilidades** frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de **los empleados, proveedores, socios de negocio o terceros.**

- La Contraloría Municipal de Itagüí **protegerá la información g**enerada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos **otorgados a terceros** (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

- La Contraloría Municipal de Itagüí **protegerá la información creada,** procesada, transmitida o resguardada por sus procesos de negocio, 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.

- La Contraloría Municipal de Itagüí **protegerá su información d**e las amenazas originadas por parte **del personal.**

- La Contraloría Municipal de Itagüí ***protegerá las instalaciones de*** *procesamiento y la infraestructura tecnológica* ***que soporta sus procesos críticos.***

- La Contraloría Municipal de Itagüí **controlará la operación** de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y la**s redes de datos.**

- La Contraloría Municipal de Itagüí **implementará control de acceso a la** información, sistemas y recursos de red.

- La Contraloría Municipal de Itagüí garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- La Contraloría Municipal de Itagüí garantizará 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.

- La Contraloría Municipal de Itagüí **garantizará la disponibilidad de sus** procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

- La Contraloría Municipal de Itagüí garantizará el cumplimiento de las **obligaciones legales, regulatorias y contractuales establecidas.**

2. FASES DE IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Desarrollo de las políticas: En esta fase la Entidad debe responsabilizar las **áreas para** la creación de las políticas, estructurarlas, escribirlas, revisarlas y aprobarlas; por lo cual para llevar a buen término esta fase se requiere que se realicen actividades de verificación e investigación de los siguientes aspectos:

Cumplimiento: Fase mediante la cual todas aquellas políticas escritas deben estar implementadas y relacionadas a los controles de seguridad de la Información, esto con el fin de que exista consistencia entre lo escrito en las políticas versus los controles de seguridad implementados y documentados.

Comunicación: Fase mediante la cual se da a conocer las políticas a los funcionarios, contratistas *y/*o terceros de la Entidad. Esta fase es muy importante toda vez que del conocimiento del contenido de las políticas depende gran parte del cumplimiento de las mismas; esta fase de la implementación también permitirá obtener retroalimentación de la efectividad de las políticas, permitiendo así realizar excepciones, correcciones y ajustes pertinentes. Todos los funcionarios contratistas *y/*o terceros de la entidad deben conocer la existencia de las políticas, la obligatoriedad de su cumplimiento y la ubicación física de tal documento o documentos, para que sean consultados en el momento que se requieran.

***M*onitoreo**: Es importante que las políticas sean monitoreadas para determinar la efectividad y cumplimiento de las mismas, deben crearse mecanismos ejemplo indicadores para verificar de forma periódica y con evidencias que la política funciona y si debe o no ajustarse.

Mantenimiento: Esta fase es la encargada de asegurar que la política se encuentra actualizada, integra y que contiene los ajustes necesarios y obtenidos de las retroalimentaciones.

Retiro: Fase mediante la cual se hace eliminación de una política de seguridad en cuanto esta ha cumplido su finalidad o la política ya no es necesaria en la Entidad.

Esta es la última fase para completar el ciclo de vida de las políticas de seguridad y requiere que este retiro sea documentado con el objetivo de tener referencias y antecedentes sobre el tema.

3. POLÍTICAS ESPECÍFICAS PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

3.1 Gestión de activos (Registro de activos de información)

A continuación, se muestra el grupo de políticas que deben hacer referencia a las directrices mediante las cuales se indica a los funcionarios los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de Información, las políticas relacionadas con gestión de activos deben contemplar como mínimo:

Identificación de Activos: Esta política debe determinar la periodicidad con la cual se va a realizar al interior de la Entidad la identificación *y/o* actualización del inventario de Activos de Información, la política debe determinar el responsable de realizar la actividad, se debe determinar bajo que instrumento se va a realizar la actividad, dicho instrumento debe permitir identificar el propietario del activo de información.

