Comentarios de Fundación Karisma al documento de Servicios Digitales Básicos

Fundación Karisma es una organización de la sociedad civil colombiana que busca responder a las amenazas y oportunidades que plantea la "tecnología para el desarrollo" al ejercicio de los derechos humanos, desde perspectivas que promuevan la libertad de expresión y las equidades de género y social. Trabajamos desde el activismo, incorporando múltiples miradas — legales y tecnológicas — en coaliciones con socios locales, regionales e internacionales.

En el marco del trabajo que adelantamos, hacemos seguimiento a las diferentes iniciativas de política pública del Gobierno colombiano. En esa línea, desde 2015 hemos prestado atención a la propuesta de Carpeta Ciudadana del Ministerio de las Tecnologías de la Información y las Comunicaciones (en adelante, Ministerio TIC) y durante el proceso de discusión abierto ara ese proyecto presentamos nuestros comentarios[1], haciendo énfasis en las preocupaciones generadas por el modelo y la poca información que el Gobierno proporcionaba sobre el mismo. Para 2016, este proyecto se unió con el de Interoperabilidad y Autenticación, a los que también les habíamos hecho seguimiento, en uno solo denominado "Servicios Digitales Básicos" (en adelante, SDB) que, de acuerdo con el Ministerio TIC, son creados "como una solución integral para resolver algunas problemáticas que viven los ciudadanos y las empresas a la hora de interactuar con el Estado".

Desde Fundación Karisma, hemos puesto nuestra atención en esta nueva propuesta del Ministerio TIC, manifestando nuestras inquietudes respecto del mismo en diferentes escenarios, incluso participamos del Taller de SDB convocado por este Ministerio, que se llevó a cabo el 10 de octubre de 2016 con la finalidad de recibir comentarios de la ciudadanía sobre el modelo que fue publicado en la página web www.urnadecristal.gov.co/serviciosdigitales.

En desarrollo del seguimiento que hemos hecho, por medio del presente documento presentamos los comentarios de la Fundación Karisma a los Servicios Digitales Básicos.

1. Comentarios sobre el proceso de participación

Para comenzar, reconocemos el esfuerzo del Ministerio TIC que en esta oportunidad y a diferencia de casos anteriores, ha publicado un texto completo que tiene una estructura y

[1] Ver "Comentarios de Fundación Karisma a la propuesta de Carpeta Ciudadana", disponible en: https://karisma.org.co/wp-content/uploads/2015/12/Comentarios-de-Fundaci%C3%B3n-Karisma-a-la-propuesta-de-Carpeta-Ciudadana-1.pdf

desarrollo concreto y no solo una presentación en PowerPoint. El documento explica el proyecto y expone el tema de forma que las personas interesadas pueden enterarse de lo que se pretende. Esta es una mejora sustancial respecto de esfuerzos pasados. Sin embargo, con el fin de que sirva para futuros procesos queremos plantear algunas observaciones sobre el proceso de participación desarrollado en este caso, que esperamos sean tenidas en cuenta cuando se abran documentos públicos a comentarios por parte de la ciudadanía:

1. El gobierno debe pensar en la ciudadanía cuando adelanta estos procesos para recibir comentarios. Si están uniendo varios proyectos, deben informar oportunamente por todos los canales habituales para que las personas que han estado haciendo seguimiento se enteren. De lo contrario, aunque no sea esa la intención, parece que estuvieran intentando cumplir formalmente, pero no en serio, con el propósito de abrir el documento a consulta.
2. Sería deseable contar con todos los documentos de las consultorías y los análisis que les sirvieron de base para el documento final, como el proyecto de decreto y los diferentes documentos técnicos (por ejemplo, diseño de la arquitectura, estándares para transmisión de datos, etc.). Eso facilita el proceso de análisis, además supone cumplir con la obligación de transparencia que tiene el Estado. Parte del problema que genera la ausencia de estos documentos es que no se entiende cómo, en este caso, se discutía en diciembre una serie posible de modelos y en el nuevo documento ya se presenta el modelo final sin justificar la selección. Eso es problemático porque, por ejemplo, el análisis de riesgo se se presenta recae sobre partes del modelo escogido pero no sobre el modelo en sí mismo. Suponemos que para la selección se realizaron análisis de riesgos sobre los posibles modelos, pero al no tener la información de este proceso es imposible saber porqué se escogió este en particular, qué consideraciones primaron y cómo se realizó la evaluación.
3. Es importante que cuando un documento se abre a comentarios públicos, se presente al tiempo un cronograma en el que se incluyan las fechas en las que se harán las reuniones de socialización y la metodología que se usará para atender los comentarios, los tiempos, etcétera.
4. También es necesario que las modificaciones a la convocatoria, metodología, las actualizaciones de documentos o de información se avisen y sean visibles. De lo contrario es difícil enterarse de los cambios. En el mejor escenario se debería dejar una historia pública del proceso donde se puedan seguir todas las modificaciones.
5. El plazo concedido para comentarios, aun cuando se amplió por petición de la ciudadanía, sigue siendo muy corto considerando la complejidad del documento en cuestión. Se espera que en la siguiente entrega, donde al parecer se podrá opinar en profundidad sobre aspectos técnicos y jurídicos se reevaluen los tiempos para facilitar la participación del a ciudadanía.
6. El nivel en que se presenta la arquitectura del proyecto es bastante básico, lo que no permite profundizar en aspectos técnicos. Por tanto, el nivel de análisis y de los

comentarios también adolece de la profundidad que amerita un sistema tan complejo.

7. Con el fin de poder tener un mejor seguimiento, cumplir con la necesidad de transparencia del proceso y ofrecer los insumos suficientes para la discusión. Es necesario que adicional a los documentos de la convocatoria particular, también se ofrezca acceso a todos los documentos de comentarios que se reciben, a las respuestas a solicitudes relacionadas y en general a cualquier documentación que permita a la ciudadanía conocer los diversos puntos de vista presentados.
8. Es deseable que los procesos de socialización incluyan mecanismos de participación remota, que también queden documentados y que se consideren espacios amplios con la participación de diferentes tipos de actores que puedan contribuir al debate con sus puntos de vista e intereses particulares.

A pesar de las fallas del proceso de comunicación del proyecto, que hacen que los consideraciones presentadas sean superficiales e insuficientes, Fundación Karisma presenta a continuación sus comentarios al documento de SDB:

2. Comentarios Generales

2.1. Integración de los 3 proyectos: Carpeta Ciudadana, Autenticación e Interoperabilidad

Queda claro que el nuevo proyecto SDB es la unión de los proyectos Carpeta Ciudadana, Autenticación e Interoperabilidad anteriores. Sin embargo, siguen siendo tres piezas diferentes que se ofertan de forma integral a través de un único servicio y esto no se refleja a lo largo del documento. El centro de atención está puesto en Carpeta Ciudadana. Se intuye que cada uno es independiente, especialmente cuando se establece que el servicio de Carpeta Ciudadana no será obligatorio para la ciudadanía, pero que las entidades del Estado tendrán que elegir obligatoriamente un operador para Interoperabilidad y Autenticación (p.17, Documento de Trabajo). Sin ser exhaustivos, esta situación supone una serie de problemas:

- En el documento no es claro si habrá operadores diferentes para autenticación, carpeta ciudadana e interoperabilidad, o puede ser uno mismo. Es importante aclarar mejor el tema para entender cómo funcionaría la propuesta y cómo se distribuirían responsabilidades.
- Las entidades del Estado están obligadas a usar el sistema pero los particulares no, pues para ellos es voluntario. Para las empresas, no está claro en el documento si el uso es obligatorio. Al formular preguntas sobre el tema en la reunión del 10 de octubre de 2016, establecimos que esto implica diferentes niveles de implementación de los diferentes proyectos, que no son claros. Especialmente, el documento no profundiza en lo que tiene que ver con el modelo de interoperabilidad, que no aparece en su total dimensión.

