POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Alcaldía de Yarumal

2025

Control de versiones

Año	Versión
2025	Versión 1

Tabla de contenido

1. Introducción

La Alcaldía Municipal de Yarumal, en su compromiso con la modernización, la transparencia y la confianza ciudadana, establece la presente Política General de Seguridad de la Información para salvaguardar los activos de información que soportan sus procesos institucionales y servicios digitales. En un entorno digital caracterizado por la rápida evolución tecnológica y los crecientes riesgos asociados, esta política define un marco integral de reglas y procedimientos claros para proteger la confidencialidad, integridad y disponibilidad de la información. Alineada con normativas nacionales, como la Ley 1581 de 2012 sobre protección de datos personales y el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), así como con los objetivos de Gobierno Abierto del Plan de Desarrollo Municipal (PDI) 2024-2027, la política promueve un entorno digital seguro, fomenta la inclusión digital y fortalece la resiliencia institucional frente a amenazas digitales. Este documento refleja el compromiso de la Alcaldía de garantizar servicios digitales confiables y accesibles, contribuyendo al desarrollo sostenible y la participación ciudadana.

2. Antecedentes

La adopción de tecnologías de la información y comunicación (TIC) ha transformado la forma en que las entidades públicas gestionan sus procesos y ofrecen servicios a los ciudadanos, generando oportunidades para la transparencia, la eficiencia y la participación. Sin embargo, este avance también ha incrementado la exposición a riesgos digitales, lo que demanda la implementación de marcos robustos para proteger la información institucional. En este contexto, la Alcaldía Municipal de Yarumal reconoce la necesidad de establecer una Política General de Seguridad de la Información que proporcione lineamientos claros y estructurados para salvaguardar la confidencialidad, integridad y disponibilidad de sus activos de información. Esta iniciativa se fundamenta en normativas nacionales, como la Ley 1581 de 2012, que regula la protección de datos personales, el CONPES 3854 de 2011, que promueve la seguridad digital en el sector público, y el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), que establece estándares para la gestión de riesgos digitales. Asimismo, la política se alinea con los objetivos del Plan de Desarrollo Municipal (PDI) 2024-2027, que prioriza el fortalecimiento de la gobernanza digital, la inclusión de todos los ciudadanos en el uso de servicios digitales, y la promoción de un modelo de Gobierno Abierto. Inspirada en buenas prácticas de seguridad

digital a nivel nacional, esta política busca consolidar un Sistema de Gestión de Seguridad de la Información (SGSI) que garantice la protección de los procesos digitales, fomente la confianza ciudadana y contribuya al desarrollo sostenible del municipio.

2.1 Dimensiones de la Política de Seguridad Digital

La Política General de Seguridad de la Información de la Alcaldía Municipal de Yarumal se fundamenta en un conjunto de dimensiones estratégicas que orientan la protección de los activos de información y la gestión de los procesos digitales. Estas dimensiones aseguran que la política sea integral, adaptable y alineada con los principios de seguridad digital, promoviendo un entorno confiable, transparente y accesible para los ciudadanos. A continuación, se describen las dimensiones clave que sustentan esta política:

1. **Confidencialidad**: Esta dimensión garantiza que la información institucional, especialmente aquella de carácter sensible o personal, solo sea accesible para personas, entidades o sistemas autorizados. La confidencialidad protege los datos de accesos no permitidos, asegurando el cumplimiento de normativas como la Ley 1581 de 2012 sobre protección de datos personales y fomentando la confianza ciudadana en los servicios digitales ofrecidos por la Alcaldía.
2. **Integridad**: La integridad asegura la exactitud, completitud y consistencia de la información a lo largo de su ciclo de vida, previniendo modificaciones no autorizadas o errores que puedan comprometer la calidad de los datos. Esta dimensión es esencial para mantener la fiabilidad de los procesos digitales y garantizar que las decisiones institucionales se basen en información precisa y confiable.
3. **Disponibilidad**: La disponibilidad asegura que los activos de información y los servicios digitales estén accesibles para los usuarios autorizados en el momento en que se requieran, minimizando interrupciones y asegurando la continuidad operativa. Esta dimensión respalda la prestación eficiente de servicios ciudadanos y la resiliencia de los procesos digitales frente a posibles incidentes.
4. **Autenticidad**: Esta dimensión garantiza que los usuarios, sistemas o procesos que interactúan con los activos de información sean legítimos y estén debidamente identificados. La autenticidad protege contra accesos fraudulentos y asegura que las transacciones o interacciones digitales sean realizadas por las partes autorizadas, reforzando la seguridad y la confianza en los servicios institucionales.

5. **Trazabilidad**: La trazabilidad permite registrar y monitorear las acciones realizadas sobre los activos de información, proporcionando un historial claro de quién accede, modifica o utiliza los datos. Esta dimensión facilita la auditoría, la detección de incidentes y el cumplimiento normativo, contribuyendo a la transparencia y la rendición de cuentas en los procesos digitales.

Estas dimensiones se complementan con un enfoque estratégico basado en los principios de Gobierno Abierto, promoviendo la participación ciudadana, la transparencia y la inclusión digital, en línea con los objetivos del Plan de Desarrollo Municipal (PDI) 2024-2027. La política se alinea con el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y otras normativas nacionales, como el CONPES 3854 de 2011, para garantizar un marco robusto que proteja la información institucional, fortalezca la confianza ciudadana y fomente un entorno digital seguro y sostenible.

2.2 Estrategia de Gestión de Riesgos de Seguridad Digital

La Alcaldía Municipal de Yarumal reconoce que la gestión efectiva de los riesgos asociados a los activos de información y los procesos digitales es fundamental para garantizar la seguridad, la continuidad operativa y la confianza en los servicios institucionales. La Estrategia de Gestión de Riesgos de Seguridad Digital establece un enfoque sistemático y proactivo para identificar, evaluar, tratar y monitorear los riesgos que puedan comprometer la confidencialidad, integridad o disponibilidad de la información. Este marco se basa en principios de gobernanza digital y se alinea con normativas nacionales, como el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), la Ley 1581 de 2012 sobre protección de datos personales, y el CONPES 3854 de 2011, así como con los objetivos de Gobierno Abierto del Plan de Desarrollo Municipal (PDI) 2024-2027. La estrategia se estructura en las siguientes fases clave:

1. **Identificación de Riesgos**: La Alcaldía implementará procesos continuos para identificar amenazas y vulnerabilidades que puedan afectar los activos de información, incluyendo datos sensibles, aplicaciones críticas y servicios digitales. Este proceso considerará riesgos internos y externos, como accesos no autorizados, interrupciones del servicio o incidentes derivados de errores humanos, y se basará en estándares reconocidos para clasificar los activos según su criticidad.

2. **Evaluación y Análisis de Riesgos**: Una vez identificados, los riesgos serán evaluados en términos de su probabilidad de ocurrencia y el impacto potencial en los procesos institucionales y los servicios ciudadanos. La evaluación priorizará la protección de la información sensible y la continuidad de los servicios digitales, utilizando metodologías alineadas con el MSPI de MinTIC para determinar niveles de riesgo y establecer prioridades de tratamiento.

