



El futuro digital
es de todos

MinTIC

Anexo 1

Lineamientos para estandarizar las ventanillas únicas, portales de programas específicos de programas transversales del Estado y sedes electrónicas

MinTIC – Viceministerio de Transformación Digital
Dirección de Gobierno Digital
Diciembre 2020

LINEAMIENTOS INTEGRACIÓN

Karen Abudinen Abuchaibe - Ministra de Tecnologías de la Información y las Comunicaciones

German Rueda - Viceministro de Transformación Digital

Aura María Cifuentes - Directora de Gobierno Digital

Nayelli Jaraba Negrete – Agencia Nacional Digital

Diana Betty Clavijo Vargas – Equipo Gov.co/Territorial

Francisco Javier Moreno – Equipo de Gov.co

Harley Roldán - Equipo de Gov.co

José Ricardo Aponte - Equipo Servicios Ciudadanos Digitales

Juan Pablo Salazar - Coordinación de Política

Marco Emilio Sánchez - Coordinación de Política

Luis Fernando Bastidas – Coordinación de Política

Juan Carlos Noriega - Coordinación de Política

Versión	Observaciones
Versión 1 Diciembre / 2020	Título Anexo 1 Lineamientos para estandarizar las ventanillas únicas, portales de programas transversales y unificación de sedes electrónicas del Estado colombiano

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico: gobiernodigital@mintic.gov.co

Lineamientos de Integración a Sedes Electrónicas, Ventanillas Únicas, Portales Específicos de Programas Transversales del Estado.



Esta guía de la Dirección de Gobierno Digital se encuentra bajo una Licencia Creative Commons Atribución 4.0 Internacional.

Contenido

1. Alcance y ámbito de aplicación	5
2. Definiciones.....	6
3. Marco normativo	10
4. Lineamientos de sede electrónica.....	12
4.1. Contenido y estructura de información de la sede electrónica	13
4.1.1. Barra superior (top bar).....	16
4.1.2. Menú principal.....	16
4.1.2.1 Menú Transparencia y acceso información pública.....	17
4.1.2.2. Menú Servicios a la ciudadanía	18
4.1.2.3. Menú Participa.....	21
4.1.3. Sección noticias	22
4.1.4. Acceso a portales de programas transversales	22
4.1.5 barra inferior (footer)	22
4.1.6. Cumplimiento de políticas	23
4.1.6.1 Términos y condiciones.....	23
4.1.6.2 Política de privacidad y tratamiento de datos personales	23
4.2. Arquitectura de referencia de la sede electrónica.....	27
4.3. Atributos de calidad de la sede electrónica	32
4.3.1. Usabilidad.....	33
4.3.2. Accesibilidad	34
4.3.3. Seguridad	36
4.3.4. Neutralidad.....	39
4.3.5. Interoperabilidad	39
4.3.6. Calidad de información	40
4.3.7. Disponibilidad.....	41
4.3.8. Infraestructura tecnológica.....	41
4.4. Lineamientos de ventanillas únicas digitales	42
4.4.1. Contenido y estructura de información de las ventanillas únicas digitales..	42
4.4.1.1. Requisitos mínimos.....	42

4.4.2 Cumplimiento de políticas	45
4.4.2.1. Términos y condiciones.....	45
4.4.2.2. Política de privacidad y tratamiento de datos personales.....	45
4.4.3 Arquitectura de referencia para ventanillas únicas digitales	46
4.4.4 Atributos de calidad de la ventanilla única digital	46
4.5. Lineamientos para portales de programas transversales	47
4.5.1. Contenido y estructura de información de portales de programas transversales.....	47
4.5.2. Requisitos mínimos para los portales de programas transversales del estado	47
4.5.3. Requisitos mínimos de contenidos.....	48
4.5.4. Cumplimiento de políticas legales.....	50
4.5.4.1. Términos y condiciones.....	50
4.5.4.2. Política de privacidad y tratamiento de datos personales.....	50
4.5.4.3. Política de derechos de autor y/o autorización de uso sobre los contenidos.....	50
4.5.5. Arquitectura de referencia para portales de programas transversales.....	51
4.5.6 Atributos de calidad de los portales de programas transversales	51
4.5.6.1. Usabilidad.....	52
4.5.6.2. Accesibilidad	53
4.5.6.3. Seguridad	55
4.5.6.4. Neutralidad.....	57
4.5.6.5. Interoperabilidad.....	58
4.5.6.6. Calidad de información.....	58
4.5.6.7. Disponibilidad	59
4.5.6.8. Infraestructura tecnológica.....	59
4.5.6.9 Condiciones de creación.....	59

1. Alcance y ámbito de aplicación

Esta guía establece los conceptos y lineamientos generales de las sedes electrónicas, ventanillas únicas y los portales de programas transversales del Estado que deberán seguir las entidades para integrar sus sedes electrónicas al Portal Único del Estado colombiano, aplicando lo señalado en los artículos 2.2.17.6.1. del título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, 60 de la Ley 1437 de 2011, 14 y 15 del Decreto 2106 del 22 de noviembre de 2019.

La guía aplica a todas las autoridades señaladas en el artículo 2.2.17.1.2. del Decreto 1078 de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".

2. Definiciones

Accesibilidad web: Condiciones y características de los contenidos dispuestos en medios digitales para que puedan ser utilizados por la más amplia mayoría de ciudadanos, independientemente de sus condiciones personales, tecnológicas o del ambiente en el que se desempeñen.

Autoridades: Son todos los organismos y entidades que conforman las ramas del poder público en sus distintos órdenes, sectores y niveles, a los órganos autónomos e independientes del Estado y a los particulares, cuando cumplan funciones administrativas o públicas.

Consultas de acceso a información pública: Información contenida en bases de datos o repositorios digitales relacionadas a trámites u otros procedimientos administrativos de las autoridades a la cual puede acceder la ciudadanía de manera digital, inmediata y gratuita para el ejercicio de un derecho, una actividad u obligación, que puede ser accedida por el titular o un tercero utilizando o no, un mecanismo de autenticación según sea la tipología de la información de que se trate.

Confidencialidad: Atributo que garantiza que la información sea accesible solo a aquellas personas autorizadas para ello.

Disponibilidad: Es la propiedad de la información que permite que ésta sea accesible y utilizable cuando se requiera

Gestión documental electrónica: Conjunto de actividades administrativas y técnicas, tendientes a la planificación, manejo y organización de la documentación producida y recibida por las entidades en formatos electrónicos, digitales y/o digitalizados, desde su origen o creación hasta su disposición final con el objeto de facilitar su utilización y preservación a largo plazo haciendo uso de tecnologías de la información y las comunicaciones.

Grupo de valor: Individuos u organismos específicos receptores de los resultados de la gestión de la entidad.

Integridad de la información: Es la condición que garantiza que la información consignada en un mensaje de datos ha permanecido completa e inalterada, salvo la adición autorizada de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación.

Incidente de seguridad: evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Otro Procedimiento Administrativo (OPA): conjunto de requisitos, pasos o acciones dentro de un proceso misional, que determina una entidad u organismo de la administración pública o particular que ejerce funciones administrativas, para permitir el acceso de los ciudadanos, usuarios o grupos de interés a los beneficios derivados de programas o estrategias cuya creación, adopción e implementación es potestativa de la entidad.

Portal específico de un programa transversal del Estado: sitio en Internet que integra información, recursos u oferta institucional de un programa o iniciativa del Estado, con impacto nacional, y que involucra más de una autoridad. Ejemplo: Portal de Economía Naranja

Sede electrónica: Es la dirección electrónica de titularidad, administración y gestión de cada autoridad competente, dotada de las medidas jurídicas, organizativas y técnicas que garanticen calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad de la información y de los servicios. La sede electrónica permitirá las interacciones digitales existentes como trámites, servicios, ejercicios de participación, acceso a la información, colaboración y control social, entre otros

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

Servicios Ciudadanos Digitales (SCD): son el conjunto de soluciones y procesos transversales que brindan al Estado capacidades y eficiencias para su transformación digital y para lograr una adecuada interacción con el ciudadano, garantizando el derecho a la utilización de medios electrónicos ante la administración pública.

Servicio de Autenticación Digital: Es el procedimiento que utilizando mecanismos de autenticación, permite verificar los atributos digitales de una persona cuando adelanten trámites y servicios a través de medios digitales. Además, en caso de requerirse, permite tener certeza sobre la persona que ha firmado un mensaje de datos, o la persona a la que se atribuya el mismo en los términos de la Ley 527 de 1999 y sus normas reglamentarias, o las normas que la modifiquen, deroguen o subroguen, y sin perjuicio de la autenticación notarial.

Servicio de Carpeta Ciudadana Digital: Es el servicio que le permite a los usuarios de servicios ciudadanos digitales acceder digitalmente de manera segura, confiable y actualizada al conjunto de sus datos, que tienen o custodian las entidades señaladas en el artículo 2.2.17.1.2. del Decreto 1078 de 2015.

Adicionalmente, este servicio podrá entregar las comunicaciones o alertas, que las entidades señaladas tienen para los usuarios, previa autorización de estos.

Servicio de Interoperabilidad: Es el servicio que brinda las capacidades necesarias para garantizar el adecuado flujo de información e interacción entre los sistemas de información de las entidades, permitiendo el intercambio, la integración y la compartición de la información, con el propósito de facilitar el ejercicio de sus funciones constitucionales y legales, acorde con los lineamientos del marco de interoperabilidad.

Trámite: Conjunto de requisitos, pasos o acciones reguladas por el Estado, dentro de un proceso misional, que deben efectuar los ciudadanos, usuarios o grupos de interés ante una entidad u organismo de la administración pública o particular que ejerce funciones administrativas, para acceder a un derecho, ejercer una actividad o cumplir con una obligación, prevista o autorizada en la ley.

Trámites y OPA automatizados: Son aquellos trámites y Otros Procedimientos Administrativos (OPA) totalmente en línea, cuya gestión al interior de la autoridad se realiza haciendo uso de tecnologías de la información y las comunicaciones, sin requerir la intervención humana.

Trámite y OPA parcialmente en línea (parcialmente: digital, electrónico o sistematizado): Es el trámite y OPA dispuesto por una autoridad en el cual el solicitante puede realizar por medios digitales o a través de la sede electrónica, al menos uno de los pasos o acciones necesarias para obtener el bien o servicio requerido.

Trámite y OPA totalmente en línea (totalmente: digital, electrónico o sistematizado): Es el trámite y OPA dispuesto por una autoridad a través de las sedes electrónicas y en el cual el solicitante puede realizar por medios digitales la totalidad del conjunto de pasos o acciones, así como la presentación de los requisitos necesarios, hasta obtener el bien o servicio requerido.

Usabilidad: Es una cualidad o atributo de calidad, que hace que un producto o servicio web sea fácil de usar y comprender

Ventanilla única: Sitio o canal que integra actuaciones administrativas de dos o más autoridades que contribuyen a una misma finalidad para atender a un ciudadano, usuario o grupo de valor. Las actuales "Ventanillas Únicas" que involucran a una sola entidad estarán en la sección transaccional de la sede electrónica.

Ventanilla única digital: Sitio o canal digital que integra actuaciones administrativas de dos o más autoridades que contribuyen a una misma finalidad para atender a un ciudadano, usuario o grupo de valor.

Ventanilla única presencial: Sitio o canal presencial que integra actuaciones administrativas de dos o más autoridades que contribuyen a una misma finalidad para atender a un ciudadano, usuario o grupo de valor.

3. Marco normativo

El Decreto 1078 de 2015 en el capítulo 1 del título 9 de la parte 2 del libro 2, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones (DUR-TIC) define que el objetivo de la Política de Gobierno Digital es “Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital”. Para la implementación de la Política de Gobierno Digital, se han definido dos componentes: TIC para el Estado y TIC para la Sociedad, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales.

Estos cinco instrumentos se desarrollan a través de lineamientos y estándares, que son los requerimientos mínimos que todos los sujetos obligados deben cumplir para alcanzar los logros de la política.

La sede electrónica tiene su fuente normativa en la Ley 1437 de 2011 en su artículo 60 al señalar que: “(...) Toda autoridad deberá tener al menos una dirección electrónica (...)”, siendo por mandato de dicha disposición que “(...) La autoridad respectiva garantizará condiciones de calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad de la información de acuerdo con los estándares que defina el Gobierno Nacional”.

En ese mismo orden, el artículo 14 del Decreto 2106 de 2019, establece que las autoridades deberán integrar a su sede electrónica todos los portales, sitios web, plataformas, ventanillas únicas, aplicaciones y soluciones existentes, que permitan la realización de trámites, procesos y procedimientos a los ciudadanos de manera eficaz. Así mismo, la titularidad, administración y gestión de la sede electrónica es responsabilidad de cada autoridad competente y estará dotada de las medidas jurídicas, organizativas y técnicas que garanticen calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad de la información y de los servicios.

A su vez, el artículo 15 del mismo Decreto señala que el Portal Único del Estado colombiano será la sede electrónica compartida a través de la cual los ciudadanos accederán a la información, procedimientos, servicios y trámites que se deban adelantar ante las autoridades. La administración gestionará y tendrá la titularidad del Portal Único del Estado colombiano y garantizará las condiciones de calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad.

Por mandato de dicha disposición, las autoridades deberán integrar su sede electrónica al Portal Único del Estado colombiano, en los términos que señale el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y

serán responsables de la calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad de la información, procedimientos, servicios y trámites ofrecidos por este medio.

Los programas transversales del Estado que cuenten con portales específicos deberán integrarse al Portal Único del Estado colombiano. Al MinTIC se le otorga la competencia para establecer las condiciones de creación e integración de dichos portales.

De la misma manera, se establece que las Ventanillas Únicas existentes deberán integrarse al Portal Único del Estado colombiano.

Por su parte el artículo 2.2.17.1.1. del Decreto 1078 de 2015 reglamenta parcialmente los artículos 53, 54. 60. 61 y 64 de la Ley 1437 de 2011, los literales e, j y el parágrafo 2" del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019. y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales y su integración a la sede electrónica.

El Decreto 1080 de 2015 en su artículo 2.8.2.5.1 determina como sujetos obligados a la gestión documental a la Administración Pública en sus diferentes niveles, nacional, departamental, distrital, municipal; a las entidades territoriales indígenas y demás entidades territoriales que se creen por ley; de las divisiones administrativas; las entidades privadas que cumplen funciones públicas, por lo tanto, la documentación que se comparta a través de las sedes electrónicas o que provenga del ciudadano debe incorporarse dentro de los lineamientos de gestión documental establecidos por la entidad, incluido cuando se usas tecnologías de la información y las comunicaciones.

