COMENTARIOS LINEAMIENTO Y GUÍAS DE INTEGRACIÓN DE SEDE ELECTRÓNICA, VENTANILLAS ÚNICAS, PORTALES ESPECÍFICOS DE PROGRAMAS TRANSVERSALES, Y TRÁMITES, OPAS, Y CONSULTAS DE ACCESO A INFORMACIÓN PÚBLICA					
No.	**Fecha de recepción**	**Remitente**	**Observación recibida**	**Estado**	**Consideración desde entidad**
1	14/08/2020	**ASOCIACIÓN INTERAMERICANA DE EMPRESAS DE TELECOMUNICACIONES - ASIET**	1. Vemos en este proyecto una oportunidad para reglamentar la creación de una ventanilla única para el recaudo de las remuneraciones por el uso de los derechos de autor, mecanismo que consideramos ideal para corregir algunas de las problemáticas que caracterizan el mercado de derechos de autor en Colombia. Como hemos manifestado en ocasiones anteriores, los usuarios de este mercado (entendidas como todas aquellas industrias que usan las obras protegidas en su cadena de valor para producir otros bienes o servicios y así agregar valor al consumidor final) han sido sujetas de cobros discriminatorios, desproporcionales y pocos transparentes que hacen algunas de las Sociedades de Gestión Colectiva (en adelante SGC), desatendiendo entonces la normativa relacionada (...) Así las cosas, en la discusión de este proyecto regulatorio donde se propone la adopción de lineamientos en la estandarización de las ventanillas únicas para el sector TIC, ponemos en consideración del MinTIC evaluar la conveniencia de crear una ventanilla única para el recaudo de las remuneraciones por los usos de derechos de autor en el sector TIC5 , la cual, de ser acompañada por las recomendaciones institucionales mencionadas anteriormente, podrá subsanar los altos grados de conflictividad y poca transparencia que caracterizan este mercado. En particular, y siguiendo parte de las recomendaciones hechas por Fedesarrollo6 , la adopción de este mecanismo reduciría los costos de transacción, complementando la función de las SGC en el sentido de bajar los costos de gestión y de transacción. En todo caso, hacemos claridad que dicha ventanilla tendría como único fin el recaudo de las remuneraciones y no el de funcionar como un mecanismo para fijar las tarifas.	No aceptada	Las competencias del MinTIC están dadas por la Ley 1341 del 2009, modificada por la Ley 1978 del 2019, que tiene como objetivos principales los siguientes: 1. Diseñar, formular, adoptar y promover las políticas, planes, pro-gramas y proyectos del sector de Tecnologías de la Información y las Comunicaciones, en correspondencia con la Constitución Política y la Ley, con el fin de promover la inversión y el cierre de la brecha digital, contribuir al desarrollo económico, social y político de la Nación, y elevar el bienestar de los colombianos. 2. Promover el uso y apropiación de las Tecnologías de la Información y las Comunicaciones entre los ciudadanos, las empresas, el Gobierno y demás instancias nacionales como soporte del desarrollo social, económico y político de la Nación. 3. Impulsar el desarrollo y fortalecimiento del sector de las
		ASOCIACIÓN INTERAMERICANA DE EMPRESAS DE TELECOMUNICACIONES - ASIET	2. En vista de las problemáticas anteriores, desde la industria hemos sugerido las siguientes recomendaciones de política pública en materia de propiedad intelectual: Habilitar la negociación sectorial de criterios paramétricos en la fijación de las tarifas. En este punto, se advierte que (en línea con Fedesarrollo -2019-): "Aunque las entidades de gobierno deben facilitar los procesos de negociación y emitir las regulaciones necesarias para alejar las amenazas de demandas por colusión, las decisiones sobre qué parámetros aplicar y sus valores deben dejarse enteramente al acuerdo entre las partes".4 La habilitación de esta negociación sectorial de tarifas puede adoptarse en desarrollo del artículo 333 de la Constitución, según el cual el Estado "evitará o controlará cualquier abuso que personas o empresas hagan de su posición dominante en el mercado nacional". Cabe señalar que el mecanismo de negociación sectorial señalado busca evitar el potencial de abuso de posición dominante que ostentan las SGC en sus respectivos mercados. • Ante la inexistencia de un marco normativo que compagine la protección de la competencia y los derechos de autor en	No aceptada	Con relación a su propuesta relacionada con la inexistencia de un marco normativo relaciondo con esquemas de derechos de autor y conexos, y la discusión del CONPES de Propiedad Intelectual, informamos que dichos asuntos no son competencia del MinTIC en virtud de las competencias asignadas en la Ley 1341 del 2009 y la Ley 1978 del 2019. Así las cosas, se invita a presentar sus comentarios de manera directa a la entidad competente, en este caso la DIrección Nacional de Derechos de Autor.
			1. Las plataformas web de las entidades del Estado proporcionan al usuario una serie de funciones y servicios. Para cumplir con ese objetivo, ellas pueden recopilar y procesar gran cantidad de datos relacionados con los usuarios u otras personas.	Aceptada	Así es, agradecemos su comentario y realizaremos la aclaración.
			2. Todo contenido y estructura de la sede electrénica, asi como del Portal Unico del Estado colombiano, debe cumplir con lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios.	Aceptada	Así es, agradecemos su comentario y realizaremos la aclaración. Se incorporará un apartado específico referido al tratamiento de datos personales así. 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
			3. Las cookies 0 tecnologias similares, como etiquetas de identificación por radiofrecuencia, que pueden estar disponibles tanto en las paginas web como en otro tipo de plataformas y aplicaciones (por ejemplo, Apps para teléfonos inteligentes y tablets), conllevan un Tratamiento de datos personales, razon por la cual, deben ajustar su funcionamiento para dar cumplimiento a la Ley 1581 de 2012.	Aceptada	Así es, agradecemos su comentario y realizaremos la aclaración. Se incorporará un apartado específico referido al tratamiento de datos personales así. Todo contenido y estructura de la sede electrónica, del Portal
			4. El regimen general de datos personales aplica también para el uso de otras tecnologias de seguimiento (Tracking technologies) y de perfilamiento.	Aceptada	Así es, agradecemos su comentario y realizaremos la aclaración. Se incorporará un apartado específico referido al
			5. Las entidades del Estado cuentan con perfiles en redes sociales para diferentes fines, entre ellos interactuar con los usuarios. Dichos perfiles facilitan que las personas compartan datos personales de manera pL'iblica, e incluso informacion de caracter sensible.	Aceptada	Así es, agradecemos su comentario y realizaremos la aclaración. Se incorporará un apartado específico referido al tratamiento de datos personales así.
			6. Si bien el concepto de "politica de privacidad" es un término usado en la practica, en Colombia esa politica se denomina "Politica de Tratamiento de Informacién Personal".	Aceptada	Así es, agradecemos su comentario y realizaremos la aclaración. Se incorporará un apartado específico referido al
			7. La adopción de una politica de tratamiento de informacién personal no es la Unica obligación que establece la normatividad en protección de datos personales.	Aceptada	Así es, agradecemos su comentario y realizaremos la aclaración. Se incorporará un apartado específico referido al
			8. El Anexo 1 del Proyecto de Resolución desconoce ese conjunto de principios, derechos y obligaciones sefialados en la Ley 1581 de 2012 y sus derechos reglamentarios.	Aceptada	Así es, agradecemos su comentario y realizaremos la aclaración. Se incorporará un apartado específico referido al
			9. Las entidades cuentan con mUltipies canales de contacto que permiten la recolección de datos. Dichos canales deben cumplir con lo establecido en la Ley 1581 de 2012.	Aceptada	Así es, agradecemos su comentario y realizaremos la aclaración. Se incorporará un apartado específico referido al

			10. Un posible incumplimiento a la Ley 1581 de 2012 es el seguimiento de terceros sin previo consentimiento. Esto resulta especialmente problematico en ios casos en que el tercero en cuestién opera bajo un modelo de negocio basado en la elaboración de perfiles y la posterior orientacién conductual de los visitantes del sitio web.	Aceptada	Así es, agradecemos su comentario y realizaremos la aclaración. Se incorporará un apartado específico referido al tratamiento de datos personales así. 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. Los sujetos obligados deberán contar con la política de tratamiento de información personal de fácil acceso y
			11. La misma problematica se presenta frente al uso de rastreadores para analisis web sin el consentimiento previo de los Usuarios (visitantes) y el envio de datos personales recopilados a través de formularios web sin cifrar conexiones.	Aceptada	Así es, agradecemos su comentario y realizaremos la aclaración. Se incorporará un apartado específico referido al tratamiento de datos personales así. 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
			12. La seguridad es un componente esencial de la protección de datos personales. Las entidades deben contar con procedimientos documentados para la web, servicio de desarrollo seguro, implementación, operacion y pruebas de seguridad siguiendo las mejores prácticas, un enfoque integrado de pruebas de seguridad y politica de capacitacion del personal.	Aceptada	Así es, agradecemos su comentario y realizaremos la aclaración. Se incorporará un apartado específico referido al tratamiento de datos personales así.
			13. "Con base en lo anteriormente expuesto, ponemos a su consideración las siguientes recomendaciones, teniendo como criterio orientador los principios que rigen la proteccion de los datos personales en el territorio nacional: 1. Principio de Legalidad Al respecto, se sugiere incluir tanto en el proyecto de decreto como en la Seccion 4.1. “Contenido y estructura de informacion de la sede electrénica”del Anexo 1°, la responsabilidad por parte de las entidades obiigadas de proteger los datos personales en su posesién o custodia, incluida aquelia informacion tratada en las sedes electronicas. También la responsabilidad de la entidad que administra el Portal Unico del Estado coiombiano. Por lo tanto se somete a su consideración la inclusion del siguiente articulo “Proteccién de Datos Persona/es. En el Tratamiento de los datos persona/es se implementarén las medidas apropiadas, efectivas y verificables para cumplir con los principios, derechos y obligaciones establecidas en la Ley 1581 de 2012 y sus decretos reg/amentarios, y las normas que las modifiquen, reg/amenten o sustituyan.”"	Aceptada	Así es, agradecemos su comentario y realizaremos la aclaración. Se incorporará un apartado específico referido al tratamiento de datos personales así. 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. 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
			14. "2. Principios de Libertad, Finalidad y Transparencia: Respecto a este punto, considera esta Entidad pertinente que las autoridades cuenten con un mecanismo (u opción) que ie permita al usuario otorgar su consentimiento expreso, previo e informado (o explicito para el Tratamiento de los datos sensibles y de nifios, nifias y adolescentes), conforme con el principio de libertad."	Aceptada	Así es, agradecemos su comentario y realizaremos la aclaración. Se incorporará un apartado específico referido al tratamiento de datos personales así. 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
			15. Adicionalmente, la Politica de Tratamiento de Informacién Personal debe, en primer lugar, ser de facii acceso y ser comprensible para los diferentes grupos de interés, como es el caso de nifios, nifias y adolescentes, o personas que no hablan el idioma casteiiano, o personas con discapacidad. También es importante que estas politicas se encuentren disponibles en zonas que capten la atención de los usuarios 0 en zonas donde el usuario medio espere encontrarla.	Aceptada	Así es, agradecemos su comentario y realizaremos la aclaración. Se incorporará un apartado específico referido al tratamiento de datos personales así. Todo contenido y estructura de la sede electrónica, del Portal
			16. Ahora bien, las cookies 0 tecnologias similares, como etiquetas de identificacion por radiofrecuencia, suponen el tratamiento de datos personaies. Portal motivo, se deben implementar las medidas y procesos necesarios para que ese tipo de tecnologias cumplan con lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias. Son ejemplos de medidas: - Abstenerse de usar cookies 0 tecnologias similares, salvo aquelias que sean estrictamente necesarias para permitir la comunicacion entre el equipo dei usuario y la red, entre otros casos. - La implementación de un mecanismo para obtener el consentimiento previo, expreso e informado del Titular para todas y cada una de las categorias de cookie, dependiendo de su finalidad y origen. - Por defecto, ninguna de esas cookies debe estar activada, salvo aquelias estrictamente necesarias para el funcionamiento y seguridad de la pagina, como se sefialc’) en anteriores lineas. - La adopcic’m de un sistema de gestion o configuración para aceptar, denegar o revocar el consentimiento para ei uso de cookies, asi como informar sobre el tipo de cookies segl’in quien las gestione, su uso y los fines del tratamiento, periodo de conservación; los cuales deben estar disponibles para el usuario, por ejemplo: en banners ubicados en la barra superior de la pagina web. - La Politica 0 el Aviso de Cookies debe estar disponible en zonas que capten ia atención de los usuarios 0 en zonas donde el usuario medio espere encontrarla.	Aceptada	Así es, agradecemos su comentario y realizaremos la aclaración. Se incorporará un apartado específico referido al tratamiento de datos personales así. 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. 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: •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

2	14/08/2020	**Superintendencia de Industria y Comercio**	17. "Ahora bien, si se pretende implementar técnicas de rastreo y de elaboración de perfiles, entre otros mecanismos innovadores, se debe determinar de manera clara la base legal de la recolección de los datos personales, asr' como evaluar los riesgos para los derechos y libertades de las personas sujetas a estas prácticas, pues las entidades deben ser transparentes e informar a los usuarios acerca de estas tecnologlas y sus propésitos."	Aceptada	Así es, agradecemos su comentario y realizaremos la aclaración. Se incorporará un apartado específico referido al tratamiento de datos personales así. 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. 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
			18. "Por otra parte, tanto en el formato electrónico para PQRSD como en los otros canales de comunicación que puedan desarrollar las entidades, por ejemplo, ""chatbot automatizado"", etc., debe tenerse en cuenta lo establecido en la Ley 1581 de 2012 y sus normas reglamentarlas. Algunas medidas que se recomiendan al respecto son las siguientes: a. La adopcic'm de mecanismos para obtener el consentimiento previo, expreso (o explicito si se tratan de datos sensibles), e informado del Titular (articulo 12 de la Ley 1581 de 2012). b. Divulgar la Politica de Tratamiento de Información Personal de la entidad, con el fin de que la persona la conozca al momento en que esta suministrando su información personal a través de esos canales. c. Recolectar la información estrictamente necesaria para la finalidad perseguida (articulo 4 del Decreto 1377 de 2013); e, implementar los mecanismos de segundad."	Aceptada	Así es, agradecemos su comentario y realizaremos la aclaración. Se incorporará un apartado específico referido al tratamiento de datos personales así. 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. 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
			19. Por último se recomienda que las entidades eviten el uso de componentes de terceros que redirigen a los usuarios a servicios web que ellos no utilizaron o requirieron con el fin de evitar alguna vulneración en el tratamiento de los datos.	Aceptada	Así es, agradecemos su comentario y realizaremos la aclaración. Se incorporará un apartado específico referido al tratamiento de datos personales así. 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. 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
			20. Principios de Seguridad, Confidencialidad y Acceso y Circulación restringida.Sin perjuicio de la obligación de las entidades de reportar los incidentes cibernéticos, graves o muy graves al CSIRT-Gobierno 0 al CoICERT del Ministerio de Defensa Nacional, esta Entidad sugiere incluir en el punto 4.4.3. (Seguridad) del Anexo 1, la obligacion de las entidades pL'Jblicas de reportar cualquier incidente de seguridad en datos personales a la Superintendencia de Industria y Comercio (SIC) conforme lo establecen los artículos 17 (n) y 18 (k) de la Ley 1581 de 2012). Es importante, ademas, que las entidades cuentan con una politica de gestión de incidentes de seguridad en datos personales."	Aceptada	Así es, agradecemos su comentario y realizaremos la siguiente aclaración: ""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. 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.
			21. Ahora bien, si se planea contratar Encargados dei Tratamiento, como proveedores de hosting, las entidades deben tener en cuenta lo que establece ia Ley 1581 de 2012 y ei articulo 2.2.2.25.5.2. del Decreto 1074 de 2015, asi como las guias que ha emitido la Delegatura para la Protección de Datos Personales respecto a los proveedores de servicios de computación en la nube.	Aceptada	Así es, agradecemos su comentario y realizaremos la siguiente aclaración: ""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. 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.

