Bogotá D.C., Junio 19 de 2020

Ministerio de Tecnologías de la Información y las Comunicaciones
Karen Abudinen
Ministra

> Ref: Comentarios al “proyecto de resolución de transparencia en el acceso a la información

Cordial saludo,

Las organizaciones abajo firmantes remitimos de manera atenta a su despacho, comentarios sobre el texto del proyecto de resolución en transparencia en el acceso a la información para que sean considerados y permitan enriquecer y ajustar el texto definitivo del acto administrativo que se presentó como borrador.

Como organizaciones suscriben Datasketch, una plataforma digital de periodismo de investigación y de datos Datasketch dedicada a la democratización y apropiación ciudadana de la información pública, así como miembro del comité de la Alianza por el Gobierno Abierto; y la Fundación Karisma, una organización de la sociedad civil colombiana que, guiada con un enfoque de justicia social, trabaja en la intersección entre tecnología y derechos humanos.

Cualquier comentario o duda con relación a las observaciones que siguen a continuación, podrá ser remitida a los correos jpmarindiaz@datasketch.co y carobotero@karisma.org.co

Atentamente,

Juan Pablo Marín
Director
Datasketch

Carolina Botero Cabrera
Directora
Fundación Karisma

***

Comentarios generales

Esta Resolución al tratar temas de transparencia en el acceso a la información a la ciudadanía debe responder a una estrategia transversal relacionada directamente con asuntos de gobierno abierto y en particular vincularse a los procesos de creación de acciones en torno a la Alianza de Estado Abierto de Colombia.

Varios de los comentarios discriminados por Anexo abajo pueden beneficiarse de una estrategia simple de incorporación de la especificación datatxt en la publicación de conjuntos de datos.

Datatxt es una especificación que facilita el descubrimiento de los conjuntos de datos que están publicados bajo un dominio web. Es un archivo de texto plano que determina cuáles conjuntos de datos están disponibles bajo un dominio cualquiera, como *ejemplo.gov.co*
Es análogo a las especificaciones robots.txt a los buscadores incluir o excluir contenido para leer automáticamente sobre un sitio web determinado, pero está creado para que sea entendible por máquinas o computadoras. Funciona como un catálogo simple de conjuntos de datos disponibles en una página web y facilita varios de los puntos mencionados a lo largo de los comentarios de este documento.

Algunas ventajas de incorporar datatxt incluyen:

- Bajo costo tecnológico de implementación al ser un solo archivo de texto.
- Permite el descubrimiento de archivos de datos únicamente con la URL de la organización
- Legible para humanos y máquinas
- Sobrepesa la falta de estándares únicos de datos al listar el nombre, descripción y URL de la información a publicar.
- Permite ver fácilmente las licencias de uso de los datos publicados si se incorporan en el texto.
- Agnóstico a los sistemas de publicación de datos abiertos (CKAN, archivos planos, estándares de datos, etc).

***

Comentarios específicos

Sobre el “Artículo 5. Información digital archivada”

El texto del artículo 5 señala que:

> **ARTÍCULO 5. *Información digital archivada*.** Los sujetos obligados deben garantizar y facilitar a los solicitantes, de la manera más sencilla posible, el acceso a toda la información previamente divulgada, de conformidad con el Decreto 1862 del 2015 y el artículo 16 del Decreto 2106 del 2019 o el que los modifique, subrogue o adicione. *En atención a lo anterior, los sujetos obligados deben garantizar condiciones de conservación y/o archivo para posterior consulta, de la documentación digital disponible en sitios web*, conforme con las Tablas de Retención Documental aprobadas acorde con los lineamientos del Archivo General de la Nación.
>
> Los sujetos obligados no podrán eliminar información publicada en sus sitios web y deberán asegurar la preservación de documentos en ambientes electrónicos, para lo cual, deberán adoptar medidas de conservación preventiva para facilitar procesos de migración, emulación o *refreshing*, o cualquier otra técnica que se disponga a futuro. Para el efecto, deberán adoptar un programa de gestión documental digital, conforme lo dispone el Decreto 2609 del 2012, o el que lo modifique, adicione o subrogue. (Subrayado propio)

Con relación al aparte que señala que las acciones de conservación y/o archivo para posterior consulta incluya la documentación digital disponible en sitios web, es relevante que se incluyan además las redes sociales oficiales que comparten información pública y de interés para la ciudadanía pues, como genuinos canales de divulgación de la información en los que se interactúa de manera directa con la ciudadanía, es preciso que los contenidos que allí sean difundidos sean igualmente conservados y archivados.

