Política de Seguridad Digital

www.itagui.gov.co

Alcaldía de Itagüí | Dirección Administrativa de las TIC

Alcaldía de Itagüí

POLÍTICA DE SEGURIDAD DIGITAL

Política de Seguridad Digital – Versión 02.
Aprobada por: Comité Institucional de Gestión y Desempeño.
Acta No. 04 del 14 de diciembre de 2023.

Tabla de Contenido[1]

[1] Referencias tomadas del Documento CONPES 3854 de 2016 (Política Nacional de Seguridad Digital) y del Documento Modelo Nacional de Gestión de Riesgos de Seguridad Digital de 2018.

1 INTRODUCCIÓN[2]

Hacia los años 90 se empezó a hablar de “seguridad informática”, con el propósito de proteger la información y las redes, es decir, se trataba de algo más digital. Para el año 2000, se empezó a hablar de “seguridad de la información” y a tener en cuenta conceptos como la confidencialidad, la integridad y la disponibilidad.

Finalmente, en los últimos 8 años el concepto de seguridad se ha modificado dos veces, pasando de “ciberseguridad” a lo que actualmente se conoce como **“seguridad digital”**, la cual tiene un enfoque más humanístico y es definida como el “conjunto de estrategias para generar confianza en el mundo digital”.

Debido a ello, **Cybersafety** y **Cybersecurity** son conceptos claves, ya que hacen parte de la seguridad del mundo digital. El primero tiene como objetivo que el entorno digital no le haga daño a la persona, por lo que se encarga de situaciones como cyberbullying, grooming, sexting y el uso excesivo de internet (adicciones conductuales); mientras que Cybersecurity se encarga de velar por que las personas no afecten el mundo digital.

Es por lo anterior que, la Administración Municipal de Itagüí articula la gestión estratégica de la seguridad digital con la normatividad nacional y las directrices emitidas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), y formula esta Política con el fin de generar valor público y confianza digital mediante el uso y aprovechamiento de las tecnologías de la información y las comunicaciones, colocando a disposición de los grupos de valor y partes interesadas, servicios digitales de confianza y calidad que cuenten con esquemas de seguridad de la información, que estén alineados con la infraestructura tecnológica institucional y que generen un ambiente digital corresponsable, previsible y seguro.

[2] Universidad Externado de Colombia (2018).

2 ANTECEDENTES

2.1 DIMENSIONES DE LA POLÍTICA DE SEGURIDAD DIGITAL[3]

Con el fin de adoptar un enfoque multidimensional, que garantice la seguridad digital y atienda las necesidades y expectativas de todas las partes interesadas, se definen cinco dimensiones estratégicas (DE). Estas dimensiones determinan los campos de acción de la Política de Seguridad Digital.

Gobernanza de la seguridad digital: Articulación y armonización de las partes interesadas, bajo un marco institucional adecuado, para gestionar la seguridad digital bajo el liderazgo del Gobierno Municipal.

Marco legal y regulatorio de la seguridad digital: Marco legal y regulatorio que soporta todos los aspectos necesarios para adelantar la Política.

Gestión sistemática y cíclica del riesgo de seguridad digital: Conjunto de iniciativas, procedimientos o metodologías coordinadas para abordar, de manera cíclica y holística, los riesgos de seguridad digital en el municipio.

Cultura ciudadana para la seguridad digital: Sensibilización de las partes interesadas para crear y fomentar una cultura ciudadana responsable en la seguridad digital.

Capacidades para la gestión del riesgo de seguridad digital: Fortalecimiento y construcción de capacidades humanas, técnicas, tecnológicas, operacionales y administrativas en las partes interesadas, para adelantar la gestión de riesgos de la seguridad digital.

2.2 ESTRATEGIA DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL[4]

La estrategia de gestión de riesgos para abordar la seguridad digital tiene un enfoque flexible y ágil para abordar las incertidumbres digitales. Lo anterior, con el fin de alcanzar beneficios sociales y económicos, proveer servicios esenciales, operar infraestructuras críticas, preservar los derechos humanos y los valores fundamentales, y proteger a las personas frente a amenazas de seguridad digital (Organización para la Cooperación y el Desarrollo Económicos [OCDE], 2015).