			22. En el evento que no se implementen las medidas necesarias para garantizar los principios de acceso y circulación restringida, seguridad y confidencialidad establecidos en la ley, se corre el riesgo de poner en peligro los datos personales de los ciudadanos. Por lo tanto, las entidades deben identificar las salvaguardas de seguridad necesarias, teniendo en cuenta las amenazas y vulnerabilidades conocidas relacionadas con Internet, basadas en arquitectura y tecnologia de servicios web especificos.	Aceptada	Así es, agradecemos su comentario. Las entidades públicas están obligadas a cumplir el habilitador de seguridad y privacidad de la información de la política de Gobierno digital, y en dicho modelo se encuentran, entre otros, los requerimientos a los que se hace referencia en su comentario.
			23. Teniendo en cuenta lo expuesto, se sugiere reforzar ei deber de los sujetos obligados a realizar evaluaciones de impacto en protección de datos, con el fin de garantizar que las medidas técnicas, administrativas y organizativas sefialadas en las secciones 4.3.3. y 4.5.6.3. "Seguridad" (Anexo 1), aseguran la proteccion de los datos y evitar vulneraciones a los derechos y libertades de los usuarios. Dichas evaluaciones deben ser permanentes.	Aceptada	Así es, agradecemos su comentario, respecto del cual se incorporará en la guía el siguiente texto: 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.
			24. Cabe sefialar que la evaluación de impacto de proteccion de datos también le permitira al Ministerio determinar si las medidas descritas en el anexo, en particular, las relacionadas con el cumplimiento de los principios de seguridad, confidencialidad, acceso y circulación restringida, garantizan ('0 contempan garantizando en un tiempo determinado) el cumplimiento de la normatividad en proteccion de datos y las politicas de seguridad digital, o si por el contrario se requiere de medidas adicionales. Por consiguiente, es importante llevar un registro de las evaluaciones en caso que la Superintendencia io requiera en su función de inspección, vigilancia y control de acuerdo con lo previsto en la Ley 1581 de 2012.	Aceptada	Así es, agradecemos su comentario, respecto del cual se incorporará en la guía el siguiente texto: 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.
			25. Principio de Responsabilidad Demostrada: En caso de que las entidades púibiicas decidan abrir cuentas en las redes sociales, ya cuenten con una, se sugiere que ellas analicen como trataran (o esté tratando ia información de carécter personal) que los ciudadanos postearon en los perfiles, por citar un ejemplo. El proposito de este estudio persigue: — Asegurar que el manejo de los datos personales que se haga desde el perfil social de una entidad del Estado cumpla con lo que señala la Ley 1581 de 2012 y sus normas reglamentarias. - Conocer los términos y condiciones, asi como las politicas de privacidad de las plataformas de redes sociales, en particular si ellas recolectan datos personales de los usuarios que acceden a los perfiles, — Incluir un disclaimer con la politica de tratamiento de la entidad en el perfil de red social. Teniendo en cuenta lo expuesto, se sugiere incluir un articulo dirigido a que las entidades realicen evaluaciones para determinar de manera previa si una publicacion o divulgacion de información personal en su pagina web y/o redes sociales 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	Aceptada	Así es, agradecemos su comentario y realizaremos la aclaración. Se incorporará un apartado específico referido al tratamiento de datos personales así. 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. 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
			26. Por último, la entidad pone a consideración las siguientes preguntas: 1. Teniendo en cuenta que la guia de integración vigente define los mecanismo de integración por Web services y trámites embebidos y que muchas entidades han hecho inversiones y esfuerzos en este sentido, Cómo se realizará esta homologación y qué pasara con los recursos invertidos en este mecanismo de integracion?	Aceptada	Está próximo a publicarse la versión 2.0 de la guía de integración de trámites con el mecanismo de redireccionamiento. Para aquellos trámites que ya tenían avanzados el condicionamiento y los ajustes en los esquemas definidos previamente (servicios web y embebidos) se ha venido coordinando para que se culmine la integración bajo este esquema, por favor contactar al colaborador de MinTIC (enlace) designado para acompañarle en este proceso; los demás trámites y servicios deben ser integrados como se define en la guía próxima a ser publicada.

			27. En la nueva guia de integracién propuesta, las entidades deberan hacer un esfuerzo en adecuacién del look and feel de sus sedes electrénicas e integrarse a través del dominio a GOV.CO, t5,Cual es el plan de integracic'm para realizar dicho proceso? gCémo se realizarén las estimaciones de esfuerzo? La estimacion de este esfuerzo se realizara por tramites o por la ventanilla complete? Cual sera el rol de la Agencia Nacional Digital en este proceso?	Aceptada	El plan de integración y la estimación del esfuerzo lo define cada entidad de acuerdo con las metodologías que utilice para tal fin. Es necesario realizar la integración de Sedes Electrónicas, Trámites y Ventanillas de acuerdo con los lineamientos establecidos en cada Guía. El rol de la Agencia Nacional Digital está definido en el decreto 620 del 2020 y funge como articulador y prestador de los Servicios Ciudadanos Digitales.
			28. Teniendo en cuenta que el servicio Ciudadano de autenticacién es importante para lograr el objetivo de "Mantener al ciudadano dentro del contexto del dominio GOV.CO, generando una experiencia de usuario amigable y unificada" - Cuándo se contará con este servicio para ser consumido por las entidades en los niveles de seguridad que requieren los trámites y servicios? ¿Existe un plan de integración que tenga en cuenta la disponibilidad de los Servicios ciudadanos digitales en este proceso?	Aceptada	El servicio de autenticación en su mecanismo de autenticación bajo, ya se encuentra disponible para que las entidades se vinculen al servicio. En las próximas semanas MinTIC anunciará las fechas en las cuales estarán disponibles los demás mecanismos. Adicionalmente, el Ministerio viene trabajando coordinadamente para que sus iniciativas de Servicios Ciudadanos Digitales y GOV CO se integren y puedan prestarle servicio a las entidades.
			1. En el Anexo se define la Sede electrónica como “el sitio oficial en Internet de cada autoridad, al que se accede a través de una dirección electrónica donde se dispone información, trámites, Otros Procedimientos Administrativos, servicios de consulta de información, entre otros, ofrecidos por la autoridad y cuya titularidad, administración y gestión le corresponde”. Al respecto se solicita agregar en la definición de la sede electrónica que debe estar “dotada de las medidas jurídicas, organizativas y técnicas que garanticen calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad de la información y de los servicios”. Lo anterior para que la definición se encuentre en concordancia con el artículo 2.2.17.6.1. del Decreto 620 de 2020 y el artículo 60 de la Ley 1437 de 2011.	Aceptada	Se agradece el comentario, respecto del cual se hace el ajuste correspondiente en la guía
			2. Por otro lado, se define el servicio de carpeta ciudadana digital como “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”, desconociendo que el Decreto 620 de 2020 indica que a través de este servicio se pueden entregar comunicaciones y alertas.	Aceptada	Se agradece el comentario y se realiza el ajuste correspondiente
			3. Además de ello, cabe recordar que el artículo 45 de la Ley 1753 de 2015 señala que la carpeta ciudadana funcionará como un repositorio de documentos que le permitirá al ciudadano “almacenar y compartir documentos públicos o privados, recibir comunicados de las entidades públicas, y facilitar las actividades necesarias para interactuar con el Estado”. De esta forma se encuentra que las definiciones señaladas en el documento en comento generan limitaciones excesivas a la carpeta ciudadana digital, contrariando la voluntad del legislador, que buscaba tener con la carpeta ciudadana digital una herramienta robusta que le permitiera al ciudadano interactuar eficazmente con el Estado, teniendo en un solo lugar todos sus documentos. De acuerdo con lo indicado, las limitaciones a la carpeta ciudadana digital no solamente son funcionalmente inconvenientes, sino que desconocen el respeto por la jerarquía normativa, pues están vulnerando lo dispuesto por el legislador en la Ley 1753 de 2015 anteriormente citada, por las razones que pasan a explicarse.	No aceptada	Se agradece el comentario. Al respecto, se aclara que el Decreto 620 de 2020 define el Servicio de carpeta ciudadana digital como el servicio que le permite a los usua-rios de servicios ciudadanos digitales acceder digitalmente de manera segura, confiable y actualizada al conjunto de sus datos, que tienen o custodian las en-tidades señaladas en el artículo 2.2.17.1.2. Adicionalmente, este servicio podrá entregar las comunicaciones o alertas, que las entidades señaladas tienen para los usuarios, previa autorización de estos. La Ley 2052 de 2020 en su artículo 12 señala: "Los sujetos obligados en los términos de le presente ley deberán crear, diseñar o adecuar los mecanismos técnicos que permitan la vinculación al servicio de carpet2 ciudadana digital y garantizar el acceso de manera segura, confiable y actualizada al conjunto de los datos de quienes se relacionan con el Estado Igualmente, deberán suministrar a los prestadores de servicios ciudadanos digitales los datos a los que se accede a través de la carpeta ciudadana digital siempre y cuando dichos prestadores cuenten con autorización previa de los titulares de los datos. Asimismo, los sujetos obligados deberán contar con

			4. Respeto por la jerarquía normativa La Corte Constitucional ha expresado sobre la jerarquía normativa lo siguiente: "5. El ordenamiento jurídico colombiano supone una jerarquía normativa que emana de la propia Constitución. Si bien ella no contiene disposición expresa que determine dicho orden, de su articulado puede deducirse su existencia, así no siempre resulte sencilla esta tarea. En efecto, diversas disposiciones superiores se refieren a la sujeción de cierto rango de normas frente a otras. Así, para empezar el artículo 4° de la Carta a la letra expresa: "La Constitución es norma de normas. En todo caso de incompatibilidad entre la Constitución y la ley u otra norma jurídica, se aplicarán las disposiciones constitucionales." Esta norma se ve reforzada por aquellas otras que establecen otros mecanismos de garantía de la supremacía constitucional, cuales son, principalmente, el artículo 241 superior que confía a la Corte Constitucional la guarda de la integridad y supremacía de la Carta y el numeral 3° del artículo 237, referente a la competencia del Consejo de Estado para conocer de las acciones de nulidad por inconstitucionalidad de los decretos dictados por el Gobierno Nacional, cuyo conocimiento no corresponda a la Corte Constitucional. Así las cosas, la supremacía de las normas constitucionales es indiscutible.	No aceptada	Se agradece el comentario. Al respecto, se aclara que el Decreto 620 de 2020 define el Servicio de carpeta ciudadana digital como el servicio que le permite a los usua-rios de servicios ciudadanos digitales acceder digitalmente de manera segura, confiable y actualizada al conjunto de sus datos, que tienen o custodian las en-tidades señaladas en el artículo 2.2.17.1.2. Adicionalmente, este servicio podrá entregar las comunicaciones o alertas, que las entidades señaladas tienen para los usuarios, previa autorización de estos. La Ley 2052 de 2020 en su artículo 12 señala: "Los sujetos obligados en los términos de le presente ley deberán crear, diseñar o adecuar los mecanismos técnicos que permitan la vinculación al servicio de carpet2 ciudadana digital y garantizar el acceso de manera segura, confiable y actualizada al conjunto de los datos de quienes se relacionan con el Estado Igualmente, deberán suministrar a los prestadores de servicios ciudadanos digitales los datos a los que se accede a través de la carpeta ciudadana digital siempre y cuando dichos prestadores cuenten con autorización previa de los titulares de los datos. Asimismo, los sujetos obligados deberán contar con
			5. El Consejo de Estado también se ha pronunciado al respecto, al realizar manifestaciones respecto a la potestad reglamentaria del Presidente, indicando: "El numeral 11 del artículo 189 de la CP confirió potestad reglamentaria al Presidente de la República, al disponer sus funciones como suprema autoridad administrativa3, mediante la expedición de los decretos, resoluciones y órdenes necesarias para la cumplida ejecución de las leyes. En el contexto del principio de legalidad con primacía constitucional, los reglamentos constituyen normas jurídicas acatables dentro de un orden jerárquico que comienza con la Constitución, como fuente suprema en la que se funda el orden jurídico del Estado, y continúa con la ley, contentiva de regulaciones generales limitadas por la propia Constitución. Así, cada disposición ejecutiva debe atender el rango normativo inmediatamente superior, con el fin último de dar coherencia y armonía al orden jurídico legal y constitucionalmente establecido4. La jurisprudencia ha señalado que los reglamentos desarrollan los principios generales sentados por la ley5, de modo que ésta determina el alcance del poder de reglamentación6, pues, como norma originaria por excelencia que proviene del órgano de representación popular encargado de expresar la voluntad	No aceptada	Se agradece el comentario. Al respecto, se aclara que el Decreto 620 de 2020 define el Servicio de carpeta ciudadana digital como el servicio que le permite a los usua-rios de servicios ciudadanos digitales acceder digitalmente de manera segura, confiable y actualizada al conjunto de sus datos, que tienen o custodian las en-tidades señaladas en el artículo 2.2.17.1.2. Adicionalmente, este servicio podrá entregar las comunicaciones o alertas, que las entidades señaladas tienen para los usuarios, previa autorización de estos. La Ley 2052 de 2020 en su artículo 12 señala: "Los sujetos obligados en los términos de le presente ley deberán crear, diseñar o adecuar los mecanismos técnicos que permitan la vinculación al servicio de carpet2 ciudadana digital y garantizar el acceso de manera segura, confiable y actualizada al conjunto de los datos de quienes se relacionan con el Estado Igualmente, deberán suministrar a los prestadores de servicios ciudadanos digitales los datos a los que se accede a través de la carpeta ciudadana digital siempre y cuando dichos prestadores cuenten con autorización previa de los titulares de los datos. Asimismo, los sujetos obligados deberán contar con
			6. Las inexactitudes del Anexo 1 generan que no se respete la jerarquía normativa Una vez expuesta la importancia de que los Decretos y actos administrativos respeten los lineamientos de una Ley, se pasa a indicar porque en el presente caso se señala que la concepción de carpeta ciudadana no se corresponde con el mandato del legislador. Al respecto, el artículo 45 de la Ley 1753 de 2015 indica: "ARTÍCULO 45. ESTÁNDARES, MODELOS Y LINEAMIENTOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES PARA LOS SERVICIOS AL CIUDADANO. Bajo la plena observancia del derecho fundamental de hábeas data, el Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC), en coordinación con las entidades responsables de cada uno de los trámites y servicios, definirá y expedirá los estándares, modelos, lineamientos y normas técnicas para la incorporación de las Tecnologías de la Información y las Comunicaciones (TIC), que contribuyan a la mejora de los trámites y servicios que el Estado ofrece al ciudadano, los cuales deberán ser adoptados por las entidades estatales y aplicarán, entre otros, para los siguientes casos: (. .)	No aceptada	Se agradece el comentario. Al respecto, se aclara que el Decreto 620 de 2020 define el Servicio de carpeta ciudadana digital como el servicio que le permite a los usua-rios de servicios ciudadanos digitales acceder digitalmente de manera segura, confiable y actualizada al conjunto de sus datos, que tienen o custodian las en-tidades señaladas en el artículo 2.2.17.1.2. Adicionalmente, este servicio podrá entregar las comunicaciones o alertas, que las entidades señaladas tienen para los usuarios, previa autorización de estos. La Ley 2052 de 2020 en su artículo 12 señala: "Los sujetos obligados en los términos de le presente ley deberán crear, diseñar o adecuar los mecanismos técnicos que permitan la vinculación al servicio de carpet2 ciudadana digital y garantizar el acceso de manera segura, confiable y actualizada al conjunto de los datos de quienes se relacionan con el Estado Igualmente, deberán suministrar a los prestadores de servicios ciudadanos digitales los datos a los que se accede a través de la carpeta ciudadana digital siempre y cuando dichos prestadores cuenten con autorización previa de los titulares de los datos. Asimismo, los sujetos obligados deberán contar con
			7. LA SEDE ELECTRÓNICA Y LA SEGURIDAD DIGITAL Al observar los requisitos de la sede electrónica dispuestos por el Ministerio se encuentran falencias en materia de seguridad digital; si bien se realizan algunas alusiones técnicas y en determinados apartes se hacen remisiones al Modelo de Servicios Ciudadanos Digitales, se debe considerar que desde la reglamentación expuesta para comentarios deben fijarse reglas y parámetros mínimos, que permitan garantizar la eficacia probatoria, validez jurídica y no repudio de los trámites realizados en la sede electrónica, tales como los siguientes: 2.1. Estampado cronológico Al hablar de las peticiones y radicaciones el Anexo 1 señala que las sedes electrónicas deberán contar con las siguientes funcionalidades: "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".	No aceptada	Se agradece el comentario. De conformidad con el artículo 53 la Ley 1437 de 2011, en las actuaciones realizadas por las autoridades públicas utilizando medios electrónicos, se podrán aplicar las normas de la Ley 527 de 1999 cuando sean compatibles. Corresponde a cada una de las entidades evaluar el nivel de seguridad requerido para cada una de las interacciones de sus usuarios por medios digitales, y establecer de acuerdo a él, el mecanismo de firmas electrónicas, estampa cronologica, notificación electrónica, de gestión documental electrónica y de comunicación cifrada, utilizados.