De conformidad con el “Mini/Manual archivamiento de medios sociales, conceptos básicos, estrategias y mejores prácticas”[1] publicado por el Archivo General de la Nación en 2015 el uso de canales de comunicación digitales que incluye también a las redes sociales, ha creado la necesidad para que los contenidos que allí se difunden sean también archivados y conservados:

[1]El archivo puede consultarse aquí: https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Recursos/Publicacionees/ArchivamientoDeMediosSociales.pdf

> “En el contexto de la administración pública, en el que los medios sociales hacen parte de su estrategia de buen gobierno, toda comunicación, publicación, respuesta o disposición transmitida en estas herramientas a la ciudadanía, es susceptible de convertirse en un documento de archivo, en la medida que corresponde al cumplimienot de funciones de la entidad y por lo tanto debe recibir el tratamiento adecuado conforme con los Programas de Gestión Documental articulados con las disposiciones definidas por el Archivo General de la Nación”, pg 11, 12

El propio Archivo General de la Nación ha advertido en dicho documento, que constituyen retos en materia de conservación y archivo de los contenidos que se comparten por las entidades del Estado en todo nivel, no solo la definición de qué es un documento de archivo de medios sociales, sino la deficiencia en la captura y mantenimiento de los medios sociales que deben garantizar su autenticidad, integralidad, inalterabilidad, fiabilidad y disponibilidad, sino también retos asociados a la continuidad de la cuenta en una red social que por falta de control en los procesos de gestión ponen “en riesgo los registros de la entidad, los cuales pueden extraviarse, modificarse o eliminarse con cualquier cambio y actualización de la aplicación, o en el peor de los casos el cierre definitivo del servicio” (pg. 14)

Al respecto, conviene recordar casos recientes relacionado a esos riesgos que advierte en su mini manual el Archivo General, y que reiteran la necesidad de que las tareas de conservación y archivo se realicen atendiendo las recomendaciones de la entidad sobre el particular. El caso de la cuenta en Twitter @EquipoPazGob cuyos trinos -genuino contenido de interés público- habrían sido eliminados, desnaturalizando el propósito de la cuenta al tiempo que afectó a futuro el ejercicio del derecho de acceso a la información a registros digitales que constituyen un registro histórico de las conversaciones de paz con el grupo armado ELN.

Sobre este caso, vale la pena recordar la investigación efectuada por Cuestión Pública[2] en 2019 que, a través de un ejercicio de periodismo forense e investigativo, logró recuperar parte del contenido eliminado por causa de un hackeo[3] que habría afectado la integridad de la cuenta. Un caso que pone en evidencia por supuesto, la necesidad de que se adopten buenas prácticas y lineamientos para que la información pública compartida y producida por entidades públicas en redes sociales, sea también sometida a acciones de conservación debida y archivamiento periódico y continuo que contribuya no solo al ejercicio del derecho de acceso a la información de la ciudadanía, sino también al ejercicio del derecho a la memoria.

---

[2] Sobre el caso, puede leerse la investigación completa aquí: https://cuestionpublica.com/cuestion-publica-recupero-dos-mil-trinos-cuenta-twitter-equipo-paz-gob/

[3] Sobre la brecha en seguridad digital que hubo en este caso, pueden leerse los comentarios de Fundación Karisma al respecto aquí: https://web.karisma.org.co/te-enteraste-de-lo-que-paso-con-la-cuenta-equipopazgob-aca-unos-consejos-de-ciberseguridad/

Anexo 1. Directrices sobre Accesibilidad Web

A lo largo del anexo no se hace referencia explícita a la accesibilidad para sistemas de lectura automatizados para personas con discapacidades o máquinas en general para las páginas web del Estado que siga buenas prácticas para accesibilidad automatizada, en particular las siguientes indicaciones prácticas ayudarían considerablemente a mejorar la accesibilidad:

- Especificar las recomendaciones de color sobre accesibilidad
- Permitir el acceso a los ítems estandarizados en los menús como se especifica en la resolución también como textos planos siempre disponibles en las mismas urls, esto aplicaría para términos y condiciones, políticas de datos, y los demás mencionados en la resolución, por ejemplo: www.ejemplo.gov.co/terminos-y-condiciones.txt o www.ejemplo.gov.co/politica-datos.txt
- A pesar de que el anexo hace referencia a la inclusión de personas con discapacidades visuales de algún tipo, no hace referencia a la discapacidad por daltonismo se recomienda incluir referencias explícitas para las selección de colores y contrastes en las páginas web. Por ejemplo referir a las razones de contraste (mayor a 3.5) definidas por el mismo consorcio W3 https://www.w3.org/WAI/WCAG21/Understanding/contrast-minimum.html
- La resolución debería aclarar que las tablas que se publican en formatos no abiertos ni reutilizables como pdf (así como documentos escaneados y entregados como imágenes), a pesar de que es información pública, debe ser puesta a disposición adicionalmente en formatos abiertos (xls, csv). Esta opción también aplica para tablas publicadas en diapositivas. Por ejemplo: Un contrato público en PDF el cuál es importante que sea público por sus firmas, deberia contener un anexo como tabla reutilizable que contenga la información de las tablas del PDF, como puede ser la tabla de los ítems del contrato.
- No es clara la razón por la cual se hace referencia a una posible configuración de seguridad en los documentos con formato pdf. Si la información publicada en las páginas web, tiene un carácter público, no es comprensible por qué eventualmente alguna tenga que tener clave.
- Si bien se hace menciona la federación de datos en el portal de datos abiertos, es importante dejar también una vía para que cualquier entidad publique su información dentro de su propio portal, ya que existe información pública, no necesariamente estructurada que debería ser más accesible a través de la web.
- En la resolución se recomienda sugerir una licencia por defecto para la información publicada con el fin de relevar a las entidades de un posible cuello de botella por desconocimiento de licencias apropiadas para publicar información pública.
- En materia de accesibilidad un componente que ha quedado por fuera de la discusión la consistencia en el acceso a los archivos y las versiones históricas de la información pública. En múltiples oportunidades diferentes entidades de la sociedad civil han levantado alarmas sobre las barreras de acceso a la información pública porque no se

mantiene la información en las mismas URLs o no se evidencian los cambios en la información o no se puede acceder a los históricos. La resolución debería contener:

- Disposiciones para mantener la información pública en las mismas URLs o mantener un catálogo simplificado activo en la misma página cuando se actualizan las mismas que evidencie la última versión disponible, una ejemplo es el uso de la especificación data.txt descrita en este documento.
- Mantener un listado actualizado de las versiones disponibles con links a los históricos, puede ser tan fácil como tener vínculos a las versiones anteriores como un archivo de texto en las páginas de gobierno.
- Mantener un listado actualizado con los metadatos relevantes de la información pública dentro de las páginas. Por ejemplo listar la última actualización de los términos y condiciones de las páginas y quiénes son los autores o responsables de mantener la información actualizada.

Anexo 2. Estándares de publicación y divulgación de información

Este apartado se encuentra muy alineado con los puntos sobre accesibilidad. El uso de una especificación simple de bajo costo tecnológico para publicar listados de información disponible y facilitar su descubrimiento facilitaría varios de los puntos mencionados en este documento.
Hacemos énfasis especial en los siguientes puntos:

- Dejar la información básica identificada como menús, también disponible para acceso por texto plano y legible por máquinas. Ejemplos:
    - El archivo example.gov.co/data.txt puede listar los siguientes archivos con alguna información adicional:
        - name: Términos y condiciones
          url: terminos-y-condiciones.txt
        - name: Política de datos
          url: documentos/politica-datos.pdf
          date_updated: 2020-04-05
- En cuando a la información adicional o metadatos es importante sugerir unos mínimos o definirlos en la Guía de datos abiertos. Entre los campos que pueden pasarse por alto está por ejemplo los que determinan si una base de datos está anonimizada o no y su respectiva metodología de anonimización.
- Reiteramos la necesidad de publicación de información en formatos que permitan ser descargados, tener acceso sin restricciones legales, usabilidad, procesamiento por máquina, y con posibilidad de realizar búsquedas y filtros de la información que existe en su interior. Esto es que la información en bases de datos se encuentre disponible en formato xls y/o csv principalmente.
- La información pública debe contar con una fuente única alojada en el menú de Transparencia y Acceso a la Información Pública evitando duplicidad y garantizando el acceso a versiones pasadas. De forma que, independiente el enlace/menú/sección en la que se divulgue la información se redireccione a una única url para cada entidad,