De acuerdo con las recomendaciones de la OCDE (2015), esta estrategia debe ser consistente con el conjunto de principios formulados, debe crear las condiciones para que

[3] Documento CONPES 3854 de 2016 (Política Nacional de Seguridad Digital).
[4] Documento CONPES 3854 de 2016 (Política Nacional de Seguridad Digital).

las partes interesadas puedan gestionar la seguridad digital de sus actividades económicas y sociales, debe fomentar la confianza en el entorno digital y, además, debe: (i) estar apoyada desde el más alto nivel de gobierno; (ii) afirmar claramente que su objetivo es aprovechar el entorno digital abierto para la prosperidad económica y social; (iii) estar dirigida a todas las partes interesadas; y (iv) ser el resultado de un enfoque intra-gubernamental, coordinado, abierto y transparente.

La Política de Seguridad Digital: (i) adopta la gestión sistemática y cíclica del riesgo; (ii) es liderada desde el alto nivel del gobierno municipal; (iii) asegura la defensa y seguridad del territorio; (iv) estimula la prosperidad económica y social; (v) adopta un enfoque multidimensional, es decir, la seguridad digital es abordada tanto desde la dimensión técnica o jurídica, como desde la dimensión económica y social; (vi) tiene en cuenta a las partes interesadas; (vii) promueve la responsabilidad compartida; (viii) salvaguarda los derechos humanos; (ix) protege los valores institucionales; y (x) concientiza y educa.

2.3 MARCO LEGAL

Norma	Descripción
Constitución Política.	Artículo 15 que reconoce el derecho a la intimidad personal y familiar y al buen nombre. Artículo 20 en donde se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación. Artículo 76 que establece que el espectro electromagnético es un bien público inajenable e imprescriptible sujeto a la gestión y control del Estado. Artículo 101 que incluye al espectro electromagnético como parte del territorio colombiano.
Ley 527 de 1999 (Comercio Electrónico).	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Se tratan conceptos como: mensaje de datos (artículos 2 y 5), el principio de equivalencia funcional (artículos 6, 7, 8, 12, 13 y 28), la autenticación electrónica (artículo 17), la firma electrónica simple (artículo 7), la firma digital (artículo 28), y la firma electrónica certificada (artículo 30, modificado por el artículo 161 del Decreto Ley 019 de 2012).

Norma	Descripción
Ley 594 de 2000 (Ley General de Archivos).	Habilita el uso de nuevas tecnologías de manera general, lo cual viabiliza el uso de firmas electrónicas simples, certificadas y firmas digitales.
Ley 599 de 2000 (Código Penal).	En particular las materias atinentes a: i) violación a los derechos patrimoniales de autor y derechos conexos (modificación introducida por la Ley 1032 de 2006); ii) protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las TIC (modificación introducida por la Ley 1273 de 2009).
Ley 1266 de 2008.	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1273 de 2009.	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1437 de 2011 (Utilización de medios electrónicos en el procedimiento administrativo).	Consagra la utilización de medios electrónicos en el procedimiento administrativo, permitiendo adelantar trámites electrónicos, el uso de registros electrónicos, de documentos públicos en medios electrónicos, notificaciones electrónicas, archivos electrónicos de documentos, expedientes electrónicos y sedes electrónicas. Lo anterior, con el fin de que los ciudadanos interactúen con validez jurídica y probatoria (Capítulo IV, artículos 53 al 64.
Ley 1581 de 2012.	Por la cual se dictan disposiciones generales para la protección de datos. Esta Ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo, a los datos financieros se les continúa aplicando la Ley 1266 de 2008, excepto los principios.
Ley 1712 de 2014.	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Norma	Descripción
Ley 1928 de 2018.	Por medio de la cual se aprueba el “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest.
Ley 2080 de 2021.	Por medio de la cual se reforma el Código de Procedimiento Administrativo y de lo Contencioso Administrativo -Ley 1437 de 2011- y se dictan otras disposiciones en materia de descongestión en los procesos que se tramitan ante la jurisdicción.
Decreto 1151 de 2008.	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.
Decreto 2609 de 2012.	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
Decreto 2758 de 2012 (Modifica la estructura del Ministerio de Defensa Nacional).	Se reestructura la organización del Ministerio de Defensa Nacional, en el sentido de asignar al despacho del viceministro la función de formular políticas y estrategias en materia de ciberseguridad y ciberdefensa. Adicionalmente, le encarga a la Dirección de Seguridad Pública y de Infraestructura, la función de implementar políticas y programas que mantengan la seguridad pública y protejan la infraestructura, así como hacerle seguimiento a la gestión relacionada con el riesgo cibernético en el sector defensa y diseñar el plan estratégico sectorial en materia de ciberseguridad y ciberdefensa.
Decreto 1377 de 2013.	Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales.
Decreto 103 de 2015.	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1078 de 2015.	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1081 de 2015.	Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República. Libro 2 Parte 1 Título 1 Disposiciones generales en materia de trasparencia y del derecho de acceso a la información pública nacional.
Decreto 1413 de 2017.	Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015,