3	14/08/2020	**CAMERFIRMA COLOMBIA S.A.S.**	8. También es importante indicar la definición del estampado cronológico establecida legamente, con lo cual se demuestra que es la herramienta idónea para cumplir con los estándares fijados por el Ministerio: "Mensaje de datos que vincula a otro mensaje de datos con un momento o periodo de tiempo concreto, el cual permite establecer con una prueba que estos datos existían en ese momento o periodo de tiempo y que no sufrieron ninguna modificación a partir del momento en que se realizó el estampado"10. Cabe subrayar que de lo contrario las distintas entidades se exponen a que la hora de radicación del trámite no corresponda con la realidad, pues no se podrá garantizar que se utilice la hora oficial del Estado colombiano, dado que la hora puede ser alterada por VPN´s, cambio de zona horaria, software malicioso, errores humanos en materia administrativa, entre otros. Estos riesgos no son menores: De ellos depende, por ejemplo, determinar si un recurso contra un acto administrativo fue interpuesto de forma oportuna o no, lo cual impacta directamente en los derechos fundamentales de los ciudadanos, por lo que es imprescindible que las sedes electrónicas de todas las entidades cuenten con el servicio estampado cronológico, dado que es la única herramienta que permite acreditar la hora real de los trámites y radicados	No aceptada	Se agradece el comentario. De conformidad con el artículo 53 la Ley 1437 de 2011, en las actuaciones realizadas por las autoridades públicas utilizando medios electrónicos, se podrán aplicar las normas de la Ley 527 de 1999 cuando sean compatibles. Corresponde a cada una de las entidades evaluar el nivel de seguridad requerido para cada una de las interacciones de sus usuarios por medios digitales, y establecer de acuerdo a él, el mecanismo de firmas electrónicas, estampa cronologica, notificación electrónica, de gestión documental electrónica y de comunicación cifrada, utilizados.
			9. Niveles de autenticación idóneos Respecto del registro y autenticación de ciudadanos el documento analizado establece que: "d. Las autoridades deberán disponer de mecanismos de consulta del estado del trámite, Otro Procedimiento Administrativo y servicio de consulta de información, 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". Pese a que se habla de registro, autenticación y conservación de documentos, no se indican los estándares de seguridad que se implementarán para garantizar "la debida confianza, seguridad, trazabilidad, calidad y protección de los datos personales", como el proyecto de reglamentación en comento.	No aceptada	Se agradece el comentario. Al respecto, se aclara que no corresponde a esta guía detallar técnicamente o seleccionar un determinado producto para garantizar las condiciones de debida confianza, seguridad, trazabilidad, calidad y protección de los datos personales; sin embargo, a lo largo de la guía se señalan los lineamientos en cada uno de estos sentidos.
			10. Aunque en el numeral 4.2. se establece que las entidades deben "Vincular a los Trámites, Otros Procedimientos Administrativos y servicios de consulta de información que se integren a la sede electrónica, los mecanismos de autenticación digital según el nivel de garantía requerido", se debe aclarar que debido a que en el marco de los trámites los ciudadanos realizan actos de importante trascendencia jurídica, como aquellos de disposición del derecho (piénsese, por ejemplo en la aceptación de una sanción administrativa) en la regulación de las sedes electrónicas se debe establecer, por lo menos, que el grado mínimo de garantía es el Medio, -siendo obligatorio que en el proceso de autenticación se realice la consulta de los datos del usuario frente a las bases de datos biográficas de la Registraduría Nacional del Estado Civil- y que, de preferencia, se utilizarán mecanismos de autenticación con niveles de garantía Alto o Muy Alto, dependiendo del trámite. También es importante aclarar que la entidad deberá realizar el análisis de niveles de garantía dependiendo del trámite, de tal forma que si bien puede haber un único canal de peticiones, para determinados procedimientos que sean calificados como de mayor riesgo la entidad debe fijar niveles de garantía más altos.	No aceptada	Se agradece el comentario. No obstante, se aclara que corresponde a cada una de las entidades evaluar el nivel de seguridad requerido para cada una de las interacciones de sus usuarios por medios digitales, y establecer de acuerdo a él, el mecanismo de autenticación digital a utilizar
			11. Conservación de documentos electrónicos En materia de documentos y expediente electrónico el documento bajo análisis estipuló lo siguiente: "Los tramites, OPAs y servicios de consulta de información 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)".	No aceptada	Agradecemos su comentario. Al respecto, informamos que el Archivo General de la Nación, ha precisado que las autoridades deben adoptar un programa de gestión documental que contemple todos los soportes de información, conforme lo dispone el Decreto 1080 del 2015, o el que lo modifique, adicione o subrogue.

			12. En el mismo sentido, se señala respecto de la 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 servicios de consulta de información 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". Al respecto, dentro del Anexo 1 se debe señalar que si bien la reglamentación de la gestión documental la realiza el Archivo General de la Nación, los criterios de autenticidad, fiabilidad, integridad y disponibilidad se deberán garantizar aplicando, entre otras cosas, el estampado cronológico respecto de cada actuación del expediente, las firmas electrónicas y/o digitales de los funcionarios que intervienen en el expediente, la firma digital del índice del expediente electrónico y la preservación a largo plazo de documentos electrónicos por parte de software especializado para el efecto.	No aceptada	Agradecemos su comentario. Al respecto, informamos que el Archivo General de la Nación, ha precisado que las autoridades deben adoptar un programa de gestión documental que contemple todos los soportes de información, conforme lo dispone el Decreto 1080 del 2015, o el que lo modifique, adicione o subrogue.
			13. Además de ello el Ministerio de Tecnologías de la Información y las Comunicaciones, en conjunto con el Archivo General de la Nación, destacaron los siguientes instrumentos tecnológicos para dar autenticidad a los documentos electrónicos: a) "Estampas de tiempo: Consiste en una secuencia de caracteres utilizada para certificar el momento específico en que se lleva a cabo un suceso sobre un documento electrónico o que éste no ha sido modificado en un espacio de tiempo determinado. La secuencia de caracteres está relacionada con la fecha y hora exacta en que ocurre dicho evento y específicamente cuando fue creado o firmado en un sistema de cómputo. Mediante la emisión de una estampa de tiempo es posible garantizar el instante de creación, modificación, recepción, firma, etc., de un determinado mensaje de datos impidiendo su posterior alteración, haciendo uso de la hora legal colombiana. b) Firmas electrónicas: Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.	No aceptada	Se agradece el comentario. De conformidad con el artículo 53 la Ley 1437 de 2011, en las actuaciones realizadas por las autoridades públicas utilizando medios electrónicos, se podrán aplicar las normas de la Ley 527 de 1999 cuando sean compatibles.
			14. Notificaciones por medio de correo electrónico certificado Al hablar de Notificaciones el Anexo expresa que: "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". Empero, debido a los efectos jurídicos de una notificación, el Ministerio no puede permitir que se utilice cualquier mecanismo para realizar notificaciones, sino que las mismas deben realizarse por medios de alta confiabilidad y que garanticen el no repudio, como lo permite el correo electrónico certificado. De lo contrario las entidades se verán desbordadas por las nulidades, procesos contenciosos administrativos y acciones de tutela derivadas de indebidas notificaciones a los administrados. Respecto de este punto, es pertinente reseñar la preponderancia del acto de notificación en el procedimiento administrativo, el cual trasciende de un mero acto formal y procesal, como lo ha	No aceptada	Se agradece el comentario, respecto del cual se aclara que corresponde a cada una de las entidades evaluar el nivel de seguridad requerido para cada una de las interacciones de sus usuarios por medios digitales, y establecer de acuerdo a él, el mecanismo de notificación electrónica utilizado.
			15. RADICACIÓN DE PQRS Se debe señalar que al radicar las peticiones el ciudadano podrá: a) Radicarlas de forma anónima16 y b) Cargar más de un archivo. También es conveniente que se regule lo referente al tamaño máximo de los archivos, dado que hay entidades que solamente permiten archivos con tamaño reducido, obligando al ciudadano a acudir a trámites presenciales. Además, la entidad deberá habilitar canales digitales para poder recibir válidamente y por medios electrónicos archivos de audio y video.	Aceptada	Se agradece el comentario. En lo que respeecta a la radicación de forma anónima, se incluirá una nota en la que se especique lo siguente: "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, 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 entidade sigue los lineamientos de anonimización de datos emitidos por el Archivo General de la Nación". De otro lado, se incluirá una nota aclaratoria en la que se señale que "Para el cargue de más de un archivo, las autoridades no podrán establecer restricciones técnicas

			16. PUBLICACIÓN DE NORMATIVA Además de los requisitos contenidos en el Anexo, en el acápite de “Normativa” de la sede electrónica se debe exigir que las entidades señalen si las normas se encuentran vigentes o no, así como las derogatorias tácitas o expresas de la misma, dado que ellos es fundamental para informarle al ciudadano el marco normativo con base en el cual se regirán sus trámites. Así mismo, ello es necesario para cumplir con los deberes establecidos en el numeral 4.3.6 “Calidad de información”, donde se señala que la información debe ser actualizada, escrita en lenguaje claro, veraz, completa y oportuna.	Aceptada	Los lineamientos sobre estandarización de contenidos se establecen por medio de Resolución 1519 del 2020, en el anexo 2 sobre Estándares de Publicación de Información y de conformidad con la competencia otorgada al MinTIC en el Decreto 1081 del 2015. El cumplimiento del principio de calidad de la información, se cumple bajo los estándares de publicación de normativa, así referida en la Resolución: 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	
4	12/11/2020		1. Establecer específicamente, cuál es el procedimiento que el ciudadano debe adelantar en los casos en que las ventanillas únicas tengan problemas técnicos. Especialmente lo referente a los plazos o la necesidad de radicar algún documento particular.	No aceptada	Se agradece el comentarios, respecto del cual se aclara que el procedimiento relacionado con plazos y procedimientos se somete a los términos del Código de Procedimiento	
			2. Especificar los mecanismos de seguimiento virtual a los trámites radicados en las ventanillas únicas.	No aceptada	Se agradece el comentarios, respecto del cual se informa que el lineamiento establece una obligación para todas las autoridades cuenten con una opción de seguimiento de trámites, y de PQRSD. Es importante aclarar, que todo tipo de procedimiento interno respecto del seguimiento de trámites será de libre configuración por cada entidad pública. Cada trámite tiene un identificador y se encuentra asociado a un usuario, a través de la plataforma el usuario podra hacer seguimiento a cada uno de los trámites que se encuentren en curso. Así mismo por diposición del Art. del Decreto 620 de 2020 para el Registro de documentos electrónicos los sujetos señalados en el artículo 2.2.17.1.2. de este Decreto deberán	
			3. Incluir en la resolución los mecanismos de autenticación y validación de la autenticación digital, para que los ciudadanos puedan acceder a las ventanillas únicas y a la sede electrónica.	No aceptada	Se agradece el comentario, respecto del cual se aclara que los mecanismos de autenticación digital están definidos en la guía de lineamientos de los Servicios Ciudadanos Digitales	
			4. Considerar mecanismos utilizados para garantizar la protección de la información del usuario y carpetas ciudadanas.	No aceptada	La circular en comento tiene como propósito instruir las obligaciones establecidas en el Régimen de Protección de los Derechos de los Usuarios de Servicios de Comunicaciones expedido por la Comisión de Regulación de Comunicaciones, cuyo cumplimiento corresponde a los operadores de dichos servicios. Las instrucciones impartidas, garantizan los principios orientadores del Régimen de Protección de los Derechos de los Usuarios de Servicios de Comunicaciones, y en todo caso protegen los derechos de los usuarios de dichos servicios, en el ofrecimiento de éstos, en la celebración de los contratos, durante su ejecución y en la terminación del mismo. Por disposición del art. 53 de la Ley 1437 de 2011 (...) "Los procedimientos y trámites administrativos podrán realizarse a	
			5. Considerar interoperabilidad con todas las entidades del Estado, en concordancia con lo establecido en el Decreto 620 del 2 de mayo de 2020 en su ARTÍCULO 2.2.17.1.2.	No aceptada	Se agradece el comentario, respecto del cual se aclara que la obligación de interoperar se encuentra presente en el Decreto 620 del 2 de mayo de 2020 y por lo tanto no es necesario	José Ricardo Aponte
			6. Considerar condicionantes y temporalidad, para que las entidades del Estado logren los diferentes niveles de transformación digital en favor de la efectiva prestación de los servicios ciudadanos digitales.	No aceptada	Se agradece el comentario, respecto del cual se aclara que el Artículo 2.2.17.7.1. Gradualidad del decreto 620 de 2020, define los plazos en los cuales las entidades deberán implementar los servicios ciudadanos digitales y la sede electrónica conforme a los lineamientos dados.	José Ricardo Aponte
4		**TIGO**	1. Establecer específicamente cuál es el procedimiento que el ciudadano debe adelantar en los casos en que las ventanillas únicas tengan problemas técnicos. Especialmente lo referente a los plazos o la necesidad de radicar algún documento particular.	No aceptada	Se agradece el comentarios, respecto del cual se aclara que el procedimiento relacionado con plazos y procedimientos se somete a los términos del Código de Procedimiento	
			2. Especificar cómo el ciudadano le podrá hacer un seguimiento virtual a los trámites radicados en las ventanillas únicas. Aun cuando los lineamientos respecto del funcionamiento de la sede electrónica, las ventanillas únicas y del Portal Único del Estado Colombiano están consignados en su documento técnico de soporte al proyecto de acto administrativo, es necesario que esto quede expresamente descrito en la resolución propiamente dicha.	No aceptada	Se agradece el comentarios, respecto del cual se informa que el lineamiento establece una obligación para todas las autoridades cuenten con una opción de seguimiento de trámites, y de PQRSD. Es importante aclarar, que todo tipo de procedimiento interno respecto del seguimiento de trámites	
			3. Se hace necesario incluir en la resolución los mecanismos de autenticación y validación de la autenticación digital para que los ciudadanos puedan acceder a las ventanillas únicas y a la sede electrónica. Actualmente, empresas como la nuestra, para servicios de ventas o reposición de chip, con el fin de evitar acciones de fraude, realiza de manera presencial validaciones biométricas, por lo tanto, es una necesidad latente que las sedes electrónicas garanticen mecanismos de validación de identidad.	No aceptada	Se agradece el comentario, respecto del cual se aclara que los mecanismos de autenticación digital están definidos en la guía de lineamientos de los Servicios Ciudadanos Digitales expedidas mediante la resolución número 2160 de 23 de octubre de 2020. Considerando lo anterior, no hace parte del alcance de esta guía definir dichos mecanismos.	