- En todo caso, el Estado pasará su información a un tercero (operador), así sea como "simple" intermediario, para que la administre y la ponga a disposición de las demás entidades y operadores. El operador tiene entonces un nivel de responsabilidad alto que debe ser claro en todo el documento, al respecto tan solo se menciona que es responsable del tratamiento de datos en forma superficial en la página 46.
- Hace falta enfatizar el rol de los privados que van a asumir funciones y responsabilidades del Estado y la forma como esto se enfrentará. No parece haber en el documento una discusión clara de la necesidad y el significado de que uno o varios operadores privados sean los intermediarios de la comunicación entre entidades del Estado y que va incluso más allá de la comunicación. Por ejemplo, en el proceso de escaneo y digitalización de documentos que hoy en día existen en el Estado solo en formato papel ¿se va a hacer con tercerización o de manera interna?
- En todo caso, la preeminencia de la Carpeta Ciudadana invisibiliza el análisis de elementos respecto de los otros proyectos, como que en la Interoperabilidad el ente regulador en relación con la protección de datos para el sector público es la Procuraduría General de la Nación y este control en Colombia aún no funciona. Si este proyecto entra a implementarse sin que ese control sea efectivo, no hay garantía apropiada para la ciudadanía en el uso de esta tecnología.

1.2. Privacidad por diseño (PpD) por omisión

Más allá de la protección de datos en la que el documento es más fuerte, la privacidad por diseño que se implementa parece ser una obligación para la forma como el operador desarrolla su negocio y no se aplica al propio diseño del modelo. Falla entonces la política al no trabajar desde el ejemplo y eso es precisamente lo que se está haciendo en otros países.

Es importante recordar que el primer paso de la PpD es analizar el impacto que el sistema va a tener en la privacidad de las personas. Se deben evaluar los riesgos que se pueden derivar de la implementación del nuevo desarrollo y, como ocurre en la evaluación de riesgos de seguridad, establecer alternativas o mecanismos para mitigarlos. En otros países se ha incluído la PpD precisamente como requisito para la "concepción" de nuevos sistemas, un análisis que debe ir paralelo al de riesgos de seguridad y que se refiere *al diseño del sistema*. La política que nos presenta el Ministerio TIC falla en este caso pues no la aplica al diseño del sistema sino que la relega a una obligación del operador.

Es importante resaltar una vez más que la PpD busca ir más allá de la protección de datos y por eso no puede pensarse como igual. No podemos hacer una evaluación completa en el plazo y con la información recibida pero podemos ofrecer algunas alertas: el análisis que se hizo en el documento sugiere que se evaluaron los riesgos de "seguridad y privacidad" y la realidad es que el análisis es de "seguridad digital y protección de datos".

En el documento sigue ausente una mirada más profunda de derechos humanos que no se detenga en la protección de datos sino que hable de la intimidad o privacidad de las

personas y sus riesgos. En este sentido, es importante recordar que se protege el derecho fundamental de las personas a la intimidad y a la protección de sus datos. No es, pues, un tema de "privacidad de los datos". Los datos no son sujetos de este derecho y por eso debe hablarse de "privacidad de las personas", no de los datos.

Por otro lado, la complejidad propia del sistema que se quiere implementar se basa en la idea del "consentimiento" de quienes lo van a usar y con razón recuerdan que el consentimiento es el soporte de la Ley de Protección de Datos. Sin embargo, aunque es legal, el riesgo de intimidad frente a un sistema como el propuesto es tan grande que, a la luz de los derechos humanos, debe reconocerse que el consentimiento (aunque con apoyo legal) es insuficiente. Se debe admitir que hay un dilema de consentimiento que ni se analiza ni se mitiga en este caso.[2] En un modelo de PpD ese tema debe ser especialmente cuidadoso y se pueden tomar medidas tales como establecer lo que se entiende por "consentimiento informado" con mucho detalle, establecer parámetros muy estrictos de las opciones por omisión que las personas deben aceptar, etcétera.

