LINEAMIENTOS PARA ESTANDARIZAR LAS VENTANILLAS ÚNICAS, PORTALES DE PROGRAMAS TRANSVERSALES Y UNIFICACIÓN DE SEDES ELECTRÓNICAS DEL ESTADO COLOMBIANO

Tabla de contenido

LINEAMIENTOS PARA VENTANILLAS ÚNICAS, PORTALES DE PROGRAMAS TRANSVERSALES Y UNIFICACIÓN DE SEDES ELECTRÓNICAS DEL ESTADO COLOMBIANO

1. ALCANCE Y AMBITO DE APLICACIÓN

Esta guía establece los conceptos y lineamientos generales de las sedes electrónicas, ventanillas únicas y los portales de programas transversales en aplicación a lo señalado en los artículos 60 de la Ley 1437 de 2011, 14 y 15 del Decreto 2106 del 22 de noviembre de 2019.

Por lo tanto, la presente guía aplica a todas las autoridades, entendidas como los organismos, entidades y personas integrantes de la Administración Pública que están señalados en el artículo 2 del Decreto 2106 de 2019, en el artículo 2.2.9.1.1.2 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 y en particular el Titulo 9, Capítulo 1, sección 1, y del artículo 2 de la Ley 1437 de 2011.

2. DEFINICIONES

Accesibilidad web: Condiciones y características de 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.
Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
Incidente de Seguridad: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa 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.
Sede electrónica: Es el sitio oficial en internet de cada autoridad, al que se accede a través de una dirección electrónica donde se dispone información, trámites, servicios y demás elementos ofertados por la autoridad y cuya titularidad, administración y gestión le corresponde.
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 permite verificar los atributos digitales de una persona cuando adelanten trámites y servicios a través de medios digitales mediante el cual se tiene certeza sobre la persona, o cuando exista certeza de la persona a la que se atribuya el documento o lo ha firmado, permite vincular su identidad a la autoría de estos.
Servicio de carpeta ciudadana digital: Es el servicio que le permite a los usuarios de los servicios ciudadanos digitales, acceder digitalmente de manera segura, confiable y actualizada al conjunto de sus datos, que tienen o custodian las entidades del Estado.
Servicio de Interoperabilidad: Servicio que brinda las capacidades necesarias para garantizar el adecuado flujo de información e interacción entre los sistemas de información de las entidades, permitiendo intercambiar, integrar y compartir 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, usuario 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 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 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 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 elementos 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".

Como parte de la estrategia para avanzar en la transformación digital del Estado, durante el año 2019 se expidió la Directiva No. 02 de abril de 2019 mediante la que se crea el Portal Único del Estado colombiano, como "único punto de acceso digital del ciudadano con los trámites, servicios, información pública, ejercicios de participación, colaboración y control social, que ofrecen las autoridades de la rama ejecutiva del orden 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 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 y al Ministerio de Tecnologías de la Información y las Comunicaciones 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.

4. LINEAMIENTOS DE LA SEDE ELECTRÓNICA

La sede electrónica debe integrar todos portales institucionales, sitios web, plataformas, ventanillas únicas, aplicaciones y soluciones existentes, que permitan la realización de trámites, procesos y procedimientos a los ciudadanos de acuerdo con lo establecido en el artículo 14 el Decreto 2106 de 2019.

A continuación, se listan cada uno de los elementos 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 traducirlos a otros idiomas o lenguas siempre que dichas traducciones cumplan la Ley

1712 de 2014, entre otros, el principio de calidad de 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 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 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.

(d) Las autoridades deberán adoptar medidas de conservación preventiva 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 el efecto, deberán adoptar un programa de gestión documental digital, conforme lo dispone el artículo 15 de la Ley 1712 de 2014 y el Decreto 2609 del 2012, o el que lo 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.

(f) No se debe incluir contenidos, publicidad, marcas o referencias que no estén estrictamente relacionadas con el cumplimientode las funciones de la autoridad.

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

4.1.2. 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.

4.1.3. MENÚ PRINCIPAL

Habilitar como mínimo es en la parte superior o encabezado de la sede electrónica 4 menús: 1. Menú de Transparencia y acceso a la información. 2. Normativa. 3. Trámites y 4. Contáctenos.