3. **Tratamiento de Riesgos**: La Alcaldía definirá medidas específicas para mitigar, transferir, aceptar o evitar los riesgos identificados, según su nivel de criticidad. Estas medidas incluirán controles técnicos, como mecanismos de autenticación robustos y copias de seguridad periódicas, así como controles administrativos, como políticas de acceso y capacitación en seguridad digital. El tratamiento de riesgos se diseñará para ser proporcional a los recursos disponibles y efectivo en la reducción de amenazas.

4. **Monitoreo y Revisión**: La gestión de riesgos será un proceso dinámico, con revisiones periódicas para actualizar el análisis de riesgos en función de nuevas amenazas, cambios tecnológicos o incidentes reportados. La Alcaldía establecerá indicadores de desempeño para evaluar la efectividad de las medidas implementadas y garantizará la trazabilidad de las acciones realizadas, promoviendo la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

5. **Cultura de Seguridad Digital**: Complementando las fases técnicas, la estrategia promoverá una cultura organizacional orientada a la seguridad digital mediante la sensibilización y capacitación de todos los actores involucrados, incluyendo funcionarios, contratistas y ciudadanos que interactúan con los servicios digitales. Esta dimensión fomenta la responsabilidad compartida y refuerza la confianza en el uso de las tecnologías de la información.

La Estrategia de Gestión de Riesgos de Seguridad Digital se implementará de manera transversal, integrándose con los procesos institucionales y los objetivos estratégicos de la Alcaldía. Al priorizar la protección de los activos de información, la estrategia contribuye a la resiliencia institucional, la transparencia y la inclusión digital, en línea con los principios de Gobierno Abierto del PDI 2024-2027. Asimismo, asegura el cumplimiento de las normativas nacionales y fortalece la capacidad de la Alcaldía para ofrecer servicios

digitales seguros, confiables y accesibles, consolidando un entorno digital que responda a las necesidades de los ciudadanos y promueva el desarrollo sostenible del municipio.

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 de comunicación masiva. 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

Norma	Descripción
	firma electrónica certificada (artículo 30, modificado por el artículo 161 del Decreto Ley 019 de 2012)
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

Norma	Descripción
	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.
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.

Norma	Descripción
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 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

Norma	Descripción
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, 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.
Decreto338 de 2022.	Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078

Norma	Descripción
	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

Norma	Descripción
	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.

2.4 Principios

La Política General de Seguridad de la Información de la Alcaldía Municipal de Yarumal se fundamenta en un conjunto de principios rectores que orientan la protección de los activos de información y la gestión de los procesos digitales. Estos principios reflejan el compromiso institucional con la seguridad, la transparencia y la inclusión digital, asegurando que todas las acciones relacionadas con la seguridad de la información sean coherentes, éticas y efectivas. A continuación, se presentan los principios clave que sustentan esta política:

1. **Protección Integral**: La Alcaldía garantizará la confidencialidad, integridad y disponibilidad de los activos de información mediante la implementación de medidas técnicas, administrativas y organizativas que aborden los riesgos digitales de manera holística. Este principio asegura que la seguridad digital se integre en todos los procesos institucionales, promoviendo la resiliencia frente a amenazas y la continuidad de los servicios digitales.

2. **Transparencia y Rendición de Cuentas**: La gestión de la seguridad de la información se llevará a cabo con un enfoque de transparencia, asegurando que las acciones, políticas y procedimientos sean claros, accesibles y trazables. Este principio fomenta la confianza ciudadana y la rendición de cuentas, en línea con los valores de Gobierno Abierto establecidos en el Plan de Desarrollo Municipal (PDI) 2024-2027.

3. **Cumplimiento Normativo**: Todas las iniciativas de seguridad digital se alinearán con las normativas nacionales, incluyendo la Ley 1581 de 2012 sobre protección de datos personales, el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), y el CONPES 3854 de 2011. Este principio asegura que la Alcaldía cumpla con los estándares legales y técnicos, fortaleciendo la legitimidad de sus procesos digitales.

4. **Participación y Responsabilidad Compartida**: La seguridad digital es una responsabilidad colectiva que involucra a funcionarios, contratistas, ciudadanos y otros actores que interactúan con los servicios digitales. La Alcaldía promoverá la sensibilización y la capacitación para fomentar una cultura de seguridad, asegurando que todos los involucrados contribuyan activamente a la protección de los activos de información.

5. **Inclusión Digital**: La política priorizará el acceso equitativo a los servicios digitales, reduciendo las brechas en el uso y aprovechamiento de las tecnologías de la información y comunicación. Este principio busca garantizar que todos los ciudadanos, independientemente de su contexto, puedan beneficiarse de un entorno digital seguro y accesible, en línea con los objetivos del PDI 2024-2027.

6. **Mejora Continua**: La Alcaldía adoptará un enfoque dinámico para la gestión de la seguridad de la información, revisando y actualizando regularmente las políticas, procedimientos y controles en respuesta a nuevas amenazas, avances tecnológicos y lecciones aprendidas. Este principio asegura que el Sistema de Gestión de Seguridad de la Información (SGSI) evolucione para mantener su efectividad y relevancia.

7. **Proporcionalidad**: Las medidas de seguridad implementadas serán proporcionales a los riesgos identificados y a la criticidad de los activos de información, optimizando los recursos disponibles sin comprometer la protección de los datos y servicios digitales. Este principio garantiza un equilibrio entre seguridad, eficiencia y accesibilidad.

Estos principios, inspirados en estándares nacionales e internacionales, constituyen la base ética y operativa de la política, guiando la implementación del Sistema de Gestión de Seguridad de la Información (SGSI). Al adoptar estos valores, la Alcaldía Municipal de Yarumal reafirma su compromiso con la protección de la información, la promoción de servicios digitales confiables y la construcción de un entorno digital que fomente la participación ciudadana, la transparencia y el desarrollo sostenible.

2.5. Definiciones

Para garantizar la claridad y la correcta interpretación de la Política General de Seguridad de la Información, se presentan las siguientes definiciones de términos clave que sustentan la gestión de la seguridad digital en la Alcaldía Municipal de Yarumal. Estos

conceptos reflejan estándares nacionales e internacionales, asegurando un lenguaje común que facilite la implementación de las políticas y procedimientos, así como el cumplimiento normativo y la promoción de un entorno digital seguro, transparente y accesible.

- **Confidencialidad**: Propiedad que asegura que la información solo sea accesible para personas, entidades o sistemas debidamente autorizados, protegiendo los datos sensibles contra divulgaciones no permitidas y garantizando el cumplimiento de normativas sobre protección de datos.
- **Integridad**: Propiedad que asegura la exactitud, completitud y consistencia de la información a lo largo de su ciclo de vida, previniendo alteraciones no autorizadas o errores que puedan comprometer la fiabilidad de los datos utilizados en los procesos institucionales.
- **Disponibilidad**: Propiedad que garantiza que los activos de información y los servicios digitales estén accesibles para los usuarios autorizados cuando se requieran, soportando la continuidad operativa y la prestación eficiente de servicios a los ciudadanos.
- **Seguridad Digital**: Conjunto de estrategias, políticas, procedimientos y medidas diseñadas para proteger los activos de información y los procesos digitales contra amenazas, promoviendo la confianza en el uso de las tecnologías de la información y comunicación.
- **Activo de Información**: Recurso digital o físico que contiene, procesa o transmite datos esenciales para las operaciones de la Alcaldía, incluyendo bases de datos, aplicaciones, sistemas y servicios digitales críticos.
- **Riesgo Digital**: Posibilidad de que una amenaza explote una vulnerabilidad en los activos de información, causando un impacto adverso en la confidencialidad, integridad o disponibilidad de los datos o servicios digitales.
- **Gobernanza Digital**: Marco de políticas, procesos y estructuras que guían la gestión estratégica de las tecnologías de la información y comunicación, promoviendo la transparencia, la participación y la eficiencia en los procesos digitales.
- **Trazabilidad**: Capacidad de registrar y monitorear las acciones realizadas sobre los activos de información, generando un historial auditable que facilite la detección de incidentes, la rendición de cuentas y el cumplimiento normativo.