Clasificación de Activos: La Entidad debe determinar la clasificación de los activos de información de acuerdo con la criticidad, sensibilidad y reserva de la misma. En la elaboración de esta política debe tenerse en cuenta las leyes y normatividades actuales que afecten a la Entidad, algunos ejemplos: Ley 1581 de 2012, Decreto 1377 de 2013, Ley 1712 de 2014, Decreto 103 de 2015, entre otras que puedan aplicar de acuerdo con la naturaleza de la entidad.

Etiquetado de la Información: Esta política debe determinar el mecanismo, responsable y obligatoriedad para el etiquetado o rotulación de Activos.

Devolución de los Activos: Esta política debe determinar el instrumento y responsable del cumplimiento, mediante el cual se genera obligatoriedad para que los funcionarios, contratistas *y/*o terceros realicen la entrega de activos físicos y de la información una vez finalizado el empleo, acuerdo o contrato que se tenga con la Entidad.

Gestión de medios removibles: Esta política debe contemplar los usos y permisos que tienen los usuarios y*/o* funcionarios de la Entidad frente a los medios removibles, entendiendo como medio removible a todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los

computadores. Esta política debe describir detenidamente en qué casos se autoriza y en los que no, el uso de medios removibles y los procedimientos en los cuales se determinen las autorizaciones; adicionalmente debe describir el responsable de las autorizaciones *y* responsabilidades de aquellas personas que tienen autorización para el uso del dicho medio de almacenamiento. El uso de medios removibles en la entidad debe ir alineados a las clasificaciones de activos dispuestas en la política de "Clasificación de Activos".

3.2 Control de Acceso (Plan de Contingencia)

Control de acceso con usuario y contraseña: Se debe elaborar una política sobre control de acceso a redes, aplicaciones, y/o sistemas de información de la entidad, mediante la cual se determinen los responsables y los procedimientos formales de autorización de creación, modificación, suspensión o eliminación de usuarios (ID) y contraseñas. La política debe enunciar las responsabilidades que los funcionarios, contratistas o terceros tienen al contar con un usuario o contraseña de la entidad, se debe estipular que los usuarios (ID) y contraseñas son personales e intransferibles y no deben prestarse, ni compartirse. La entidad debe establecer que por cada funcionario, contratista o tercero debe tenerse un usuario y una contraseña para el acceso.

Suministro del control de acceso: Esta política debe determinar los procedimientos formales y directrices que se deben construir para la gestión de asignación, modificación, revisión o revocación de derechos privilegios a cada uno de los usuarios (ID) creados, también deben tenerse en cuenta en esta política los casos especiales como lo son usuarios (ID) con privilegios superiores utilizados para la administración de infraestructura, aplicaciones y sistemas de información de la entidad.

Gestión de Contraseñas: Esta política debe definir los lineamientos mínimos en cuanto a calidad que deben tener las contraseñas para ser utilizadas como mecanismo de autenticación en los accesos a la red, aplicaciones y/o sistemas de información de la entidad. Esta política debe indicar a los funcionarios, contratistas *y/*o terceros los parámetros mínimos para que una contraseña sea considera como fuerte, gestión de cambio de contraseña, debe determinar que los accesos a la red, las aplicaciones y sistemas de información deben requerir un usuario (ID) y una contraseña fuerte para que realice la correspondiente autenticación y acceso a la información de forma segura.

Perímetros de Seguridad: La política debe definir los perímetros físicos de seguridad donde se encuentra información crítica, sensible o se realice almacenamiento *y/*o procesamiento de información a los cuales los funcionarios,

contratistas o terceros, tienen acceso y a cuáles no, la política debe definir los responsables de autorizar o no ingresos a las áreas delimitadas como de acceso restringido.

Áreas de Carga: La política debe definir las condiciones e instalaciones físicas en las cuales se va a realizar despacho y carga de paquetes físicos para bodegas o espacios definidos de carga, esto con el fin de evitar el acceso no autorizado a otras áreas de la entidad. Esta política debe determinar el seguimiento que se debe realizar para garantizar.