Además de estos 4 menús mínimos obligatorios, las autoridades podrán habilitar en la parte superior otros menús de acuerdo a su preferencia, sus necesidades y su caracterización de usuarios.

El orden de los 4 menús mínimos obligatorios en la parte superior o encabezado de la sede electrónica será determinado por cada autoridad.

Los 4 menús mínimos obligatorios deberán contener los siguientes lineamientos:

4.1.4. Menú transparencia y acceso a la información pública

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

(b) Toda la información, documentos o datos deben ser publicados en forma cronológica del más reciente al más antiguo.

(c) Los contenidos e información dispuestos para los usuarios deberán ser accesibles y usables conforme las disposiciones del presente lineamiento, y utilizar un lenguaje claro.

(d) 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.

(e) Toda la información debe ser publicada en formatos que permitan: su descarga, acceso sin restricciones legales, para su uso libre, procesable por máquina y que permitan realizar búsquedas en su interior.

(f) Todo documento o información debe indicar la fecha de su publicación en la sede electrónica.

(g) 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 MINTIC 3564 del 2015 o la que la modifique, adicione o desarrolle.

Nota: La información sobre normativa y trámites, debe redirigir a los respectivos menús conforme los lineamientos referidos en los numerales 4.1.5 y 4.16.

4.1.5. Menú normativa:

Este menú permitirá el acceso a las normas correspondientes a la autoridad, de acuerdo con los siguientes lineamientos:

(a) Toda la normativa debe ser publicada en formatos que permitan: su descarga, acceso sin restricciones legales, para su uso libre, procesable por máquina y que permitan realizar búsquedas en su interior.
(b) 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, enlace para su consulta.

De otro lado, las autoridades deben incluir los siguientes contenidos:

(a) Normativa de la autoridad: En esta sección la autoridad deberá publicar leyes, decreto único reglamentario (si aplica), normativa aplicable, resoluciones, actos administrativos, ordenanzas, acuerdos, decretos, circulares, vínculo al diario o gaceta oficial.

(b) Búsqueda de normas: Esta sección deberá permitir la búsqueda de normas bajo el Sistema Único de Información Normativa – SUIN, del Ministerio de Justicia, y el sistema de búsquedas de normas propio de la autoridad.

(c) Proyectos normativos para comentarios: En esta sección se encontrarán los proyectos normativos para participación de la ciudadanía y de otros interesados, posibilidad de comentar los proyectos, publicación a la respuesta a comentarios, y mecanismo de participación que adopte el Sistema Único de Consulta Pública – SUCOP, del Departamento Nacional de Planeación.

4.1.6. Menú de trámites

Este menú debe permitir acceder a la información y contenidos relacionados con la gestión de trámites, procesos y procedimientos administrativos, así como a 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: las autoridades deberán habilitar un buscador de trámites o procedimientos. El acceso a información de trámites también podrá realizarse por medio de categorías que asocien a grupos temáticos, de forma que se facilite la navegación y búsqueda por parte de los usuarios

(b) Para habilitar el acceso a los trámites totalmente en línea y parcialmente en línea, las autoridades deberán:

(I) Disponer la información completa del trámite, pudiendo direccionarlo 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/TXXXXX, donde XXXXX corresponde al código trámite asignado en el Departamento Administrativo de la Función Pública en el Sistema Único de Información de Trámites (SUIT)

(II) Direccionar al trámite en línea o parcialmente en línea.

(c) En cada trámite deberá indicar si el procedimiento puede realizarse totalmente en línea, parcialmente en línea o presencial; además, informar si el trámite tiene asociado un costo o es gratuito; e indicar el tiempo de resolución del mismo.

(d) Las autoridades deberán disponer de mecanismos de consulta del estado del trámite, registro y autenticación para que los usuarios puedan realizar sus trámites o procedimientos digitales, con la debida confianza, seguridad, trazabilidad, calidad y protección de los datos personales. Lo anterior de conformidad a lo establecido en la política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones.

(e) Cada autoridad deberá disponer en este menú un acceso a las ventanillas únicas digitales de las cuales es responsable. Asimismo, podrá incluir en su respectiva sede electrónica el acceso a las ventanillas únicas las que hace parte activa en la cadena de trámites que la conforman.