- **Autenticidad**: Propiedad que asegura que los usuarios, sistemas o procesos que interactúan con los activos de información sean legítimos y estén debidamente identificados, previniendo accesos o transacciones fraudulentas.
- **Brecha Digital**: Desigualdad en el acceso, uso o aprovechamiento de las tecnologías de la información y comunicación, que limita la inclusión digital y el acceso equitativo a los servicios digitales.

Definiciones/Glosario

- **Confidencialidad**: Propiedad que asegura que la información no sea accesible ni divulgada a individuos o entidades no autorizadas, protegiendo datos sensibles como los de ciudadanos o del Sisbén.
- **Integridad**: Propiedad que garantiza la exactitud y completitud de la información, evitando modificaciones no autorizadas en sistemas como Saimyr, Quipux o Siredoe.
- **Disponibilidad**: Propiedad que asegura que la información y los sistemas estén accesibles cuando sean requeridos por usuarios autorizados, como en la gestión de PQRS o recaudación por PSE.
- **Seguridad Digital**: Conjunto de estrategias y medidas para generar confianza en el uso de tecnologías digitales, protegiendo a las personas y los sistemas de amenazas como ciberataques.
- **Activo Crítico**: Recurso de información esencial para la operación de la Alcaldía, incluyendo sistemas misionales (Saimyr, Quipux, Siredoe), bases de datos del Sisbén, sistemas del área de salud, y datos confidenciales de ciudadanos.
- **Brecha Digital**: Desigualdad en el acceso, uso o impacto de las tecnologías de la información y comunicación (TIC), especialmente en las zonas rurales de Yarumal.

3. Política

3.1 Política de Seguridad Digital Institucional

La Alcaldía Municipal de Yarumal, en su compromiso con la modernización digital, la transparencia y la confianza ciudadana, establece la Política de Seguridad Digital Institucional como el pilar fundamental para proteger los activos de información y garantizar la resiliencia de los procesos digitales que soportan sus operaciones y servicios.

Esta política define un marco estratégico de reglas claras y procedimientos robustos para salvaguardar la confidencialidad, integridad y disponibilidad de la información, promoviendo un entorno digital seguro, inclusivo y confiable. Alineada con normativas nacionales, como la Ley 1581 de 2012 sobre protección de datos personales, el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), y el CONPES 3854 de 2011, así como con los objetivos de Gobierno Abierto del Plan de Desarrollo Municipal (PDI) 2024-2027, la política refleja el compromiso institucional de fortalecer la gobernanza digital y responder a las necesidades de los ciudadanos.

La Política de Seguridad Digital Institucional se fundamenta en los siguientes lineamientos estratégicos:

1. **Protección de Activos de Información**: La Alcaldía implementará medidas integrales para proteger todos los activos de información, incluyendo datos, aplicaciones y servicios digitales, contra amenazas internas y externas. Estas medidas abarcarán controles técnicos, como mecanismos de autenticación y copias de seguridad, y controles administrativos, como políticas de acceso y capacitación, asegurando la seguridad en todo el ciclo de vida de la información.

2. **Cumplimiento Normativo y Ético**: Todas las acciones de seguridad digital se realizarán en estricto cumplimiento de las normativas nacionales e internacionales, priorizando la protección de datos personales y la adherencia a estándares de seguridad digital. La Alcaldía promoverá prácticas éticas en la gestión de la información, garantizando la transparencia y la rendición de cuentas en sus procesos digitales.

3. **Fomento de la Confianza Ciudadana**: La política priorizará la generación de confianza en los servicios digitales mediante la implementación de procesos seguros, accesibles y transparentes. Esto incluye la protección de la información sensible de los ciudadanos y la promoción de canales digitales que faciliten la participación y la interacción con la Alcaldía.

4. **Inclusión Digital y Accesibilidad**: La Alcaldía se compromete a reducir las brechas digitales, asegurando que los servicios digitales sean accesibles para todos los ciudadanos, independientemente de su contexto socioeconómico o geográfico. La seguridad digital se diseñará para apoyar la inclusión, garantizando que las medidas de protección no limiten el acceso equitativo a los servicios.

5. **Gestión Proactiva de Riesgos**: La Alcaldía adoptará un enfoque proactivo para identificar, evaluar y mitigar los riesgos digitales que puedan afectar los activos de información. Este enfoque incluirá la actualización continua de las medidas de seguridad en respuesta a nuevas amenazas y avances tecnológicos, asegurando la resiliencia de los procesos digitales.
6. **Cultura de Seguridad Digital**: Se promoverá una cultura organizacional que fomente la responsabilidad compartida en la protección de la información, involucrando a funcionarios, contratistas y ciudadanos. La capacitación y la sensibilización serán herramientas clave para fortalecer las competencias digitales y garantizar el cumplimiento de las políticas de seguridad.
7. **Mejora Continua**: La Alcaldía revisará y actualizará periódicamente las políticas y procedimientos de seguridad digital, incorporando lecciones aprendidas, mejores prácticas y avances tecnológicos. Este compromiso asegura que el Sistema de Gestión de Seguridad de la Información (SGSI) permanezca efectivo y relevante en un entorno digital en constante evolución.

3.2. Objetivos

3.2.1 Objetivo General

Garantizar la confidencialidad, integridad y disponibilidad de los activos de información de la Alcaldía Municipal de Yarumal mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en reglas claras, políticas robustas y prácticas de gobernanza digital. Este objetivo busca proteger los datos y servicios digitales contra amenazas internas y externas, fortalecer la confianza ciudadana en los procesos digitales, y promover la inclusión digital, asegurando que los servicios sean accesibles, seguros y transparentes para todos los ciudadanos. Alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC, la Ley 1581 de 2012, y los principios de Gobierno Abierto del Plan de Desarrollo Municipal (PDI) 2024-2027, el objetivo general impulsa la resiliencia institucional, el cumplimiento normativo y la construcción de un entorno digital que fomente la participación, la transparencia y el desarrollo sostenible.