Norma	Descripción
	para reglamentarse parcialmente el capítulo IV del título 111 de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Decreto 1008 de 2018.	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 338 de 2022.	Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
Decreto 767 de 2022.	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1263 de 2022.	Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública.
Decreto Municipal 477 de 2021.	Por medio del cual se establece y regula la estrategia territorial de ciberseguridad en el municipio de Itagüí para la vigencia 2020-2023.
Acuerdo 003 de 2015.	Por el cual se establecen lineamientos generales para las entidades del Estado en cuanto a la gestión de documentos electrónicos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el capítulo IV del Decreto 2609 de 2012.
CONPES 3701 de 2011.	Lineamientos de política para ciberseguridad y ciberdefensa.
CONPES 3854 de 2016.	Política Nacional de Seguridad Digital.

Norma	Descripción
Norma Técnica Colombiana NTC 5854 de 2011.	Accesibilidad a páginas web.
Norma Técnica Colombiana NTC-ISO/IEC 27001 de 2022.	Señala los requisitos de los Sistemas de Gestión de Seguridad de la Información.
Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSD).	El MGRSD está diseñado para desarrollar una gestión de riesgos de seguridad digital en cualquier entidad, ya sea pública (de orden nacional o territorial), organización privada, mixta o fuerza pública.
Manual de Gobierno Digital.	Define los lineamientos, estándares y acciones a ejecutar por parte de los sujetos obligados de la Política de Gobierno Digital.
Guía para la administración del riesgo y el diseño de controles en entidades públicas.	Establece los principios básicos y el marco general de actuación para la prevención, control y gestión de los riesgos de toda naturaleza a los que se enfrentan las entidades públicas.

2.4 PRINCIPIOS[5]

I. Salvaguardar los derechos humanos y los valores fundamentales de los ciudadanos en el municipio de Itagüí, incluyendo la libertad de expresión, el libre flujo de información, la confidencialidad de la información y las comunicaciones, la protección de la intimidad y los datos personales y la privacidad, así como los principios fundamentales consagrados en la Constitución Política de Colombia.

II. Adoptar un enfoque incluyente y colaborativo que involucre activamente a las partes interesadas, y que permita establecer condiciones para el desarrollo eficiente de alianzas, con el fin de promover la seguridad digital del territorio y sus habitantes, y aumentar la capacidad de resiliencia municipal frente a eventos no deseados en el entorno digital.

III. Asegurar una responsabilidad compartida entre las partes interesadas, promoviendo la máxima colaboración y cooperación. Lo anterior, teniendo en

[5] Documento CONPES 3854 de 2016 (Política Nacional de Seguridad Digital).

cuenta el rol y el grado de responsabilidad de cada parte para gestionar los riesgos de seguridad digital y para proteger el entorno digital.

IV. Adoptar un enfoque basado en la gestión de riesgos, que permita a los individuos el libre, seguro y confiable desarrollo de sus actividades en el entorno digital. Lo anterior, fomentará la prosperidad económica y social, buscando la generación de riqueza, innovación, productividad, competitividad, y empleo en todos los sectores de la economía.

2.5 DEFINICIONES[6]

Amenaza cibernética: Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado.

Ataque cibernético: Acción organizada o premeditada de una o más agentes para causar daño o problemas a un sistema a través del Ciberespacio.

Cibercrimen (delito cibernético): Conjunto de actividades ilegales asociadas con el uso de las Tecnologías de la Información y las Comunicaciones, como fin o como medio.