4. Lineamientos de sede electrónica

La sede electrónica debe integrar todos los portales institucionales, sitios web, plataformas, ventanillas únicas, aplicaciones y soluciones existentes, que le permitan la realización de trámites, procesos y procedimientos a los ciudadanos, servicios, ejercicios de participación, acceso a la información. colaboración y control social, entre otros, de acuerdo con lo establecido en el artículo 14 del Decreto 2106 de 2019 y 2.2.17.6.1. del Decreto 1078 de 2015.

En adelante el portal web principal de cada autoridad deberá constituirse como su sede electrónica a partir del cumplimiento de las siguientes condiciones:

- Dicho portal será el sitio oficial en Internet de cada autoridad,
- Dicho portal deberá permitir su acceso a través de una dirección electrónica,
- Dicho portal deberá disponer tanto de información como de acceso a los trámites, Otros Procedimientos Administrativos, consulta de acceso a información pública, ejercicios de participación, acceso a la información. colaboración y control social, y demás servicios ofertados por la autoridad.
- La titularidad, administración y gestión de dicho portal estará a cargo de la autoridad correspondiente.

A continuación, se listan cada uno de los lineamientos que deben ser considerados en la implementación y unificación de la sede electrónica de las autoridades.

4.1. Contenido y estructura de información de la sede electrónica

Todas las autoridades deberán adecuar su sede electrónica de manera que cuente con los siguientes requisitos:

- a) Todo contenido o información de la sede electrónica debe estar relacionado con la misión de la autoridad.
- b) La información contenida en la sede electrónica debe estar en idioma castellano. No obstante, las autoridades podrán traducirla a otros idiomas o lenguas, siempre que dichas traducciones cumplan la Ley 1712 de 2014, entre otros, con el principio de calidad de la información. Lo anterior, de conformidad con lo establecido en el artículo 10 de la Constitución Política de Colombia.
- c) Las autoridades deben garantizar condiciones de creación o captura, organización, conservación y/o archivo para posterior consulta de la documentación digital disponible en su sede electrónica, conforme con las Tablas de Retención Documental aprobadas y los lineamientos del Archivo General de la Nación. Lo anterior, de conformidad con el Decreto 1080 del 2015, el Decreto Nacional 1862 del 2015 y el artículo 16 del Decreto 2106 del 2019 o el que los modifique, subrogue, adicione o desarrolle. Las autoridades deben garantizar y facilitar a los solicitantes, de la manera más sencilla posible, el acceso a toda la información previamente divulgada de conformidad con el artículo 17 de la Ley 1712 de 2014, para asegurar que los sistemas de información electrónica sean efectivamente una herramienta para promover el acceso a la información pública.
- d) Las autoridades deberán adoptar medidas de conservación preventiva a largo plazo para facilitar procesos de migración, emulación o refreshing, o cualquier otra técnica que se disponga a futuro, y deberán asegurar la preservación de los documentos en formatos digitales. Para tal efecto, deberán adoptar un programa de gestión documental digital, conforme lo dispone el artículo 15 de la Ley 1712 de 2014, el Decreto 2609 del 2012 y el artículo 16 de Decreto 2106 de 2019 o el que los modifique, adicione o desarrolle.
- e) La sede electrónica deberá contar con un buscador general en su home para acceder a cualquiera de sus contenidos, conforme con los lineamientos de usabilidad. El buscador de la sede electrónica de cada autoridad es independiente al de la sede compartida GOV.CO.

- f) No se deben incluir contenidos, enlaces, publicidad, marcas o referencias que no estén estrictamente relacionadas con el cumplimiento de las funciones de la autoridad.
- g) De conformidad con el artículo 2.2.17.6.1. del título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, la sede electrónica deberá disponer los servicios de registro de documentos electrónicos, accedidos a través de la sede electrónica para la recepción y remisión de peticiones escritas y documentos. Los sistemas de información que soportan la sede electrónica deberán garantizar la disponibilidad e integridad de la información y la correcta gestión documental electrónica en los distintos procedimientos y trámites electrónicos, en los términos de la Ley 594 de 2000 y sus decretos reglamentarios.

Asimismo, deberán:

1. Admitir documentos electrónicos correspondientes a los servicios, procedimientos y trámites que se especifiquen, los cuales podrán ser aportados por el ciudadano utilizando los servicios de la sede electrónica u otros medios electrónicos. Los documentos se podrán presentar todos los días del año durante las veinticuatro horas.
2. Disponer en la sede electrónica la relación actualizada de las peticiones, escritos y documentos recibidos incluyendo la fecha y hora de recepción.
3. Asignar un número consecutivo a las comunicaciones recibidas o producidas, dejando constancia de la fecha y hora de recibo, con el propósito de oficializar el trámite y cumplir con los términos de vencimiento que establezca la ley y hacer seguimiento a todas las actuaciones recibidas y enviadas.
4. Enviar automáticamente por el mismo medio un mensaje acusando el recibo y registro de las peticiones, escritos o documentos de que se trate, en el que constarán los datos proporcionados por los ciudadanos, la fecha y hora de presentación y el número consecutivo de radicación asignado.
5. Recibir los documentos anexos a la correspondiente solicitud, mensaje o comunicación. El registro electrónico generará mensajes que acrediten la entrega de estos documentos.
6. Distribuir electrónicamente en los términos que establezca la entidad para cada trámite, los documentos registrados al destinatario o destinatarios o entidad responsable de atender el trámite correspondiente.
7. Utilizar formatos o formularios preestablecidos para la presentación de documentos electrónicos normalizados, correspondientes a los servicios y trámites que se especifiquen en el sistema.
8. Incorporar el calendario oficial de la entidad con fecha y hora, los días hábiles y los declarados inhábiles,
9. Posibilitar la interconexión de todas las dependencias de la entidad para el acceso a la información por medios electrónicos.
10. Establecer un esquema de interoperabilidad entre los diferentes sistemas o soluciones utilizados por las entidades públicas para atender de manera adecuada y oportuna los trámites, otros procedimientos administrativos y consultas de acceso a información pública.

A continuación, se listan cada uno de los lineamientos que deben ser considerados en la implementación y unificación de la sede electrónica:

4.1.1. Barra superior (top bar)

Acondicionar una barra superior completa con acceso al Portal Único del Estado colombiano - GOV.CO, que estará ubicada en la parte superior, la cual deberá aparecer en todas sus páginas y vistas. La barra de GOV.CO contendrá su respectivo logotipo el cual deberá dirigir al sitio web <https://www.gov.co> y demás referencias que sean adoptadas en el lineamiento gráfico.

4.1.2. Menú principal

La definición de las opciones o secciones que se incluyan en el menú principal deberán estar justificadas en el cumplimiento del marco normativo colombiano y en la caracterización de las necesidades y contenidos más consultados de sus usuarios.

Con el fin de lograr una estandarización que facilite a la ciudadanía el acceso a la información pública, así como a trámites, Otros Procedimientos Administrativos, consulta de acceso a información pública, y participación en las diferentes sedes electrónicas de las autoridades del Estado colombiano, se incluirán las siguientes opciones en el menú principal: Transparencia y acceso información pública, 2. Servicios a la ciudadanía y 3. Participa.

Las entidades podrán habilitar en el menú principal el número opciones o secciones de manera autónoma para incluir allí la información adicional que por normas o necesidades particulares deban o deseen publicar. No obstante, siguiendo las buenas prácticas de experiencia de usuario se recomienda que este número no sea superior a 7, conforme lo permita las posibilidades de diseño y usabilidad conforme con la Anexo 2.1 Guía de diseño gráfico para sedes electrónicas.

Las opciones o secciones que se incluyan en el menú principal podrán contener menús desplegables para facilitar el acceso a otras subsecciones de la sede electrónica con el fin de reducir el número de clics por parte del usuario.

Opcionalmente, las autoridades también podrán incluir otras formas de menú desplegable para publicar otras categorías de información, tal y como se muestra en la Anexo 2.1 Guía de diseño gráfico para sedes electrónicas, específicamente en la sección “Aplicación Home”.

Para las anteriores 3 secciones referidas, las autoridades deberán adoptar los siguientes lineamientos:

4.1.2.1 Menú Transparencia y acceso información pública

En esta sección se publica la información sobre transparencia y acceso a la información pública, para lo cual se deben adoptar fuentes únicas de información y de datos para evitar la duplicidad y asegurar su integridad, calidad y disponibilidad, incluyendo los siguientes criterios de publicación:

- (a) Toda la información, documentos o datos deben ser publicados en forma cronológica del más reciente al más antiguo.
- (b) Los contenidos e información dispuestos para los usuarios deberán ser accesibles y usables conforme las disposiciones del presente lineamiento, y las directrices de accesibilidad web aprobadas por MinTIC y utilizar un lenguaje claro.
- (c) Se debe contar con un buscador en el que la ciudadanía pueda encontrar información, datos o contenidos relacionados con asuntos de transparencia y acceso a la información. Se sugiere disponer de búsquedas a partir del texto del contenido, tipologías, temas, subtemas, palabras claves, entre otros.
- (d) Toda la información debe ser publicada en formatos que permitan: su descarga, acceso sin restricciones legales, uso libre, procesamiento por máquina y realizar búsquedas en su interior.
- (e) Todo documento o información debe indicar la fecha de su publicación en la sede electrónica.
- (f) Las autoridades deben incluir contenidos en el menú de Transparencia y acceso a la información pública, de acuerdo con la Ley 1712 del 2014 y la Resolución 1519 del 2020 de MinTIC o la que la modifique, adicione o desarrolle.
- (g) La información pública debe contar con una fuente única alojada en el menú de Transparencia y Acceso a la Información Pública evitando duplicidad, de forma que, independiente el enlace/menú/sección en la que se divulgue la información se redireccionará a la fuente única.
- (h) La publicación de normativa deberá seguir los siguientes criterios:
 - Toda la normativa debe ser publicada en formatos que permitan: su descarga, acceso sin restricciones legales, uso libre, procesamiento por máquina y realizar búsquedas en su interior.
 - La publicación de las normas debe incluir lo siguiente: tipo de norma, fecha de expedición, fecha de publicación, epígrafe o descripción corta de la misma, y enlace para su consulta.
 - Los documentos deben estar organizados del más reciente al más antiguo.

- La norma expedida debe ser publicada en forma inmediata o en tiempo real.
- Los proyectos de normativa deben indicar la fecha máxima para presentar comentarios, en todo caso se debe incluir por lo menos un medio digital o electrónico.
- Se deberá señalar si la norma se encuentra en vigor o no.

(g) Las autoridades deben publicar la información y los contenidos de forma estandarizada como lo indica la Resolución 1519 del 2020 y las demás que modifiquen o adicionen. En especial, deberán publicar en forma destacada una subsección para publicar los informes relacionados con la gestión institucional, tal y como es el caso de los informes de gestión sobre la pandemia por causa del COVID-19. Así mismo, se debe publicar la información y los contenidos de transparencia que sean establecidos por medio de Directivas Presidenciales y en los demás lineamientos de la Política de Gobierno Digital.

4.1.2.2. Menú Servicios a la ciudadanía

1. Trámites, Otros Procedimientos Administrativos y consultas acceso a información pública.

Permite acceder a la información y contenidos relacionados con la gestión de trámites, otros procedimientos administrativos y consulta de acceso a información pública, así como las ventanillas únicas asociadas a la sede electrónica.

A continuación, se listan los requerimientos exigibles a las autoridades en este menú:

a. Información y gestión de trámites, Otros Procedimientos Administrativos y consulta de acceso a información pública: las autoridades deberán implementar mecanismos para que los usuarios encuentren sus trámites, Otros Procedimientos Administrativos y consulta de acceso a información pública dispuestos en la Sede Electrónica, de forma que la información esté disponible de manera efectiva y cumpliendo los siguientes lineamientos de usabilidad:

- Garantizar que se visualice al menos un resultado en la pantalla sin necesidad de hacer scroll.
- Garantizar el cumplimiento de las directrices de accesibilidad web.
- Garantizar la aparición de los mecanismos de acceso y sus elementos secundarios, tales como el número de resultados que se visualizan y el componente de paginación.

Los mecanismos de acceso pueden ser: etiquetas, desplegados o campo de texto para consultar dentro de la sección de Trámites,

OPA'S y Consultas de acceso a la información pública, de la autoridad.

Las etiquetas permiten seleccionar un criterio de búsqueda de manera inmediata. Cuando la entidad hace uso de etiquetas, debe garantizar que se vea al menos un resultado de búsqueda en la primera pantalla, dado el caso que la cantidad de etiquetas sea extensa debe usar un desplegable, donde agrupe todas las etiquetas, permitiendo incluso seleccionar varios criterios de búsqueda, por ejemplo, una categoría, subcategoría y/o ubicación.

- b. Para habilitar el acceso a los trámites totalmente en línea y parcialmente en línea, Otros Procedimientos Administrativos totalmente en línea y parcialmente en línea y consulta de acceso a información pública, las autoridades deberán hacerlo de la siguiente manera:

Direccionar a la ficha disponible en el Portal Único del Estado colombiano, cuya dirección electrónica contiene la siguiente estructura: <https://www.gov.co/servicios-y-tramites/T345>, donde 345 corresponde al código trámite asignado en el Departamento Administrativo de la Función Pública en el Sistema Único de Información de Trámites (SUIT).

Ejemplo: El trámite de convalidación de estudios de pregrado en el exterior corresponde al código T345, por lo cual, el link que le corresponde en el Portal Único del Estado colombiano es: <https://www.gov.co/servicios-y-tramites/T345>

- c. Direccionar al trámite en línea. En cada trámite, Otro Procedimiento Administrativo o consulta de acceso a información pública, se deberá indicar si puede realizarse totalmente en línea, parcialmente en línea o presencial. Además, informar si tiene asociado un costo o es gratuito; e indicar el tiempo de resolución del mismo, así como la información inherente al mismo.

- d. Las autoridades deberán disponer de mecanismos de consulta del estado del trámite, Otro Procedimiento Administrativo y consulta de acceso a información pública, registro y autenticación para que los usuarios puedan realizar sus procedimientos digitales con la debida confianza, seguridad, trazabilidad, calidad y protección de los datos personales, y garantizando las condiciones de conservación y/o archivo para posterior consulta de la documentación electrónica disponible en su sede electrónica, conforme a los lineamientos de gestión documental dispuestos por el Archivo General de la Nación. Lo anterior de conformidad a lo establecido en la política de Gobierno Digital del

MinTIC y en la Guía de Racionalización de Trámites del Departamento Administrativo de la Función Pública.