3.2.2 Objetivos Específicos

1. **Establecer Reglas y Controles Claros**: Desarrollar e implementar políticas, procedimientos y controles técnicos y administrativos que garanticen la protección de los activos de información, asegurando la confidencialidad, integridad y disponibilidad de los datos y servicios digitales en todos los procesos institucionales.
2. **Fomentar una Cultura de Seguridad Digital**: Promover la sensibilización y capacitación continua de funcionarios, contratistas y ciudadanos que interactúan con los servicios digitales, fortaleciendo una cultura organizacional que priorice la seguridad y la responsabilidad compartida en la protección de la información.
3. **Garantizar el Cumplimiento Normativo**: Asegurar que todas las prácticas de seguridad digital cumplan con las normativas nacionales, como la Ley 1581 de 2012 y el MSPI de MinTIC, así como con estándares internacionales, para proteger los datos personales y mantener la legitimidad de los procesos digitales.
4. **Mitigar Riesgos Digitales**: Implementar un enfoque proactivo para identificar, evaluar y tratar los riesgos digitales que puedan afectar los activos de información, utilizando metodologías estandarizadas para minimizar amenazas y garantizar la continuidad operativa.

5. **Promover la Inclusión Digital**: Diseñar e implementar medidas de seguridad que faciliten el acceso equitativo a los servicios digitales, reduciendo las brechas digitales y asegurando que todos los ciudadanos puedan beneficiarse de un entorno digital seguro y accesible.
6. **Fortalecer la Transparencia y la Confianza**: Desarrollar procesos digitales transparentes y trazables que refuercen la confianza ciudadana, promoviendo la rendición de cuentas y la participación activa en los servicios ofrecidos por la Alcaldía.
7. **Impulsar la Mejora Continua**: Revisar y actualizar periódicamente las políticas, procedimientos y controles de seguridad digital, incorporando lecciones aprendidas, avances tecnológicos y mejores prácticas para mantener la efectividad del SGSI en un entorno digital dinámico.

4. Alcance

La Política General de Seguridad de la Información de la Alcaldía Municipal de Yarumal se aplica a todos los activos de información, procesos digitales y servicios que soportan las operaciones institucionales y la interacción con los ciudadanos. Este alcance abarca un marco integral diseñado para proteger la confidencialidad, integridad y disponibilidad de la información, promoviendo un entorno digital seguro, transparente y accesible. La política se extiende a todos los niveles de la organización y a las partes interesadas que interactúan con los recursos digitales de la Alcaldía, asegurando la alineación con normativas nacionales, como la Ley 1581 de 2012 sobre protección de datos personales, el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), y el CONPES 3854 de 2011, así como con los objetivos de Gobierno Abierto del Plan de Desarrollo Municipal (PDI) 2024-2027.

El alcance de la política incluye, pero no se limita a, los siguientes elementos:

1. **Activos de Información**: Todos los recursos digitales y físicos que contienen, procesan o transmiten datos esenciales para las operaciones de la Alcaldía, incluyendo bases de datos, aplicaciones, sistemas, documentos electrónicos y cualquier otro medio que almacene información crítica o sensible.
2. **Procesos Digitales**: Todos los procesos institucionales que dependen de tecnologías de la información y comunicación, abarcando la gestión de datos, la

prestación de servicios digitales, la comunicación interna y externa, y la interacción con los ciudadanos a través de plataformas digitales.

3. **Servicios Digitales**: Los canales y plataformas digitales utilizados para ofrecer servicios a los ciudadanos, facilitar la participación ciudadana y promover la transparencia, asegurando que sean seguros, accesibles y confiables para todos los usuarios.

4. **Personas y Entidades Involucradas**: La política aplica a todos los funcionarios, contratistas, proveedores y terceros que interactúan con los activos de información o los servicios digitales de la Alcaldía, así como a los ciudadanos que utilizan estos servicios, quienes deberán cumplir con las políticas y procedimientos establecidos para garantizar la seguridad digital.

5. **Infraestructura Tecnológica**: Todos los componentes tecnológicos, como servidores, redes, dispositivos y software, que soportan los procesos digitales y los servicios de la Alcaldía, los cuales deberán ser gestionados bajo los principios de seguridad digital establecidos en esta política.

6. **Datos Sensibles y Personales**: Toda la información clasificada como sensible o personal, que requiere protección especial conforme a la Ley 1581 de 2012, incluyendo datos relacionados con los ciudadanos, las operaciones institucionales y los procesos administrativos.

La política se implementará de manera transversal, integrándose con los objetivos estratégicos y operativos de la Alcaldía para garantizar que la seguridad digital sea un componente fundamental de todos los procesos. Este alcance refleja el compromiso institucional con la protección de la información, la promoción de servicios digitales inclusivos y la construcción de un entorno digital que fomente la confianza ciudadana, la transparencia y la participación, en línea con los principios de Gobierno Abierto del PDI 2024-2027. Al abarcar estos elementos, la Alcaldía asegura que la gestión de la seguridad digital sea integral, efectiva y adaptable a las necesidades de un entorno tecnológico en constante evolución.

5. Responsables

La implementación efectiva de la Política General de Seguridad de la Información de la Alcaldía Municipal de Yarumal requiere la participación activa y coordinada de todos los actores que interactúan con los activos de información y los procesos digitales de la

institución. Esta sección establece las responsabilidades de los diferentes roles y partes interesadas, asegurando que la seguridad digital sea una prioridad compartida que fomente la confidencialidad, integridad y disponibilidad de la información. Alineada con normativas nacionales, como la Ley 1581 de 2012 sobre protección de datos personales, el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), y el CONPES 3854 de 2011, así como con los objetivos de Gobierno Abierto del Plan de Desarrollo Municipal (PDI) 2024-2027, la asignación de responsabilidades promueve la transparencia, la rendición de cuentas y la inclusión digital. A continuación, se detallan los roles y sus respectivas obligaciones:

1. **Alta Dirección**:
    - Definir la visión estratégica de la seguridad digital, aprobando la Política General de Seguridad de la Información y asegurando su integración con los objetivos institucionales.
    - Asignar los recursos necesarios para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), promoviendo una cultura organizacional orientada a la seguridad.
    - Supervisar el cumplimiento de la política y revisar periódicamente los resultados de las auditorías y los indicadores de desempeño en materia de seguridad digital.
2. **Responsable de Seguridad de la Información**:
    - Coordinar la implementación, monitoreo y mejora continua del SGSI, asegurando que las políticas y procedimientos se apliquen de manera consistente en toda la organización.
    - Liderar los procesos de identificación, evaluación y tratamiento de riesgos digitales, elaborando planes de acción para mitigar amenazas.
    - Actuar como punto de contacto principal para incidentes de seguridad digital, gestionando su respuesta y asegurando la comunicación oportuna con las partes interesadas.