Ciberdefensa: Es el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales.

Ciberespionaje: Es el acto o práctica de obtener secretos sin el permiso del dueño de la información (personal, sensible, propietaria o de naturaleza clasificada) para ventaja personal, económica, política o militar en el Ciberespacio, a través del uso de técnicas malintencionadas.

Ciberlavado: Es el uso del Ciberespacio, en cualquiera de sus formas, para dar apariencia de legalidad a bienes obtenidos ilícitamente o para ocultar dicha ilicitud ante las autoridades.

Ciberterrorismo: Es el uso del Ciberespacio, como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o estado.

[6] Documento CONPES 3854 de 2016 (Política Nacional de Seguridad Digital). Ministerio de Tecnologías de la Información y las Comunicaciones [MINTIC] (s.f.).

Entorno digital: Ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web.

Entorno digital abierto: Entorno digital en el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica.

Gestión de riesgos de seguridad digital: Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.

Incidente digital: Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el entorno digital y que genera impactos sobre los objetivos.

Infraestructura crítica cibernética nacional: Aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública.

Riesgo: Es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas.

Riesgo de seguridad digital: Es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan.

Resiliencia: Es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información (ISO/IEC 27000).

Seguridad digital o ciberseguridad: Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio.

Seguridad informática: Comprende los métodos, procesos o técnicas para la protección de los sistemas informáticos (redes e infraestructura) y la información contenida en formato digital.

Vulnerabilidad: Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan.

3 POLÍTICA

3.1 POLÍTICA DE SEGURIDAD DIGITAL INSTITUCIONAL

La Administración Municipal de Itagüí establece la seguridad digital como una **responsabilidad institucional** y un **compromiso de todos** los servidores públicos, contratistas y terceros que desarrollan actividades contractuales, liderada por la Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones TIC.

3.2 OBJETIVOS

3.2.1 Objetivo general

Diseñar e implementar la Política de Seguridad Digital en la Administración Municipal de Itagüí, en un marco de gestión de los riesgos de seguridad digital, en el que la Entidad puede estar expuesta desde la perspectiva de entorno cibernético y siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI).

3.2.2 Objetivos específicos

I. Identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en la Administración Municipal de Itagüí.

II. Desarrollar el Modelo de Seguridad y Privacidad de la Información (MSPI), en concordancia con la Política de Gobierno Digital.

III. Promover en los servidores públicos, contratistas y otros terceros, el uso y comportamiento responsable y ético, en el entorno digital, que pueda afectar la seguridad de los activos digitales, los datos y la información de la Entidad.

IV. Establecer articulación con las autoridades definidas por el gobierno nacional en la identificación, prevención y gestión de incidentes de seguridad digital que afecten a la infraestructura TIC de la Administración Municipal.

4 ALCANCE

Para el cumplimiento de la Política de Seguridad Digital del municipio de Itagüí, se define el siguiente alcance:

1. El Departamento Administrativo de Planeación, la Secretaría General por medio del Equipo de Gestión Documental y la Dirección Administrativa de las TIC por medio del Grupo de Infraestructura Tecnológica (GIT) y el Líder I+D+I, revisarán y actualizarán los activos de información, y para ello tendrán en cuenta la clasificación según su naturaleza, como, por ejemplo, documentos, información, software, hardware y/o componentes de red.

2. El Grupo de Infraestructura Tecnológica (GIT), hará el levantamiento de la Infraestructura Tecnológica Crítica de la Entidad.

3. El Grupo de Infraestructura Tecnológica (GIT), apoyará la actualización de los riesgos de seguridad digital, siguiendo la metodología dispuesta por el Departamento Administrativo de la Función Pública (DAFP) y el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).

4. Todas las Unidades Administrativas con el apoyo de la Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC- y la Secretaría de Evaluación y Control, implementarán el Modelo de Seguridad y Privacidad de la Información (MSPI) con las herramientas que el Ministerio de Tecnologías de la Información y las Comunicaciones destine para ello, el cual

integra en cada una de sus fases, tareas asociadas a la gestión de riesgos de seguridad digital.

5. La Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC- y la Secretaría de Evaluación y Control, el Grupo GIT y el Líder I+D+I, establecerán los controles definidos en el Anexo A de la ISO 27001, que en el MSPI se define como la Declaración de Aplicabilidad.