	14/08/2020		4. Recomendamos que, a través del Portal Único del Estado, se incluyan elementos de protección de la información del usuario y carpetas ciudadanas, eliminando la obligatoriedad de que empresas, como las de telecomunicaciones, deban contar con información física en sus tiendas de servicio en cumplimiento a la Circular Única de la Superintendencia de Industria y Comercio Título III Capítulo Primero Numeral 1.2.1.1 Oficinas físicas de atención al usuario.	No aceptada	Agradecemos su comentario, al respecto aclaramos que el presente lineamiento es de obligatorio cumplimiento para las autoridades, sin perjuicio del cumplimiento de obligaciones regulatorias escíficas que le apliquen, en especial, a las contempladas en el régimen de protección de usuarios y las instrucciones correspondientes desarrolladas por la SIC.
			5. Incluir en el Portal Único del Estado una carpeta ciudadana donde la DIAN pueda acceder a consultar toda la documentación aduanera y del estatuto tributario nacional referente a facturas, registro de importación, certificados de origen, documento de transporte, certificación de fletes, declaración de importación, entre otros documentos, que actualmente son exigibles de custodia de manera física y durante cinco (5) años a los PRST.	No aceptada	Se agradece el comentario. Al respecto, se aclara que el objetivo de estas guías es establecer lineamientos generales para todas las autoridades. Por lo anterior, no se acepta el comentario.
			7. Permitir que las solicitudes ante las entidades del Estado para el otorgamiento de licencias de construcción de estructuras en el despliegue de red, sean incluidas en este modelo de servicios digitales.	No aceptada	Se agradece el comentario. Al respecto, se aclara que el objetivo de estas guías es establecer lineamientos generales para todas las autoridades. Por lo anterior, no se acepta el comentario.
			7. Incluir en estas sedes electrónicas servicios de radicación de solicitudes para modificación y cancelación de redes de microondas; para lo cual se sugiere la creación de expedientes o carpetas ciudadanas por entidades, de manera tal que los diferentes usuarios podamos acceder y consultar el estado de los trámites y licencias de microondas otorgados.	No aceptada	Se agradece el comentario. Al respecto, se aclara que el objetivo de estas guías es establecer lineamientos generales para todas las autoridades. Por lo anterior, no se acepta el comentario.
			8. Disponer una alternativa dentro de los proyectos de interoperabilidad y autenticación digital, que facilite el pago de impuestos territoriales (estampillas e industria y comercio), de manera centralizada y en línea, bajo formatos únicos y armonizados.	No aceptada	Se agradece el comentario. Al respecto, se aclara que el objetivo de estas guías es establecer lineamientos generales para todas las autoridades. Por lo anterior, no se acepta el
			9. Finalmente, si bien se habla de la interoperabilidad del Portal Único y las páginas web de las entidades estatales; bajo las disposiciones actuales, queda un vacío respecto a cómo se deberán seguir realizando los trámites ante las diferentes entidades, es decir, cuáles se gestionarán de manera exclusiva a través del Portal Único y cuáles, continuarán tramitándose ante las plataformas de cada entidad. Por lo tanto, se recomienda al MinTIC incluir menciones específicas a este asunto en la regulación definitiva, así como realizar un ejercicio de socialización sobre el relacionamiento de la ciudadanía con estos medios virtuales, así como de apropiación social para el buen manejo de los servicios digitales del Estado.	No aceptada	Agradecemos su comentario. Sobre el particular se aclara que cualquier usuario puede acceder a los trámites a través del Portal Único del Estado Colombiano GOV.CO así como a través de la sección de atención y servicio a la ciudadanía habilitada en la sede electrónica de cada autoridad, conforme los lineamientos establecidaos en estas guías por el MinTIC. Respecto de su solicitud de socialización de la nueva Resolución, Le informamos que la Dirección de Gobierno

5	14/08/2020	**CÁMARA DE COMERCIO COLOMBO AMERICANA**	1. Sobre el mercado de derechos de autro y derechos conexos, menciona que en el país existen distorsiones como consecuencia de cobros discriinatorios y desporporcionados por parte de alguna de las Sociedades de Gestión Colectiva, dado que conforme con el artícul 2.6.1.2.7 ddel Decreto 1066 del 2015 las tarifas deben ser proporcionales. Propone la creación de una Ventanilla única para el racaudo de remuneraciones por los usos de derechos de autor y derechos conexos.	No aceptada	Las competencias del MinTIC están dadas por la Ley 1341 del 2009, modificada por la Ley 1978 del 2019, que tiene como objetivos principales los siguientes: 1. Diseñar, formular, adoptar y promover las políticas, planes, pro-gramas y proyectos del sector de Tecnologías de la Información y las Comunicaciones, en correspondencia con la Constitución Política y la Ley, con el fin de promover la
			2. Se propone que el MinTIC considere también las siguientes recomendaciones: - Habilitar la negociación sectorial de criterios paramétricos en la fijación de tarifas. - Desarrollo de un marco normativo que compendie la protección de la competencia y los derechos de autor.	No aceptada	En línea con la respuesta anterior, conforme con la Ley 1341 del 2009 y la Ley 1978 del 2019, el MinTIC no cuenta con competencias para determinar políticas o regulación en materia de derechos de autor y conexos, por lo que se invita a
			1. Frente al numeral 4.2 relativo a "Arquitectura de referencia de la sede electronica" del Anexo 1, en lo que respecto al concepto de Notificaciones previsto en el literal m), dado que las entidades publicas deberan contar con las pruebas documentales de la respuesta a las notificaciones remitidas por correo electronico, se sugiere de manera respetuosa, que dichas entidades tengan la posibilidad de hacer uso de herramientas tecnologicas robustas como el correo electronico certificado. Lo anterior debido a que este tipo de herramientas tecnologicas verdaderamente permiten asegurar la recepcion de la notificacion electronica, para lo cual cuentan con toda la trazabilidad tecnica del intercambio de mensaje de datos, y permiten la generacion de los acuses de envio y recibo sobre el mensaje de datos. El correo electronico certificado es un mecanismo tecnologico que de conformidad a la normativa vigente, se considera el equivalente funcional de un correo fisico certificado, siendo asi que cuenta con la misma validez juridica y probatoria de este ultimo. Adicionalmente, aporta seguridad juridica, tecnica e integra funcionalidades que optimizan la administracion. Es de anotar que la Ley 527 de 1999 es el marco normativo que permite la implementacion de mecanismos como el mencionado, siendo asi que el objetivo de este es garantizar la integridad y trazabilidad de un mensaje enviado a traves de correo electronico, por un remitente a un destinatario, mediante la certificacion de la recepcion de los mensajes por medio del acuse de recibo, documento se estampa cronologicamente.	No aceptada	Se agradece el comentario. De conformidad con el artículo 53 la Ley 1437 de 2011, en las actuaciones realizadas por las autoridades públicas utilizando medios electrónicos, se podrán aplicar las normas de la Ley 527 de 1999 cuando sean compatibles. En este orden no es objeto de la presente resolución incorporar normas y disposiciones existentes. Corresponde a cada una de las entidades evaluar el nivel de seguridad requerido para cada una de las interacciones de sus usuarios por medios digitales, y establecer de acuerdo a él, los mecanismos de certificación del correo electrónico, estampado cronológico y de firma electrónica.
			2. En los anexos 1, 2, 3 y 4 del Proyecto de Resolucion de la referencia, se establece que las ventanillas unicas digitales deberan contar con unos estandares minimos de seguridad para integrarse al Portal Unico del Estado colombiano - GOV.CO, como lo son: (a) Implementar un certificado SSL con validacion de organizacion, 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. Al respecto, se sugiere de manera respetuosa a la entidad, que se defina dentro de los anexos en mencion que conforman el proyecto, un certificado de servidor seguro SSL robusto, adecuado y suficiente desde el punto de vista de seguridad, para las sedes electronicas. Precisamente, resulta importante modificar el nivel de seguridad minimo a certificados SSL con validacion extendida, toda vez que son los unicos que permiten garantizar plenamente la debida confianza, seguridad y calidad requeridas en distintos numerales del documento. Adicionalmente, dichos certificados blindan el portal institucional contra posibles ataques de suplantacion de sitio o phishing, ademas que hoy en dia se han convertido en el estandar minimo de seguridad para portales transaccionales. Lo anterior, resulta relevante subrayarlo, ya que no es suficiente contar con cualquier certificado de servidor seguro (tecnologia SSL), sino con el que realmente sea idoneo y adecuado para el tipo de portal web y transacciones que sean llevadas a cabo en el mismo. Particularmente, en la actualidad existen tres (3) tipos de certificados SSL que otorgan distintos niveles de seguridad, siendo los de modalidad VE los unicos que permiten mitigar el riesgo de suplantacion o phishing. Al respecto, es de anotar que el uso de servidores seguros se convierte en un elemento imprescindible en todos aquellos servicios que utilicen informacion confidencial, como operaciones bancarias en linea, compras por Internet, acceso a servidores de datos sensibles, entre otros	No aceptada	Se agradece el comentario. Al respecto, se aclara en el texto del documento incluyendo lo siguiente: "Las entidades deberán 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. Lo anterior, además de los controles suficientes y adecuados dispuestos por la autoridad a partir del análisis de riesgos y controles que ésta determine."

Harley Roldán

	11/11/2020		3. En el numeral 4.1 denominado “contenido y estructura de informacion de la sede electronica” del Anexo 1 del proyecto de Resolucion, se senala que todas las autoridades deberan adecuar su sede electronica de manera que esta ultima cuente con los siguientes requisitos y gestiones, tales como: “4. Enviar automaticamente por el mismo medio un mensaje acusando el recibo y registro de las peticiones, escritos o documentos de que se trate, en el que constaran los datos proporcionados por los ciudadanos, la fecha y hora de presentacion y el numero consecutivo de radicacion asignado”. Al respecto, consideramos pertinente hacer una mencion a la Ley 527 de 1999, toda vez que esta ultima consagra el uso de los mensaje de datos, dentro de los cuales se encuentran inmersos los correos electronicos, asi como establece la validez juridica y la admisibilidad probatoria que dichos mensajes deben recibir en el entorno digital, ello de conformidad con los articulos de la citada ley. De igual forma, consideramos apropiado que dentro de este punto se especifique que el mensaje que se genere debe enviarse cumpliendo los lineamientos senalados en los articulos 20 y 21 de la citada ley. En cuanto al envio de mensajes de datos es importante hacer una reflexion, encaminada a que los correos electronicos desde los cuales se emitan dichos mensajes y que se generen los acuses correspondientes, deben estar provistos de una mayor seguridad de la que brindan los correos electronicos de uso tradicional. Al respecto, la Agencia Espanola de Proteccion de Datos (AEPD) y el Instituto Nacional de Ciberseguridad (INCIBE) en su reciente informe denominado “Privacidad y Seguridad en Internet”, senalan que se pueden presentar brechas de seguridad en un correo electronico tradicional. Precisamente, teniendo presente las advertencias que nos hacen estas autoridades de peso en la materia, seria importante que en este punto el Anexo incluya herramientas mas robustas, como los correos electronicos certificados, lo cuales brindan mayor certeza, confianza y seguridad en el envio y recepcion de mensajes de datos, ya que permiten verificar con exactitud la fecha y hora del envio del mensaje, asi como encriptar el intercambio de informacion	No aceptada	Se agradece el comentario. De conformidad con el artículo 53 la Ley 1437 de 2011, en las actuaciones realizadas por las autoridades públicas utilizando medios electrónicos, se podrán aplicar las normas de la Ley 527 de 1999 cuando sean compatibles. En este orden no es objeto de la presente resolución incorporar normas y disposiciones existentes. Corresponde a cada una de las entidades evaluar el nivel de seguridad requerido para cada una de las interacciones de sus usuarios por medios digitales, y establecer de acuerdo a él, el mecanismo de firma electrónica	
			4. En el numeral 4.2. Arquitectura de referencia de la sede electronica se senala lo siguiente: “b) Seguridad: las arquitecturas de solucion deben poseer los compontes que permitan la autorizacion, autenticacion, cifrado de datos, estampado cronologico y firmas electronicas que garanticen la seguridad (integridad, control de acceso, no repudio, entre otros) de todas las funcionalidades y servicios que ofrece la sede electronica. En la zona de seguridad, tambien deben existir conectores para la integracion del servicio ciudadano digital de Autenticacion Digital, cuando este disponible”. En atencion al anterior punto, se sugiere de manera respetuosa, que los anexos tecnicos planteen los diferentes niveles de seguridad que pueden ser requeridos frente a la multiplicidad de tramites que el ciudadano o empresario adelante ante la entidad estatal. Si bien todas las firmas electronicas que cumplan los requisitos de “confiable” y “apropiado” conforme al Decreto 2364 de 2012, son validas juridicamente, no todas gozan del mismo nivel de seguridad que pueda requerir la entidad estatal. En virtud de lo anterior, se hace necesario que se presente una distincion entre los diversos tipos de firmas electronicas de cara a los diferentes niveles de seguridad que estas pueden ofrecer. Al respecto, juridicamente las firmas digitales son el unico mecanismo que tiene consagrado a su favor presunciones legales de autenticidad y no repudio, previstas en el articulo 28 de la Ley 527 de 1999, de las cuales no gozan los demas tipos de firmas electronicas, siendo asi que en los demas casos de firmas electronicas, estas solo garantizan la autenticidad e integridad. En ese sentido, se deberia hacer una precision en el literal citado. Por otra parte, se sugiere tambien de manera respetuosa que los Anexos den claridad frente a la diferencia juridica y tecnica que representan las firmas electronicas simples y firmas electronicas certificadas, las cuales ofrecen niveles de seguridad sustancialmente diferentes y que deberian ser puestos de presente en el proyecto de Resolucion.	No aceptada	Se agradece el comentario. De conformidad con el artículo 53 la Ley 1437 de 2011, en las actuaciones realizadas por las autoridades públicas utilizando medios electrónicos, se podrán aplicar las normas de la Ley 527 de 1999 cuando sean compatibles. En este orden no es objeto de la presente resolución incorporar normas y disposiciones existentes. Corresponde a cada una de las entidades evaluar el nivel de seguridad requerido para cada una de las interacciones de sus usuarios por medios digitales, y establecer de acuerdo a él, el mecanismo de firma electrónica.	
			5. En aras de garantizar la conservacion de documentos electronicos, transacciones y registros, asi como la precision en la fecha de hora de los mismos, se sugiere de manera respetuosa, la utilizacion del estampado cronologico certificado, toda vez que permite, por una parte, dar certeza juridica de la fecha y hora legal, garantizando el precepto de primero en el tiempo, primero en el derecho, y por otra, garantizar la integridad de los datos que se estan estampando, esto a partir del calculo de hash de dicho mensaje de datos. Es de anotar adicionalmente que se trata de un mecanismo tecnologico que se basa en la certificacion digital y por lo tanto, en infraestructuras de clave publica (PKI) acreditadas ante el Organismo Nacional de Acreditacion de Colombia (ONAC), que proporcionan seguridad juridica y tecnologica, de acuerdo con lo establecido por el marco legal colombiano.	No aceptada	Se agradece el comentario. De conformidad con el artículo 53 la Ley 1437 de 2011, en las actuaciones realizadas por las autoridades públicas utilizando medios electrónicos, se podrán aplicar las normas de la Ley 527 de 1999 cuando sean compatibles. Corresponde a cada una de las entidades evaluar el nivel de seguridad requerido para cada una de las interacciones de sus usuarios por medios digitales, y establecer de acuerdo a él, el mecanismo de acuse de recibo, para lo cual se requeriría eventualmente el estampado cronológico (certificado o no certificado, según el caso). Respecto a Entidades habilitadas para ofrecer esos servicios, se realizarán los ajustes conducentes, quedando en el texto que: "... estas herramientas sean provistas por entidades habilitadas por la normativa vigente."	
9		**CÁMARA COLOMBIANA DE**				Harley Roldán