3. **Funcionarios y Contratistas**:
    - Cumplir con las políticas, procedimientos y controles de seguridad establecidos, utilizando los activos de información y los servicios digitales de manera responsable y segura.
    - Participar en actividades de capacitación y sensibilización sobre seguridad digital, aplicando las buenas prácticas en sus actividades diarias.
    - Reportar cualquier incidente o vulnerabilidad detectada en los procesos digitales, contribuyendo a la prevención y mitigación de riesgos.
4. **Proveedores y Terceros**:
    - Asegurar que los servicios o productos tecnológicos proporcionados a la Alcaldía cumplan con los estándares de seguridad digital establecidos en la política.
    - Implementar medidas de protección para los activos de información que gestionen en nombre de la Alcaldía, garantizando el cumplimiento de las normativas aplicables, como la Ley 1581 de 2012.
    - Colaborar con la Alcaldía en auditorías y revisiones de seguridad, proporcionando información relevante sobre la gestión de los activos confiados.
5. **Ciudadanos**:
    - Utilizar los servicios digitales de la Alcaldía de manera responsable, respetando las políticas de uso y protegiendo la información personal compartida durante las interacciones digitales.
    - Reportar cualquier anomalía o incidente detectado en los canales digitales, contribuyendo a la mejora de la seguridad y la calidad de los servicios.
    - Participar activamente en iniciativas de inclusión digital, aprovechando los servicios digitales para fomentar la transparencia y la participación ciudadana.
6. **Equipo de Tecnología de la Información**:

- Gestionar la infraestructura tecnológica de la Alcaldía, implementando controles técnicos, como sistemas de autenticación, cifrado y copias de seguridad, para proteger los activos de información.
- Monitorear el desempeño de los sistemas digitales, identificando y resolviendo vulnerabilidades que puedan comprometer la seguridad.
- Apoyar al Responsable de Seguridad de la Información en la implementación de medidas de mitigación y en la respuesta a incidentes digitales.

6. Seguimiento y Evaluación de la Política

La Alcaldía Municipal de Yarumal reconoce que el éxito de la Política General de Seguridad de la Información depende de un proceso continuo de seguimiento y evaluación que garantice su implementación efectiva, su alineación con los objetivos institucionales y su capacidad para responder a las dinámicas del entorno digital. Esta sección establece los mecanismos y procedimientos para monitorear el cumplimiento de la política, evaluar su impacto en la protección de los activos de información y los procesos digitales, y promover la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI). Alineada con normativas nacionales, como la Ley 1581 de 2012 sobre protección de datos personales, el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), y el CONPES 3854 de 2011, así como con los principios de Gobierno Abierto del Plan de Desarrollo Municipal (PDI) 2024-2027, la estrategia de seguimiento y evaluación fomenta la transparencia, la rendición de cuentas y la resiliencia digital.

Los mecanismos de seguimiento y evaluación se estructuran en los siguientes componentes clave:

1. **Monitoreo Continuo**:
   - La Alcaldía establecerá indicadores de desempeño claros y medibles para evaluar la efectividad de las políticas y controles de seguridad digital, incluyendo métricas relacionadas con la protección de la confidencialidad, integridad y disponibilidad de los activos de información.
   - El Responsable de Seguridad de la Información, en coordinación con el equipo de tecnología de la información, realizará revisiones periódicas de

los sistemas y procesos digitales para identificar desviaciones, vulnerabilidades o incidentes que requieran atención.

- Se implementarán herramientas de monitoreo automatizadas, cuando sea aplicable, para detectar en tiempo real posibles amenazas o anomalías en los servicios digitales.

2. **Auditorías Periódicas**:
    - Se realizarán auditorías internas y externas, al menos una vez al año, para evaluar el cumplimiento de la política, los procedimientos asociados y las normativas aplicables, como la Ley 1581 de 2012 y el MSPI de MinTIC.
    - Las auditorías incluirán revisiones de los controles técnicos y administrativos, la gestión de riesgos digitales y la capacitación de los actores involucrados, generando informes detallados con recomendaciones para la mejora.
    - Los resultados de las auditorías serán presentados a la Alta Dirección para su revisión y aprobación, asegurando que las acciones correctivas se implementen de manera oportuna.
3. **Evaluación de Impacto**:
    - La Alcaldía evaluará periódicamente el impacto de la política en la confianza ciudadana, la inclusión digital y la eficiencia de los procesos digitales, utilizando encuestas, retroalimentación de los usuarios y análisis de indicadores de satisfacción.
    - Se medirán los avances en la reducción de incidentes de seguridad digital y en el cumplimiento de los objetivos estratégicos definidos en la política, ajustando las metas según sea necesario para reflejar las necesidades del entorno digital.
4. **Mejora Continua**:
    - Con base en los resultados del monitoreo, las auditorías y la evaluación de impacto, la Alcaldía identificará oportunidades de mejora en las políticas, procedimientos y controles de seguridad digital, incorporando lecciones aprendidas y mejores prácticas nacionales e internacionales.

- Se actualizarán regularmente los planes de acción y las estrategias de mitigación de riesgos para responder a nuevas amenazas, avances tecnológicos o cambios en el marco normativo.
- La Alta Dirección y el Responsable de Seguridad de la Información liderarán la implementación de las mejoras, asegurando la participación de todos los actores relevantes.

5. **Reporte y Transparencia**:
   - Se elaborarán informes periódicos sobre el estado de la seguridad digital, incluyendo los resultados del monitoreo, las auditorías y las acciones correctivas, los cuales estarán disponibles para las partes interesadas, en cumplimiento con los principios de transparencia del PDI 2024-2027.
   - Los ciudadanos tendrán acceso a información general sobre las medidas de seguridad digital implementadas, fomentando la confianza y la participación en los servicios digitales.
   - La Alcaldía comunicará de manera proactiva los avances en la gestión de la seguridad digital, promoviendo la rendición de cuentas y la alineación con los objetivos de Gobierno Abierto.

7. Políticas Particulares de Seguridad Digital

La Política General de Seguridad de la Información de la Alcaldía Municipal de Yarumal establece un conjunto de políticas particulares diseñadas para garantizar la confidencialidad, integridad y disponibilidad de los activos de información y los procesos digitales, promoviendo un entorno seguro, transparente y accesible. Estas políticas, basadas en reglas claras y prácticas robustas, se alinean con normativas nacionales, como la Ley 1581 de 2012 sobre protección de datos personales, el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), y el CONPES 3854 de 2011, así como con los principios de Gobierno Abierto del Plan de Desarrollo Municipal (PDI) 2024-2027. Las políticas se aplican a todos los funcionarios, contratistas, proveedores y ciudadanos que interactúan con los servicios digitales de la Alcaldía, asegurando una gestión efectiva de la seguridad digital. A continuación, se detallan las políticas particulares:

1. Control de Acceso a Redes de Comunicación:
    - Todas las conexiones a internet, ya sean cableadas o inalámbricas (Wi-Fi), deberán ser aprobadas y configuradas por el equipo de tecnología de la información. Las conexiones cableadas utilizarán direcciones IP fijas asignadas, mientras que las conexiones Wi-Fi requerirán credenciales seguras proporcionadas por el equipo de TI.
    - Está prohibido configurar redes o puntos de acceso sin autorización, y cualquier intento de conexión no autorizada será monitoreado y reportado como un incidente de seguridad.
    - Esta política protege la infraestructura digital frente a accesos no autorizados, garantiza la trazabilidad de las conexiones y reduce los riesgos de intrusiones.
2. Política de Dispositivos Removibles:
    - El uso de dispositivos removibles (como USB, discos externos o tarjetas de memoria) estará restringido y requerirá autorización previa del equipo de tecnología de la información. Solo se permitirán dispositivos escaneados y aprobados para evitar la introducción de malware.
    - Los dispositivos removibles no deberán utilizarse para almacenar datos sensibles o personales sin cifrado, conforme a la Ley 1581 de 2012.
    - Esta política minimiza los riesgos de pérdida de datos, infecciones por malware y accesos no autorizados a información crítica.
3. Política de Uso de Correo Institucional:
    - El correo institucional deberá utilizarse exclusivamente para fines laborales, evitando el envío o recepción de contenido personal, no autorizado o potencialmente malicioso.
    - Los correos que contengan datos sensibles deberán cifrarse, y los usuarios deberán reportar cualquier correo sospechoso al equipo de tecnología de la información.