6. La Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC-, con el apoyo del Departamento Administrativo de Planeación y la Secretaría de Evaluación y Control, evaluarán el desempeño del Modelo de Seguridad y Privacidad de la Información (MSPI), a través de la aplicación de la Política de Seguridad Digital, la ejecución de los controles definidos en la declaración de aplicabilidad y el monitoreo de los indicadores de seguridad de la información.

7. La Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC- por medio del Grupo GIT, desarrollará el Procedimiento de Gestión de Incidentes de Seguridad de la Información y en él se establecerá como actividad el reporte de los incidentes a las autoridades como el CSIRT o COLCERT.

8. La Secretaría de Servicios Administrativos a través de la Oficina de Talento Humano, brindará capacitación técnica y tecnológica para atender riesgos de seguridad digital y fortalecerá la capacidad humana de los servidores públicos adscritos a la Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC-.

9. La Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC- por medio del Grupo GIT y la Oficina de Talento Humano, sensibilizarán a usuarios internos en el uso de medios digitales y en buenas prácticas para mitigar los riesgos de seguridad digital que puedan afectar a la Entidad.

5 RESPONSABLES

Comité Institucional de Gestión y Desempeño de la Administración Municipal de Itagüí: Responsable de aprobar la Política de Seguridad Digital de la Entidad.

Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC- del Municipio de Itagüí: Responsable de liderar la implementación de la Política de Seguridad Digital en la Entidad.

Departamento Administrativo de Planeación del Municipio de Itagüí: Responsable de asesorar en la aplicación de la herramienta para la administración de los riesgos de seguridad digital.

Secretaría de Evaluación y Control del Municipio de Itagüí: Responsable de hacer seguimiento al cumplimiento de la Política de Seguridad Digital en la Entidad.

Todas las unidades administrativas, así como los servidores públicos, contratistas y terceros que desarrollan actividades contractuales en la Administración Municipal de Itagüí, son corresponsables de la implementación y puesta en marcha de la Política de Seguridad Digital en la Entidad.

6 SEGUIMIENTO Y EVALUACIÓN DE LA POLÍTICA

La Administración Municipal de Itagüí realizará seguimiento a través de las tres líneas de defensa definidas en el MIPG en la Dimensión 7 Control Interno, mediante el componente de actividades de control.

La Entidad realizará seguimiento al avance de la Política, a través de la definición de indicadores para el Plan de Seguridad y Privacidad de la Información.

Se realizará el seguimiento a la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), con la herramienta dispuesta por el Ministerio de Tecnologías de la Información y las Comunicaciones.

La medición de la Política se realizará a través del reporte de la herramienta en línea dispuesta por el DAFP (FURAG).

7 POLÍTICAS PARTICULARES DE SEGURIDAD DIGITAL

El servicio de acceso a internet, intranet, sistemas de información, medios de almacenamiento, aplicaciones (software), cuentas de red, equipos de cómputo y en general todo dispositivo tangible o intangible que tenga relación directa o indirecta con las tecnologías de la información y las comunicaciones TIC, son propiedad de la Alcaldía Municipal de Itagüí y deben ser usados únicamente para el cumplimiento de las funciones misionales asignadas a los servidores públicos, contratistas y/o terceros que desarrollan actividades contractuales en la Entidad.

La Administración Municipal de Itagüí se compromete con la protección de la información, buscando la disminución del impacto generado sobre sus activos por los riesgos identificados de manera sistemática, con el objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y disponibilidad de ésta, acorde con las necesidades de los diferentes grupos de interés identificados.

Para dar cumplimiento a la Política de Seguridad Digital, la Administración Municipal de Itagüí ha definido las siguientes políticas como parte integral de la misma:

7.1 Política de dispositivos removibles

Son medios removibles todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores, para lo cual se establecen los siguientes lineamientos:

- Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se deshabilita la opción de escritura en dispositivos USB, unidades ópticas de grabación en todos los equipos de cómputo institucionales excepto de las autorizadas por los secretarios o directores de despacho, asumiendo así la responsabilidad de posibles fujas de información por éstos.