Esto pasa por analizar los riesgos y es lo que no se ha hecho. Si se hiciera, se establecería los riesgos de que este sistema se base en consentimiento y se podría identificar cómo mitigarlos. Adicionalmente, se puede anticipar que los SDB van a suponer el acceso de muchas personas que no tienen la capacidad, la destreza o el interés de personalizar la configuración que viene por omisión y, por tanto, la forma como ellas usarán los SDB estará en manos de los operadores. Un sistema diseñado con base en PpD obligará a que esas configuraciones sean especialmente protectoras de una población que, además, puede ser la más vulnerable. **Por lo tanto, es necesario evaluarlo y anticipar un proceso pedagógico y una información didáctica a la ciudadanía para que puedan familiarizarse con estos nuevos útiles.**

Es necesario que el sistema también establezca mecanismos de mitigación de riesgos que se identifiquen en materia de PpD. Por ejemplo, un riesgo que seguramente se establecerá es que el sistema sea abusado y se entregue información (Carpeta Ciudadana) a quien no corresponda o que se comparta (Interoperabilidad e incluso Autenticación) con quién no está legitimado. En ese caso, una estrategia de mitigación es que los operadores produzcan informes sobre con quién se comparten los datos que deben llegar a las personas usuarias, pero también a un ente de control independiente. Todos los actores deberán producir informes de transparencia sobre temas de protección de datos y también de privacidad (que incluyen otros tópicos que van más allá de la protección de datos).

1.3. Perímetro del análisis de riesgos

El primer paso de un análisis de riesgo es definir su perímetro. En el análisis de riesgos, "frente a la privacidad y seguridad de la información y datos personales", no se define este

[2] Pueden consultar "Autogestión de la privacidad y el dilema del consentimiento" de Daniel Solove, publicado en la revista chilena de Derecho y Tecnología que puede consultarse en http://www.rchdt.uchile.cl/index.php/RCHDT/article/view/30308

perímetro. Sin embargo, por su alcance podemos deducir que el análisis se limita a los operadores y, en consecuencia, no considera el sistema en su globalidad con todas las interconexiones de los 3 proyectos y sus muy diversos actores. En su mayoría, el operador al que se refieren es al de carpeta ciudadana.

La ausencia de un perímetro de análisis más amplio excluye los riesgos derivados del sistema como tal (de los 3 proyectos, no solo del de Carpeta Ciudadana), además de los otros actores: los operadores – más allá de las funciones de Carpeta Ciudadana –, el Estado, las personas usuarias, el ente regulador, etcétera.

Es necesario que el documento amplíe el perímetro del análisis de riesgo y definirlo de manera clara.

1.4. Servicios básicos + Servicios de valor agregado

Otro ejemplo de la necesidad de determinar la independencia de los proyectos que conforman los SDB, es que el Ministerio TIC debe especificar cómo funcionarían los servicios de valor agregado para interoperabilidad y autenticación. De nuevo, parece estar centrado en Carpeta Ciudadana.

De otro lado, dado que los servicios básicos son pagados por el Estado deben estar protegidos por omisión de su explotación comercial (publicidad, minería de datos, etcétera). Específicamente, debe haber una provisión clara sobre la necesidad de que los datos estén cifrados tanto en tránsito como en reposo, lo que añadiría un elemento técnico de confianza a la decisión política de impedir la explotación comercial de los datos e incluso los metadatos materia del proyecto.

Aunque se ha mencionado que los operadores pueden ofrecer “servicios de valor agregado” con el fin de atraer usuarios. Aún no hay lineamientos para este tipo de servicios. Aun así, estos nuevos servicios también deben considerar las necesidades de garantías para la privacidad de las personas usuarios y la seguridad de los datos asociada con dichos servicios.

1.5. Estrategias de mitigación

El análisis de riesgos que ofrece el documento incluye estrategias de mitigación. El documento debería explicar quién es el responsable de la mitigación en cada caso, establecer cronogramas, crear obligaciones de evaluación de la implementación del plan y de documentar los cambios que se hagan en adelante si es que no funciona como inicialmente se planeó.