3.3 Privacidad y Confiabilidad

Esta política debe contener una descripción de las políticas de tratamiento y protección de datos personales que deben ser aplicados, conforme a lo establecido en la normatividad vigente. La política de privacidad debe contener como mínimo lo siguiente:

- Ámbito de aplicación

- Excepción al ámbito de aplicación de las políticas de tratamiento de datos Personales.

- Principios del tratamiento de datos personales:

  - **Principio de la Legalidad**: El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente.
  - **Principio de finalidad:** Indicar la finalidad del tratamiento de datos personales, la cual debe ser informada al titular.
  - **Principio de libertad:** El tratamiento sólo puede hacerse con el consentimiento previo, expreso e informado del titular de los datos
  - **Principio de veracidad o calidad:** La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible
  - **Principio de transparencia:** Garantizar al titular de los datos el derecho a obtener información que le concierna del encargado del tratamiento.
  - **Principio de acceso y circulación restringida:** El tratamiento sólo podrá hacerse por personas autorizadas por el titular o por personas previstas en la normatividad vigente.
  - **Principio de seguridad:** La información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- **Principio de confidencialidad:** Todas las personas que participen en el Tratamiento de Datos Personales deben garantizar la reserva de dicha información.

- **Derechos de los titulares:** La política debe indicar los derechos de los titulares de los datos, tales como:

  - Conocer, actualizar y rectificar sus datos personales.
  - Solicitar la prueba de su autorización para el tratamiento de sus datos personales.
  - Ser informado respecto del uso que se les da a sus datos personales.
  - Revocar la autorización *y/o* solicitar la supresión de sus datos personales de las bases de datos o archivos cuando el titular lo considere, siempre y cuando no se encuentren vigentes con el Banco los servicios o productos que dieron origen a dicha autorización.
  - Presentar quejas ante la entidad administrativa encargada de la protección de los datos personales

- **Autorización del titular**: La política debe indicar cómo obtener autorización del titular para el tratamiento de sus datos personales, así como los casos en los cuales no se requiere autorización del titular.

- **Deberes de los responsables del Tratamiento**: La política debe indicar cuales son los deberes de los responsables *y/o* encargados del tratamiento de los datos personales.

- **Política de controles criptográficos**: Esta política deberá especificar como se asegura la confidencialidad y autenticidad de la información que circula o se genera a través de los diferentes sistemas de información

3.4 Integridad

La política de integridad debe ser conocida y aceptada por todos los funcionarios, contratistas y/o terceros que hagan parte de la Entidad, la cual se refiere al manejo íntegro e integral de la información tanto interna como externa, conocida o administradas por los mismos.

De esta manera, toda información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas *y/o* responsables de dicha información. En el caso de

vinculación contractual, el Compromiso de administración y manejo integro e integral de la información interna y externa hará parte de las cláusulas del respectivo contrato, bajo la denominación de Cláusula de integridad de la información.

La política de inte89gridad deberá establecer asimismo la vigencia de la misma acorde al tipo de vinculación del personal al cual aplica el cumplimiento

3.5 Disponibilidad del servicio e información

La Entidad deberá contar con un plan de continuidad del negocio con el fin de asegurar, recuperar o restablecer la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la Información y procesos misionales de la Entidad, ante el evento de un incidente de seguridad de la información.

La política de disponibilidad debe incluir como mínimo los siguientes aspectos:

- **Niveles de disponibilidad: E**sta política debe velar por el cumplimiento de los niveles de disponibilidad de servicios e información acordados con clientes, proveedores *y/o* terceros en función de las necesidades de la Entidad, los acuerdos de nivel de servicios ofrecidos y evaluaciones de riesgos.
- **Planes de recuperación:** La política debe incluir los planes de recuperación que incluyan las necesidades de disponibilidad del negocio.
- **Interrupciones:** La política debe velar por la gestión de interrupciones de mantenimiento de los servicios que afecten la disponibilidad del mismo.
- **Acuerdos de Nivel de servicio**: Tener en cuenta los acuerdos de niveles de servicios (ANS) en las interrupciones del servicio.
- **Segregación de ambientes:** Esta política debe establecer la segregación de ambientes para minimizar los riesgos de puesta en funcionamiento de cambios y nuevos desarrollos con el fin de minimizar el impacto de la indisponibilidad del servicio durante las fases de desarrollo, pruebas y producción.
- **Gestión de Cambios: L**a política debe incluir gestión de cambios para que los pasos a producción afecten mínimamente la disponibilidad y se realicen bajo condiciones controladas.