- Esta política protege la confidencialidad de las comunicaciones institucionales y reduce los riesgos de ciberataques a través del correo electrónico.

4. Política de Seguridad para los Equipos Institucionales:
    - Todos los equipos institucionales (computadoras, laptops, servidores) deberán contar con software antivirus actualizado, parches de seguridad aplicados y configuraciones aprobadas por el equipo de tecnología de la información.
    - Está prohibido instalar software no autorizado o realizar modificaciones en la configuración de los equipos sin la aprobación del equipo de TI.
    - Esta política asegura la protección de los equipos frente a amenazas digitales y garantiza su funcionamiento seguro y eficiente.
5. Política de Control de Acceso a los Servicios de Red:
    - El acceso a los servicios de red estará restringido a usuarios autorizados, autenticados mediante credenciales únicas gestionadas por el equipo de tecnología de la información.
    - Se aplicará el principio de privilegio mínimo, garantizando que los usuarios solo accedan a los servicios necesarios para sus funciones.
    - Esta política reduce los riesgos de accesos no autorizados y protege los recursos de red de la Alcaldía.
6. Requerimientos para el Control de Acceso:
    - Los sistemas de control de acceso deberán incluir autenticación multifactor para servicios críticos y registros de auditoría para monitorear accesos.
    - Los accesos serán revisados periódicamente para desactivar cuentas inactivas o de usuarios que ya no requieran acceso.
    - Esta política asegura un control riguroso de los accesos, promoviendo la trazabilidad y la seguridad de los servicios digitales.

7. Administración de Accesos de Usuarios:
    - El equipo de tecnología de la información será responsable de crear, modificar y desactivar cuentas de usuario, siguiendo procedimientos documentados.
    - Las solicitudes de acceso deberán ser aprobadas por el supervisor correspondiente y justificadas según las necesidades laborales.
    - Esta política garantiza una gestión ordenada y segura de los accesos, minimizando riesgos de uso indebido.
8. Creación de Usuarios:
    - Cada usuario recibirá una cuenta única asociada a su identidad, creada tras la verificación de su rol y necesidades por parte del equipo de tecnología de la información.
    - Las cuentas temporales tendrán una fecha de expiración definida al momento de su creación.
    - Esta política asegura que las cuentas sean asignadas de manera controlada y alineada con los principios de seguridad.
9. Administración de Contraseñas de Usuario:
    - Las contraseñas deberán cumplir con estándares de complejidad (mínimo 12 caracteres, combinando letras, números y símbolos) y renovarse cada 90 días.
    - Está prohibido compartir contraseñas o almacenarlas en lugares no seguros.
    - Esta política fortalece la autenticidad de los usuarios y reduce los riesgos de accesos no autorizados.
10. Uso de Contraseñas:
    - Los usuarios deberán utilizar contraseñas únicas para cada sistema o servicio institucional, evitando la reutilización de contraseñas personales.
    - El equipo de tecnología de la información proporcionará herramientas para la gestión segura de contraseñas, como gestores de contraseñas aprobados.

- Esta política promueve prácticas seguras de autenticación y protege los activos de información.

11. Equipos Desatendidos en Áreas de Usuarios:

- Los equipos en áreas de usuarios deberán bloquearse automáticamente tras un período de inactividad (máximo 5 minutos) para prevenir accesos no autorizados.
- Los usuarios deberán cerrar sesión al abandonar su estación de trabajo, especialmente en áreas compartidas.
- Esta política protege los equipos frente a usos indebidos y garantiza la confidencialidad de la información.

12. Autenticación de Usuarios para Conexiones Externas:

- Las conexiones externas a los servicios digitales de la Alcaldía (ej: VPN, acceso remoto) requerirán autenticación multifactor y deberán realizarse desde dispositivos aprobados.
- Todas las conexiones externas serán monitoreadas, y los registros de acceso serán revisados periódicamente.
- Esta política asegura la seguridad de las conexiones remotas, minimizando riesgos de accesos no autorizados.

13. Seguridad en los Servicios de Red:

- Los servicios de red estarán protegidos mediante firewalls, sistemas de detección de intrusos y cifrado de datos en tránsito.
- El equipo de tecnología de la información realizará pruebas periódicas de seguridad para identificar y mitigar vulnerabilidades en la red.
- Esta política protege la infraestructura de red frente a amenazas externas e internas.

14. Sesiones Inactivas:

- Las sesiones digitales se cerrarán automáticamente tras un período de inactividad de 15 minutos.
- Los usuarios deberán reautenticarse para reanudar una sesión inactiva, garantizando la seguridad de los datos.
- Esta política reduce los riesgos de accesos no autorizados durante períodos de inactividad.

15. Limitación del Tiempo de Conexión:

- Las conexiones a servicios críticos estarán limitadas a un tiempo máximo por sesión, requiriendo reautenticación para continuar.
- El equipo de tecnología de la información podrá establecer límites personalizados según el tipo de servicio o usuario.
- Esta política minimiza la exposición a riesgos durante conexiones prolongadas.

16. Política de Gestión de Incidentes de Seguridad:

- Todo incidente de seguridad digital (ej: accesos no autorizados, pérdida de datos, malware) deberá reportarse inmediatamente al Responsable de Seguridad de la Información, quien coordinará la respuesta.
- Se seguirán procedimientos documentados para clasificar, investigar y resolver incidentes, documentando lecciones aprendidas para la mejora continua.
- Esta política asegura una respuesta rápida y efectiva, minimizando el impacto de los incidentes.

17. Política de Capacitación en Seguridad Digital:

- Todos los funcionarios y contratistas participarán en capacitaciones obligatorias anuales sobre buenas prácticas de seguridad digital, incluyendo reconocimiento de amenazas y manejo seguro de datos.
- Los ciudadanos recibirán orientación sobre el uso seguro de los servicios digitales a través de campañas educativas.

- Esta política fomenta una cultura de seguridad y reduce los riesgos derivados de errores humanos.

18. Política de Gestión de Copias de Seguridad:

- Cada funcionario será responsable de realizar copias de seguridad periódicas de la información crítica en su equipo, almacenándolas en ubicaciones seguras designadas por el equipo de tecnología de la información.
- El equipo de TI mantendrá copias centralizadas de todos los equipos en la red, verificando su integridad y disponibilidad regularmente.
- Esta política asegura la continuidad operativa y la recuperación de datos frente a incidentes.