- e. Cada autoridad deberá disponer en este menú un acceso a las ventanillas únicas digitales de las cuales es responsable. Así mismo, podrá incluir en su respectiva sede electrónica el acceso a las ventanillas únicas de las que hace parte activa en la cadena de trámites que la conforman.
 - f. En los casos en que se habiliten enlaces o hipervínculos a páginas externas a la sede electrónica de la autoridad, se deberá informar al usuario mediante un aviso lo siguiente: “Usted está punto de ingresar a un sitio externo a esta sede electrónica (NOMBRE), a partir de este momento es responsabilidad de (NOMBRE ENTIDAD RESPONSABLE) el cumplimiento de las normas que regulan su relación. Cualquier solicitud deberá ser dirigida al responsable de dicho sitio (NOMBRE ENTIDAD RESPONSABLE)”
 - g. Los tramites, OPAs y consulta de acceso a información pública que la entidad disponga, deberán garantizar la creación y captura de los documentos electrónicos, a su vez la creación y conformación de los expedientes electrónicos. La entidad debe articular sus trámites con el Sistema de Gestión Documental Electrónico de Archivo (SGDEA).
 - h. Las autoridades de las que trata la Directiva Presidencial 02 del 2019 deberán observar los requerimientos de la Guía de Integración de Trámites, Otros Procedimientos Administrativos y consulta de acceso a Información Pública al Portal Único del Estado Gov.co.
2. Canales de atención y pida una cita. Para identificar y dar a conocer los canales digitales oficiales de recepción de solicitudes, peticiones y de información, de conformidad con el artículo 2.2.17.6.1. del Decreto 1078 de 2015 y el artículo 14 del Decreto 2106 de 2019, las autoridades deberán incluir en su respectiva sede electrónica la información y contenidos relacionados con los canales habilitados para la atención a la ciudadanía y demás grupos caracterizados. Además, se deberá habilitar un mecanismo para que el usuario pueda agendar una cita para atención presencial e indicar los horarios de atención en sedes físicas. Los diversos canales digitales oficiales dispuestos por cada autoridad deberán estar integrados a la sede electrónica.
3. PQRSD.
En este menú deberá habilitarse el mecanismo para el registro, radicación, envío y seguimiento de PQRS, relacionado con la presentación, tratamiento y respuesta de las mismas (incluyendo las peticiones

presentadas verbalmente), de conformidad con lo establecido en la Ley 1437 de 2011, la ley 1755 de 2015, el decreto 1166 de 2016 y en la Resolución 1519 del 2020, o aquellas normas que las modifiquen o sustituyan.

En los casos en los que el usuario seleccione la opción para el envío de PQRSD de manera anónima, se deberá deshabilitar los campos para el envío de datos que puedan identificar a la persona tales como: nombre, correo electrónico, dirección, entre otros. Adicionalmente, la entidad deberá incluir una nota con las recomendaciones en torno a las garantías de anonimato que están en cabeza del usuario tales como deshabilitación de georeferenciación del dispositivo desde el cual se envía la PQRSD, el enmascaramiento de la IP, la metadata, el uso de un navegador con ventana privada, ente otros. Así mismo, las autoridades deberán incluir en el aviso de aceptación de las condiciones un mensaje indicando que la entidad sigue los lineamientos de anonimización de datos emitidos por el Archivo General de la Nación y efectivamente da cumplimiento a los mismos.

En los casos en los que el usuario seleccione la opción para el envío de PQRSD de manera anónima, se deberá deshabilitar los campos para el envío de datos que puedan identificar a la persona tales como: nombre, correo electrónico, dirección, entre otros. Adicionalmente, la entidad deberá incluir una nota con las recomendaciones en torno a las garantías de anonimato que están en cabeza del usuario tales como deshabilitación de georeferenciación del dispositivo desde el cual se envía la PQRSD, el enmascaramiento de la IP, la metadata, el uso de un navegador con ventana privada, ente otros. Así mismo, las autoridades deberán seguir los lineamientos de anonimización de datos emitidos por el Archivo General de la Nación.

Para el cargue de archivos, las autoridades no podrán establecer restricciones técnicas (en lo que respecta a formatos, tamaños, cantidad de documentos, entre otros) para la radicación de PQRSD, por lo cual, el formulario deberá contar con las facilidades necesarias para garantizar el derecho de petición.

4.1.2.3. Menú Participa

Las autoridades deberán publicar en el Menú Participa los contenidos de información sobre los espacios, mecanismos y acciones que permiten la participación ciudadana en el ciclo de la gestión pública, dinamizando la vinculación de la ciudadanía en las decisiones y acciones públicas durante el diagnóstico, formulación, implementación, evaluación y seguimiento a la gestión institucional conforme con los lineamientos específicos que expida el Departamento Administrativo de la Función Pública.

4.1.3. Sección noticias

En la página principal, la autoridad publicará las noticias más relevantes para la ciudadanía y los grupos de valor, de conformidad con lo establecido en la Ley 1712 de 2014 y las normas que la reglamentan. La información deberá publicarse de acuerdo con las pautas o lineamientos en materia de lenguaje claro, accesibilidad y usabilidad.

4.1.4. Acceso a portales de programas transversales

En los casos en los cuales la autoridad es responsable de uno o más portales específicos de programas transversales del Estado, deberá habilitar en su respectiva sede electrónica el acceso a dichos portales. Así mismo, las autoridades involucradas en estos programas transversales podrán habilitar en su respectiva sede electrónica el acceso a dichos portales.

4.1.5 barra inferior (footer)

(a) Las autoridades deberán incluir una barra inferior (*footer*), que estará ubicada en el pie de página de su sede electrónica, para lo cual utilizará el diseño y la paleta de colores referido en los lineamientos para el acondicionamiento gráfico de sitios web al Portal Único del Estado colombiano - GOV.CO. Esta barra inferior contendrá la siguiente información:

- I. Imagen del Portal Único del Estado colombiano y el logo de la marca país CO - Colombia.
- II. Nombre de la entidad, dirección, código postal incluyendo el departamento (si aplica) y municipio o distrito.
- III. Vínculos a redes sociales para ser redireccionado en los botones respectivos. Para lo anterior, la autoridad deberá, en virtud del artículo 16 del Decreto 2106 de 2019 y del capítulo V del Decreto Nacional 1080 de 2015 y las demás normas expedidas por el Archivo General de la Nación relacionados, disponer de lo necesario para que la emisión, recepción y gestión de comunicaciones oficiales, a través de los diversos canales electrónicos, asegure un adecuado tratamiento archivístico y estar debidamente alineado con la gestión documental electrónica y de archivo digital.
- IV. Datos de contacto, incluyendo lo siguiente: teléfono conmutador, línea gratuita o línea de servicio a la ciudadanía/usuario, línea anticorrupción, diversos canales físicos y electrónicos para atención al público, correo de notificaciones judiciales, enlace para el mapa del sitio y un enlace para

vincular las políticas a las que se hace referencia en la sección de cumplimiento legal. Todas las líneas telefónicas deberán incluir el prefijo de país +57 y el número significativo nacional (indicativo nacional) que determine la Comisión de Regulación de Comunicaciones, excepto en las líneas gratuitas 018000 y 019000.

4.1.6. Cumplimiento de políticas

Las entidades deberán incorporar un enlace en la barra inferior (*footer*), que dirija a la siguiente información:

4.1.6.1 Términos y condiciones

Las autoridades deberán aprobar y publicar los términos y condiciones para el uso de todos sus portales web, plataformas, aplicaciones, trámites, Otros Procedimientos Administrativos, consulta de acceso a información pública, servicios de pasarela de pago, entre otros. Como mínimo deberán incluir lo siguiente: condiciones, alcances y límites en el uso; derechos y deberes de los usuarios; alcance y límites de la responsabilidad; contacto para asuntos relacionados con los términos y condiciones; referencia a la política de privacidad y tratamiento de datos personales, y política de seguridad.

En los casos en los que se cuente con trámites en línea o parcialmente en línea, Otros Procedimientos Administrativos en línea o parcialmente en línea y/o consulta de acceso a información pública, la autoridad deberá habilitar una opción que le permita al usuario la aceptación de los términos y condiciones.

4.1.6.2 Política de privacidad y tratamiento de datos personales

Las autoridades deberán definir, aprobar y publicar su política de privacidad y tratamiento de datos personales, conforme a las disposiciones de la Ley 1581 del 2012, la Ley 1712 de 2014 y demás instrucciones o disposiciones relacionadas, o aquellas que las modifiquen, adicionen o deroguen.

En los casos en los que se cuente con trámites en línea o parcialmente en línea, Otros Procedimientos Administrativos en línea o parcialmente en línea y/o consulta de acceso a información pública, la autoridad deberá habilitar una opción que le permita al usuario la aceptación de la política de privacidad y tratamiento de datos personales.

Todo contenido y estructura de la sede electrónica, del Portal Único del Estado colombiano, de las Ventanillas únicas y de los Portales de Programas transversales, y en general de los diversos canales electrónicos o digitales, incluidos los canales de contacto, chatbot automatizado, entre otros, utilizados por los sujetos obligados, en la medida que traten datos personales, deben cumplir con lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios.

La divulgación de datos personales a través de los diversos canales digitales debe respetar el principio de acceso y circulación restringida señalado en la Ley 1581 de 2012, para ello, la autoridad deberá determinar de manera previa si una publicación o divulgación de datos personales en su sede electrónica y/o redes sociales, u otro canal oficial utilizado, puede vulnerar lo establecido en la Ley 1581 de 2012 y el Decreto 1377 de 2013, especialmente en aquellos casos relacionados con datos de niños, niñas y adolescentes, población en situación de vulnerabilidad, datos que pueden generar algún tipo de discriminación, revelación de aspectos íntimos de las personas, datos de carácter sensible o que pueden afectar otros derechos fundamentales.

Los sujetos obligados deberán contar con la política de tratamiento de información personal de fácil acceso y comprensible a los diversos grupos de interés, incluidos discapacitados, además, debe cumplir con el conjunto de obligaciones derivadas de la Ley 1581 de 2012, entre otras, las derivadas de la aplicación de los siguientes principios:

- Acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la ley. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley.
- Confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma.
- Finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

- Legalidad: En el Tratamiento de los datos persona/es se implementarán las medidas apropiadas, efectivas y verificables para cumplir con los principios, derechos y obligaciones establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios y las normas que las modifiquen, reglamenten o sustituyan.
- Libertad, Finalidad y Transparencia: Contar con un mecanismo (u opción) que permita al usuario otorgar su consentimiento expreso, previo e informado (o explícito para el Tratamiento de los datos sensibles y de niños, niñas y adolescentes), cuando se requiera.
- Seguridad: La información sujeta a Tratamiento se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Veracidad o calidad: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

Uso de cookies, rastreadores de análisis web y uso de tecnologías similares:

Los sujetos obligados por las presentes guías tendrán en cuenta que las cookies, rastreadores de análisis web o tecnologías similares, como, entre otras, etiquetas de identificación por radiofrecuencia, suponen el tratamiento de datos personales sometidos a la Ley 1581 de 2012 y sus decretos reglamentarios, en tal sentido, deberán:

1. Abstenerse de usar cookies, rastreadores de análisis web, o tecnologías similares, salvo aquellas que sean estrictamente necesarias para el cumplimiento de sus funciones constitucionales, legales y reglamentarias y así permitir la comunicación entre el equipo del usuario y la red, entre otros.
2. Implementar un mecanismo para obtener el consentimiento previo, expreso e informado del Titular para todas y cada una de las categorías de cookie, dependiendo de su finalidad y origen.
3. Disponer por defecto, en caso de uso de cookies, que ninguna de esas cookies esté activada, salvo aquellas que sean estrictamente necesarias para el cumplimiento de sus funciones constitucionales, legales y reglamentarias y las estrictamente necesarias para el funcionamiento y seguridad de la página.

4. Adoptar un sistema de gestión o configuración para aceptar, denegar o revocar el consentimiento para el uso de cookies, así como informar sobre el tipo de cookies, quien las gestiona, uso y los fines del tratamiento, periodo de conservación; los cuales deben estar disponibles para el usuario, en una zona donde pueda ser vista por el usuario.

5. Adoptar la Política y aviso de uso de cookies y está debe estar disponible al lado de la política de tratamiento de datos personales

4.1.6.3 Política de derechos de autor y/o autorización de uso sobre los contenidos

Las autoridades deberán definir, aprobar y publicar su política de derechos de autor y/o autorización de uso de los datos y contenidos, en la cual deberán incluir el alcance y limitaciones relacionados con el uso de datos, documentos, información, contenidos y códigos fuente producidos por los sujetos obligados.

La plataforma GOV.CO territorial (<https://www.gov.co/territorial>), que suministra el Ministerio de Tecnologías de la Información y las Comunicaciones a las entidades territoriales, adoptará durante el año 2020 los lineamientos de la sede electrónica indicados en este documento, logrando así la aplicación masiva y el cumplimiento de los requerimientos por parte de todas las entidades que la utilizan.

La adecuación de la plataforma GOV.CO territorial será sufragada y realizada por el Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la Dirección de Gobierno Digital. No obstante, es necesaria la interiorización de los lineamientos por parte de las entidades territoriales para garantizar su cumplimiento en lo que se refiere a la publicación de contenidos y administración funcional de esta plataforma.