7.2 Política de uso de correo institucional

- La cuenta de correo electrónico y la clave asociada asignada es personal, intransferible y por razones de seguridad deberá ser cambiada periódicamente, con una periodicidad de 3 meses.

- Los usuarios deben tratar los mensajes de correo electrónico, chat y archivos adjuntos como información de propiedad de la Alcaldía de Itagüí.

- La cuenta de correo es de uso exclusivo para cumplir las funciones misionales del servidor público al cual fue asignada, no deberá usarse para otros fines.

- Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

- Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera exclusiva a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones.

- El usuario será responsable de revisar y depurar su buzón de correo periódicamente, a fin de evitar que éste se sature.

- Cuando un servidor público tenga asignada una cuenta de correo de la Entidad, y éste se retira de la misma, deberá entregar a la Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC-, los usuarios y password asignados, de igual manera dicha información debe entregarse cuando exista un proceso de empalme.

7.3 Política de seguridad para los equipos institucionales

Para lograr un alto rendimiento y salvaguarda de computadores y portátiles, la Administración Municipal ha definido los siguientes parámetros:

- Los computadores de mesa, portátiles y cualquier activo de tecnología de información, podrán salir de las instalaciones únicamente con la aprobación del jefe del área de gestión.

- El equipo de cómputo asignado deberá ser para uso exclusivo del servidor público para el ejercicio de las funciones asignadas en la Alcaldía del municipio de Itagüí.

- Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del computador.

- Los usuarios deberán asegurarse de respaldar la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previniendo así la pérdida involuntaria de información, derivada del proceso de reparación.

- Los equipos de la Alcaldía de Itagüí sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

- Debe respetarse y no modificar la configuración de hardware y software establecida por la Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC-.

- Para prevenir la intrusión de personas maliciosas o mal intencionadas (hackers) a través de puertas traseras, no está permitido el uso de VPNs en computadores que tengan conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas

las comunicaciones de datos deben efectuarse a través de la LAN o WAN de la Alcaldía de Itagüí.

- A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la institución está protegido por derechos de autor y requiere licencia de uso. Por tal razón, es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

- Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente a la Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC-, y poner el computador en cuarentena hasta que el problema sea resuelto.

- No debe utilizarse software descargado de internet y en general software que provenga de una fuente no confiable, a menos que haya sido comprobado de forma rigurosa y que esté aprobado su uso por la Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC- del municipio de Itagüí.

- Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio servidor público.

- El personal que utiliza un computador portátil que contenga información confidencial de la institución, no debe dejarlo desatendido, sobre todo cuando esté por fuera de las instalaciones de la Administración Municipal.

- La Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC- del municipio de Itagüí, no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y/o manejo de información) a equipos que no sean de la Entidad.

- Se prohíben que los equipos (computador y/o portátil) estén en contacto con el piso, el usuario debe disponerlos sobre el escritorio.

7.4 Política de control de acceso a los servicios de red

7.4.1 Requerimientos para el control de acceso

Los controles de acceso deberán contemplar:

a) Requerimientos de seguridad de cada una de las aplicaciones.

b) Definir los perfiles o privilegios de acceso de los usuarios a las aplicaciones de acuerdo con su perfil de cargo en la Entidad.

7.4.2 Administración de accesos de usuarios

La Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC-, establece procedimientos para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

7.4.3 Creación de usuarios

La Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC-, deberá mantener los registros donde cada uno de los líderes de las unidades administrativas haya autorizado a los servidores públicos y/o contratistas el acceso a los diferentes sistemas de información de la Entidad.

Los datos de acceso a los sistemas de información deberán estar compuestos por un ID o nombre de usuario y contraseña que deben ser únicos por cada servidor público o tercero.

Cuando se retire o cambie de contrato cualquier servidor público o tercero, se deberá aplicar la eliminación o cambios de privilegios en los sistemas de información a los que el usuario estaba autorizado.

La Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC-, deberá realizar revisiones de privilegios de acceso a los diferentes sistemas de información por parte de los servidores públicos y/o contratistas, manteniendo los registros de las revisiones y/o hallazgos.

7.4.4 Administración de contraseñas de usuario

Las contraseñas de acceso deberán cumplir con un mínimo de 8 caracteres y la combinación de números, letras mayúsculas y minúsculas, en lo posible utilizar caracteres especiales.