6		**COMERCIO ELECTRÓNICO**	6. Frente a la arquitectura descrita en los Anexos 2, 3 y 4, en relacion con los servicios alli indicados, resulta importante que se de claridad respecto a la implementacion de los mecanismos que alli se indican. Al respecto, dentro de los citados anexos se senala que mecanismos como las estampas cronologicas, firmas digitales, entre otros, son optativos, lo cual genera preocupacion, toda vez que deberian ser de caracter obligatorio dado que blindan juridica y tecnicamente las transacciones electronicas. Lo anterior, teniendo en cuenta que estamos frente a un sistema de interoperabilidad, por lo que no es viable concebir este modelo sin la implementacion obligatoria de este tipo de herramientas tecnologicas que proveen seguridad juridica y electronica.	No aceptada	Se agradece el comentario. De conformidad con el artículo 53 la Ley 1437 de 2011, en las actuaciones realizadas por las autoridades públicas utilizando medios electrónicos, se podrán aplicar las normas de la Ley 527 de 1999 cuando sean compatibles. Se agradece el comentario, respecto del cual se aclara que corresponde a cada una de las entidades evaluar el nivel de seguridad requerido para cada una de las interacciones de sus usuarios por medios digitales, y establecer de acuerdo a él, el mecanismo de firmas electrónicas, estampa cronologica, notificación electrónica, de gestión documental electrónica y de comunicación cifrada utilizados.	Harley Roldán
			"7. Frente a este punto sugerimos incluir en el proyecto de Resolucion y sus anexos, una mencion a la Ley 527 de 1999, ley de comercio electronico, la cual regula y senala los lineamientos para la implementacion de las herramientas tecnologicas senaladas en este proyecto. Sumado a lo anterior y dado que los anexos del proyecto de Resolucion hacen referencia al uso de firmas electronicas, consideramos apropiado dentro del sustento normativo incluir la Ley 527 de 1999 y el Decreto 2364 de 2012, toda vez que este es el marco normativo que rige a este tipo de mecanismos. "	No aceptada	Se agradece el comentario. De conformidad con el artículo 53 la Ley 1437 de 2011, en las actuaciones realizadas por las autoridades públicas utilizando medios electrónicos, se podrán aplicar las normas de la Ley 527 de 1999 cuando sean compatibles. En este orden no es objeto de la presente resolución incorporar normas y disposiciones existentes. Corresponde a cada una de las entidades evaluar el nivel de seguridad requerido para cada una de las interacciones de sus	Marco Sánchez
			1. En los anexos 1, 2, 3 y 4 del Proyecto de Resolución de la referencia, se establece que las ventanillas únicas digitales deberán contar con unos estándares mínimos de seguridad para integrarse al Portal Único del Estado colombiano - GOV.CO, como lo son: (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. Respecto a este punto, consideramos importante dejar definido dentro de los cuatro anexos que conforman el proyecto, un certificado de servidor seguro SSL robusto, adecuado y suficiente desde el punto de vista de seguridad, para las sedes electrónicas. Lo anterior, debido a que en la actualidad existen tres (3) tipos de certificados SSL que otorgan distintos niveles de seguridad, siendo los de modalidad VE los únicos que permiten mitigar el riesgo de suplantación o phishing. Al respecto, es de anotar que el uso de servidores seguros es un elemento imprescindible en todos aquellos servicios que utilicen información confidencial, como operaciones bancarias en línea, compras por Internet, acceso a servidores de datos sensibles, entre otros. Reforzando lo anterior, es importante tener en cuenta, como lo ha reconocido el Instituto de Ingeniería Eléctrica y Electrónica -Asociación Mundial de Ingenieros dedicada a la normalización y el desarrollo en áreas técnicas-, que existen diversos tipos de certificados SSL, los cuales se clasifican en virtud del riesgo que se pretende mitigar, a saber: •Certificados SSL de Validación Dominio (VD): nivel de seguridad bajo (se obtienen en seguros, solo se valida la existencia del dominio). •Certificados SSL de Validación de Organización (VO): nivel de seguridad medio (se valida la existencia del dominio y su asociación con el nombre comercial de una empresa legalmente registrada). •Certificados SSL de Validación Extendida (VE): nivel de seguridad alto (se valida la existencia del dominio, su asociación con el nombre comercial de una empresa legalmente registrada y se verifica por un estricto proceso de validación de identidad que la petición de certificado viene de la organización que ha registrado el dominio y que tiene derecho a usar el nombre legal).	No aceptada	Se agradece el comentario. Al respecto, se aclara en el texto del documento incluyendo lo siguiente: "Las entidades deberán 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. Lo anterior, además de los controles suficientes y adecuados dispuestos por la autoridad a partir del análisis de riesgos y controles que ésta determine."	
	14/08/2020		2. En el numeral 4.1 denominado "contenido y estructura de información de la sede electrónica", del Anexo 1 del proyecto de Resolución, se señala que todas las autoridades deberán adecuar su sede electrónica de manera que esta última cuente con los siguientes requisitos y gestiones, tales como: 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. En cuanto a este numeral, consideramos pertinente hacer una mención a la Ley 527 de 1999, toda vez que esta última consagra el uso de los mensajes de datos, dentro de los cuales se encuentran inmersos los correos electrónicos, así como establece la validez jurídica y la admisibilidad probatoria que dichos mensajes deben recibir en el entorno digital, ello de conformidad con los artículos de la citada ley. De igual forma, consideramos apropiado que dentro de este punto se especifique que el mensaje que se genere debe enviarse cumpliendo los lineamientos señalados en los artículos 20 y 21 de la citada ley. En cuanto al envío de mensajes de datos es importante hacer una reflexión, encaminada a que los correos electrónicos desde los cuales se emitan dichos mensajes y que se generen los acuses correspondientes, deben estar provistos de una mayor seguridad de la que brindan los correos electrónicos de uso tradicional. Al respecto, la Agencia Española de Protección de Datos (AEPD) y el Instituto Nacional de Ciberseguridad (INCIBE) en su reciente informe denominado "Privacidad y Seguridad en Internet", señalan que se pueden presentar brechas de seguridad en un correo electrónico tradicional. Precisamente, teniendo presente las advertencias que nos hacen estas autoridades de peso en la materia, sería importante que en este punto el Anexo incluya herramientas más robustas, como los correos electrónicos certificados, lo cuales brindan mayor certeza, confianza y seguridad en el envío y recepción de mensajes de datos, ya que permiten verificar con exactitud la fecha y hora del envío del mensaje, así como encriptar el intercambio de información.	No aceptada	Se agradece el comentario. De conformidad con el artículo 53 la Ley 1437 de 2011, en las actuaciones realizadas por las autoridades públicas utilizando medios electrónicos, se podrán aplicar las normas de la Ley 527 de 1999 cuando sean compatibles. En este orden no es objeto de la presente resolución incorporar normas y disposiciones existentes. Corresponde a cada una de las entidades evaluar el nivel de seguridad requerido para cada una de las interacciones de sus usuarios por medios digitales, y establecer de acuerdo a él, el mecanismo de firma electrónica.	

			3. En el numeral 4.2. Arquitectura de referencia de la sede electrónica se señala lo siguiente: b) Seguridad: las arquitecturas de solución 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. En atención al anterior punto, consideramos importante poner de presente una distinción entre el uso de las firmas digitales y los demás tipos de firmas electrónicas. Al respecto, jurídicamente las firmas digitales son el único mecanismo que tiene consagrado a su favor presunciones legales de autenticidad y no repudio, siendo así que, en los demás casos de firmas electrónicas, estas solo garantizan la autenticidad e integridad. En ese sentido, se debería hacer una precisión en el literal citado. Sumado a lo anterior, los atributos jurídicos que tiene la firma digital, como un tipo de firma electrónica que se encuentra expresamente señalado en la Ley 527 de 1999, constituyen una garantía para que no se desconozca por parte de quien emite el acto o suscribe el documento, la vinculación a su contenido y a la existencia del mismo. Por otra parte, encontramos que en ninguno de los Anexos se hace claridad respecto a las firmas electrónicas simples y firmas electrónicas certificadas, las cuales ofrecen niveles de seguridad sustancialmente diferentes y que deberían ser puestos de presente en el proyecto de Resolución.	No aceptada	Se agradece el comentario. De conformidad con el artículo 53 la Ley 1437 de 2011, en las actuaciones realizadas por las autoridades públicas utilizando medios electrónicos, se podrán aplicar las normas de la Ley 527 de 1999 cuando sean compatibles. En este orden no es objeto de la presente resolución incorporar normas y disposiciones existentes. Corresponde a cada una de las entidades evaluar el nivel de seguridad requerido para cada una de las interacciones de sus usuarios por medios digitales, y establecer de acuerdo a él, el mecanismo de firma electrónica.
			4. El estampado cronológico certificado permite dar certeza jurídica de la fecha y hora legal, garantizando el precepto de primero en el tiempo, primero en el derecho, siendo así que se trata de un mecanismo tecnológico que se basa en la certificación digital y por lo tanto, en infraestructuras de clave pública (PKI) que proporcionan seguridad jurídica y tecnológica, de acuerdo con lo establecido por el marco legal colombiano. En consecuencia, debe mencionarse que esta herramienta sea provista por entidades habilitadas por la normativa vigente.	No aceptada	Se agradece el comentario. De conformidad con el artículo 53 la Ley 1437 de 2011, en las actuaciones realizadas por las autoridades públicas utilizando medios electrónicos, se podrán aplicar las normas de la Ley 527 de 1999 cuando sean compatibles. Corresponde a cada una de las entidades evaluar el nivel de seguridad requerido para cada una de las interacciones de sus usuarios por medios digitales, y establecer de acuerdo a él, el mecanismo de acuse de recibo, para lo cual se requeriría eventualmente el estampado cronológico (certificado o no certificado, según el caso).
			5. Aspectos de arquitectura indicados en los Anexos 2, 3 y 4. Frente a la arquitectura descrita en los Anexos 2, 3 y 4, en relación con los servicios allí indicados, a saber: ▪ Las firmas digitales. ▪ Estampas cronológicas. ▪ Notificaciones Electrónicas. ▪ Gestión documental electrónica ▪ Comunicación cifrada. Resulta importante que se dé claridad respecto a la implementación de los mismos, pues dentro de los citados anexos se indican que son optativos, lo cual genera preocupación, toda vez que deberían ser de carácter obligatorio dado que blindan jurídica y técnicamente las transacciones electrónicas. Lo anterior, teniendo en cuenta que estamos frente a un sistema de interoperabilidad, por lo que no es viable concebir este arquetipo sin la implementación de este tipo de herramientas tecnológicas que proveen seguridad jurídica y electrónica. ▪ Inclusión de normas que regulan la implementación de herramientas tecnológicas. Frente a este punto sugerimos incluir en el proyecto de Resolución y sus anexos, una mención a la Ley 527 de 1999, ley de comercio electrónico y al Decreto 2364 de 2012. Mediante los cuales se señalan los lineamientos para la implementación de las herramientas tecnológicas señaladas en este proyecto, como también en lo que respecta a firmas electrónicas.	No aceptada	Se agradece el comentario. De conformidad con el artículo 53 la Ley 1437 de 2011, en las actuaciones realizadas por las autoridades públicas utilizando medios electrónicos, se podrán aplicar las normas de la Ley 527 de 1999 cuando sean compatibles. Se agradece el comentario, respecto del cual se aclara que corresponde a cada una de las entidades evaluar el nivel de seguridad requerido para cada una de las interacciones de sus usuarios por medios digitales, y establecer de acuerdo a él, el mecanismo de firmas electrónicas, estampa cronologica, notificación electrónica, de gestión documental electrónica y de comunicación cifrada, utilizados.
7	14/08/2020	**ANDI**	1. Tras revisar el alcance del documento puesto en consulta, vemos en este proyecto una oportunidad para reglamentar la creación de una ventanilla única para el recaudo de las remuneraciones por el uso de los derechos de autor, mecanismo que consideramos ideal para corregir algunas de las problemáticas que caracterizan el mercado de derechos de autor en Colombia. Como hemos manifestado en ocasiones anteriores, los usuarios de este mercado (entendidas como todas aquellas industrias que usan las obras protegidas en su cadena de valor para producir otros bienes o servicios y así agregar valor al consumidor final) han sido sujetas de cobros discriminatorios, desproporcionales y poco transparentes que hacen algunas de las Sociedades de Gestión Colectiva (en adelante SGC), desatendiendo la normativa relacionada1. Adicional a lo anterior, y sobre el punto de discriminación de precios, Fedesarrollo (2019)2, advierte que en Colombia: "(…) las SGC establecen las tarifas de referencia y luego se hace una negociación individual con cada usuario. Situación que lleva a la existencia de tarifas diferentes para un mismo repertorio para usuarios de una misma industria. Esto es inusual en comparación a otros mercados de derechos de autor y conexos, en los que la negociación incluye a todos los usuarios de una misma industria, de tal forma que las tarifas negociadas rigen para todos los usuarios comparables. Esta situación, es entonces, la mayor fuente de tensiones entre las SGC y las empresas en Colombia"3	No aceptada	Las competencias del MinTIC están dadas por la Ley 1341 del 2009, modificada por la Ley 1978 del 2019, que tiene como objetivos principales los siguientes: 1. Diseñar, formular, adoptar y promover las políticas, planes, pro-gramas y proyectos del sector de Tecnologías de la Información y las Comunicaciones, en correspondencia con la Constitución Política y la Ley, con el fin de promover la inversión y el cierre de la brecha digital, contribuir al desarrollo económico, social y político de la Nación, y elevar el bienestar de los colombianos. 2. Promover el uso y apropiación de las Tecnologías de la Información y las Comunicaciones entre los ciudadanos, las empresas, el Gobierno y demás instancias nacionales como soporte del desarrollo social, económico y político de la Nación.
			1. El sistema de PQRSD de las entidades del gobierno deben tener un mecanismo ideal sin pedir mail u otra información para que al colocar una PQRSD el ciudadano por vía anónima tenga tranquilidad de su anonimato.	Aceptada	Se agradece el comentario. Al respecto, se incluirá una nota en la que se especique lo siguente: "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