4.2. Arquitectura de referencia de la sede electrónica

La arquitectura de referencia que debe implementarse en una sede electrónica contiene las siguientes zonas, de acuerdo con la figura 1:

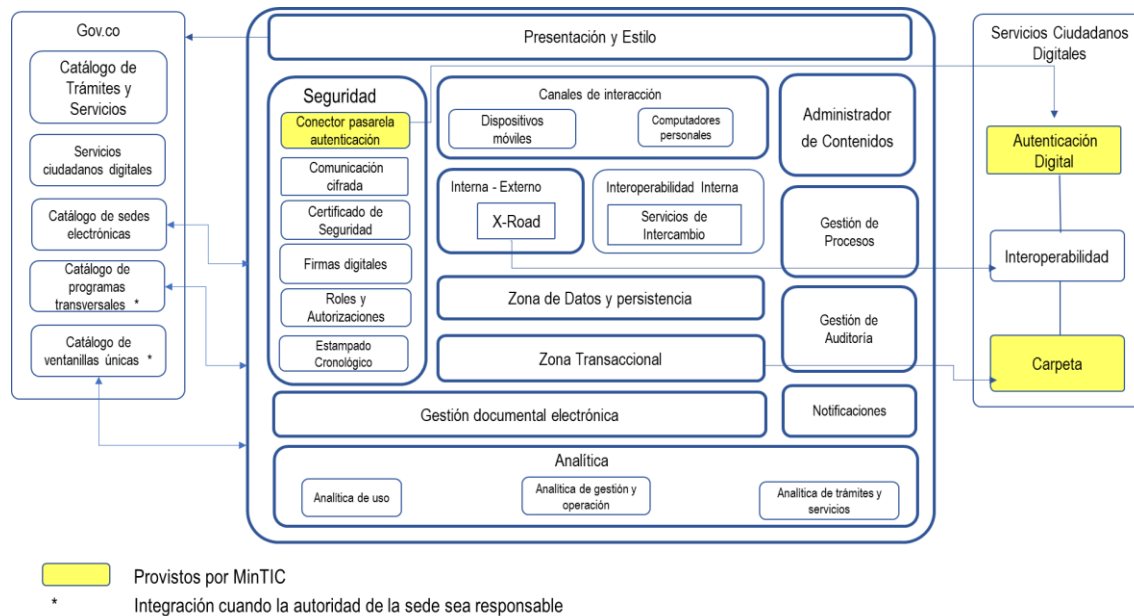


Figura 1. Arquitectura de referencia de una sede electrónica

A continuación, se describe el propósito de cada zona y por qué debe estar presente en las soluciones de sede electrónica que adquieran o desarrollen las autoridades.

- (a) **Presentación y estilo:** Las arquitecturas de solución de las sedes electrónicas deben contar con componentes que permitan adaptar la presentación y estilo de las sedes electrónicas a los estilos definidos para la integración al Portal Único del Estado colombiano - GOV.CO.
- (b) **Seguridad:** las arquitecturas de solución deben poseer los componentes que permitan la autorización, autenticación, cifrado de datos, estampado cronológico y firmas electrónicas que garanticen la seguridad (integridad, control de acceso, no repudio, entre otros) de todas las funcionalidades y servicios que ofrece la sede electrónica; estas herramientas deberán ser provistas por entidades acreditadas y habilitadas por la normativa vigente para su expedición. En la zona de seguridad, también deben

existir conectores para la integración del servicio ciudadano digital de Autenticación Digital, cuando esté disponible.

- (c) Gestión documental electrónica: Todas las sedes electrónicas deben estar integradas con el sistema de gestión electrónica de documentos de archivo (sistemas de gestión documental), de acuerdo con los lineamientos que en la materia establezca el Archivo General de la Nación, a fin de realizar la gestión integral de los documentos por medios digitales y las autoridades serán las responsables de gestionar los documentos e información electrónica resultante de la ejecución de los trámites, Otros Procedimientos Administrativos y consulta de acceso a información pública y asegurar su adecuado tratamiento archivístico, garantizando como mínimo: el tratamiento de: documentos electrónicos, expedientes electrónicos, metadatos y asegurando los criterios de autenticidad, fiabilidad, integridad y disponibilidad.

Todos los formularios que estén asociados a una solicitud de trámite, Otro Procedimiento Administrativo o consulta de acceso a información pública deben hacer parte del expediente electrónico.

Para los documentos que son producto de una cadena de trámites y que para su producción requieren intervención de diferentes entidades. La conformación del expediente electrónico, de su tratamiento archivístico y su preservación debe estar a cargo de la entidad líder. La sede electrónica debe implementar procedimientos de preservación a largo plazo de los documentos electrónicos.

Las autoridades serán las responsables de gestionar los documentos e información resultante de la ejecución de los trámites, Otros Procedimientos Administrativos y consulta de acceso a información pública a través de sus sedes electrónicas y/o ventanillas únicas digitales asegurando su adecuado tratamiento archivístico. Para la gestión de la documentación electrónica, la entidad debe seguir los lineamientos establecidos por el Archivo General de la Nación, garantizando la autenticidad, integridad, fiabilidad y usabilidad de los documentos durante el tiempo que se requieran.

La sede electrónica deberá disponer los servicios de registro de documentos electrónicos para la recepción y remisión de peticiones, escritos y documentos. Los sistemas de información que soportan la sede electrónica deberán garantizar la disponibilidad e integridad de la información y la correcta gestión documental electrónica, en los términos de la Ley 594 de 2000 y sus decretos reglamentarios, en los distintos procedimientos y trámites electrónicos. Asimismo, deberán:

1. Admitir documentos electrónicos correspondientes a los servicios, procedimientos y trámites que se especifiquen, los cuales podrán ser aportados por el ciudadano utilizando los servicios de la sede electrónica u otros medios electrónicos. Los documentos se podrán presentar todos los días del año durante las veinticuatro horas.

2. Disponer en la sede electrónica la relación actualizada de las peticiones, escritos y documentos recibidos incluyendo la fecha y hora de recepción.

3. Asignar un número consecutivo a las comunicaciones recibidas o producidas, dejando constancia de la fecha y hora de recibo o de envío, con el propósito de oficializar el trámite y cumplir con los términos de vencimiento que establezca la ley y hacer seguimiento a todas las actuaciones recibidas y enviadas.

4. Enviar automáticamente por el mismo medio un mensaje acusando el recibo y registro de las peticiones, escritos o documentos de que se trate, en el que constarán los datos proporcionados por los ciudadanos, la fecha y hora de presentación y el número consecutivo de radicación asignado.

5. Recibir los documentos anexos a la correspondiente solicitud, mensaje o comunicación. El registro electrónico generará mensajes que acrediten la entrega de estos documentos.

6. Distribuir electrónicamente en los términos que establezca la entidad para cada trámite, los documentos registrados al destinatario o destinatarios o entidad responsable de atender el trámite correspondiente.

7. Utilizar formatos o formularios preestablecidos para la presentación de documentos electrónicos normalizados, correspondientes a los servicios y trámites que se especifiquen en el sistema.

8. Incorporar el calendario oficial de la entidad con fecha y hora, los días hábiles y los declarados inhábiles.

9. Posibilitar la interconexión de todas las dependencias de la entidad para el acceso a la información por medios electrónicos.

10. Establecer un esquema de interoperabilidad entre los diferentes sistemas o soluciones utilizados por las entidades públicas para atender de manera adecuada y oportuna los trámites, otros

procedimientos administrativos y consultas de acceso a información pública.

- (d) Canales de acceso: La arquitectura de solución de las sedes electrónicas debe habilitar los componentes que permitan a los usuarios internos y externos acceder a la oferta de servicios dispuesta por la autoridad a través de cualquier dispositivo móvil o computador personal.
- (e) Zona transaccional: La arquitectura de solución debe contar con componentes que permitan realizar transacciones como trámites, Otros Procedimientos Administrativos y consulta de acceso a información pública y otras acciones de participación ciudadana que tenga a disposición la entidad a través de su sede electrónica.
- (f) Administrador de contenidos: La arquitectura de solución de la sede electrónica debe contar con un administrador de contenidos que permitan la creación y administración de la información que se publica allí.
- (g) Datos y persistencia. La arquitectura de solución de la sede electrónica debe poseer componentes que permitan almacenar y gestionar los datos estructurados, semiestructurados y no estructurados, así como los metadatos asociados a estos.
- (h) Analítica: La arquitectura de la sede electrónica debe poseer componentes que permitan a las autoridades generar capacidades para realizar agregación de datos transaccionales, *big data*, analítica de datos de uso, analítica de gestión y operación de la infraestructura que soporta la sede electrónica, entre otras, con el fin de optimizar la toma de decisiones basadas en datos y la mejora continua de la sede.
- (i) Auditoría: La arquitectura de solución de la sede electrónica debe poseer componentes de auditoría que permitan realizar la trazabilidad de las acciones y eventos que se realicen, mediante la gestión de logs para la correlación de los eventos que se generen dentro de la sede electrónica.
- (j) Gestión de procesos: La arquitectura de solución de la sede electrónica debe contar con componentes que permitan la gestión automática y optimización de los procesos de negocio que soportan los trámites, Otros Procedimientos Administrativos y consulta de acceso a información pública ofrecidos allí.
- (k) Interoperabilidad interna: Todas las sedes electrónicas deben poseer componentes que permitan realizar intercambio de información seguro y confiable entre los sistemas de información que posea la entidad,

garantizando la autenticidad, integridad y fiabilidad de la información y los documentos electrónicos

(l) Interoperabilidad externa: Todas las sedes electrónicas deben poseer componentes que permitan realizar intercambio de información, datos o documentos de manera segura con otras autoridades, empresas privadas u otros organismos, con el objeto de dinamizar y optimizar los trámites, Otros Procedimientos Administrativos y consulta de acceso a información pública de las autoridades. Lo anterior siguiendo los lineamientos que sobre la materia emita MinTIC para la vinculación al servicio de interoperabilidad de los Servicios Ciudadanos Digitales, garantizando la autenticidad, integridad y fiabilidad de los documentos electrónicos.

(m) Notificaciones: Todas las sedes electrónicas deben poseer componentes que permitan la gestión de las notificaciones de manera digital, los cuales puede incluir: servicios de correo electrónico, mensajes de texto, notificaciones en aplicaciones específicas, notificaciones en el gestor documental, entre otros, siguiendo las normas procesales de notificación electrónica. Así mismo, la sede electrónica debe poseer el componente que permita vincular la comunicación de la notificación con el servicio ciudadano de Carpeta Ciudadana Digital, Lo anterior siguiendo los lineamientos que sobre la materia emita MinTIC para la vinculación al servicio de Carpeta Ciudadana Digital de los Servicios Ciudadanos Digitales.

(n) Integración con los Servicios Ciudadanos Digitales: Los Trámites, Otros Procedimientos Administrativos y consulta de acceso a información pública que ofrezca una sede electrónica deben realizar la vinculación a los Servicios Ciudadanos, siguiendo los lineamientos que sobre la materia emita MinTIC y atendiendo los siguientes requisitos:

- I. Vincular a los Trámites, Otros Procedimientos Administrativos y consulta de acceso a información pública que se integren a la sede electrónica, los mecanismos de autenticación digital según el nivel de garantía requerido.
- II. Disponer de un mecanismo de roles y autorizaciones que permita aprobar o denegar el acceso a los recursos de la sede electrónica para el usuario autenticado desde el servicio de autenticación digital.
- III. Identificar la información de interés de los usuarios que custodia la entidad y que debe ser vinculada a la Carpeta Ciudadana Digital desde la sede electrónica.
- IV. Disponer de mecanismos para informar al ciudadano a través de la Carpeta Ciudadana Digital el estado o avance de los trámites, Otros

- Procedimientos Administrativos y consulta de acceso a información pública o solicitudes realizadas en la sede electrónica.
- V. Identificar los trámites, Otros Procedimientos Administrativos y consulta de acceso a información pública que emiten alertas o comunicaciones para ser informada a los usuarios en la Carpeta Ciudadana Digital
 - VI. Configurar, habilitar y exponer los servicios de intercambio de información que permitan, a través del servicio de Interoperabilidad, enviar la información identificada en el literal III de este apartado a la Carpeta Ciudadana Digital.
 - VII. Contar en la sede electrónica con mecanismos que permitan a los usuarios desde la Carpeta Ciudadana Digital informar sobre la actualización y/o corrección de sus datos, y acceder a las comunicaciones oficiales.
 - VIII. La sede electrónica debe garantizar la gestión de la disponibilidad asegurando que la infraestructura, los procesos, las herramientas y las funciones de TI sean adecuados para cumplir con los objetivos de disponibilidad propuestos para los Servicios Ciudadanos Digitales.

La sede electrónica de cada una de las autoridades debe ser estructurada a partir de la arquitectura de referencia planteada y la autoridad responsable de esta debe asumir los costos que implique evolucionar hacia esta arquitectura de referencia objetivo.

4.3. Atributos de calidad de la sede electrónica

Los siguientes son los atributos de calidad a tener en cuenta desde los aspectos legales, procedimentales, organizacionales y técnicos, a fin de garantizar el cumplimiento de los niveles establecidos para cada uno de ellos. Se entiende por calidad el conjunto de características de un producto o servicio que satisface las necesidades de sus grupos de interés y es conforme a las especificaciones de diseño.

El conjunto de atributos de calidad que debe acreditar la sede electrónica de las autoridades en materia de accesibilidad, usabilidad, seguridad, disponibilidad, neutralidad e interoperabilidad, adicionales a las dispuestas en la Ley 1712 del 2014 y en la Resolución MinTIC 1519 del 2020, son las que se describen a continuación.

4.3.1. Usabilidad

Las sedes electrónicas deben asegurar como mínimo los siguientes criterios en el diseño de la interfaz de usuario:

- (a) Todas las sedes deben poseer un mapa del sitio, al cual pueden acceder los usuarios a través de un enlace en la barra inferior (*footer*), el cual debe estar actualizado con los cambios en la estructura de la sede cuando estos ocurran. El mapa del sitio debe facilitar la búsqueda y accesibilidad a los contenidos o temáticas incluidas en la sede.
- (b) El mapa del sitio debe estar en formato XML para que sea visible a los motores de búsqueda, de forma que se facilite la accesibilidad.
- (c) Todas las sedes electrónicas deben cumplir con los elementos de diseño gráfico, definidos en la Anexo 2.1 Guía de Diseño gráfico para sedes electrónicas. Las entidades de la rama ejecutiva del orden nacional deberán aplicar adicionalmente las disposiciones de la Directiva Presidencial 03 de 2019.
- (d) La sede electrónica debe mantener el diseño ordenado y limpio; el contraste de brillo y color; la justificación y ancho del cuerpo de los textos y las fuentes tipográficas uniformes; énfasis en títulos y/o encabezados; uso adecuado de espacios en blanco; vínculo a la página de inicio, y miga de pan, de manera que cumpla con el Anexo 2.1 Guía de Diseño gráfico para sedes electrónicas. Las entidades de la rama ejecutiva del orden nacional deberán aplicar adicionalmente las disposiciones de la Directiva Presidencial 03 de 2019.
- (e) La sede electrónica debe transmitir de forma clara y efectiva la información sobre sus contenidos utilizando un lenguaje claro. Lo anterior, adoptando la guía de lenguaje claro para servidores públicos de Colombia disponible en: <https://www.dnp.gov.co/programa-nacional-del-servicio-al-ciudadano/Paginas/Lenguaje-Claro.aspx>
- (f) La sede electrónica en casos excepcionales puede habilitar el desplazamiento horizontal, sin embargo, este no es recomendado.
- (g) La sede electrónica debe controlar el aspecto mediante la implementación de hojas de estilos (CSS) que permitan separar los contenidos de su presentación.
- (h) La sede electrónica debe permitir destacar los vínculos visitados para orientar al usuario sobre cuáles contenidos ha consultado con anterioridad.
- (i) La sede electrónica debe ser implementada con independencia y neutralidad al navegador con el cual se accede.
- (j) La autoridad responsable de la sede electrónica debe asegurar la calidad del código de tal manera que no existan tags y/o vínculos rotos.
- (k) La sede electrónica debe incorporar en los formularios de captura de información ejemplos que de forma sencilla y clara orienten al usuario en el formato a utilizar en el diligenciamiento. Una vez los formularios sean

diligenciados, deben incorporarse como documento electrónico¹ al expediente electrónico que le corresponda.