independiente de si la información está siendo federada en datos.gov.co ya que existe mucha información que no necesariamente es estructurada que debería ser fácil de descubrir, vincular y acceder, por ejemplo: normativas, presentaciones de resultados, resoluciones organigramas, entre otros.

- Al interior de la sección de Transparencia y Acceso a la información Pública que deben tener todas las páginas web asociadas con la presente Resolución, se debe contar con un buscador en el que la ciudadanía pueda encontrar información, datos o contenidos. Se sugiere disponer de búsquedas a partir del texto del contenido, tipologías, temas, subtemas, palabras claves, entre otros. Al utilizar catálogos de texto plano estas búsquedas pueden ser potenciadas por motores externos o estrategias de federación de datos en datos.gov.co
- La sección de Transparencia y Acceso a la información Pública puede también disponer de un catálogo completo de todos los datos abiertos y la información pública que se encuentra disponible en dicha web, legible tanto para máquinas como para humanos. Esto con el fin de facilitar el acceso a la información a la ciudadanía.
- Se sugiere que la sección de Datos Abiertos que deben tener todas páginas web asociadas a esta Resolución direccione a la vista de datos del Portal de Datos Abiertos del Gobierno (datos.gov.co) para la información federada en ese portal, para la otra manejar vínculos a las páginas internas con URL's únicas.
- La cédula, si bien es un campo opcional en los formularios de PSRSD según la resolución debería ser más explícito que No es obligatorio para las solicitudes de información pública. Debería ser igual de fácil para la ciudadanía realizar peticiones de acceso a la información mediante el Formulario PSRSD con identidad reservada.
- Es fundamental que cada una de las entidades haga explícita la información que es reservada y que no puede ser pública de acuerdo a lo establecido por la Ley. Esta información puede estar disponible en la sección de Transparencia y Acceso a la información Pública y en el catálogo en texto plano de cada página ejemplo.gov.co/data.txt

Anexo 3. Condiciones mínimas técnicas y de seguridad digital

- La Resolución debería tener unos lineamientos claros de transparencia sobre compartir información con terceros. Los ciudadanos deberían poder conocer fácilmente el detalle de información que se comparte y con quién, ejemplo registro con facebook o google analytics para servicios del estado.
- La Resolución no tiene un contenido explícito respecto a auditorías de código de datos capturados o seguridad de la información con respecto al uso de aplicaciones. Es importante mencionar que la apertura del código fuente como código abierto permite un escrutinio público sobre cómo se manipula la información de los ciudadanos para garantizar su seguridad. Es fundamental el código abierto para garantizar el acceso a la información a la ciudadanía y por consiguiente su verificabilidad y auditoría.

- En el apartado de monitoreos de seguridad se debe aclarar que el uso legítimo de descarga masiva de información por máquina según los principios de la Ley de acceso a la información pública no puede ser interpretado como un ataque de negación de servicio (3.2.2. punto 22 al parecer duplicado con el 6).
- Así como se invita al uso de control de versiones para el código, también debería hacerse para los registros de versiones y archivos de documentos y bases de datos.
- Se invita al gobierno nacional que dentro de este anexo se establezcan mecanismos de autenticación de información dentro de los sitios web, a través de la creación de contraseñas fuertes, solicitar renovaciones periódicas de las mismas e incluso realizar verificaciones de dos pases. Además permitir la accesibilidad de persona con discapacidad a través del acceso a cuentas dentro de los sitios web.
- Se debería hacer la aclaración que los portales de gobierno por ninguna razón deberían almacenar contraseñas en texto plano. En oportunidades anteriores ciudadanos han evidenciado estas falencias con repercusiones contra ellos innecesarias cuando es responsabilidad de las entidades garantizar estos mínimos de seguridad.
- En los casos donde sea necesario hacer trazas de seguridad a comportamientos de usuarios normales, como logins, se debería comunicar públicamente qué información se está almacenando.
- Hablar de "proteger el binario de la aplicación, a través de métodos de ofuscación que impidan realizar procedimientos de ingeniería inversa (reversing) para analizar la lógica de la aplicación" va en contra de los principios de Transparencia hacía la ciudadanía para hacer verificación y control sobre aplicativos, especialmente cuando estos mismos empiezan a tomar decisiones automatizadas.
- Dentro de este anexo se debe establecer la necesidad de hacer públicas las filtraciones de información y de datos que han tenido sus propios sistemas o los servicios de terceros que se utilizan.