	17/08/2020		2. Es importante que se incluya en las resoluciones que en la web de las entidades de gobierno se informe del modo y los límites de la preservación del anonimato que ofrece, que deben ser explicados detalladamente, para que el denunciante o ciudadano que presenta la PQRSD tenga toda la información necesaria y no pueda ser inducido a error por omisión de información.	Aceptada	Se agradece el comentario. Al respecto, se incluirá una nota en la que se especique lo siguente: "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."
			3. LAS WEB de PQRSD deberían presentar mecanismos de comunicación electrónica que garanticen su acceso a través de navegación y conexión anónimas. Las web deberán informar con indicaciones previas claras y sencillas sobre cómo utilizarlos sin exponer la propia identidad – incluyendo la "identidad electrónica" (Internet Protocol o IP) – y sobre las formas de eliminación de los metadatos para que los documentos no comprometan la anonimidad del ciudadano. Deberán proveer al denunciante o ciudadano anonimo de acuse de recibo con código identificador, que permita el seguimiento de las actuaciones y las comunicaciones sucesivas con el eventual denunciante sin perjudicar su anonimato.	Aceptada	Se agradece el comentario. Al respecto, se incluirá una nota en la que se especique lo siguente: "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."
			1. Mi aporte es que al establecer criterios comunes para las ventanillas únicas digitales tengan en cuenta complementar en los formularios PQRS la opción anónima. La denuncia anónima además de ser un derecho constitucional es una herramienta efectiva anticorrupción, por lo que darle la importancia adecuada vale la pena.	No aceptada	Se agradece el comentario. Al respecto se aclara que conforme a lo dispuesto en la Resolución 1519 de 2020 (que deroga la resolución 3564 de 2015), el formulario de PQRDS deberá permitir el recibo de peticiones de manera anónima. Por lo tanto se entiende incorporado
			2. En el "anexo_2_ 1_guia_diseno_sedes_electronicas" en la página 13: incluir como criterio comun la definición de PQRSD anonima y como minimo las siguientes recomendaciones: -Se garantiza que se borraran los posibles datos que pudieran señalar la identidad del ciudadano anonimo -Se recomienda que los documentos adjuntos no tengan metadatos (informacion del autor ,etc) - Se garantiza que queda inhabilitado el servicio de geolocalización al diligenciar su formulario en la opción anónima -el formulario de PQRS solo envia su mensaje , no nos proporciona informacio adicional como IP o servidor de internet -se sugiere navegar con un software de navegación anonima. -Tenga presente tomar el consecutivo que aparecera al final al enviar la PQRSD - El mecanismo de seguimiento en línea para verificar el estado de la respuesta de la PQRSD anonimas tambien garantiza el anonimato.	Aceptada	Se agradece el comentario. Al respecto, se incluirá una nota en la que se especique lo siguente: "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, 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 entidade sigue los lineamientos de anonimización de datos emitidos por el Archivo General de la
			3. En el "anexo_2_1_guia_diseno_sedes_electronicas" en la pagina 14 y 15 incluir como criterio comun: -Como aparecería la información, si el ciudadano escoge la opción PQRSD anónima, resaltando que información quedaria inhabilitada, incluyendo nombre, mail ,etc. -Que similar al al pagina sdps.bogota.gov.co siempre aparezca "geolocation error :user denied geolocation" - En este anexo debe aparecer la imagen de como sería el diseño de la web de consulta de pqrsd, y en que se diferenciaria cuando la web es de consulta de seguimiento es de PQRSD anonima.	Aceptada	Se agradece el comentario. Al respecto, se incluirá una nota en los Anexos 1 y 2, dado que es allí donde se establecen los lineamientos sobre temas de estructura y contenido relacionados con PQRSD, mientras que en el Anexo 2.1 se incorporan temas de diseño gráfico. La nota referida anteriormente, que se incluiyrá en el Anexos 1 y 2.1 es la siguente: "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

8	14/08/2020	**Hollman Beltrán**	4. En el anexo_1_lineamientos_generales, 4.1.2.2. Menú Servicios a la ciudadanía, pagina 34 incluir que en este menu debe estar la opcion de pqrsd anonimas con su parametrización que garantice el anonimato tanto en su registro cmo en su consulta.	Aceptada	Se agradece el comentario. Al respecto, se incluirá una nota en la que se especique lo siguente: "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, 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 entidade sigue los lineamientos de anonimización de datos emitidos por el Archivo General de la
			5. En el anexo_1_lineamientos_generales 4.4.1.1. Requisitos mínimos pagina 52 y 53 incluir la descripción de pqrsd anonima y las particularidades en el formulario de este tipo de PQRSD	Aceptada	Se agradece el comentario. Al respecto, se incluirá una nota en la que se especique lo siguente: "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, 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 entidade sigue los lineamientos de anonimización de datos emitidos por el Archivo General de la
			6. En el anexo_1_lineamientos_generales 4.5.2. Requisitos mínimos para los portales de programas transversales del estado incluir en el numeral c , la responsabilidad de gestion de pqrsd anonimo y de garantizar que el tratamiento de datos perosnales sea acorde a este tipo de denuncia al igual que el mecanismo de seguimiento en línea para verificar el estado de la respuesta de la PQRSD anonimas tambien garantiza anonimato.	Aceptada	Se agradece el comentario. Al respecto, se incluirá una nota en la que se especique lo siguente: "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, 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 entidade sigue los lineamientos de anonimización de datos emitidos por el Archivo General de la
			7. Mi aporte es que tengan en cuenta criterios tecnicos y practicos en los formularios PQRS en la opción anónima que es una herramienta eficaz anticorrupción que vale la pena promover en toda la normatividad y publicidad del MINTIC. 1) en el anexo_2_estandares_publicacion_divulgacion, pagina 3, 3.Requisitos mínimos de políticas y cumplimiento legal. se incluya que se va a garantizar que se borraran los posibles datos que pudieran señalar la identidad del ciudadano anonimo que diligencie el formulario de pqrs	Aceptada	Se agradece el comentario. Al respecto, se incluirá una nota en la que se especique lo siguente: "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, 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 entidade sigue los lineamientos de anonimización de datos emitidos por el Archivo General de la
			8. en el anexo_2_estandares_publicacion_divulgacion,Condiciones de acceso a la información: pagina 18, incluir el concepto y lineamientos de manejo de pqrsd anonimas	Aceptada	Se agradece el comentario. Al respecto, se incluirá una nota en la que se especique lo siguente: "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, 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 entidade sigue los lineamientos de anonimización de datos emitidos por el Archivo General de la

			9. en el anexo_2_estandares_publicacion_divulgacion, pagina 19, "queja anónima", colcoar que se publique obligatoriamente las garantias de seguridad a denucias anonimas, entre otras: - Se garantiza que se borraran los posibles datos que pudieran señalar la identidad del ciudadano anonimo -Se recomienda que los documentos adjuntos no tengan metadatos (informacion del autor ,etc) - Se garantiza que queda inhabilitado el servicio de geolocalización al diligenciar su formulario en la opción anónima -el formulario de PQRS solo envia su mensaje , no nos proporciona informacio adicional como IP o servidor de internet -se sugiere navegar con un software de navegación anonima. -Tenga presente tomar el consecutivo que aparecera al final al enviar la PQRSD - El mecanismo de seguimiento en línea para verificar el estado de la respuesta de la PQRSD anonimas tambien garantiza el anonimato.	Aceptada	Se agradece el comentario. Al respecto, se incluirá una nota en la que se especique lo siguente: "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, 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 entidade sigue los lineamientos de anonimización de datos emitidos por el Archivo General de la
			10. en el anexo_2_estandares_publicacion_divulgacion, pagina 20, "Aviso de aceptación de condiciones", incluir las garantías a las pqrsd anónimas tanto en su registro como en su consulta.	Aceptada	Se agradece el comentario. Al respecto, se incluirá una nota en la que se especique lo siguente: "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, 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 entidade sigue los lineamientos de anonimización de datos emitidos por el Archivo General de la
			11. en el anexo_3_condiciones_minimas_tecnicas_seguridad_digital, incluir la parametrización para garantizar seguridad a las pqrsd anonimas.entre otras: -eliminar la geolocalización similar a similar al al pagina sdps.bogota.gov.co - inhabilitar la recopilación de métricas como las de google analytics -garantizar que se borraran los posibles datos que pudieran señalar la identidad del ciudadano en menos de 2 horas - garantizar técnicamente que el formulario de PQRS solo envia su mensaje , no proporciona informacio adicional como IP o servidor de internet - garantizar técnicamente que el mecanismo de seguimiento en línea para verificar el estado de la respuesta de la PQRSD anonimas tambien garantiza anonimato, (ip, geolocalización, recopilación de métricas, etc)	Aceptada	Se agradece el comentario. Al respecto, se incluirá una nota en la que se especique lo siguente: "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, 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 entidade sigue los lineamientos de anonimización de datos emitidos por el Archivo General de la
9	14/08/2020	**ANDESCO**	Desde ANDESCO, vemos en este proyecto una oportunidad para reglamentar la creación de una ventanilla única para el recaudo de las remuneraciones por el uso de los derechos de autor, mecanismo que consideramos ideal para corregir algunas de las problemáticas que caracterizan el mercado de derechos de autor en Colombia. Como hemos manifestado en ocasiones anteriores, los usuarios de este mercado (entendidas como todas aquellas industrias que usan las obras protegidas en su cadena de valor para producir otros bienes o servicios y así agregar valor al consumidor final) han sido sujetas de cobros discriminatorios, desproporcionales y pocos transparentes que hacen algunas de las Sociedades de Gestión Colectiva (en adelante SGC), desatendiendo entonces la normativa relacionada1. Adicional a lo anterior, y sobre el punto de discriminación de precios, Fedesarrollo (2019)2, advierte que en Colombia: "(…) las SGC establecen las tarifas de referencia y luego se hace una negociación individual con cada usuario. Situación que lleva a la existencia de tarifas diferentes para un mismo repertorio para usuarios de una misma industria. Esto es inusual en comparación a otros mercados de derechos de autor y conexos, en los que la negociación incluye a todos los usuarios de una misma industria, de tal forma que las tarifas negociadas rigen para todos los usuarios comparables. Esta situación, es entonces, la mayor fuente de tensiones entre las SGC y las empresas en Colombia" 3	No aceptada	Las competencias del MinTIC están dadas por la Ley 1341 del 2009, modificada por la Ley 1978 del 2019, que tiene como objetivos principales los siguientes: 1. Diseñar, formular, adoptar y promover las políticas, planes, pro-gramas y proyectos del sector de Tecnologías de la Información y las Comunicaciones, en correspondencia con la Constitución Política y la Ley, con el fin de promover la inversión y el cierre de la brecha digital, contribuir al desarrollo económico, social y político de la Nación, y elevar el bienestar de los colombianos. 2. Promover el uso y apropiación de las Tecnologías de la Información y las Comunicaciones entre los ciudadanos, las empresas, el Gobierno y demás instancias nacionales como soporte del desarrollo social, económico y político de la Nación.
			1. Accesibilidad, pagina 39. Sugiero mencionar en el primer párrafo que las condiciones de contenido y disponibilidad están contenidas en la ley 1712, el marco regulatorio y la actualización de la resolución 3564 y no reiterar información con el riesgo de mencionar menos que en la resolución.	Aceptada	Agradecemos su comentario, respecto de los temas de accesibilidad, las disposiciones se encuentran sincronizadas con el contenido de las Directrices de Accesibilidad Web, no obstante se hará la claridad que las entidades deben cumplir las disposiciones de la Directriz, sin perjuicio de los requisitos específicos que pueda referir la Guía.

			2. Seguridad, pagina 42. Sugiero mencionar en el primer párrafo que las condiciones de contenido y disponibilidad están contenidas en la ley 1712, el marco regulatorio y la actualización de la resolución 3564 y no reiterar información con el riesgo de mencionar menos que en la resolución.	Aceptada	Agradecemos el comentario, se realizará la aclaración al inicio del texto
			3. Calidad, pagina 42. Sugiero mencionar en el primer párrafo que las condiciones de calidad de información están contenidas en la ley 1712, el marco regulatorio y la actualización de la resolución 3564 y no reiterar información con el riesgo de mencionar menos que en la resolución.	Aceptada	Agradecemos el comentario, se realizará la aclaración al inicio del texto
			4. Anexo 2: Guía técnica de integración de sedes electrónicas al portal único del Estado colombiano - gov.co 1.Frente a los Atributos de calidad mínimos de la sede electrónica, revisar y acoger los comentarios dados en el anexo 1 donde se señala que con mayor especificidad se aborda la temática en los anexos de la resolución de transparencia que Min TIC sacará pronto, por lo que abordar información con diferente grado de especificidad en diferentes documentos expedidos por una misma entidad es poco estratégico para facilitar la implementación y comprensión por parte de las entidades.	Aceptada	Agradecemos el comentario, se realizará la precisión para asegurar el debido cumplimiento de la Resolución 1519 del 2020
			5. Sobre la definición de servicio de consulta de información, teniendo en cuenta la reunión efectuada el 11 de agosto, se solicita ajustar a Consultas de acceso a información pública: Información contenida en bases de datos o repositorios digitales. relacionada a procesos misionales de las autoridades a la cual pueden acceder la ciudadanía de manera digital, inmediata y gratuita para el ejercicio de un derecho, una actividad u obligación.	Aceptada	Se agradece el comentario y se harán los ajustes correspondinentes

6. En el numeral 4.1.3 Barra inferior, se establece que en la ventanilla única se presenten datos de contacto entre ellos el correo de notificaciones judiciales, esta obligación no debería establecerse dado que este buzón será de obligatorio cumplimiento en la sede electrónica de la entidad y no de la ventanilla como tal. Las notificaciones judiciales se efectúan ante entidades no ante la ventanilla.	Aceptada	Gracias por el comentario, estamos de acuerdo y se realizará el ajuste.
7. Es necesario precisar que toda la información que se solicita esté incorporada hace referencia a las ventanillas y su propósito, por la redacción general, se puede confundir que la información corresponde a la entidad que lidera la ventanilla.	Aceptada	Gracias por el comentario, estamos de acuerdo, se revisara y se realizará el ajuste en lo pertinente.
8. Numeral 4.1.3 se indica que cuando la autoridad tenga más de una dirección física. Es necesario precisar que se habla de la autoridad que lidera la ventanilla única y que tiene integrada la ventanilla en su sede electrónica.	Aceptada	Gracias por el comentario, estamos de acuerdo, se revisara y se realizará el ajuste en lo pertinente.
9. Sobre numeral 4.1.4 de contenidos mínimos, se sugiere simplificar la cantidad de botones en el menú superior o menú principal. Actualmente se contemplan los siguientes: 1. Información de la ventanilla, 2. Entidades participantes, 3. Servicios a la ciudadanía, 4. Noticias, 5. Ayuda. 6. Contáctenos. La Propuesta sería integrar las entidades participantes en la información de la ventanilla, eliminar el botón obligatorio de noticias, y renombrar los botones así: 1. Información de la ventanilla, 2. Oferta de trámites 3. Contáctenos y 4. Ayuda. A continuación los contenidos dentro de cada botón: oInformación de la ventanilla: ¿qué es?, ¿cuál es el propósito?, ¿a quién está dirigida?, normatividad, entidades participantes indicando que tramites de la ventanilla gestiona cada una. oOferta de trámites: listado de trámites que se pueden gestionar en la ventanilla, descripción de estos trámites, información sobre las cadenas de trámites que se gestionan en la ventanilla, tiempos, tarifas y el acceso a la parte transaccional de esos trámites. oContáctenos: incluir allí los canales de atención que la entidad líder tiene a disposición de la operación y trámites de la ventanilla única, enlace al botón de PQRD de la entidad líder de la ventanilla única. oAyuda: manuales, videos, tutoriales, preguntas frecuentes.	No aceptada	Agradecemos el comentario, no obstante no es posible acogerla. Para la definición de los menú se tuvo en cuenta los contenidos actuales y los mínimos requeridos por la ciudadanía, para lo cual, así quedó estipulado.