19. Notificación Anticipada para la Gestión de Ingresos, Salidas y Cambios de Puesto:

- El área de gestión humana o el supervisor correspondiente deberá notificar al equipo de tecnología de la información, con al menos dos días hábiles de anticipación, cualquier ingreso, salida o cambio de puesto de empleados, contratistas o funcionarios, con el objetivo de validar los requerimientos de permisos de acceso y equipamiento tecnológico.
- La notificación deberá incluir: nombre completo del individuo, cargo o rol, fecha efectiva del cambio, ubicación física (si aplica), y necesidades específicas de acceso o equipamiento.
- Restricciones Adicionales:
  - Ingresos: Antes del ingreso, el equipo de TI verificará la asignación de credenciales únicas, configurará el equipamiento tecnológico necesario con el equipamiento disponible y garantizará que el usuario reciba una inducción sobre políticas de seguridad digital.
  - Salidas: Al notificarse una salida, el equipo de TI desactivará inmediatamente todas las credenciales de y recuperará el equipamiento tecnológico asignado, realizando una auditoría para asegurar que no queden datos institucionales en dispositivos personales o no autorizados.

- Cambios de Puesto: Para cambios de puesto, el equipo de TI ajustará los permisos de acceso según el nuevo rol, aplicando el principio de privilegio mínimo, y reasignará o reconfigurará el equipamiento si es necesario. Los permisos anteriores serán revocados si no son requeridos en el nuevo puesto.
- Incumplimiento de la Notificación: La falta de notificación anticipada será considerada una violación de la política, sujeta a las sanciones establecidas en la sección 9 Sanciones por la Violación a las Políticas de Seguridad.
- Auditoría Periódica: El equipo de TI realizará revisiones trimestrales de los registros de notificaciones para verificar el cumplimiento y detectar posibles accesos no autorizados o equipamiento no asignado correctamente.

- Excepciones: En casos excepcionales, se podrá reducir el plazo de notificación a un día hábil, siempre que se justifique por escrito y se garantice la supervisión del equipo de TI durante la configuración inicial de accesos y equipamiento.
- Esta política asegura una gestión ordenada y segura de los accesos y recursos tecnológicos, minimiza los riesgos de accesos no autorizados, protege los activos de información y garantiza la continuidad operativa frente a cambios de personal.

20. Política de Monitoreo y Auditoría:
    - El equipo de tecnología de la información implementará sistemas de monitoreo continuo para detectar anomalías en los servicios digitales y los accesos a la red.
    - Se realizarán auditorías internas y externas anuales para evaluar el cumplimiento de las políticas de seguridad y generar recomendaciones de mejora.
    - Esta política promueve la trazabilidad y la mejora continua del SGSI.

8. Políticas de Acceso a Internet

La Alcaldía Municipal de Yarumal reconoce que el acceso a internet es un componente crítico de sus operaciones digitales, facilitando la prestación de servicios, la comunicación

interna y la interacción con los ciudadanos. Para garantizar la seguridad, la eficiencia y el uso responsable de las redes de comunicación, se establecen las siguientes políticas de acceso a internet, aplicables a todas las conexiones cableadas y inalámbricas (Wi-Fi) utilizadas por funcionarios, contratistas, proveedores y, en su caso, ciudadanos que accedan a redes institucionales. Estas políticas, diseñadas con reglas claras, protegen los activos de información, aseguran la confidencialidad, integridad y disponibilidad de los datos, y promueven un entorno digital confiable y transparente. Alineadas con normativas nacionales, como la Ley 1581 de 2012 sobre protección de datos personales, el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), y el CONPES 3854 de 2011, así como con los principios de Gobierno Abierto del Plan de Desarrollo Municipal (PDI) 2024-2027, las políticas de acceso a internet refuerzan la gobernanza digital y la resiliencia institucional.

Las políticas de acceso a internet se detallan a continuación:

1. **Aprobación y Configuración por el Equipo de Tecnología de la Información**:
    - Todas las conexiones a internet, ya sean cableadas o inalámbricas (Wi-Fi), deberán ser aprobadas y configuradas exclusivamente por el equipo de tecnología de la información de la Alcaldía.
    - Las conexiones cableadas utilizarán direcciones IP fijas asignadas por el equipo de TI, garantizando la trazabilidad y el control de los dispositivos conectados.
    - Las conexiones Wi-Fi requerirán credenciales únicas y seguras, proporcionadas por el equipo de TI, con cifrado robusto (ej: WPA3) para proteger los datos en tránsito.
    - Esta regla asegura que solo dispositivos autorizados accedan a la red, reduciendo los riesgos de intrusiones no autorizadas.
2. **Prohibición de Conexiones No Autorizadas**:
    - Está estrictamente prohibido configurar redes, puntos de acceso Wi-Fi o conexiones a internet sin la autorización previa del equipo de tecnología de la información.

- Cualquier intento de conexión no autorizada, incluyendo el uso de dispositivos personales no aprobados o puntos de acceso externos, será detectado, bloqueado y reportado como un incidente de seguridad.
- Esta política protege la infraestructura digital frente a accesos indebidos y garantiza la integridad de la red institucional.

3. **Uso Responsable del Acceso a Internet**:
   - El acceso a internet proporcionado por la Alcaldía deberá utilizarse exclusivamente para fines laborales relacionados con las funciones institucionales, como la gestión de procesos, la comunicación oficial y la prestación de servicios digitales.
   - Está prohibido utilizar las conexiones institucionales para actividades personales, como navegación en redes sociales no relacionadas con el trabajo, streaming de contenido no laboral o descargas no autorizadas.
   - Esta regla promueve la eficiencia en el uso de los recursos digitales y reduce los riesgos asociados con sitios web maliciosos o contenido inapropiado.
4. **Monitoreo y Registro de Conexiones**:
   - El equipo de tecnología de la información implementará sistemas de monitoreo continuo para registrar y analizar el tráfico de red, identificando patrones anómalos o actividades sospechosas.
   - Todos los accesos a internet, incluyendo los dispositivos conectados, las direcciones IP utilizadas y los sitios visitados, serán registrados para fines de auditoría y respuesta a incidentes, respetando la privacidad conforme a la Ley 1581 de 2012.
   - Esta política asegura la trazabilidad de las conexiones y facilita la detección de amenazas digitales.
5. **Segmentación de Redes**:
   - La Alcaldía implementará redes separadas para diferentes tipos de usuarios y propósitos (ej: red administrativa, red para visitantes, red para servicios críticos), utilizando tecnologías de segmentación como VLANs para aislar el tráfico.

- Las redes destinadas a ciudadanos o visitantes tendrán restricciones estrictas, limitando el acceso a recursos internos y aplicando filtros de contenido para garantizar la seguridad.
- Esta regla minimiza los riesgos de accesos cruzados no autorizados y protege los activos de información críticos.

6. **Protección contra Amenazas Digitales**:
   - Todas las conexiones a internet estarán protegidas mediante firewalls, sistemas de detección y prevención de intrusos (IDS/IPS), y filtros de contenido que bloqueen sitios web maliciosos o no autorizados.
   - El equipo de tecnología de la información realizará actualizaciones periódicas de las herramientas de seguridad y pruebas de vulnerabilidad para mantener la robustez de la infraestructura de red.
   - Esta política reduce la exposición a ciberataques, como malware, phishing o explotación de vulnerabilidades.
7. **Capacitación para el Uso Seguro de Internet**:
   - Los funcionarios y contratistas recibirán capacitación periódica sobre prácticas seguras de navegación en internet, incluyendo el reconocimiento de sitios web sospechosos, la gestión de descargas y la prevención de ataques de phishing.
   - Los ciudadanos que utilicen redes institucionales (ej: en puntos de acceso públicos) recibirán orientación básica sobre el uso responsable de internet a través de materiales educativos.
   - Esta regla fomenta una cultura de seguridad digital y reduce los riesgos derivados de errores humanos.
8. **Restricción de Dispositivos Personales**:
   - El uso de dispositivos personales para acceder a las redes institucionales estará restringido y requerirá autorización excepcional del equipo de tecnología de la información, previa verificación de seguridad (ej: antivirus actualizado, configuración aprobada).