Con relación a este anexo, también es importante considerar que el texto del artículo 6 del proyecto de resolución señala que:

> **ARTÍCULO 6.** ***Condiciones mínimas técnicas y de seguridad digital*****.** Los sujetos obligados deberán observar las condiciones mínimas técnicas y de seguridad digital que se definen en el anexo 3 de la presente resolución.

Observar esas “condiciones mínimas técnicas” a las que se refiere el anexo que comentamos más arriba, genera también la necesidad de que se apropien lineamientos o políticas sobre rutas de divulgación sobre las vulnerabilidades en seguridad digital que afecten a los sitios web del Estado. Es necesario implementar para Colombia rutas de divulgación coordinadas, que hoy no existen y que redundará en el beneficio de todas las personas. Si bien la Política Nacional en Seguridad Digital aborda este aspecto, creemos que mientras se consolida su actualización, el borrador de resolución debiera poder considerar algunas de las recomendaciones sobre mejores prácticas que fueron propuestas por la Fundación Karisma en

su informe titulado “Estudio sobre rutas de divulgación en seguridad digital”[4]. Allí se propuso la necesidad de integrar una política sobre rutas de vulnerabilidad que:

1. Se apoye en estándares y experiencias internacionales.
2. Identifique las problemáticas existentes en este sentido y permita mejorar las rutas de divulgaciones existentes.
3. Implemente rutas de divulgación de confianza.
4. Minimice los riesgos legales para quien encuentra vulnerabilidades.
5. Desarrolle una comunicación que sensibilice sobre las divulgaciones responsables y coordinadas.
6. Cree una obligación de reporte de incidentes o violaciones de seguridad de datos en sectores específicos.

Este informe y recomendaciones como las que se resumen más arriba, puedan constituir un aporte en el mejoramiento que está buscando el Estado colombiano para incrementar su capacidad de detección y, por lo tanto, de resolución de los problemas en seguridad digital que creemos, puede enriquecer el contenido de la resolución sometida a comentarios.

Anexo 4. Datos Abiertos

- No se hace referencia a la pertinencia de enfoques diferenciales para la ciudadanía. Invitamos al gobierno nacional a evaluar la importancia de utilizar datos e información relevante en términos de diversidad y enfoque de género, de raza, entre otros, que pueda ser de utilidad para luchar contra la discriminación de las personas históricamente excluidas y hacer este esfuerzo explícito en la resolución.
- En el punto que dice "Los sujetos obligados que cuenten con portal propio de datos abiertos deben federar o vincular la información con el Portal de Datos Abiertos www.datos.gov.co o el que haga sus veces", se debe aclarar que esto aplica para la información estructurada como tablas de datos abiertos compatibles con el sistema de datos.gov.co, para otros tipos de información las entidades deben garantizar el acceso independiente de si existe una integración con el portal nacional, en ese caso recomendamos implementar soluciones de bajo costo como la publicación de catálogos y vínculos a información abierta como archivos de texto plano usando las especificación data.txt descrita anteriormente.
- El numeral 3 del artículo 4.2 establece los términos de licenciamiento. Se recomienda sugerir una licencia apropiada para no generar cuello de botella en la publicación de información. Unas sugerencias de licencia utilizadas en otros países son las Creative Commons, CC0 y CC-BY.

[4] El informe completo puede leerse aquí:
https://web.karisma.org.co/aportes-para-un-entorno-seguro-y-confiable/