Todos los servidores públicos y contratistas deberán cambiar su contraseña de acceso a los diferentes sistemas de información con una frecuencia mínima de 3 meses, a excepción de aquellos que contengan información confidencial o secreta en cuyo caso el cambio se debe realizar cada mes.

Los sistemas de información deberán bloquear permanentemente al usuario luego de 5 intentos fallidos de autenticación a excepción de aquellos que contengan información confidencial o secreta en cuyo caso después de 3 intentos fallidos de autenticación se realizará el bloqueo.

7.4.5 Uso de contraseñas

Los usuarios deben cumplir las siguientes normas:

a) Mantener los datos de acceso en secreto.

b) Contraseñas fáciles de recordar y difíciles de adivinar.

c) Que las contraseñas no estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo, nombres, números de teléfono, fechas de nacimiento, etc.

d) Notificar de acuerdo con lo establecido cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

7.5 Equipos desatendidos en áreas de usuarios

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente.

a) Los equipos instalados en áreas de usuarios, por ejemplo, estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

b) Bloquear el equipo de cómputo tras abandonar el puesto de trabajo.

c) Bloqueo automático de la sesión en el equipo de cómputo tras inactividad superior a 5 minutos.

d) Apagar los equipos de cómputo al finalizar la jornada laboral.

7.6 Control de acceso a la red

La Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC-, debe asegurar el bloqueo al acceso de páginas de contenido para adultos, redes sociales, hacking, descargas (FTP), mensajería instantánea y cualquier página que represente riesgo potencial para la Entidad mediante el uso de servidor proxy, firewall o el software que mejor se ajuste a la necesidad. Las excepciones de acceso, serán aprobadas por los secretarios de despacho o directores, según la necesidad del cargo y verificación previa de que las páginas solicitadas no contengan código malicioso con el visto bueno del Grupo de Infraestructura Tecnológica (GIT).

7.7 Autenticación de usuarios para conexiones externas

La autenticación de usuarios remotos deberá ser aprobada por el Director Administrativo de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC-, con previa solicitud de los secretarios de despacho o directores.

7.8 Control de conexión a redes

La infraestructura tecnológica de la Administración Municipal deberá estar separada por VLANs para garantizar la confidencialidad de los datos que se transmitan.

Sólo la Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC-, podrá dar la autorización o realizar los cambios y adiciones a la red de cableado estructurado de la Administración Municipal.

7.9 Seguridad en los servicios de red

a) Mantener instalados y habilitados sólo aquellos servicios y puertos que sean utilizados por los sistemas de información y software de la Entidad.

b) Controlar el acceso lógico a los servicios, tanto a su uso como a su administración mediante bloqueo de puertos en el firewall de la Entidad.

7.10 Control de identificación y autenticación de usuarios

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades tengan trazabilidad.

7.11 Sistema de administración de contraseñas

El sistema de administración de contraseñas debe:

a) Obligar el uso de User IDs y contraseñas individuales para determinar responsabilidades.

b) Permitir que los usuarios seleccionen y cambien sus propias contraseñas luego de cumplido el plazo mínimo de mantenimiento de las mismas o cuando consideren que éstas han sido comprometidas e incluir un procedimiento de confirmación para contemplar los errores de ingreso.

c) Obligar a los usuarios a cambiar las contraseñas provisionales o que han sido asignadas por el administrador del sistema de información.

d) No mostrar las contraseñas en texto claro cuando son ingresadas.

e) Almacenar las contraseñas en forma cifrada.

7.12 Sesiones inactivas

Si el usuario debe abandonar la estación de trabajo momentáneamente, activará protectores de pantalla con contraseñas, con el fin de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

Si los sistemas de información detectan inactividad por un periodo igual o superior a diez (10) minutos, deben automáticamente aplicar “time out”, es decir, finalizar la sesión de usuario.

7.13 Limitación del tiempo de conexión

Las restricciones al horario de conexión deben suministrar seguridad adicional a las aplicaciones de alto riesgo:

a) Limitar los tiempos de conexión al horario normal de oficina, de no existir un requerimiento operativo de horas extras o extensión horaria.

b) Documentar los servidores públicos o contratistas que no tienen restricciones horarias y los motivos y evidencia de la autorización expedida por el respectivo secretario o director de la unidad administrativa.