(f) En los casos en que haya un redireccionamiento desde la sede electrónica hacia una página externa a la sede electrónica, la autoridad deberá informar al usuario mediante un aviso lo siguiente:

> "Usted está punto de ingresar al sitio web de la Ventanilla Única Digital (NOMBRE) que es responsabilidad de (NOMBRE ENTIDAD RESPONSABLE)" Cualquier solicitud deberá dirigirla a (NOMBRE ENTIDAD RESPONSABLE)" .

4.1.7. Menú de contáctenos

Para identificar y dar a conocer los canales digitales oficiales de recepción de solicitudes, peticiones y de información de conformidad con el artículo 14 del Decreto 2106 de 2019, las autoridades deberán incluir en su respectiva sede electrónica un Menú de Contáctenos que contenga 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.

En este menú deberá habilitarse el mecanismo para el registro, envío y seguimiento de PQRS de conformidad con lo establecido en Ley 1437 de 2011 y la Resolución 3564 de 2015, o aquellas normas que las modifiquen o sustituyan.

4.1.8. SECCIÓN NOTICIAS

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

4.1.9. 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, ésta deberá habilitar en su respectiva sede electrónica el acceso a dichos portales. Las autoridades involucradas en los programas transversales del Estado podrán habilitar en su respectiva sede electrónica el acceso a dichos portales.

4.1.10 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 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, 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.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 link para vincular a las políticas que 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.

4.1.11. CUMPLIMIENTO DE POLÍTICAS

Las entidades deberán incorporar un enlace en la barra inferior (foooter), que direccione a la siguiente información:

4.1.12. Términos y condiciones.

Las autoridades deberán aprobar y publicar los términos y condiciones para el uso de todos sus portales web, plataformas, aplicaciones, servicios de trámites y servicios, servicios de pasarela de pago, servicios de consulta de información, 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.

4.1.13. 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 las disposiciones de la Ley 1581 del 2012, y la Circular Externa Conjunta 04 entre la Agencia Nacional

de Defensa Jurídica del Estado y la Superintendencia de Industria y Comercio, y demás instrucciones o disposiciones relacionadas, o aquellas que las modifiquen, adicionen o deroguen.

4.1.14. 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 el cual, deberán incluir el alcance y limitaciones relacionados con el uso de datos, información, contenidos, 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 utilizan esta plataforma.

La adecuación de 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 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:

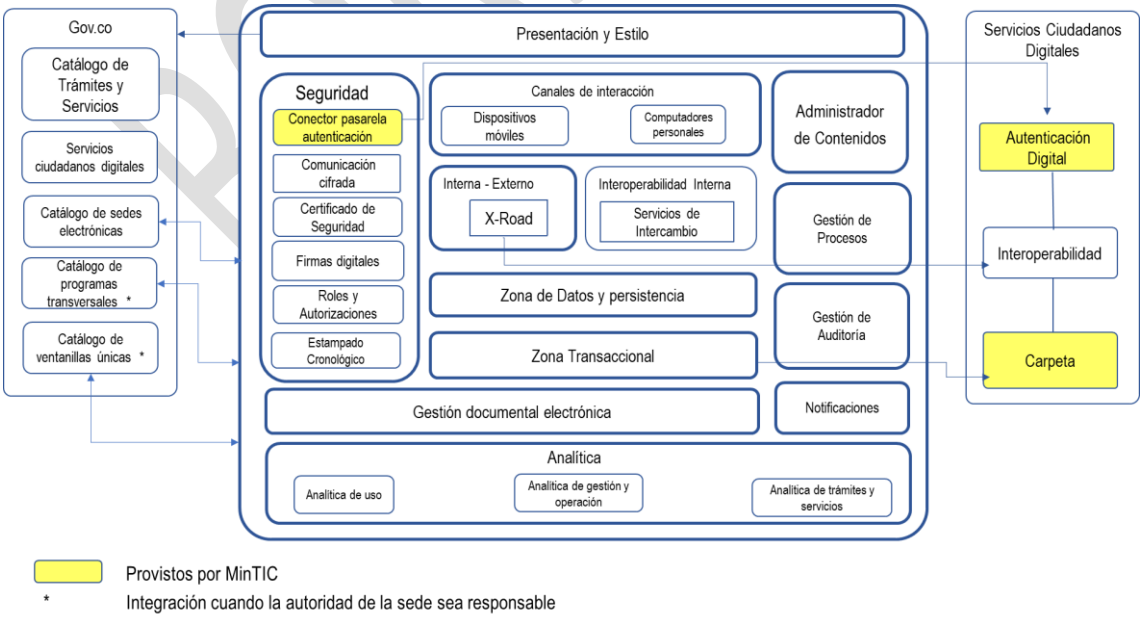

Figura 1 Arquitectura de referencia de una sede electrónica

A continuación, se describe el propósito de cada zona y porque 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 de las sedes electrónicas deben poseer los compontes 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. 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.