- (l) La sede electrónica debe tener etiquetados los campos de captura de los formularios, permitiendo visualizar la información que está digitando en cada uno de ellos.
- (m) La sede electrónica debe controlar el uso de ventanas emergentes que interrumpan o interfieran la navegación, y que puedan ser interpretadas como publicidad o afectaciones a la seguridad de la sede.
- (n) La sede electrónica debe realizar un adecuado control del tiempo de carga de los contenidos de las páginas, evitando dar la impresión de que no están disponibles o que presentan errores.
- (o) La sede electrónica debe proporcionar mensajes de confirmación cuando se requieran sobre las acciones que el usuario realice.
- (p) La sede electrónica debe ofrecer un buscador interno que permita al usuario encontrar su información y contenido.
- (q) La sede electrónica debe incorporar tecnología *responsive* de tal forma que los contenidos puedan ser visualizados adecuadamente en dispositivos móviles.
- (r) La sede electrónica debe permitir una encuesta que permita evaluar su usabilidad.

4.3.2. Accesibilidad

La sede electrónica deberá cumplir con el estándar AA de la W3C (WCAG – *Web Content Accessibility Guidelines*) disponibles en <https://www.w3c.es/estandares/> de conformidad con las Directrices de Accesibilidad Web dispuestas en el Anexo 1 de la Resolución MinTIC 1519 del 2020, y adoptar los siguientes como mínimo:

- (a) Los contenidos de la sede electrónica deben poder ser leídos a través de herramientas para lectura magnificada o lector de pantalla que faciliten el acceso a los contenidos por parte de las personas con discapacidad visual. El MinTIC pondrá a disposición de las autoridades un software que facilite la lectura de sitios web de los sujetos obligados. Las licencias de uso se extenderán en forma gratuita para uso de las entidades de nivel nacional, territorial, y organismos autónomos.
- (b) Barra de accesibilidad: Se debe contar con una barra de accesibilidad visible, en la que se pueda modificar el contraste, reducir o aumentar la letra, y la opción de cambiar idioma.

¹ Se entenderá por documento electrónico de acuerdo con lo establecido en la Ley 594 de 2000 y el decreto que la reglamenta, Decreto 2609 de 2012.

- (c) Disponer de un enlace de accesibilidad ubicado en el *footer* del home principal, en el que se deberán indicar las medidas adoptadas por los sujetos obligados para el cumplimiento de las disposiciones de accesibilidad.
- (d) Adecuar los contenidos audiovisuales de sus sitios web bajo los siguientes requerimientos: Subtítulos o *Closed Caption*. En el plazo que determine las Directrices de Accesibilidad del MinTIC, todos los sujetos obligados deberán incluir en el 100% de los contenidos audiovisuales (vídeos) nuevos los subtítulos incorporados o el texto escondido (*closed caption*) auto activable por los usuarios. Esta disposición no aplica para transmisiones en vivo y en directo.
- (e) Alternativas de texto: Para cualquier contenido que no sea texto de forma que pueda ser interpretado del modo que precisen otras personas, tal como tamaño de letra extragrande, texto hablado, lenguaje de signos o un lenguaje más sencillo.
- (f) Contenido alternativo al audio o video: Alternativas para cualquier información presentada exclusivamente a través de audio o vídeo. En el desarrollo web, ciertos contenidos como las imágenes o los vídeos disponen de la posibilidad de incluir texto alternativo.
- (g) Adaptable: Crear contenidos en los que se puedan establecer tamaños de fuente, imágenes, botones, entre otros, para que los usuarios puedan configurar fácilmente el tamaño de letra con el que se sienten más cómodos para la lectura, con características *responsive* las cuales se adopten a cualquier dispositivo electrónico.
- (h) Distinguible: Facilitar los contenidos para que los usuarios puedan disfrutarlos a través de su visualización o escucha. Se debe evitar el uso de tamaños de fuente reducidos o el uso de texto en gris sobre fondos blancos, dado que estos dificultan la lectura por parte de ciertas personas.
- (i) Accesible mediante el teclado: Implementar las distintas funcionalidades para que se pueda acceder a ellas desde un teclado. Por ejemplo, los formularios pueden estar preparados para poder saltar de campo a campo mediante la tecla de tabulación, lo que hace más fácil su diligenciamiento.
- (j) Suficiente tiempo: En los contenidos que tengan tiempo de lectura controlado por *timer*, tipo *banners* desplegable u otros, establecer tiempos razonables para que los usuarios puedan leer o usar adecuadamente el contenido.
- (k) Evite efectos *flash* que puedan ocasionar ataques a quien los visualice: no diseñar contenidos de tal forma que pueda ocasionar ataques, especialmente por el uso de ciertos contrastes de color en asociación con efectos de *flash* y parpadeo rápido de las imágenes.
- (l) Navegabilidad: Ofrecer formas de ayudar a sus usuarios a navegar, encontrar el contenido y determinar dónde están dentro de su sitio web. Use URL semánticos, mapas del sitio, y otros recursos que faciliten la navegación de los usuarios.

- (m) Legibilidad: Contenido de texto legible y fácilmente comprensible para los usuarios. Aspectos como el contraste y la posibilidad de variar el tamaño de las fuentes de letra, favorecen la legibilidad de los textos. Estos cambios se pueden presentar, siempre y cuando no afecte la autenticidad, integridad y fiabilidad del documento electrónico.
- (n) Predictibilidad: Las páginas web deben aparecer y funcionar de una forma predecible por sus usuarios. Use las convenciones establecidas en su página de inicio también en todas las secciones y páginas internas.
- (o) Facilite la entrada de datos: Ayude a sus usuarios a evitar y corregir los errores que puedan cometer al interactuar con su página web, rellenar formularios y seleccionar una opción. También hay funcionalidades que pueden ayudar a los usuarios autor rellenado los formularios cuando se detecta que los valores que esperan ciertos campos ya están disponibles en la memoria del navegador.
- (p) Etiqueta para elementos de texto y gráficos (*Title* y *Alt*): Los portales específicos de programas transversales del Estado deberán brindar en su contenido, bien sea, botones, enlaces, imágenes, videos y/o textos una etiqueta (*label*) con su respectiva descripción.

4.3.3. Seguridad

Las autoridades deben contar con medidas preventivas y reactivas, sistemas tecnológicos, entre otros, que garanticen la integridad, disponibilidad y autenticidad de los datos, documentos e información dispuesta en la sede, para ello deberán cumplir, además de las dispuestas en la Resolución MinTIC 1519 del 2020, los siguientes requisitos:

- (a) Implementar un certificado SSL con validación de organización, para garantizar comunicaciones seguras del Protocolo de Transferencia de Hipertexto (HTTP), proporcionando privacidad, integridad y autenticidad entre el usuario y la entidad; es importante tener en cuenta, que existen diversos tipos de certificados SSL, los cuales se clasifican y se deben aplicar en virtud del riesgo que se pretende mitigar; esta herramienta deberá ser provista por entidades acreditadas y habilitadas por la normativa vigente para su expedición.
- (b) Realizar configuraciones de seguridad adicionales a las configuraciones por defecto de los equipos, realizando afinamiento de seguridad (*hardening*), en la infraestructura tecnológica de la sede electrónica (sistemas operativos, servidor web, base de datos) y mantener actualizado el software, *frameworks* y *plugins* utilizados por la sede.
- (c) Restringir la escritura de archivos en el servidor web a través de la asignación de permisos de solo lectura.
- (d) Implementar sistemas antivirus sobre la infraestructura que soporta la sede electrónica, para evitar infecciones de *malware* a sus archivos.

- (e) Deshabilitar en la comunicación HTTP los métodos peligrosos como PUT, DELETE, TRACE.
- (f) Para la administración remota de la infraestructura tecnológica que hace parte de la sede electrónica, se deben establecer canales y protocolos para el control de acceso y administración, por ejemplo, VPN.
- (g) Habilitar las cabeceras de seguridad para el envío de información entre el navegador y el servidor web, entre otras: (*Content-Security-Policy (CSP)*, *X-Content-Type-Options*, *X-Frame-Options*, *X-XSS-Protection*, *Strict-Transport-Security (HSTS)*: *Public-Key-Pins (HPKP)* *Referrer-Policy*, *Feature-Policy*, para cookies habilitar *secure* y *HttpOnly*
- (h) Aplicar técnicas de sanitización de parámetros de entrada mediante la eliminación de etiquetas, saltos de línea, espacios en blanco y otros caracteres especiales que comúnmente conforman un «script».
- (i) Realizar sanitización de caracteres especiales (secuencia de escape de variables en el código de programación).
- (j) Habilitar mecanismos de autenticación, mediante la generación de contraseñas robustas y solicitar renovaciones periódicas de estas contraseñas; así como implementar mecanismos de captcha, para los trámites, Otros Procedimientos Administrativos y consulta de acceso a información pública que se dispongan a través de la sede y que de acuerdo con el análisis de riesgos así lo requieran.
Nota: se debe tener en cuenta que en el momento que el Servicio de Autenticación Digital de los Servicios Ciudadanos Digitales esté disponible, los mecanismos de registro y autenticación de la sede electrónica deben vincularse en las condiciones que el ministerio disponga.
- (k) Para el acceso a Trámites, Otros Procedimientos Administrativos y consulta de acceso a información pública u otras acciones de tipo transaccional en la sede electrónica, se recomienda la implementación de token de sesión personal o el control que se considere más adecuado para evitar *Cross Site Reference Forgery* CSRF o XSRF.
- (l) Implementar mensajes de error genéricos que no revelen información acerca de la tecnología usada, excepciones o parámetros que dispararon el error específico.
- (m) Establecer los planes de contingencia, recuperación ante desastres (DRP) de acuerdo al análisis del Impacto del Negocio (BIA) y alineado al Plan de continuidad del negocio (BCP) de la entidad, que permita garantizar la disponibilidad de la sede electrónica y los servicios que a través de ella se expongan 7/24, los 365 días del año.
- (n) Los componentes de la arquitectura de solución que soportan la sede electrónica deben estar actualizados a la última versión soportada, que incluye las mejoras de seguridad liberadas por el fabricante en atención al plan de actualización de la entidad y los riesgos de seguridad identificados.
- (o) Publicar en la sede electrónica la política de datos personales y su aviso de privacidad con el fin de dar cumplimiento de la Ley 1581 de 2012.

- (p) Exigir medidas de seguridad al proveedor del hosting (políticas de seguridad informática y acciones prácticas de ciberseguridad) y exigir el cumplimiento de las políticas internas de seguridad de la información de la entidad.
- (q) Proteger el código fuente de la aplicación que dificulte realizar procedimientos de ingeniería inversa (*reversing*) para analizar la lógica de la aplicación.
- (r) Definir e implementar políticas y procedimientos para la generación de copias de seguridad de los componentes de la arquitectura de solución que soportan la sede electrónica.
- (s) Se deben implementar monitoreos de seguridad sobre la infraestructura tecnológica que soporta la sede electrónica (escaneo de vulnerabilidades, escaneo de archivos infectados, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios) y realizar las acciones de mitigación correspondientes.
- (t) Implementar las políticas de seguridad en los equipos de seguridad perimetral (firewall), de conformidad con el Modelo de Seguridad y Privacidad de la Información (MSPI).
- (u) Adoptar las buenas prácticas que ofrece la guía para construir aplicaciones y servicios web seguros de OWASP.
- (v) Reportar los incidentes cibernéticos graves o muy graves, conforme con los criterios de su sistema de gestión de seguridad digital y seguridad de la información, de manera oportuna al CSIRT-Gobierno o al ColCERT del Ministerio de Defensa Nacional, de acuerdo con los procedimientos establecidos para tal fin.
- (w) Implementar un sistema de control de versiones, que permita planear y controlar el ciclo de vida de las aplicaciones que soportan la sede electrónica, y, en una fase a mediano plazo, poder implementar un sistema de integración, cambio y despliegue continuo.
- (x) Controlar el escalamiento de privilegios en los sistemas operativos, servidor web, base de datos y demás elementos que hacen parte de la arquitectura de solución que soporta la sede electrónica.
- (y) La entidad debe realizar la identificación de activos y gestión de riesgos de seguridad de la infraestructura tecnológica que soporta la sede electrónica de acuerdo con lo establecido en el Modelo de Seguridad y Privacidad de la Información (MSPI) y la Guía para la administración del riesgo y el diseño de controles.
- (z) La inclusión de pasarelas de pago deberá cumplir los lineamientos definidos por la Superintendencia Financiera sobre el particular) Gov.co
- (aa) Cuando las autoridades deban cumplir normas de seguridad digital especiales dictadas por otras autoridades de su sector, los lineamientos definidos en este documento deberán ser implementados de manera armónica con aquellas disposiciones. Lo anterior, además de los controles suficientes y adecuados dispuestos por la autoridad a partir del análisis de riesgos y controles que ésta determine.

4.3.4. Neutralidad

La sede electrónica debe ser implementada con independencia de los navegadores para computadores personales y dispositivos móviles utilizados por el usuario para no afectar su experiencia y debe operar en al menos tres (3) de los navegadores más utilizados.