- Los dispositivos personales autorizados deberán conectarse a una red segmentada con acceso limitado, evitando la interacción con recursos críticos.
- Esta política protege la red institucional frente a dispositivos no controlados que puedan introducir vulnerabilidades.

9. **Gestión de Incidentes Relacionados con el Acceso a Internet**:
   - Cualquier incidente relacionado con el acceso a internet, como conexiones no autorizadas, detección de malware o uso indebido de la red, deberá reportarse inmediatamente al Responsable de Seguridad de la Información.
   - El equipo de tecnología de la información investigará los incidentes, implementará medidas de mitigación y documentará lecciones aprendidas para prevenir recurrencias.
   - Esta regla asegura una respuesta rápida y efectiva, minimizando el impacto de los incidentes en la seguridad digital.

9. Sanciones por la Violación a las Políticas de Seguridad

La Alcaldía Municipal de Yarumal está comprometida con la protección de sus activos de información y la promoción de un entorno digital seguro, confiable y transparente. Para garantizar el cumplimiento de las políticas de seguridad digital, incluidas aquellas relacionadas con el acceso a internet, la gestión de datos y el uso responsable de los recursos digitales, se establecen sanciones claras y proporcionales para cualquier violación, aplicables a funcionarios, contratistas, proveedores y ciudadanos que interactúen con los servicios digitales de la institución. Estas sanciones, diseñadas para reforzar la responsabilidad compartida y la cultura de seguridad digital, se alinean con normativas nacionales, como la Ley 1581 de 2012 sobre protección de datos personales, el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el CONPES 3854 de 2011, y el marco disciplinario aplicable a los servidores públicos y contratistas en Colombia. Además, las sanciones reflejan los principios de transparencia, rendición de cuentas e inclusión digital del Plan de Desarrollo Municipal (PDI) 2024-2027, asegurando que las consecuencias sean justas, disuasorias y orientadas a la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

Las sanciones por violaciones a las políticas de seguridad digital se detallan a continuación, considerando la gravedad, el impacto y la intencionalidad de la infracción:

1. Advertencia Formal:
    - Aplicación: Para violaciones menores o no intencionales que no comprometan gravemente los activos de información o los procesos digitales, como el uso indebido de internet para fines personales no autorizados o el incumplimiento de procedimientos de autenticación sin consecuencias significativas.
    - Procedimiento: El Responsable de Seguridad de la Información o el supervisor correspondiente emitirá una advertencia escrita, documentando la infracción y requiriendo la corrección inmediata del comportamiento. El infractor deberá participar en una sesión de sensibilización sobre seguridad digital.
    - Objetivo: Fomentar la corrección del comportamiento y reforzar la cultura de seguridad sin escalar a medidas más severas.
2. Suspensión Temporal de Accesos:
    - Aplicación: Para violaciones moderadas que representen un riesgo potencial para la seguridad digital, como el uso de dispositivos removibles no autorizados, la configuración de conexiones a internet sin aprobación, o el incumplimiento repetido de políticas de contraseñas.
    - Procedimiento: El equipo de tecnología de la información suspenderá temporalmente los privilegios de acceso del infractor a los servicios digitales, con una duración proporcional a la gravedad. Se notificará al infractor y se requerirá capacitación adicional.
    - Objetivo: Proteger los activos de información mientras se corrige el comportamiento, asegurando que el infractor comprenda las consecuencias de sus acciones.
3. Acciones Disciplinarias para Funcionarios:
    - Aplicación: Para violaciones graves o repetidas por parte de funcionarios, como accesos no autorizados a datos sensibles, divulgación indebida de

información protegida por la Ley 1581 de 2012, o negligencia significativa en la gestión de copias de seguridad.

- Procedimiento: Las infracciones serán reportadas al área competente para procesos disciplinarios, siguiendo el marco de la Ley 734 de 2002 (Código Disciplinario Único). Las sanciones podrán incluir amonestaciones, suspensiones o, en casos extremos, terminación del vínculo laboral, según lo determine el proceso disciplinario.
- Objetivo: Garantizar el cumplimiento de las políticas de seguridad y mantener la integridad de los procesos institucionales.

4. Terminación de Contratos para Contratistas o Proveedores:
   - Aplicación: Para violaciones graves por parte de contratistas o proveedores, como el incumplimiento de estándares de seguridad en los servicios prestados, el acceso no autorizado a recursos digitales, o la falta de protección de datos confiados.
   - Procedimiento: La Alcaldía iniciará un proceso de revisión contractual, pudiendo imponer sanciones económicas o la terminación del contrato, conforme a los términos acordados y la normativa de contratación pública. Las infracciones serán documentadas y reportadas a las autoridades competentes si es necesario.
   - Objetivo: Asegurar que los terceros cumplan con las políticas de seguridad y proteger los activos de información de la Alcaldía.
5. Restricción de Acceso para Ciudadanos:
   - Aplicación: Para violaciones por parte de ciudadanos que utilicen servicios digitales, como el uso indebido de redes institucionales o intentos de acceso no autorizado a plataformas digitales.
   - Procedimiento: El equipo de tecnología de la información restringirá el acceso del ciudadano a los servicios digitales afectados, notificando la infracción y proporcionando orientación sobre el uso responsable. En casos graves, se podrán iniciar acciones legales si la infracción constituye un delito (ej: hacking).

- Objetivo: Promover el uso responsable de los servicios digitales y proteger la infraestructura digital de la Alcaldía.

6. Acciones Legales por Violaciones Graves:
    - Aplicación: Para infracciones que constituyan delitos bajo la normativa colombiana, como la violación de datos personales (Ley 1581 de 2012), el acceso abusivo a sistemas informáticos (Ley 1273 de 2009), o el daño a la infraestructura digital.
    - Procedimiento: La Alcaldía presentará las denuncias correspondientes ante las autoridades competentes y colaborará en las investigaciones, proporcionando evidencia de la infracción. Las sanciones podrán incluir multas, penas privativas de la libertad u otras medidas establecidas por la ley.
    - Objetivo: Disuadir conductas delictivas y proteger los derechos de los ciudadanos y la integridad de los activos de información.
7. Documentación y Seguimiento de Infracciones:
    - Todas las violaciones a las políticas de seguridad serán documentadas por el Responsable de Seguridad de la Información, incluyendo la naturaleza de la infracción, el impacto, las sanciones aplicadas y las acciones correctivas tomadas.
    - Los casos serán revisados periódicamente para identificar patrones de incumplimiento y ajustar las políticas o programas de capacitación, promoviendo la mejora continua del SGSI.
    - Esta regla asegura la trazabilidad de las infracciones y fomenta la transparencia en la gestión de sanciones.

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-c5e5-8ba2-00bc58f801d3657b

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