(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 oferta de servicios dispuesta por la autoridad a través de cualquier dispositivo móvil o computador personal.

(e) Zona transaccional: la arquitectura de solución de las sedes electrónicas debe contar con componentes que permitan realizar transacciones como trámites o procedimientos administrativos y utilizar servicios que tenga a disposición la entidad a través de su sede electrónica.

(f) Administrador de contenido: la arquitectura de solución de la sede electrónica debe contar con un administrador de contenidos que permitan la creación y administración de información que se publica en la sede electrónica.

(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 nos estructurados.

(h) Analítica: la arquitectura de la sede electrónica debe poseer componentes que permitan a las autoridades generar capacidades para realizar agregación de datos transaccionales, bigdata, analítica de datos de uso, analítica de gestión y operación de la infraestructura que soporta la sede electrónica, entre otras con el fin de mejorar la toma de decisiones basadas en datos y la mejora continua de la sede electrónica.

(a) 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 en la sede electrónica mediante la gestión de logs para la correlación de los eventos que se generen dentro de la sede electrónica.

(b) 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, procesos y procedimientos ofrecidos por la sede electrónica.

(i) 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.

(j) Interoperabilidad externa. Todas las sedes electrónicas deben poseer componentes que permitan realizar intercambio de información con otras autoridades, empresas privadas u otros organismos, esto con el objeto de dinamizar y optimizar los trámites, procesos y procedimientos 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.

(k) 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.

(l) Integración con servicios ciudadanos digitales: Los trámites, servicios y procedimientos administrativos que ofrezca una sede electrónica deben realizar la vinculación a los Servicios Ciudadanos, atendiendo los siguientes requisitos. Lo anterior siguiendo los lineamientos que sobre la materia emita MinTIC para la vinculación a los Servicios Ciudadanos Digitales:

I. Vincular a los trámites, servicios o procedimientos administrativos 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 permitan 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 o solicitudes realizadas en la sede electrónica
V. Identificar los trámites y/o procedimientos 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
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 estructurar su arquitectura siguiendo el modelo de referencia definido anteriormente.

4.3. A*TRIBUTOS 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 son: accesibilidad, usabilidad, seguridad, disponibilidad, neutralidad e interoperabilidad 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 sedes deben poseer un mapa del sitio el cual puede ser accedido por 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 búsquedas, de forma que se facilite la accesibilidad.

(c) Todas las sedes electrónicas deben cumplir con los elementos de diseño gráfico, definidas en la directiva presidencial 03 de 2019 (cuando aplique) y el anexo 1: Guía de diseño gráfico para sedes electrónicas.

(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 la directiva presidencial 03 de 2019 (cuando aplique) y el anexo 1: Guía de diseño gráfico para sedes electrónicas.

(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 a orientar al usuario de cuales 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.

(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 de tiempo de carga de los contenidos de 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 la información y contenido de la sede.

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 los lineamientos que para tal efecto defina el MinTIC.

4.3.3. Seguridad

Las autoridades deben contar con medidas preventivas y reactivas, sistemas tecnológicos, entre otros, que garanticen la confidencialidad, la integridad y autenticidad de la información dispuesta en la sede, para ello deberá cumplir 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 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 los archivos del mismo.

(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´s.

(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, procesos y procedimientos 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 Servicios 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, procesos o procedimientos 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 y que incluyen 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 dificulten 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 permitan 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 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.

4.3.4. Neutralidad

a. 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 en cada uno de sus dominios para atender dichas las 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.
(c) Los trámites, procesos y procedimientos administrativos que requieran intercambiar datos e información, deberán realizar la estandarización de los conjuntos de datos a intercambiar aplicado el lenguaje común de intercambio de información del Estado colombiano.