4.3.5. Interoperabilidad

- (a) Todos los componentes de la arquitectura de solución de la sede electrónica que requieran intercambiar información deben aplicar el marco de interoperabilidad de la política de gobierno digital en cada uno de sus dominios para atender dichas necesidades.
- (b) Todos los formularios de captura de información dispuestos en la sede electrónica deben estar normalizados de acuerdo con el Estándar de Lenguaje Común de Intercambio. Cuando los formularios sean diligenciados por los usuarios, estos deben hacer parte del trámite, OPA o consulta de acceso a información pública y conformar el expediente electrónico.
- (c) Los trámites, Otros Procedimientos Administrativos y consulta de acceso a información pública que requieran intercambiar datos, documentos, información, deberán realizar la estandarización de los conjuntos de datos a intercambiar aplicando el lenguaje común de intercambio de información del Estado colombiano.
- (d) La sede electrónica debe configurar, habilitar y exponer a través del servicio ciudadano de interoperabilidad (la herramienta X-ROAD) los servicios de intercambio de información (para consumo y exposición) que faciliten la interoperabilidad con otras autoridades.
- (e) La sede electrónica para el intercambio de información debe vincularse a la plataforma de interoperabilidad y registrar el servidor de X-ROAD ante el articulador de los servicios ciudadanos digitales.
- (f) Para los trámites, Otros Procedimientos Administrativos y consulta de acceso a información pública que se integran a la sede electrónica, la entidad debe incluir los mecanismos de interoperabilidad necesarios que permitan hacer más ágiles y eficientes los trámites, Otros Procedimientos administrativos y consulta de acceso a información pública, evitando solicitar información a ciudadanos y empresas que puede ser consultada u obtenida a través de otra autoridad del Estado.
- (g) La sede electrónica debe disponer de las herramientas e infraestructura suficientes y adecuadas que apoyen la disponibilidad y cobertura del servicio de interoperabilidad. Los requerimientos mínimos para la

integración al servicio de Interoperabilidad se describen en la “Guía Despliegue Servidor de Seguridad Plataforma de Interoperabilidad”.

4.3.6. Calidad de información

La calidad de la información dispuesta en la sede electrónica debe cumplir con los principios definidos en el artículo 3 de la Ley 1712 de 2014, así como lo dispuesto en la Resolución MinTIC 1519 del 2020, y las siguientes características:

- (a) Actualizada: la información dispuesta en las sedes electrónicas debe estar actualizada con el propósito de no brindar datos errados a los grupos de interés.
- (b) Escrita en lenguaje claro: toda la información publicada en las sedes electrónicas debe estar escrita en lenguaje claro de acuerdo con la guía del Departamento Nacional de Planeación y las demás que apliquen.
- (c) Veraz: la información publicada en las sedes electrónicas debe ser correcta y fidedigna.
- (d) Reutilizable y procesable: la información publicada en las sedes electrónicas a través de archivos debe disponerse en formatos que permitan su libre uso; reutilización bajo licencia abierta, sin restricciones legales de aprovechamiento, y disponibilidad bajo formatos de datos abiertos (CSV, XML, RDF, RSS, JSON, ODF, WMS, WFS, entre otros).
- (e) Oportuna: la información dispuesta en las sedes electrónicas debe ser publicada de manera oportuna, de tal forma que pueda ser consultada en el momento en que necesita utilizar.
- (f) Objetiva: La información dispuesta en las sedes electrónicas no debe ser independiente de prejuicios e intereses personales, políticos o religiosos.
- (g) Completa: la información disponible en las sedes electrónicas debe ser completa no parcial.
- (h) Disponible en formatos accesibles: La información disponible en las sedes electrónicas, debe estar dispuesta según en formatos que puedan ser leídos o interpretados fácilmente por software o tecnologías disponibles

Para el cumplimiento de las anteriores características se deberá tener en cuenta los procedimientos de gestión documental de la respectiva entidad y

los lineamientos del Archivo General de la Nación cuando la información presentada por la sede se constituya como un documento electrónico.

4.3.7. Disponibilidad

La autoridad determinará el nivel de disponibilidad mensual de la sede electrónica, el cual debe ser igual o superior al 98%, en concordancia con el análisis de criticidad de los trámites, Otros Procedimientos Administrativos y consulta de acceso a información pública ofrecidos. Así mismo, se asegurará que la información se encuentre disponible para su posterior consulta, para ello se deben implementar los procedimientos de preservación documental dispuestos en las normas de gestión documental definidas por el Archivo General de la Nación.

4.3.8. Infraestructura tecnológica

- (a) Se podrá acceder a la sede electrónica a través del direccionamiento a una IP pública IPv4 e IPv6, de acuerdo con la Resolución 2710 de 2017, o la norma que la sustituya.
- (b) La infraestructura tecnológica de la sede electrónica debe contar con un servicio DNS con resolución de doble pila.
- (c) Se recomienda que la infraestructura tecnológica que soporta la sede electrónica se encuentre en un ambiente de nube y no local (*on-premise*).

4.4. Lineamientos de ventanillas únicas digitales

4.4.1. Contenido y estructura de información de las ventanillas únicas digitales

Las autoridades responsables de las ventanillas únicas para la información y gestión de cadenas de trámites entre dos o varias entidades, deberán dar cumplimiento a lo siguiente:

4.4.1.1. Requisitos mínimos

- (a) Diseño gráfico. Cada Ventanilla Única Digital podrá disponer de un diseño gráfico, marca y experiencia diferenciada de la sede electrónica de la entidad responsable, de acuerdo con lo definido en el Anexo 3.1 de diseño gráfico de ventanillas únicas digitales. Las entidades de la rama ejecutiva del orden nacional deberán aplicar asimismo lo dispuesto en la Directiva Presidencial 03 de 2019.
- (b) *Header*: Acondicionar una barra superior completa con acceso al Portal Único del Estado colombiano - GOV.CO, que estará ubicada arriba de la pantalla, transversal a todas sus vistas. La barra de GOV.CO contendrá su logotipo el cual deberá dirigir al sitio web www.GOV.CO, texto descriptivo modificable y enlaces que establezca los lineamientos del Portal Único del Estado colombiano - GOV.CO.
- (c) *Footer*: Las autoridades deberán incluir una barra inferior (*footer*), que estará ubicada en el pie de página de su sede electrónica, para lo cual utilizará el diseño y la paleta de colores referido en los lineamientos para acondicionamiento gráfico de la sede electrónica al Portal Único del Estado colombiano - GOV.CO. Esta barra inferior contendrá los siguientes datos:
 - I. Imagen del Portal Único del Estado colombiano y el logo de la marca país CO - Colombia.
 - II. Nombre de la entidad, dirección, código postal incluyendo el departamento (si aplica) y municipio o distrito.
 - III. Vínculos a las redes sociales para ser redireccionado en los botones respectivos.
 - IV. Datos de contacto, incluyendo lo siguiente: teléfono conmutador; línea gratuita o línea de servicio a la ciudadanía/usuario de la Ventanilla Única Digital; línea anticorrupción: correo institucional para la atención

al público: correo de notificaciones judiciales: enlace para el mapa del sitio, y un enlace para vincular políticas como las siguientes: términos y condiciones, privacidad y derechos de autor. Todas las líneas telefónicas deberán incluir el prefijo del país +57 y el número significativo nacional (indicativo nacional) que determine la Comisión de Regulación de Comunicaciones, excepto en las líneas gratuitas 018000 y 019000.

(d) Contenidos mínimos: Los siguientes son los contenidos mínimos con los que debe contar una Ventanilla Única Digital:

- I. Contenidos e información: todo contenido o información de la Ventanilla Única Digital debe estar relacionado con su finalidad. No se deben incluir marcas o referencias que no estén estrictamente relacionadas con las entidades participantes, ni con el propósito de la Ventanilla.
- II. Información acerca de la Ventanilla Única Digital: describirá el propósito de la Ventanilla, el público al que está dirigido y la entidad responsable.
- III. Entidades participantes de la Ventanilla Única Digital: indicar los logos de las entidades participantes e identificar claramente el logo de la entidad responsable.
- IV. Noticias: publicará las noticias más relevantes para la ciudadanía y los grupos de valor. Así mismo, deberá publicar el contenido de toda decisión y/o política que haya adoptado y afecte o beneficie al público, junto con sus fundamentos y toda interpretación de la autoridad sobre ella. La información deberá publicarse conforme con las pautas o lineamientos en materia de lenguaje claro, accesibilidad y usabilidad.
- V. Ayuda: la Ventanilla Única Digital deberá crear una sección de ayuda que incorpore preguntas y respuestas que permitan un adecuado entendimiento de los usuarios frente al servicio prestado para facilitar la gestión de la cadena de trámites.
- VI. Servicios a la Ciudadanía: Este menú debe permitir acceder a la información y contenidos relacionados con la gestión de trámites, otros procedimientos administrativos, información de contacto y formulario PQRS, así:
 1. Trámites, Otros Procedimientos Administrativos y consulta de acceso a información pública. Se deberá indicar claramente el tipo de trámite, Otro Procedimiento Administrativo y consulta de acceso a información pública indicando lo siguiente:
 - a) Nombre de la cadena trámite, OPA o consulta de acceso a información pública.

b) Información general, procedimiento y plazos de la cadena de trámites (plazo total de la cadena de trámite, y plazos específicos de gestión del trámite en cada entidad).

c) Entidades responsables de cada trámite que hace parte de la cadena.

Para la gestión digital de la cadena de trámites, se deberá disponer de mecanismos de registro y autenticación para que los usuarios puedan realizar sus procedimientos en línea o digitales, con la debida confianza, seguridad, trazabilidad, calidad y protección de los datos personales.

A través del mecanismo de registro, el usuario recibirá el radicado y podrá consultar el estado de su trámite, plazo de respuesta e, incluso, podrá descargar documentación asociada a los mismos. Todas las entidades involucradas o responsables de la cadena de trámite deberán actualizar en tiempo real su estado, para que al usuario se le informe su situación real con independencia de las responsabilidades de las entidades participantes en la gestión del trámite.

De conformidad con la Directiva Presidencial 02 del 2019 o aquella que la modifique o subrogue, las autoridades de la rama ejecutiva del orden nacional deberán observar los requerimientos de la Guía de Integración de Trámites, Otros Procedimientos Administrativos y consulta de acceso a información pública al Portal Único del Estado Gov.co.

Nota: se debe tener en cuenta que en el momento que la Carpeta Ciudadana Digital y la Autenticación Digital de los Servicios Ciudadanos Digitales estén disponibles, los mecanismos de registro y autenticación para los usuarios, la consulta del estado del trámite y la descarga de la documentación asociada deben ser vinculados a estos servicios en las condiciones que el ministerio disponga.

2. Canales de Atención: la entidad publicará el listado completo de canales de atención presenciales (si aplica), telefónicos (si aplica) y digitales, estableciendo claramente los horarios de atención (si aplica) y demás indicaciones que estime pertinentes para sus usuarios. Los diversos canales digitales oficiales dispuestos por cada autoridad deberán estar integrados a la sede electrónica.
3. PQRS: En este menú deberá habilitarse el mecanismo para el registro, radicación, envío y seguimiento de PQRS, relacionado con la presentación, tratamiento y respuesta de las mismas (incluyendo las peticiones presentadas verbalmente), de conformidad con lo establecido en la Ley 1437 de 2011, la ley 1755

de 2015, el decreto 1166 de 2016 y en la Resolución 1519 del 2020 del MinTIC, o aquellas normas que las modifiquen o sustituyan

Se dispondrá de un formulario único de PQRSD que la entidad responsable gestionará y en caso de que no sea de su competencia, realizará los traslados que considere pertinente. En el menú se deberá activar un mecanismo para consultar el estado en la respuesta de la PQRSD radicada. En todo caso deberá indicarse el tiempo máximo de respuesta, conforme a lo dispuesto en la ley. En caso de que la PQRSD haya sido trasladada a la entidad competente, se deberá indicar la fecha en la que se trasladó y el nombre de la entidad a la que se remitió.

4.4.2 Cumplimiento de políticas

Las entidades deberán incorporar en una sección, a la que se acceda por la barra inferior o *footer*, la documentación asociada al cumplimiento de las siguientes políticas:

4.4.2.1. Términos y condiciones

Las autoridades deberán aprobar y publicar los términos y condiciones para el uso de todos sus portales web; plataformas; aplicaciones; trámites y servicios; servicios de pasarela de pago; consulta de acceso a información pública; entre otros. Como mínimo deberán incluir lo siguiente: condiciones, alcances y límites en el uso; derechos y deberes de los usuarios; alcance y límites de la responsabilidad; contacto para asuntos relacionados con los términos y condiciones; referencia a la política de privacidad y tratamiento de datos personales, y de seguridad.

En los casos en los que se cuente con trámites en línea o parcialmente en línea, otros procedimientos administrativos y/o consulta de acceso a información pública, la autoridad deberá habilitar una opción que le permita al usuario la aceptación de los Términos y condiciones.

4.4.2.2. Política de privacidad y tratamiento de datos personales

Las autoridades deberán definir, aprobar y publicar su política de privacidad y tratamiento de datos personales, conforme a las disposiciones de la Ley 1581 del 2012, y la Ley 1712 de 2014 y demás instrucciones o disposiciones relacionadas, o aquellas que las modifiquen, adicionen o deroguen.

En los casos en los que se cuente con trámites en línea o parcialmente en línea, otros procedimientos administrativos en línea o parcialmente en línea y/o

consulta de acceso a información pública, la autoridad deberá habilitar una opción que le permita al usuario la aceptación de la política de privacidad y tratamiento de datos personales.

4.4.3 Arquitectura de referencia para ventanillas únicas digitales

La arquitectura de referencia de una Ventanilla Única Digital es la misma definida para la sede electrónica, la cual se encuentra definida en el numeral 4.2

4.4.4 Atributos de calidad de la ventanilla única digital

Los atributos de calidad que deben ser asegurados en las Ventanillas Únicas son los mismos que los definidos para la sede electrónica en el numeral 4.3

4.5. Lineamientos para portales de programas transversales

4.5.1. Contenido y estructura de información de portales de programas transversales

Las autoridades que cuenten con portales de programas transversales del Estado con contenidos, información o servicios dirigidos a públicos específicos, o que cuenten con una identidad temática, que se presten para la ciudadanía o para las entidades de gobierno, deberán observar los siguientes requisitos:

4.5.2. Requisitos mínimos para los portales de programas transversales del estado

Para crear un portal de programa transversal del Estado, se requiere el cumplimiento de los siguientes requisitos mínimos:

- (a) Verificar que el portal de programa transversal del Estado involucre información, recursos u oferta institucional de un programa o iniciativa del Estado, con impacto nacional, que involucre a más de una autoridad.
- (b) Determinar la entidad líder que será responsable del portal transversal del Estado; a su cargo estará el cumplimiento del presente lineamiento y normas que le sean aplicables.
- (c) La entidad líder será responsable por la gestión documental, tratamiento de datos personales, gestión de PQRS (incluyendo el traslado cuando aplique) y la administración del sitio. La recepción de PQRS, debe realizarse contemplando lo establecido por el Archivo General de la Nación -AGN en el Acuerdo 060 del 2001.
- (d) La entidad responsable deberá solicitar al MinTIC la integración del portal del programa transversal del Estado al Portal Único del Estado colombiano - GOV.CO.
- (e) Cumplir los lineamientos técnicos para publicar los contenidos en el portal del programa transversal del Estado.
- (f) Los portales de programas transversales del Estado deben crearse a partir de una URL con nombre de dominio (DNS): GOV.CO.
- (g) Los portales específicos de programas transversales del Estado que se creen con posterioridad a la publicación de este documento deberán

desde su creación estar integrados a la sede electrónica de la autoridad responsable de dicho portal y al portal único del Estado colombiano GOV.CO.