			10. Anexo 3.1 Guía de diseño gráfico de ventanillas 1.Se sugiere que la imagen de la página 1 sea más aterrizado a lo que sería una ventanilla ya integrada en una sede electrónica de una entidad para ver como juegan los top bar de ambas cosas, incluso hacer el ejemplo con una ventanilla existente	Aceptada	Gracias por el comentario, estamos de acuerdo, se revisara y se realizará el ajuste en lo pertinente.
			11. Página 4. revisar si toda la información de contacto aplica para ventanillas. Revisar comentario 7 sobre el Anexo.	Aceptada	Gracias por el comentario, estamos de acuerdo, se revisara y se realizará el ajuste en lo pertinente.
			12. Dentro del literal e) del numeral 4.1.1. dispone que se cumplan los lineamientos técnicos para publicar contenidos, pero no se señala cuáles son los lineamientos o donde se pueden encontrar.	Aceptada	Gracias por el comentario, los lineamientos para publicar contenidos están referidos en el numeral 4.1.2, se precisará el término.
			13. Numeral 4.2 En la imagen que aparece en la página 21, los menús destacados son: i) Información PPT , ii) Noticias, iii) Contenidos e información, iv) Ayuda, v) servicios a la ciudadania. No es clara la sigla de PPT y no corresponde a los contenidos mínimos de los capítulos anteriores.	Aceptada	Gracias por el comentario, se aclarará la sigla PPT.

10	6/05/2020	**DAFP**	14. Numeral 4.3.2.7: Se habla de información en lenguaje claro. Teniendo en cuenta que las herramientas pueden moderrnizarse, se sugiere no cerrar que la herramienta a utilizar sea la guia de servicio al ciudadano de DNP.	Aceptada	Gracias por el comentario, se precisará el contenido conforme con la propuesta que realizan.
			15. Anexo 1: Lineamientos para estandarizar Las ventanillas únicas, portales de programas específicos de programas transversales del Estado y sedes electrónicas 1.Este primer anexo contiene información reiterada en otros marcos normativos y anexos, por lo que las 73 páginas de contenido pareciera ser innecesarias, adicionalmente al abordar los tres componentes reiterando en un porcentaje considerable la misma información para cada uno de estos componentes. Por lo que nuevamente la sugerencia es revisar el contenido y aligerar el mismo eliminando la información repetida en otros anexos de esta misma resolución y de otras existentes. En este sentido, los comentarios a continuación están detallados para sedes electrónicas, no obstante aplican para ventanillas y programas transversales.	No aceptada	Se agradece el comentario. Se comparte que los documentos deben ser lo más ligeros posibles. Justamente por eso están separados en diferentes anexos: El Anexo 1 que define los lineamientos generales que deben tener las sedes electrónicas, las ventanillas únicas digitales y los portales específicos de programas transversales del Estado. Los Anexos 2 y 2.1, que contienen los requisitos mínimos que deberán cumplir las entidades para integrar sus sedes electrónicas al Portal Único del Estado Colombiano. Los Anexos 3 y 3.1, que contienen los requisitos mínimos que deberán cumplir las entidades para integrar las ventanillas únicas digitales de las que son responsables al Portal Único del Estado Colombiano. Los Anexos 4 y 4.1 que contienen los requisitos mínimos que deberán cumplir las entidades para integrar los portales
			16. Anexo 1: Lineamientos para estandarizar Las ventanillas únicas, portales de programas específicos de programas transversales del Estado y sedes electrónicas 1.Revisión de definiciones. Pág. 9 validar el uso del termino “grupo objetivo” dado que el término que se usa es Grupo de valor para las políticas del Modelo Integrado de Planeación y Gestión, sugerimos revisar e incluir la definición existente y disponible en el siguiente enlace: https://www.funcionpublica.gov.co/glosario/-/wiki/Glosario+2/Grupo+de+Valor. Adicional es clave usar este termino durante el documento reemplazándolo por usuario.	Aceptada	Se agradece el comentario y se hace el ajuste. Sin embargo, no se acoge la definición que está en el enlace sino la que se presenta en el documento llamado ""Ficha metodológica de la medición del desempeño institucional"" del Modelo Integrado de Planeación y Gestión que se encuentra en el siguiente enlace: https://www.funcionpublica.gov.co/documents/28587410/36200637/2020-06-30_Ficha_metodologica_v2.pdf/c08038a0-21fe-fc16-9020-69e8e50af361?t=1593794275569
			17. Anexo 1: Lineamientos para estandarizar Las ventanillas únicas, portales de programas específicos de programas transversales del Estado y sedes electrónicas 1.Sobre la definición de servicio de consulta de información, teniendo en cuenta la reunión efectuada el 11 de agosto, se solicita ajustar a Consultas de acceso a información pública: Información contenida en bases de datos o repositorios digitales. relacionada a procesos misionales 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. Adicional a esto homogenizar el nombre en todo el documento pág. 24 titulo y desarrollo diferente.	Aceptada	Se agradece el comentario y se harán los ajustes correspondinentes

18. Numeral b, página 19. Es necesario ajustar la redacción, dado que la obligación no solo es para que la información este en idioma castellano, sino que el contenido de la sede debe ser accesible para los grupos de valor, es así que en la ley 1712 y en la resolución que desarrolla la parte de accesibilidad, se establece esta como un requerimiento indispensable para el acceso a la información pública.	No aceptada	Se agradece el comentario, respecto del cual se aclara que el numeral b, hace referencia a la la ley específicamente en lo que respecta al idioma. En lo que conciernee a que los contenidos deben ser accesibles para los grupos de valor esta señalado en el documento, específicamente en el numeral 4.3.2. Accesibilidad
19. Anexo 1: Lineamientos para estandarizar Las ventanillas únicas, portales de programas específicos de programas transversales del Estado y sedes electrónicas 1.Numeral e, página 19. Revisar como va a ser la vinculación de los buscadores de las sedes electrónicas con la sede compartida, esta vinculación debería ser incluida dentro de la guía de manera explicita.	Aceptada	Se agradece el comentario. En la guía se hará la aclaración de que los buscadores de las sedes electrónicas y de la sede compartida GOV CO son independientes. Las entidades deberán implementar un buscador para su sede electrónica.
20. Anexo 1: Lineamientos para estandarizar Las ventanillas únicas, portales de programas específicos de programas transversales del Estado y sedes electrónicas 1.Numeral g, página 20. Revisión de redacción y puntuación.	Aceptada	Se agradece el comentario y se hacen los ajustes correspondientes
21. Anexo 1: Lineamientos para estandarizar Las ventanillas únicas, portales de programas específicos de programas transversales del Estado y sedes electrónicas 1.Numeral 1 y siguientes, página 20. Si bien se entiende la relevancia de señalar estas funcionalidades de manera genérica, es clave que se presenten de manera diferencial de los numerales y se contextualice dichos requerimientos transversales en materia de funcionalidades, adicional de una categorización de los mismos que permita comprender la mezcla en su abordaje. Adicional, revisar la especificidad del punto 10.	No aceptada	Se agradece el comentario, sin embargo, no es clara la observación, inquietud o recomendación que se hace respecto al Anexo 1 - Lineamientos para estandarizar las ventanillas únicas, portales de programas transversales y unificación de sedes electrónicas del Estado colombiano

22. Anexo 1: Lineamientos para estandarizar Las ventanillas únicas, portales de programas específicos de programas transversales del Estado y sedes electrónicas 1.Menú transparencia, página 22. Sugiero mencionar en el primer párrafo que las condiciones de contenido y disponibilidad están contenidas en la ley 1712, el marco regulatorio y la actualización de la resolución 3564 y no reiterar información con el riesgo de mencionar menos que en la resolución.	No aceptada	Agradecemos su comentario. Las Guías están debidamente articuladas con el contenido vigente de la Resolución 1519 del 2020, de forma que cualquier persona pueda dar cumplimiento a las obligaciones vigentes.
23. Anexo 1: Lineamientos para estandarizar Las ventanillas únicas, portales de programas específicos de programas transversales del Estado y sedes electrónicas 1.Los numerales estipulados en el menú de servicios a la ciudadanía, tramites, OPAS Y consultas no reflejan la integración de la sede a gov.co, el funcionamiento es independiente en presentación, búsqueda y funcionamiento. Con estas disposiciones en las sedes no se ve el cambio con la generación de la sede compartida. Si la ficha de presentación, el funcionamiento, la categorización es autónomo en la sede, no es claro como los lineamientos de integración están cambiando la realidad actual y viéndose potenciado con la sede compartida. El espíritu del legislador en el decreto reglamentario anti trámites era lograr certeza, integridad y seguridad en la oferta institucional, las indicaciones confirmar la situación actual.	No aceptada	El objetivo del Portal Unico del Estado - Gov.co es facilitar la iteraccion del ciudadano con la oferta institucional del Estado y para esto desde Gov.co se habilitarán diferentes mecanismos de búsqueda y acceso directo a los Trámites, OPA´s o consulta de acceso a información pública, a las Sedes Electrónicas, a las Ventanillas Unicas y a los Portales de programas transversales, dando cumplimiento a los dispuesto en el decreto 2106 de 2019; este acceso es independiente al que deben habilitar las entidades en sus respectivas sedes electrónicas, las cuales también se podrán acceder desde Gov.co. Por tanto, el acceso se habilita desde la sede electrónica compartida Gov.co y también desde la sede electrónica de cada entidad.
24. 10.Eliminar el numeral f, pagina 26. No debe ser posible el re direccionamiento desde la sede externa a una página externa, esto seria el incumplimiento del decreto, donde se señala que solo se debe tener una sede completa y operante.	Aceptada	Así es, se agradece el comentario y se ajusta la redacción de la siguiente manera: ""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 di dicho sitio (NOMBRE ENTIDAD RESPONSABLE)
25. 11.PQRSD, pagina 27, debería ser explicito en la inclusión de las solicitudes de información. "	No aceptada	Agradecemos su comentario, al respecto es importante informar que los criterios relacionados con el formulario PQRSD deben implementarse de acuerdo como lo dispone el Anexo 2 de la Resolución 1519 del 2020.

			26. 12.Pagina 28, numeral 4.1.1 No señala la integración a los mismos, como se presentan, bajo que categorías se agrupan, etc.	Aceptada	Se agradece el comentario, respecto del cual no es claro a qué se refiere. No obstante lo anterior, se revisarán las guías de manera que queden de conformidad a lo establecido en la Resolución 1519 de 2020	
			27. 13.Página 37, identificar y redistribuir aquellas indicaciones de usabilidad que están abordadas en las ubicaciones o secciones anteriormente descritas en el texto (debe ser claro para las entidades si las indicaciones se dan por ubicación o son transversales por características). El párrafo de neutralidad, página 45 esta reiterado en este espacio, revisar y ajustar.	No aceptada	Se agradece el comentario, el anexo indica de forma clara cuales son los atributos de calidad relacionados con los portales de programas transversales asi como para las sedes electrónicas y ventanillas únicas.	
			1. No queda claro cómo es la interacción esperada cuando se trata de i) dos o más VU que interactuarán y ii) de todas las VU entre diferentes sedes electrónicas de las entidades y paso por gov.co.	No aceptada	Se agradece el comentario: Cada Ventanilla Unica Digital debe tener su propia direccion electrónica (pagina web) la cual debe cumplir los lineamientos definidos en la guia de integración correspondiente. y esa ventanilla única podrá se accedida desde GOV.CO y desde la sede electrónica de la entidad responsable de esa ventanilla única. Para la inteacción de dos o más ventanillas únicas, las entidades deberán utilizar el servicio de interoperabilidad.	Francisco Moreno
			2. ¿La sede electrónica al final subsume la misma página web de la entidad o se comporta como un micrositio? Bajo la forma de asociación descrita en el proyecto de resolución se infiere que sí, pero es un tema muy confuso por cuanto una vez migrada la información a la sede electrónica, no es claro cuál debe ser el contenido de la página web. Si es un avance gradual, cómo se manejará la transición y los tiempos de gradualidad para su integración en una VU.	No aceptada	No es un micrositio. La sede electrónica es el sitio web principal de la entidad y por esto debe consolidar la información, servicios y demás sitos de la misma. En este sentido, la página web se transforma en la sede electrónica, siempre que cumpla con las siguientes características: 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. Se precisa que la integración a GOV.CO es de manera inmediata una vez cumplidas las condiciones mencionadas anteriormente. La Ventanilla Única se integrará a la sede electrónica en el término señalado en el parágrado 2 del artículo 15 del Decreto 2106 de 2019	Marco Sánchez y Francisco