(d) La sede electrónica debe configurar, habilitar y exponer a través de 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 y servicios 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, procesos y procedimientos 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 suficiente 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 las siguientes características:

(a) Actualizada: la información dispuesta en las sedes electrónicas debe estar actualizada con el propósito de no brindar información errada a los grupos de interés que acceden a la sede electrónica.
(b) La información producida, gestionada y difundida deberá ser oportuna, objetiva, veraz, completa, reutilizable, procesable y estar disponible en formatos accesibles para los solicitantes e interesados en ella, teniendo en cuenta los procedimientos de gestión documental de la respectiva entidad.
(c) 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.
(d) Veraz: La información publicada en las sedes electrónicas debe ser correcta y fidedigna.
(e) Publicación en formatos abiertos: La información publicada en las sedes electrónicas a través de archivos debe disponerse en formatos que permiten 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).

4.3.7. Disponibilidad

(a) 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 servicios, trámites o procedimientos administrativos ofrecidos.

4.3.8. Infraestructura Tecnológica.

(a) La sede electrónica debe poder ser accedida a través de direccionamiento a una IP pública IPv4 e IPv6, de acuerdo con la resolución 2710 de 2017.
(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 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 en la directiva presidencial 03 de 2019 (cuando aplique) y el anexo de diseño.

(b) **Header:** Acondicionar un Top Bar completo con acceso al Portal Único del Estado colombiano - GOV.CO, que estará ubicado en la parte superior, 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 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, línea anticorrupción, correo institucional para atención al público, correo de notificaciones judiciales, link para el mapa del sitio, y un link para vincular a las políticas como las siguientes: términos y condiciones, política de privacidad, y política de 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.

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

I. **Contenidos e información:** Todo contenido o información de la Ventanilla Única Digital debe estar relacionado con la finalidad de la misma. No se debe incluir marcas o referencias que no estén estrictamente relacionadas con las entidades participantes, ni con el propósito de la Ventanilla Única Digital.

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 autoridad de 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. **Menú de Trámites:** Se deberá indicar claramente el tipo de trámite, informando lo siguiente:

a) Nombre de la cadena trámite
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 trámites o 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 el estado del trámite, para que al usuario se le informe su situación real con independencia de las responsabilidades de las entidades participantes en la gestión del trámite.

Nota: Se debe tener en cuenta que en el momento que los Servicios de Carpeta Ciudadana Digital y 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 debe ser vinculados a estos servicios en las condiciones que el ministerio disponga.

VII. **Menú de Contáctenos:** 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 pertinente para sus usuarios. Dentro de los canales de atención se dispondrá de un formulario único de PQRS 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 PQRS radicada. En todo caso deberá indicarse el tiempo máximo de respuesta, conforme con lo dispuesto en la ley. En caso de que la PQRS 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 la PQRS.

4.4.2 Cumplimiento de políticas

Las entidades deberán incorporar una sección 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, servicios de trámites y servicios, servicios de pasarela de pago, servicios de consulta de información, 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.

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 las disposiciones de la Ley 1581 del 2012, y la Circular Externa Conjunta 04 entre la Agencia Nacional de Defensa Jurídica del Estado y la Superintendencia de Industria y Comercio, y demás instrucciones o disposiciones relacionadas, o aquellas que las modifiquen, adicionen o deroguen.

4.4.2.3. ARQUITECTURA DE REFERENCIA PARA VENTANILLAS ÚNICAS

La arquitectura de referencia de una ventanilla única es la misma definida para la sede electrónica, la cual se encuentra definida en el numeral 1.4.2

4.4.2.4. Atributos de calidad de la ventanilla única

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 1.4.3

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 a nivel 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.

(d) La entidad responsable deberá solicitar al Ministerio de las Tecnologías de la Información y las Comunicaciones la integración del Portal de Programa Transversal del Estado al Portal Único del Estado colombiano - GOV.CO.

(e) Cumplir los lineamientos técnicos para publicar los contenidos al 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.

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, hace 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: "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, una gestión o comunicarse con la entidad, por favor dirigirse a la Sede Electrónica de MinTIC en el link *www.mintic.gov.co".*

(b) Diseño gráfico. Cada portal transversal podrá disponer de un diseño gráfico, marca y experiencia diferenciada de la Sede Electrónica de la entidad responsable del Portal Transversal.