8 POLÍTICAS DE ACCESO A INTERNET

- Los servicios de correo electrónico e internet, son administrados por la Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC-. Para el enlace de internet el proveedor es el responsable de garantizar su disponibilidad, de un mínimo de 99.6%.

- La Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC-, monitoreará las actividades de la red, tanto para correo electrónico, internet y uso de red de datos con el fin de vigilar el cumplimiento de las políticas establecidas para el uso de tecnologías de la información.

- La conexión a internet, sólo podrá realizarse por los medios dispuestos por la Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC-, a cada uno de los diferentes funcionarios.

- No se podrá utilizar el internet de la Administración Municipal como un medio de participación, acceso y distribución de actividades o materiales que vayan en contra de la Ley.

- La Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC-, asignará a cada usuario permisos y perfiles de navegación dependiendo de las actividades que realice. Si se necesita habilitar cualquier contenido de internet a los servidores públicos y/o contratistas, los secretarios y/o directores de cada unidad administrativa enviarán el listado del personal, a qué páginas de internet y con qué objetivo, a la antedicha Dirección Administrativa, y éstos asumirán la responsabilidad total sobre los daños o perturbaciones que se presenten debido a dicha autorización.

- En la jornada laboral se tendrán las restricciones de normativa y sólo se permitirá el acceso a internet de los servidores públicos y/o contratistas que de acuerdo con sus funciones y/o designaciones del jefe inmediato tengan la autorización expresa de éste.

- Sólo se permitirá la navegación libre en los horarios de almuerzo según lo establezca la norma y las disposiciones de la Administración Municipal, en este horario seguirán aplicándose las políticas de ciberseguridad y ciberdefensa, así como las restricciones de utilizar la red con fines comerciales.

- La Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones -TIC-, es la única encargada de solicitar enlaces de datos e internet, aumento de ancho de banda, o suspensión de servicio a proveedores.

9 SANCIONES POR LA VIOLACIÓN A LAS POLÍTICAS DE SEGURIDAD

Cualquier usuario de los servicios digitales de la Administración Municipal que viole estas políticas, será sujeto a la revocación de privilegios de red por un periodo de tres (3) días y cualquier otra acción disciplinaria corporativa dispuesta por la normativa nacional y territorial.

10 CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Descripción del Cambio
01	12/12/2022	Creación del documento. Aprobada en Acta No. 04 del 12 de diciembre de 2022 del Comité Institucional de Gestión y Desempeño.
02	14/12/2023	**Se modificó:** Se realiza corrección de estilo a todo el documento, la redacción de la introducción, y las definiciones de “Seguridad de la información” y “Seguridad digital o ciberseguridad”. **Se incluyó:** Las notas al pie de página y las referencias, y en el “Marco Legal” la Ley 2080 de 2021, los Decretos 1078 de 2015, 1081 de 2015, 1413 de 2017, 338 de 2022, 767 de 2022, 1263 de 2022 y el Decreto Municipal 477 de 2021. **Se eliminó:** En el “Marco Legal” el Decreto Distrital 316 de 2008 y el Decreto Nacional 1377 de 2013, el cual contaba con doble registro. Cambios socializados y aprobados en Acta No. 04 del 14 de diciembre de 2023 del Comité Institucional de Gestión y Desempeño.

11 REFERENCIAS

Consejo Nacional de Política Económica y Social [CONPES]. (2016). *Documento CONPES 3854. Política Nacional de Seguridad Digital*. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones [MINTIC]. (s.f.). *Glosario*. https://www.mintic.gov.co/portal/inicio/Glosario/

Ministerio de Tecnologías de la Información y las Comunicaciones [MINTIC]. (2018). *Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD)*. https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b

OECD. (2015). Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity in *Digital Security Risk Management for Economic and Social Prosperity, OECD Recommendation and Companion Document*. OECD Publishing, Paris. https://web-archive.oecd.org/2015-10-18/373718-digital-security-risk-management.pdf

Universidad Externado de Colombia. (2018, 9 de noviembre). *Cómo funciona la seguridad digital en la actualidad*. https://www.uexternado.edu.co/derecho/como-funciona-la-seguridad-digital-en-la-actualidad/

Alcaldía de

Itagüí