3.6 Registro y auditoría

Esta política vela por el mantenimiento de las evidencias de las actividades y acciones que afectan los activos de información.

Esta política deberá contener:

- **Responsabilidad:** Incluir la responsabilidad de la Oficina de Control Interno y similares, acerca de la responsabilidad de llevar a cabo las auditorías periódicas a los sistemas y actividades relacionadas a la gestión de activos de información, así como la responsabilidad de dicha Oficina de informar los resultados de las auditorías.
- **Almacenamiento de registros:** La política debe incluir el almacenamiento de los registros de las copias de seguridad en la base de datos correspondiente y el correcto funcionamiento de estas. Los registros de auditoría deben incluir toda la información registro y monitoreo de eventos de seguridad.
- **Normatividad:** La política de auditoría debe velar porque las mismas sean realizadas acorde a la normatividad y requerimientos legales aplicables a la naturaleza de la Entidad.
- **Garantía cumplimiento:** La política de auditoría debe garantizar la evaluación de los controles, la eficiencia de los sistemas, el cumplimiento de las políticas y procedimientos de la Entidad; así como recomendar las deficiencias detectadas.
- **Periodicidad:** La política debe determinar la revisión periódica de los niveles de riesgos a los cuales está expuesta la Entidad, lo cual se logra a través de auditorías periódicas alineada a los objetivos estratégicos y gestión de procesos de la Entidad auditorías periódicas alineada a los objetivos estratégicos y gestión de procesos de la Entidad.

3.7 Gestión de Incidentes de seguridad de la información

La entidad deberá documentar una política general de gestión de eventos, incidentes y vulnerabilidades de seguridad de la información. Debe ir dirigida a todos los usuarios que tienen un acceso autorizado a cualquier sistema de información.

La política debe contemplar para su elaboración los siguientes parámetros:

- Debe estar aprobada por la alta dirección, certificando así el compromiso con el proceso.
- **Visión General:** ¿Qué se debe reportar? ¿A quién debe reportarse?, ¿Qué medios pueden emplearse para hacer el reporte?
- **Definir Responsables**: Se deben mencionar de manera muy general quienes serán los responsables de gestionar los eventos.
- **Actividades**: Explicar de manera general en que consiste el proceso de gestión de incidentes desde el reporte hasta la resolución.
- **Documentación:** Se debe hacer referencia sobre la documentación del esquema de gestión y los procedimientos.
- **Descripción del Equipo que Manejará los Incidentes:** Se debe indicar como está compuesta la estructura general para la gestión de incidentes y vulnerabilidades de seguridad.

- **Aspectos Legales: D**eben citarse los aspectos legales que se deben tener en cuenta o los cuales debe darse cumplimiento.

La Contraloría Municipal de Itagüí realizará una sensibilización sobre la Política de Seguridad y Privacidad de la Información para los funcionarios de la Entidad. En esta capacitación se deben resaltar los compromisos y obligaciones por parte de los funcionarios de la Contraloría Municipal de Itagüí, así como la Política de Escritorio Limpio, Política de Uso Aceptable y Ética Empresarial.

En el evento en que se requiera realizar ajustes al anexo que hace parte de esta Resolución, estos serán aprobados por el Comité de Gobierno en Línea.

El cumplimiento de la política de Seguridad y Privacidad de la Información y de actualización de contenidos tiene carácter obligatorio y el seguimiento estará cargo de la Oficina Asesora de Control Interno.

ALBA INÉS OSPINA MONTOYA
Líder CIO (Resolución 002/2022)