(c) Header: Acondicionar un Top Bar completo con acceso al Portal Único del Estado colombiano - GOV.CO, que estará ubicado 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 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, línea anticorrupción, correo institucional para atención al público, correo de notificaciones judiciales, link para el mapa del sitio, y un link para vincular a las políticas como las siguientes: términos y condiciones, política de privacidad, y política de 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.

(e) Contenidos mínimos: Los siguientes son los contenidos mínimos que debe contar un portal transversal:

(g) Información acerca del Portal: describirá el propósito del portal, el público al que está dirigido, y la entidad responsable.

(h) 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 autoridad de ella. La información deberá

publicarse conforme con las pautas o lineamientos en materia de lenguaje claro, accesibilidad y usabilidad.

(i) **Contenidos e información:** Todo contenido o información del Portal de Programa Transversal del Estado debe estar relacionado con su finalidad. No se debe incluir contenidos, publicidad, marcas o referencias que no estén estrictamente relacionadas con el objeto del Portal.

4.5.4. CUMPLIMIENTO DE POLÍTICAS LEGALES

Las autoridades deberán incorporar una sección 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, servicios de trámites y servicios, servicios de pasarela de pago, servicios de consulta de información, 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; referencia a la política 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 las disposiciones de la Ley 1581 del 2012, y para las autoridades la Circular Externa Conjunta 04 entre la Agencia Nacional de Defensa Jurídica del Estado y la Superintendencia de Industria y Comercio, 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 el cual, deberán incluir el alcance y limitaciones relacionados con el uso de datos, información, contenidos, códigos fuente producidos por la autoridad.

5. ARQUITECTURA DE REFERENCIA PARA PORTALES DE PROGRAMAS TRANSVERSALES.

(a) Los portales de programas transversales deberán ser estructurados utilizando la siguiente arquitectura de referencia, que define unas zonas genéricas.

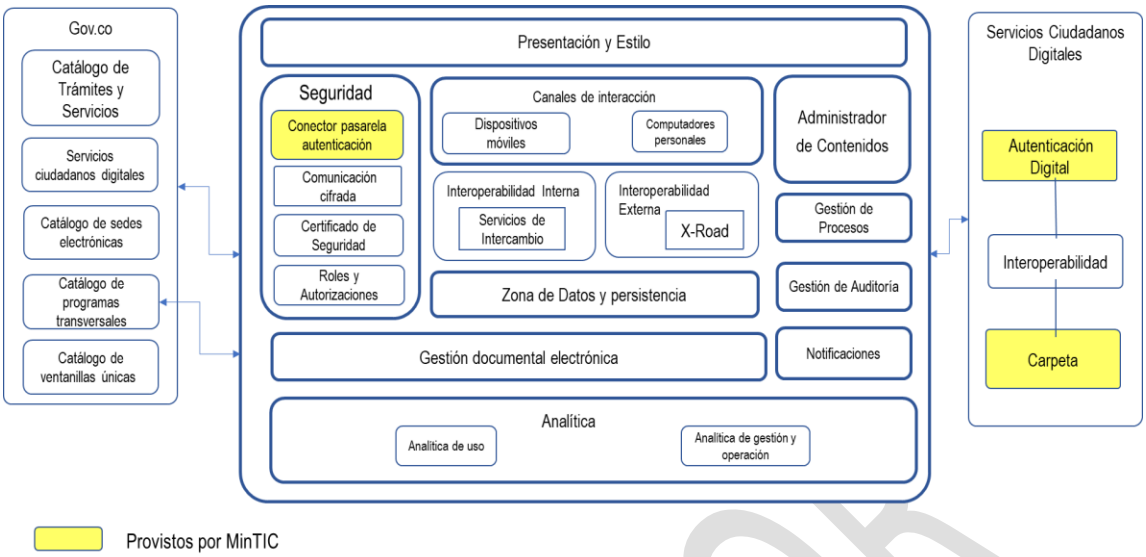

Figura 2 Arquitectura de Referencia de un portal de programa transversal

(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, proceso o procedimiento administrativo vinculado a un portal de un programa transversal se deberá direccionar al trámite digital.

(d) Los componentes de gestión documental electrónica, gestión de procesos, gestión de auditoria, notificaciones deberán estar presentes si existen funcionalidades que lo requieran.

5.1. Atributos de calidad de 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 son: accesibilidad, usabilidad, seguridad, disponibilidad, neutralidad e interoperabilidad que se describen a continuación.