4.5.3. Requisitos mínimos de contenidos

- (a) Aviso de portal de programa transversal: En un lugar visible deberá indicarse que los contenidos, información o servicios hacen parte de un portal transversal bajo coordinación de la entidad. Así mismo, se deberá indicar al usuario que en caso de que desee realizar una gestión o comunicarse con la entidad deberá dirigirse a la sede electrónica.

A continuación, se sugiere el siguiente texto de ejemplo:

“Usted ha ingresado al Portal de Datos Abiertos (ejemplo), portal transversal del Gobierno Nacional para promover los datos abiertos coordinado por MinTIC. Si desea realizar un trámite, Otro Procedimiento Administrativo o consulta de acceso a información pública, una gestión o comunicarse con la entidad, por favor dirigirse a la sede electrónica de MinTIC (o de la entidad) en el enlace www.mintic.gov.co (o de la entidad)”.

- (b) Diseño gráfico: Cada portal transversal podrá disponer de un diseño gráfico, marca y experiencia diferenciada de la sede electrónica de la entidad responsable.

- (c) *Header*: Acondicionar una barra superior completo con acceso al Portal Único del Estado colombiano - GOV.CO, que estará ubicada en la parte superior, transversal a todas sus vistas. La barra de GOV.CO contendrá su logotipo, el cual deberá dirigir al sitio web <https://www.gov.co>, texto descriptivo modificable y enlaces que establezca los lineamientos del Portal Único del Estado colombiano - GOV.CO.

- (d) *Footer*: Las autoridades deberán incluir una barra inferior (*footer*) que estará ubicada en el pie de página de su sede electrónica, para lo cual utilizará el diseño y la paleta de colores referido en los lineamientos para acondicionamiento gráfico de sitios web al Portal Único del estado colombiano - GOV.CO. Esta barra inferior contendrá los siguientes datos:
- I. Imagen del Portal Único del Estado Colombiano y el logo de la marca país CO - Colombia.
 - II. Nombre de la entidad, dirección, código postal incluyendo el departamento (si aplica) y municipio o distrito.

III. Vínculos a las redes sociales para ser redireccionados en los botones respectivos.

IV. Datos de contacto, incluyendo lo siguiente: teléfono conmutador; línea gratuita o línea de servicio a la ciudadanía/usuario; línea anticorrupción; correo institucional para atención al público; correo de notificaciones judiciales; enlace para el mapa del sitio, y un enlace para vincular a las políticas como: términos y condiciones, privacidad y derechos de autor. Todas las líneas telefónicas deberán incluir el prefijo de país +57, y el número significativo nacional (indicativo nacional) que determine la Comisión de Regulación de Comunicaciones, excepto en las líneas gratuitas 018000 y 019000.

En los casos en los que la autoridad tenga más de una dirección física de atención a la ciudadanía podrá colocar la información correspondiente de hasta 3 locaciones diferentes.

En los casos en los que la autoridad requiera incluir información de otras dependencias o de un número superior a 3 direcciones físicas deberá incluir el nombre correspondiente de las dependencias o sedes físicas de atención a la ciudadanía con el respectivo hipervínculo, de manera que, al picar sobre estos nombres, se redirija al usuario al Directorio de contactos de la autoridad.

(h) Contenidos mínimos: Los siguientes son los contenidos mínimos con los que debe contar un portal específico de un programa transversal del Estado, los cuales deberán estar en el menú principal, de manera que el usuario pueda acceder a ellos desde todas las páginas:

- Información acerca del programa: Describirá el propósito del programa, el público al que está dirigido y la entidad responsable.
- Noticias: Publicará las noticias más relevantes para la ciudadanía y los grupos de valor que estén relacionadas con el programa transversal. La información deberá publicarse conforme a las pautas o lineamientos en materia de lenguaje claro, accesibilidad y usabilidad.
- Contenidos e información: Todo contenido o información del portal de programa transversal del Estado debe estar relacionado con su finalidad. No se deben incluir contenidos, publicidad, marcas o referencias que no estén estrictamente relacionadas con el objeto del portal.
- Ayuda: El portal del programa transversal del Estado deberá crear una sección de ayuda que incorpore preguntas y respuestas que permitan un adecuado entendimiento de los usuarios frente al servicio prestado.

- Servicios a la Ciudadanía: El portal del programa transversal debe contar con un acceso que direcciona a los canales de atención al ciudadano en la sede electrónica de la autoridad responsable.

4.5.4. Cumplimiento de políticas legales

Las autoridades deberán incorporar en una sección a la que se acceda por la barra inferior o *footer*, la documentación asociada al cumplimiento de las siguientes políticas:

4.5.4.1. Términos y condiciones

Las autoridades deberán aprobar y publicar los términos y condiciones para el uso de todos sus portales web; plataformas; aplicaciones; trámites, Otros Procedimientos Administrativos, consulta de acceso a información pública; servicios de pasarela de pago; entre otros. Como mínimo deberán incluir lo siguiente: condiciones, alcances y límites en el uso; derechos y deberes de los usuarios; alcance y límites de la responsabilidad; contacto para asuntos relacionados con los términos y condiciones, y referencia a las políticas de privacidad y tratamiento de datos personales, seguridad y de derechos de autor.

4.5.4.2. Política de privacidad y tratamiento de datos personales

Todas las autoridades deberán aprobar y publicar su política de privacidad y tratamiento de datos personales, conforme a las disposiciones de la Ley 1581 del 2012 y la Ley 1712 de 2014 y demás instrucciones o disposiciones relacionadas, o aquellas que las modifiquen, adicionen o deroguen.

4.5.4.3. Política de derechos de autor y/o autorización de uso sobre los contenidos

Las autoridades deberán aprobar y publicar su política de derechos de autor y/o autorización de uso de los datos y contenidos, en la cual deberán incluir el alcance y limitaciones relacionados con el uso de datos, documentos, información, contenidos y códigos fuente producidos por la autoridad.

4.5.5. Arquitectura de referencia para portales de programas transversales

- (a) Los Portales de Programas Transversales del Estado deberán ser estructurados utilizando la siguiente arquitectura de referencia, que define unas zonas genéricas:

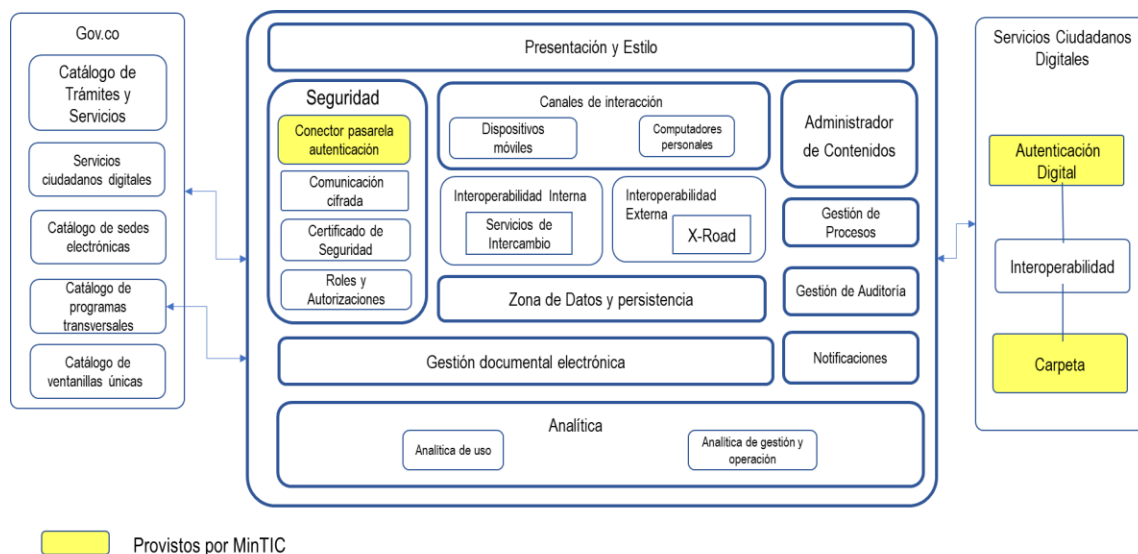


Figura 2. Arquitectura de referencia de un portal de programa transversal

- (b) El componente de roles y autorizaciones aplica obligatoriamente, solo si existen funcionalidades en el portal del programa transversal que requieran realizar autenticación para ofrecer acceso, registro y/u otras funcionalidades relacionadas
- (c) En caso de que exista un trámite, Otro procedimiento administrativo o consulta de acceso a información pública vinculado a un portal de un programa transversal se deberá direccionar al trámite total o parcialmente en línea, o al Otro procedimiento administrativo total o parcialmente en línea o consulta de acceso a información pública.
- (d) Los componentes de gestión documental electrónica, gestión de procesos, gestión de auditoría y notificaciones deberán estar presentes si existen funcionalidades que lo requieran.

4.5.6 Atributos de calidad de los portales de programas transversales

Los siguientes son los atributos de calidad a tener en cuenta desde los aspectos legales, procedimentales, organizacionales y técnicos, a fin de

garantizar el cumplimiento de los niveles establecidos para cada uno de ellos. Se entiende por calidad, el conjunto de características de un producto o servicio que satisface las necesidades de sus grupos de interés y es conforme a las especificaciones de diseño.

El conjunto de atributos de calidad que debe acreditar un portal de programas transversales de las autoridades en materia de accesibilidad, usabilidad, seguridad, disponibilidad, neutralidad e interoperabilidad, adicionales a las dispuestas en la Ley 1712 del 2014 y en la Resolución MinTIC 1519 del 2020, son las que se describen a continuación:

4.5.6.1. Usabilidad

Los portales deben asegurar como mínimo los siguientes criterios en el diseño de la interfaz de usuario:

- (a) Deben poseer un mapa del sitio, al cual los usuarios pueden acceder a través de un enlace en la barra inferior (*footer*), el cual debe estar actualizado con los cambios en la estructura de la sede, cuando estos ocurran. El mapa del sitio debe facilitar la búsqueda y accesibilidad a sus contenidos o temáticas.
- (b) El mapa del sitio debe estar en formato XML para que sea visible a los motores de búsqueda, de forma que se facilite la accesibilidad.
- (c) Todos los portales deben cumplir con los elementos de diseño gráfico definidos en el Anexo 4.1 Guía de diseño gráfico para portales específicos de programas transversales del Estado. Las autoridades de la rama ejecutiva del orden nacional deberán cumplir adicionalmente lo dispuesto en la Directiva Presidencial 03 de 2019.
- (d) Los portales deben mantener el diseño ordenado y limpio; el contraste de brillo y color; la justificación y ancho del cuerpo de los textos, y las fuentes tipográficas uniformes; el énfasis en títulos y/o encabezados; uso adecuado de espacios en blanco; el vínculo a la página de inicio, y la miga de pan, de manera que cumpla con lo señalado en el Anexo 4.1 Guía de diseño gráfico para portales específicos de programas transversales del Estado y, en los casos de las entidades de la rama ejecutiva del orden nacional, con lo señalado en la Directiva Presidencial 03 de 2019.
- (e) Los portales deben transmitir de forma clara y efectiva la información sobre sus contenidos utilizando un lenguaje claro. Lo anterior adoptando la guía de lenguaje claro para servidores públicos de Colombia disponible en: <https://www.dnp.gov.co/programa-nacional-del-servicio-al-ciudadano/Paginas/Lenguaje-Claro.aspx> o las demás que apliquen.
- (f) Los portales en casos excepcionales pueden habilitar el desplazamiento horizontal, sin embargo, este no es recomendado.

- (g) Los portales deben controlar el aspecto mediante la implementación de hojas de estilos (CSS) que permitan separar los contenidos de su presentación.
- (h) Los portales deben permitir destacar los vínculos visitados para orientar al usuario sobre cuáles contenidos ha consultado con anterioridad.
- (i) Los portales deben ser implementados con independencia y neutralidad al navegador con el cual se accede.
- (j) La autoridad responsable del portal debe asegurar la calidad del código de tal manera que no existan tags y/o vínculos rotos.
- (k) Los portales deben etiquetar los campos de los formularios que capturan datos, permitiendo conocer la información que digita en cada uno de ellos facilitando una lectura rápida y un ingreso ágil de la información.
- (l) Los portales deben controlar el uso de ventanas emergentes que interrumpen o interfieran la navegación, y que puedan ser interpretadas como publicidad o afectaciones a la seguridad de la sede.
- (m) Los portales deben realizar un adecuado control del tiempo de carga de los contenidos de las páginas, evitando dar la impresión de que no están disponibles o que presentan errores.
- (n) Los portales deben incorporar en los formularios de captura de información ejemplos que, de forma sencilla y clara, orienten al usuario en el formato a utilizar en el diligenciamiento.
- (o) Los portales deben proporcionar mensajes de confirmación a todas las acciones que el usuario realice.
- (p) Los portales deben ofrecer páginas personalizadas para el manejo del error 404, con el fin de ofrecer una mejor experiencia de usuario.
- (q) Los portales deben ofrecer un buscador interno que permita al usuario encontrar la información y contenido de la sede.
- (r) Los portales deben incorporar tecnología *responsive* de tal forma que los contenidos puedan ser visualizados adecuadamente en dispositivos móviles.
- (s) Los portales deben permitir una encuesta que permita evaluar su usabilidad.