			3. Se solicita precisión e información de detalle sobre la forma cómo se aprobará la integración gradual de planes de VU. ¿Cuáles serán los plazos para la implementación de los lineamientos formulados en el proyecto de resolución a las VU, existentes o en desarrollo?	No aceptada	Se aclara que la forma como se aprobará la integración se de la ventanilla única está en el numeral 6 del Anexo 3. Respecto de los plazos para la implementación de los lineamientos, se reitera que estos se aplciarán en el término señalado en el parágrado 2 del artículo 15 del Decreto 2106 de 2019	Marco Sánchez y Francisco
			4. Dentro de la arquitectura definida para la sede electrónica se menciona que dentro de Gov.co existe un catálogo de ventanillas electrónicas, ¿ese catálogo ya existe?, ¿cómo se accede a él?, quién lo administra? Por otra parte, se menciona que se debe presentar información acerca del trámite, sin embargo, no está claro si dentro de las VU se incluirá la ficha técnica del trámite tomada directamente desde el SUIT. La sugerencia sería implementarla a través de SCD1 de interoperabilidad directamente del origen, tomando esta ficha técnica del SUIT.	No aceptada	En Gov.co ya se cuenta con la estructura del catálogo de ventanillas únicas. Actualmente MinTIC está trabajando con el DAFP para que la información que alimenta este catálogo se haga desde el SUIT. Está previsto que este catálogo se use para el proceso de integración y visualización de información a Gov.co, mas no para que las entidades accedan e interactúen con él. Quien administrará esta información en a fuente primaria es el DAFP	Francisco Moreno
			5. Se solicita revisar el planteamiento de expediente electrónico en función de las siguientes consideraciones: Desde lo tecnológico: Teniendo en cuenta que las VU por regla general no son gestoras de trámites, sino pasarelas en las que cada trámite se mantiene en cabeza de su entidad responsable, en este sentido, ¿cómo aplica exactamente el concepto de Expediente Electrónico bajo este mecanismo de integración de trámites de varias entidades? □ En el contexto anterior, es necesario definir claramente el lineamiento para el expediente electrónico en caso de una VU. Se formulan las siguientes preguntas: ¿Las VU son activadoras o gestoras de expedientes electrónicos de trámites? ¿Genera dualidad de expedientes e información? ¿Supone que hay conexión con las plataformas de gestión interna del trámite de cada entidad? ¿Y con los sistemas de gestión documental? ¿Y eso como se refleja en los servicios centralizados de una VU? Si es así, ¿qué pasaría en los casos en los que las entidades que participan en VU no tienen sistemas robustos ni de gestión electrónica del expediente? □ Para lo anterior considerar el requisito de lineamientos técnicos aplicables a expedientes p.ej. de acuerdo con archivo general. Desde lo funcional ¿Qué pasa con la oferta que ya está en VU que no necesariamente opera con un concepto de expediente electrónico en cadenas de trámites? Si de frente a negociaciones y acuerdos de servicio con entidades y una VU se garantiza el criterio de servicio y transacción única, ¿debería existir un lineamiento complementario que aplique para estos	No aceptada	Se agradece el comentario, respecto del cual se aclara qu elas guías en cuestión no tienen como objetivo abordar asuntos de la política de gestión documental y de archivo, toda vez que la misma es de competencia del Archivo General de la Nación	Francisco
			6.4.1.4.5 Menú de Servicios a la ciudadanía Información general, procedimiento y plazos de la cadena de trámites (plazo total de la cadena de trámite y plazos específicos de gestión en cada autoridad). Tratándose de una cadena de trámites que se encuentre integrada en una VU, se solicita revisar la determinación de proporcionar de plazos específicos, pues en virtud de lo primero, actualmente todos los ANS2 están en función del trámite y no de la cadena. Es decir, en una VU se asume que hay una respuesta única a la gestión de los trámites que acoge la cadena. Para el ciudadano/usuario es este el resultado final relevante.	No aceptada	Los plazos de un trámite están regulados en la Ley y sus normas reglamentarias. No es objeto de esta resolución señalar plazos, mucho menos modificar los establecidos en las normas que de forma particular los regulan. Cada trámite tiene y cuenta con plazos que se deben respetar en virtu del artíuclo 29 de la constitución y en este orden, las VU, deberán respetar los mismos.	Marco Sanchez

11	15/11/2020	**MINCOMERCIO**	7. "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." ¿Es necesario tener obligatoriamente sistema de registro independiente a autenticación? Tanto por la naturaleza de unos servicios como por la existencia de un mecanismo de autenticación, se debe revisar la posible redundancia de las dos actividades, en particular si el registro resulta inocuo bajo determinadas condiciones del diseño.	No aceptada	Se agradece el comentario, respecto del cual se aclara que los usuarios al vincularse al servicio de autenticación digital hacen un único registro y las entidades que se vinculen al servicio podrán acceder a estos datos. De otra parte, si la entidad para su proceso debe incorporara datos adicionales deberá complementarlos, así como implementar los proceso de autorización necesarios	José Ricardo
			8. "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 al mismo." La funcionalidad de otorgar al usuario un número de radicado puede lograrse a través de mecanismos que no dependan de existencia de registro de usuario, se sugiere indicar únicamente que las VU deben proporcionar al usuario el número de radicado único y mecanismos necesarios para acceder a la trazabilidad del trámite.	Aceptada	Se agradece el comentario respecto de cual se hará el ajuste correspondiente, de manera que se aclare que el mecanismo de registro no será requerido para la generación y recepción de radicado. En este sentido, la guía quedará así: 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. El usuario recibirá el radicado y podrá consultar el estado de su trámite, plazo de respuesta e incluso, podrá descargar documentación asociada al mismo. Todas las autoridades involucradas o responsables de la cadena de trámite deberán actualizar en tiempo real el estado del trámite, para que al	José Ricardo Aponte
			9. "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." Se solicita establecer cómo se espera dar aplicabilidad práctica a este atributo.	No aceptada	La definición, aprobación y publicación de una 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, corresponde a cada sujeto obligado de que trata el artículo 2.2.17.1.2. del Decreto 1078 de 2015. En tal sentido, cada uno de ellos deberá dar aplicación al principio de veracidad o calidad con respecto a la información sujeta a tratamiento, con base en su propia libertad de configuraciób.	Luis Bastidas
			10. ″10. Adecuar un nivel de interoperabilidad entre los registros electrónicos y otros sistemas diferentes establecidos por las entidades públicas para atender otros trámites o requerimientos especiales." No se entiende el objetivo y planteamiento técnico frente a la última afirmación (en rojo), pues no es claro a qué se refiere con “otros trámites o requerimientos”.	Aceptada	Se agradece el comentario, se ajustará la redacción para dar mayor claridad, quedando de la siguiente 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.	Jairo Riascos

			11. "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 di dicho sitio (NOMBRE ENTIDAD RESPONSABLE)" Esta afirmación aplica para el tema redireccionamiento o por trámites específicos. Sin embargo, existen casos donde la oferta integrada a una VU acuerda estándares únicos de tiempo de respuesta al trámite integral. Si es así, este lineamiento entra en contradicción al exigir detallar tiempos de subprocesos. Se pierde el sustento de las VU como integradoras de servicio y de darle un único front al ciudadano/usuario. En lugar de "sedes electrónicas" (rojo), ¿se refiere a VU?	No aceptada	Agradecemos su comentario: Este lineamiento aplica para todos los enlaces que desde la sede electrónica direccionen a sitios externos a la misma. La ventanillas únicas están conformadas por trámites encadenados de manera armónica consumiendo servicios e interoperando para facilitar la interaccion con el ciudadano, en las VU el redireccionamiento a trámites no es una buena practica. Se ratifica que se refiere a las sedes electrónicas, que son las que deben dar lugar a redireccionamiento, y no a a vetaníllas únicas deberán interoperar.	Francisco Moreno y Juan Pablo Salazar
			12. "4.3.2.2 Interoperabilidad La autoridad titular o responsable de la ventanilla única digital debe estructurar y presentar un plan de vinculación al servicio de interoperabilidad y estandarización de acuerdo con el Lenguaje común de intercambio (lenguaje.mintic.gov.co) de los formularios de captura de información y de servicios de intercambio de información para trámites, Otros Procedimientos Administrativos, servicios de consulta de información." Para VU en construcción se requiere un lineamiento explícito pues la interoperabilidad definida para los SCD pueden ser viables a mediano plazo en determinadas entidades que hacen parte de los planes de implementación de una VU. En este caso y si materializar la VU depende de dichas entidades se debe avanzar (hacer la integración, aunque la entidad no tenga el servicio estandarizado), detener las inversiones, priorizar en plan de vinculación?	No aceptada	Se agradece el comentario, respecto del cual se aclara que de manera permanente el MinTIC cuenta con el equipo de apoyo para la estandarización y del cumplimiento del marco de interoperabilidad. De esta forma las entidades pueden hacer la planeación de la estandarización de acuerdo con el Lenguaje común de intercambio (lenguaje.mintic.gov.co) de los formularios de captura de información y de servicios de intercambio de información para trámites, Otros Procedimientos Administrativos, servicios de consulta de información en el momento que lo requieran. De otra parte, el plan de vinculación al servicio de interoperabilidad debe ajustarse a el Artículo 2.2.17.7.1. Gradualidad del decreto 620 de 2020, donde se define los plazos en los cuales las entidades deberán implementar los servicios ciudadanos digitales y la sede electrónica conforme a los lineamientos dados.	José Ricardo Aponte
			13. "(a) 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." En lugar de "sedes electrónicas" (rojo), ¿se refiere a VU?	Aceptada	Se agradece el comentario. Sí se refiere a ventanillas únicas. Se acepta el comentario y se hace el ajuste correspondiente	Luis Bastidas y Juan Pablo Salazar
			14. "4.3.2.4 Disponibilidad La autoridad determinará el nivel de disponibilidad mensual de la sede electrónica, el cual debe ser igual o superior al 95%, en concordancia con el análisis de criticidad de los trámites, Otros Procedimientos Administrativos, servicios de consulta de información ofrecidos en atención al análisis de riesgos que realice la autoridad. Así mismo, se asegurará que la información se encuentre disponible para su posterior consulta, para ello se deben implementar los procedimientos de preservación documental a largo plazo dispuestos en las normas de gestión documental definidas por el Archivo General de la Nación." Se define disponibilidad de la VU sin tener en cuenta que esta depende de la disponibilidad de cada servicio que atiende un trámite. En el contexto de una VU, más allá de la disponibilidad de la VU, se debería medir la disponibilidad del servicio en la cadena de trámites	No aceptada	Agradecemos el comentario. La disponibilidad de la VU efectivamente depende de la disponibilidad de los servicios necesarios para para atender el trámite, en ese sentido, se espera que las entidades garanticen la disponibilidad de todos los servicios o componentes requeridos para proveer sus trámites de manera oportuna.	Jairo Riascos

			15. "Unificar y adecuar la sede electrónica de acuerdo con los requisitos mínimos establecidos." En lugar de “sedes electrónicas” (rojo), ¿se refiere a VU?	Aceptada	Se agradece el comentario. Sí se refiere a ventanillas únicas. Se acepta el comentario y se hace el ajuste correspondiente	Luis Bastidas y Juan Pablo Salazar
12	12/11/2020	**SECRETARÍA DISTRITAL DE MOVILIDAD**	1. ¿qué entidad ya está integrada con los lineamientos de las ventanillas únicas digitales?	No aceptada	A la fecha no se cuenta con información sobre el número de entidades que están cumplimento con eestos lineamientos	
			2. Se menciona que si no se tiene aún la integración con los servicios de autenticación GOV.CO, se puede seguir utilizando el modelo propio. ¿Se soportará la federación de identidad?	No aceptada	Agradecemos el comentario. la entidad determina los controles que debe implementar para garantizar la seguridad de la información. Para esto lo deseable es que la entidad haga uso del servicio ciudadano digital de autenticacion y de esta manera el cuidadano aproveche los beneficios que ésta le ofrece. Sin embargo las entidades podrán integrarse a Gov.co con esquemas de autenticación propios donde la identidad del usuario y el control de acceso y autorización serán responsabilidad de la entidad que implementte dicho servicio de autenticación	Francisco Moreno
			3. ¿Se soporta en los servicios de Autenticación GOV.CO técnicas de Autenticación Multi-Factor (MFA) y MFA Contextuales?	No aceptada	Se agradece el comentario, respecto del cual se indica que en el servicio ciudadano de autenticación digital se soportaran mecanismos de autenticación de múltiple factor, a la fecha se cuenta con una verificación en dos pasos a través de la verificación de una contraseña de un solo uso	José Ricardo

13	31/07/2020	**Julián Ruíz**	1. En el borrador del proyecto de resolución si bien se adoptan los anexos técnicos, en el mismo no se especifica por ningún lado nada respecto a los plazos de adopción por parte de las entidades públicas del orden nacional y el orden territorial. Adicionalmente en los considerandos de la resolución no se menciona nada referente al Decreto 620 de 2020 y cómo será su articulación respecto a este Decreto. Adicionalmente en el artículo 2.2.17.7.1 Gradualidad del Decreto 620 de 2020 se menciona en el numeral 1 que el plazo de implementación es de 9 meses para las entidades del orden nacional y en el numeral 2 que las entidades del orden territorial implementará el modelo respecto a la disponibilidad presupuestal. Por favor aclarar: 1. ¿Cuales son los plazos para la adopción del proyecto de resolución para la facilitar la consulta y acceso a información, trámites y servicios del Estado tanto para entidades del orden nacional como del orden territorial?	No aceptada	Se agradece el comentario. No obstante, las fechas de integración a Gov.co están definidas en la Directiva presidencial 02 de 2019 y la de integración de ventanillas únicas en el Decreto 2106 de 2019. El decreto 620 de 2020 en el Artículo 2.2.17.7.1. Gradualidad. De conformidad con el artículo 64 de la Ley 1437 de 2011, las autoridades y particulares a que se refiere el artículo 2.2.17.1.2 del presente Decreto deberán implementar los servicios ciudadanos digitales y la sede electrónica conforme a los lineamientos dados en este título, dentro de los siguientes plazos: 1. Las entidades públicas de la rama ejecutiva del orden nacional y los particulares que desempeñen funciones públicas tendrán un plazo de nueve (9) meses conta-dos a partir de la publicación de la Guía para la vinculación y uso de los servicios ciudadanos digitales, por parte del Ministerio de Tecnologías de la Información y las Comunicaciones. 2. Las entidades públicas del orden territorial y las demás a las	
			2. ¿Cuál plazo vencerá primero?, el del Decreto 620 de 2020 o él de la presente resolución, o ¿ambos vencen al mismo tiempo?. No son claras las articulaciones entre el decreto y el proyecto de resolución.	No aceptada	Se agradece el comentario y se aclara que el Decreto 1078 de 2015 (que incorpora el decreto 620 de 2020) se relaciona con esta resolución. Los plazos para la implmentación están dados en el Decreto 620 / 2020 Artículo 2.2.17.7.1. Gradualidad. De conformidad con el artículo 64 de la Ley 1437 de 2011, las autoridades y particulares a que se refiere el artículo 2.2.17.1.2 del presente Decreto deberán implementar los servicios ciudadanos digitales y la sede electrónica conforme a los lineamientos dados en este título, dentro de los siguientes plazos: 1. Las entidades públicas de la rama ejecutiva del orden nacional y los particulares que desempeñen funciones públicas tendrán un plazo de nueve (9) meses conta-dos a partir de la publicación de la Guía para la vinculación y uso de los servicios ciudadanos digitales, por parte del Ministerio de Tecnologías de la Información y las Comunicaciones.	
			3. ¿Hasta qué punto llega la obligatoriedad de la implementación del proyecto de resolución para la facilitar la consulta y acceso a información, trámites y servicios del Estado para entidades del orden territorial?, teniendo en cuenta que en el Decreto 620 de 2020 se menciona que será de acuerdo con la disponibilidad presupeustal.	Aceptada	Se agradece el comentario y se aclara que la obligatoriedad se realizará	Marco Sanchez