5.1.1. Usabilidad

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

(a) Todas las sedes electrónicas deben poseer un mapa del sitio el cual puede ser accedido por 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 búsquedas, de forma que se facilite la accesibilidad.

(c) Todas las sedes electrónicas deben cumplir con los elementos de diseño gráfico, definidas en la directiva presidencial 03 de 2019 (cuando aplique) y el anexo 1: Guía de diseño gráfico para sedes electrónicas.
(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 la directiva presidencial 03 de 2019 (cuando aplique) y el anexo 1: Guía de diseño gráfico para sedes electrónicas.
(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 a orientar al usuario de cuales 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 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) 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.
(m) La sede electrónica debe realizar un adecuado control de tiempo de carga de los contenidos de páginas evitando dar la impresión de que no están disponibles o que presentan errores.
(n) La sede electrónica debe incorporar en los formularios de captura de información ejemplos que de forma sencilla y clara orienten al usuario al usuario en el formato a utilizar en el diligenciamiento.
(o) La sede electrónica debe proporcionar mensajes de confirmación a todas las acciones que el usuario realice.
(p) La sede electrónica debe ofrecer páginas personalizadas para el manejo del error 404, con el fin de ofrecer una mejor experiencia de usuario.
(q) La sede electrónica debe ofrecer un buscador interno que permita al usuario encontrar la información y contenido de la sede.

5.1.2. Accesibilidad

La sede electrónica debe cumplir con el estándar AA de la W3C (WCAG – Web Content Accessibility Guidelines), de conformidad con los lineamientos que expida el MinTIC, y adoptar los siguientes lineamientos mínimos:

(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 Ministerio de Tecnologías de la Información y la Comunicación 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 los que se pueda modificar el contraste, reducir o aumentar la letra, comunicarse con el centro de relevo, y la opción de cambiar idioma.

(c) Disponer de un link de accesibilidad ubicada en el footer del home principal, en el que se deberá 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 la Guía de Accesibilidad del MinTIC, todos los sujetos obligados deberán incluir en el 100% de los contenidos audiovisuales (vídeos) nuevos con subtítulos incorporados o bajo la opción de texto escondido (*closed caption*) auto activable por los usuarios. Esta disposición no aplica para transmisiones en vivo y en directo.

(e) Alternativas de texto: 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 contenido en el que se pueda establecer tamaños de fuente relativos permite que los usuarios puedan configurar fácilmente el tamaño de letra con que se sienten más cómodos para la lectura, sin afectar a la presentación de los sitios Web.

(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 éstos 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 visualizas: no diseñar contenido 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.

(n) Predictibilidad: páginas Web aparezcan y funcionen 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) Ayuda en 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, seleccionar una opción. También hay funcionalidades que pueden ayudar a los usuarios autorrellenado de formularios cuando se detecta que los valores que esperan ciertos campos ya están disponibles en la memoria del navegador.

5.1.3. Seguridad

Las autoridades deben contar con medidas preventivas y reactivas, sistemas tecnológicos entre otros que garanticen la confidencialidad, la integridad y autenticidad de la información dispuesta en los portales de programas transversales, para ello deberá cumplir 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 de que soporta el portal del programa transversal (sistemas operativos, servidor web, Base de datos) y mantener actualizado 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´s.
(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 renovaciones periódicas de estas contraseñas; así como implementar mecanismos de captcha, cuando se requiera disponer a través del portal funcionalidades que requieran este tipo de mecanismos. *Nota: Se debe tener en cuenta que en el momento que el Servicios de 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 al 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 y que incluyen 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 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 dificulten 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 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.

5.1.4. 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.

5.1.5. 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 las 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.
(c) Cuando el portal requiera o posea funcionalidades para intercambiar información, se debe realizar la estandarización de los conjuntos de datos a intercambiar aplicado 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”.

5.1.6. Calidad de información.

La calidad de la información dispuesta en el portal del programa transversal debe cumplir 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 al portal.
(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 permiten 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).

5.1.7. Disponibilidad

(a) 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 o procedimientos administrativos ofrecidos.

5.1.8. Infraestructura Tecnológica.

(a) El portal del programa transversal debe poder ser accedido a través de 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).

5.2. 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 el portal y la información deberá estar disponible en la sede electrónica según corresponda, esto con el fin de evitar la proliferación de portales del Estado.