4.5.6.2. Accesibilidad

La sede electrónica debe cumplir con el estándar AA de la W3C (WCAG – Web Content Accessibility Guidelines), de conformidad con la Directriz de Accesibilidad Web incorporadas en el Anexo 1 de la Resolución MinTIC 1519 del 2020, y adoptar los siguientes como mínimo:

- (a) Los contenidos de la sede electrónica deben poder ser leídos a través de herramientas para lectura magnificada o lector de pantalla que faciliten el acceso a los contenidos por parte de las personas con

- discapacidad visual. El MinTIC pondrá a disposición de las autoridades un software que facilite la lectura de sitios web de los sujetos obligados. Las licencias de uso se extenderán en forma gratuita para uso de las entidades de nivel nacional, territorial, y organismos autónomos.
- (b) Barra de accesibilidad: contar con una barra de accesibilidad visible, en la que se pueda modificar el contraste, reducir o aumentar la letra, y la opción de cambiar idioma.
 - (c) Disponer de un enlace de accesibilidad ubicado en el *footer* del home principal, en el que se deberán indicar las medidas adoptadas por los sujetos obligados para el cumplimiento de las disposiciones de accesibilidad.
 - (d) Adecuar los contenidos audiovisuales de sus sitios web bajo los siguientes requerimientos: Subtítulos o *Closed Caption*. En el plazo que determine las Directrices de Accesibilidad del MinTIC, todos los sujetos obligados deberán incluir en el 100% de los contenidos audiovisuales (vídeos) nuevos los subtítulos incorporados o el texto escondido (*closed caption*) auto activable por los usuarios. Esta disposición no aplica para transmisiones en vivo y en directo.
 - (e) Alternativas de texto: para cualquier contenido que no sea texto de forma que pueda ser interpretado del modo que precisen otras personas, tal como tamaño de letra extragrande, texto hablado, lenguaje de signos o un lenguaje más sencillo.
 - (f) Contenido alternativo al audio o video: alternativas para cualquier información presentada exclusivamente a través de audio o vídeo. En el desarrollo web, ciertos contenidos como las imágenes o los vídeos disponen de la posibilidad de incluir texto alternativo.
 - (g) Adaptable: crear contenidos en los que se puedan establecer tamaños de fuente, imágenes, botones, entre otros, para que los usuarios puedan configurar fácilmente el tamaño de letra con el que se sienten más cómodos para la lectura, con características *responsive* las cuales se adopten a cualquier dispositivo electrónico.
 - (h) Distinguible: facilitar los contenidos para que los usuarios puedan disfrutarlos a través de su visualización o escucha. Se debe evitar el uso de tamaños de fuente reducidos o el uso de texto en gris sobre fondos blancos, dado que estos dificultan la lectura por parte de ciertas personas.
 - (i) Accesible mediante el teclado: implementar las distintas funcionalidades para que se pueda acceder a ellas desde un teclado. Por ejemplo, los formularios pueden estar preparados para poder saltar de campo a campo mediante la tecla de tabulación, lo que hace más fácil su diligenciamiento.
 - (j) Suficiente tiempo: en los contenidos que tengan tiempo de lectura controlado por *timer*, tipo *banners* desplegables u otros, establecer tiempos razonables para que los usuarios puedan leer o usar adecuadamente el contenido.

- (k) Evite efectos *flash* que puedan ocasionar ataques a quien los visualice: no diseñar contenidos de tal forma que pueda ocasionar ataques, especialmente por el uso de ciertos contrastes de color en asociación con efectos de flash y parpadeo rápido de las imágenes.
- (l) Navegabilidad: ofrecer formas de ayudar a sus usuarios a navegar, encontrar el contenido y determinar dónde están dentro de su sitio web. Use URL semánticos, mapas del sitio, y otros recursos que faciliten la navegación de los usuarios.
- (m) Legibilidad: contenido de texto legible y fácilmente comprensible para los usuarios. Aspectos como el contraste y la posibilidad de variar el tamaño de las fuentes de letra, favorecen la legibilidad de los textos. Estos cambios se pueden presentar, siempre y cuando no afecte la autenticidad, integridad y fiabilidad del documento electrónico.
- (n) Predictibilidad: las páginas web deben aparecer y funcionar de una forma predecible por sus usuarios. Use las convenciones establecidas en su página de inicio también en todas las secciones y páginas internas.
- (o) Facilite la entrada de datos: ayude a sus usuarios a evitar y corregir los errores que puedan cometer al interactuar con su página web, rellenar formularios y seleccionar una opción. También hay funcionalidades que pueden ayudar a los usuarios autor rellenado los formularios cuando se detecta que los valores que esperan ciertos campos ya están disponibles en la memoria del navegador.
- (p) Etiqueta para elementos de texto y gráficos (*Title* y *Alt*): Los portales específicos de programas transversales del Estado deberán brindar en su contenido, bien sea, botones, enlaces, imágenes, videos y/o textos una etiqueta (*label*) con su respectiva descripción.

5.6.3. Seguridad

Las autoridades deben contar con medidas preventivas y reactivas, sistemas tecnológicos, entre otros, que garanticen la confidencialidad, la integridad y autenticidad de los datos, documentos y de la información dispuestos en los Portales de Programas Transversales, para ello deberá cumplir, además de lo dispuesto en la Resolución MinTIC 1519 del 2020, los siguientes requisitos:

- (a) Implementar un certificado *SSL* con validación de organización, para garantizar comunicaciones seguras del Protocolo de transferencia de hipertexto (*HTTP*), proporcionando privacidad, integridad y autenticidad entre el usuario y la entidad.
- (b) Realizar la configuración de seguridad adicionando un *WAF* (*Web Aplicación Firewall*).
- (c) Realizar configuraciones de seguridad adicionales a las configuraciones por defecto de los equipos, realizando afinamiento de seguridad (*hardening*) en la infraestructura tecnológica que soporta el portal del programa transversal (sistemas operativos, servidor web, base de datos)

- y mantener actualizados el software, *frameworks* y *plugins* utilizados por la sede.
- (d) Restringir la escritura de archivos en el servidor web a través de la asignación de permisos de solo lectura.
- (e) Implementar sistemas antivirus sobre la infraestructura que soporta el portal del programa transversal, para evitar infecciones de *malware* a los archivos del mismo.
- (f) Deshabilitar en la comunicación HTTP los métodos peligrosos como PUT, DELETE, TRACE.
- (g) Para la administración remota de la infraestructura tecnológica que soporta el portal transversal, se deben establecer canales y protocolos para el control de acceso y administración, por ejemplo, VPN.
- (h) Habilitar las cabeceras de seguridad para el envío de información entre el navegador y el servidor web, entre otras: (*Content-Security-Policy* (CSP), *X-Content-Type-Options*, *X-Frame-Options*, *X-XSS-Protection*, *Strict-Transport-Security* (HSTS): *Public-Key-Pins* (HPKP) *Referrer-Policy*, *Feature-Policy*, para *cookies* habilitar *secure* y *HttpOnly*
- (i) Aplicar técnicas de sanitización de parámetros de entrada mediante la eliminación de etiquetas, saltos de línea, espacios en blanco y otros caracteres especiales que comúnmente conforman un «script».
- (j) Realizar sanitización de caracteres especiales (secuencia de escape de variables en el código de programación).
- (k) Habilitar mecanismos de autenticación, mediante la generación de contraseñas robustas y solicitar su renovación periódica; así como implementar mecanismos de captcha, cuando se requiera disponer, a través del portal, de funcionalidades que requieran este tipo de mecanismos. *Nota: se debe tener en cuenta que en el momento que la Autenticación Digital de los Servicios Ciudadanos Digitales esté disponible, los mecanismos de registro y autenticación del portal deben vincularse en las condiciones que el ministerio disponga.*
- (l) Implementar mensajes de error genéricos que no revelen información acerca de la tecnología usada, excepciones o parámetros que dispararon el error específico.
- (m) Establecer los planes de contingencia, recuperación ante desastres (DRP) de acuerdo con el análisis del Impacto del Negocio (BIA) y alineado al Plan de continuidad del negocio (BCP) de la autoridad, que permita garantizar la disponibilidad del portal del programa transversal 7/24, los 365 días del año.
- (n) Los componentes de la arquitectura de solución que soportan el portal transversal deben estar actualizados a la última versión soportada, incluyendo las mejoras de seguridad liberadas por el fabricante en atención al plan de actualización de la entidad y los riesgos de seguridad identificados.
- (o) Publicar en el portal del programa transversal la política de datos personales y su aviso de privacidad con el fin de dar cumplimiento a la Ley 1581 de 2012.

- (p) Exigir medidas de seguridad al proveedor del hosting (políticas de seguridad informática y acciones prácticas de ciberseguridad) y exigir el cumplimiento de las políticas internas de seguridad de la información de la entidad.
- (q) Proteger el código fuente de la aplicación que dificulte realizar procedimientos de ingeniería inversa (*reversing*) para analizar la lógica de la aplicación.
- (r) Definir e implementar políticas y procedimientos para la generación de copias de seguridad de los componentes de la arquitectura de solución que soportan el portal del programa transversal.
- (s) Se deben implementar monitoreos de seguridad sobre la infraestructura tecnológica que soporta el portal transversal (escaneo de vulnerabilidades, escaneo de archivos infectados, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios) y realizar las acciones de mitigación correspondientes.
- (t) Implementar las políticas de seguridad en los equipos de seguridad perimetral (firewall), de conformidad con el Modelo de Seguridad y Privacidad de la Información (MSPI).
- (u) Adoptar las buenas prácticas que ofrece la guía para construir aplicaciones y servicios web seguros de OWASP.
- (v) Reportar los incidentes cibernéticos graves o muy graves, conforme con los criterios de su sistema de gestión de seguridad digital y seguridad de la información, de manera oportuna al CSIRT-Gobierno o al ColCERT del Ministerio de Defensa Nacional, de acuerdo con los procedimientos establecidos para tal fin.
- (w) Implementar un sistema de control de versiones, que permitan planear y controlar la vida de las aplicaciones, y en una fase a mediano plazo poder implementar un sistema de integración, cambio y despliegue continuo.
- (x) Controlar el escalamiento de privilegios en los sistemas operativos, servidor web, base de datos y demás elementos que hacen parte de la arquitectura de solución que soporta el portal del programa transversal.
- (y) La entidad debe realizar la identificación de activos y gestión de riesgos de seguridad de la infraestructura tecnológica que soporta el portal del programa transversal de acuerdo con lo establecido en el Modelo de Seguridad y Privacidad de la Información MSPI y la Guía para la administración del riesgo y el diseño de controles.

4.5.6.4. Neutralidad

El portal del programa transversal debe ser implementado con independencia de los navegadores para computadores personales y dispositivos móviles utilizados por el usuario para no afectar su experiencia y debe operar en al menos tres (3) de los navegadores más utilizados.

4.5.6.5. Interoperabilidad

- (a) Todos los componentes de la arquitectura de solución del portal del programa transversal que requieran intercambiar información deben aplicar el marco de interoperabilidad en cada uno de sus dominios para atender dichas necesidades.
- (b) Todos los formularios de captura de información dispuestos o que se dispongan en el portal del programa transversal deben estar normalizados de acuerdo con el Estándar de Lenguaje Común de Intercambio (lenguaje.mintic.gov.co)
- (c) Cuando el portal requiera o posea funcionalidades para intercambiar información, datos o documentos, se debe realizar la estandarización de los conjuntos de datos a intercambiar, aplicando el lenguaje común de intercambio de información del Estado colombiano.
- (d) El portal del programa transversal para el intercambio de información debe vincularse a la plataforma de interoperabilidad y registrar el servidor de X-ROAD ante el articulador de los Servicios Ciudadanos Digitales. Los requerimientos mínimos para la integración al servicio de Interoperabilidad se describen en la “Guía Despliegue Servidor de Seguridad Plataforma de Interoperabilidad”.

4.5.6.6. Calidad de información

La calidad de la información dispuesta en el portal del programa transversal debe cumplir, adicionales a las dispuestas en la Ley 1712 del 2014 y en la Resolución MinTIC 1519 del 2020, con las siguientes características:

- (a) Actualizada: la información dispuesta en los portales de programas transversales debe estar actualizada con el propósito de no brindar información errada a los grupos de interés que acceden a él.
- (b) Escrita en lenguaje claro: toda la información publicada en los portales de programas transversales debe estar escrita en lenguaje claro, de acuerdo con la guía del Departamento Nacional de Planeación.
- (c) Veraz: la información publicada en los portales de programas transversales debe ser correcta y fidedigna.
- (d) Publicación en formatos abiertos: la información publicada en los portales de programas transversales a través de archivos debe disponerse en formatos que permitan su libre uso; reutilización bajo licencia abierta, sin restricciones legales de aprovechamiento, y disponibles bajo formatos de datos abiertos (CSV, XML, RDF, RSS, JSON, ODF, WMS, WFS, entre otros).

- (e) Oportuna: la información dispuesta en los portales transversales debe ser publicada de manera oportuna, de tal forma que pueda ser consultada en el momento en que necesita utilizar.
- (f) Objetiva: La información dispuesta en los portales transversales no debe ser independiente de prejuicios e intereses personales, políticos o religiosos.
- (g) Completa: la información disponible en los portales transversales debe ser completa no parcial.
- (h) Disponible en formatos accesibles: La información disponible en los portales de programas transversales, debe estar dispuesta según en formatos que puedan ser leídos o interpretados fácilmente por software o tecnologías disponibles.
- (i) La información producida, gestionada y difundida por los portales trasversales deberá cumplir con las anteriores características para los solicitantes e interesados en ella, teniendo en cuenta los procedimientos de gestión documental de la respectiva entidad y los lineamientos del Archivo General de la Nación cuando la información presentada por la sede se constituya como un documento electrónico.

4.5.6.7. Disponibilidad

La autoridad determinará el nivel de disponibilidad mensual del portal de programas transversales, el cual debe ser igual o superior al 98%, en concordancia con el análisis de criticidad de los servicios, trámites, Otros Procedimientos Administrativos y consulta de acceso a información pública ofrecidos.

4.5.6.8. Infraestructura tecnológica

- (a) Se podrá acceder al portal del programa transversal a través del direccionamiento a una IP pública IPv4 e IPv6, de acuerdo con la Resolución 2710 de 2017.
- (b) La infraestructura tecnológica del portal del programa transversal debe contar con un servicio DNS con resolución de doble pila.
- (c) Se recomienda que la infraestructura tecnológica que soporta el portal del programa transversal se encuentre en un ambiente de nube y no local (*on-premise*).

4.5.6.9 Condiciones de creación

Un portal transversal se define como un sitio en Internet que integra información, recursos u oferta institucional de un programa o iniciativa del Estado, con impacto nacional y que involucra más de una autoridad. Por tanto, si no cumple con las condiciones anteriores no podrá ser creado y la información

deberá estar disponible en la sede electrónica según corresponda, esto con el fin de evitar la proliferación de portales.