Parece que en algunos casos la mitigación se hará en la reglamentación y, en otros, se hará por el operador. Debería haber más y mejores detalles sobre esta mitigación, indicar los mínimos que se permitirán, incluso para efectos de aplicar mejor la PpD, y ser claros sobre

cuáles de esas estrategias serán parte de la regulación, cuáles se trasladan al operador, etcétera.

Adicionalmente, debe haber claridad sobre los tiempos de implementación de las medidas y la forma como se ajustarían una vez implementadas, en caso de que no fueran suficientes para mitigar el riesgo identificado.

1.6. Seguridad digital

- Falta hacer énfasis sobre quienes son los responsables y encargados del tratamiento de datos personales y extenderles obligaciones al respecto. El operador recibirá datos que corresponden a funciones que son en esencia del Estado, por tanto, el estándar debe ser más alto. Esto es algo que falta desarrollar a profundidad.
- Ante la ausencia de un análisis de riesgo que se ocupe de los 3 proyectos que recogen los SDB, también vemos con preocupación la ausencia de identificación del riesgo de abusos que puedan generarse en el uso de equipos que verifican la identidad de las personas usuarias en la etapa de enrolamiento y, por tanto, la falta de acciones concretas sobre este tema en el plan de mitigación.
- La implementación del cifrado de datos puede apuntar hacia una tensión fundamental del proyecto. Cifrar los datos en reposo y en tránsito puede ser una medida efectiva para evitar que los operadores accedan a ellos sin autorización de las personas usuarias. Sin embargo, los sistemas de cifrado fuertes suelen ser funcionalmente complejos y esto puede desestimular el uso del sistema para aquellas personas menos familiarizadas con los protocolos de seguridad necesarios para mantener y gestionar documentos y comunicaciones cifradas. Reconociendo esta tensión, en cualquier caso, no puede ganar la funcionalidad sobre la seguridad, por tanto, es necesario establecer la evaluación que el gobierno hizo del modelo elegido de cifrado y de la forma como se realizará la gestión y almacenamiento de las claves públicas y privadas que protegen ese cifrado. En la reunión del 10 de octubre pasado, el gobierno mencionó que las claves que permiten descifrar los documentos de las personas usuarias que estén almacenados en la Carpeta Ciudadana van a ser separadas en dos mitades, que estarán en custodia del operador con una separación organizacional y técnica de los accesos, en una(s) base(s) de datos. Sin embargo, esto significa que el operador tiene la capacidad, juntando los conocimientos y derechos de acceso de varios de sus empleados, de descifrar estos datos lo que se mantiene como una preocupación. En relación con los servicios de interoperabilidad y autenticación tampoco sabemos nada del sistema de cifrado.
- Desafortunadamente, la información técnica del proyecto ha sido publicada hasta el jueves 13 de octubre en horas de la tarde, por lo que para la redacción de estos comentarios no conocimos los detalles de la arquitectura del sistema y solo podemos suponer cosas y plantear preocupaciones con base en ella. Suponemos que el descifrado de los documentos se haría en un servidor del operador y no en el

dispositivo del cliente (en el equipo de la persona usuaria). Si esto es así, implica que probablemente habrá un servidor (aplicativo, por ejemplo) que tendrá las cuentas y las claves de acceso a estas dos bases de datos que contienen las mitades de clave. Es decir, habrá un punto y unas personas en el sistema de los operadores con la posibilidad de tener acceso a las claves completas y, por lo tanto, con capacidad de descifrar los documentos de las personas. Este punto seguramente será susceptible de futuros análisis técnicos que requieren mucho más tiempo.

2. Otros problemas

- La implementación de la biometría como medio de identificación genera un alto riesgo de privacidad, en particular si se tiene en cuenta que en ese caso el operador posiblemente deberá almacenar datos biométricos. Además, la identificación biométrica plantea riesgos intrínsecos de seguridad digital. Por ejemplo, si mi huella digital está comprometida (alguien logró copiarla y hacer un molde), no la puedo cambiar y por tanto este factor de identificación y cualquier sistema asociado a él, se vuelve inútil. En cambio, cuando lo que se usa es una clave, una tarjeta chip, un token, si el certificado es robado o se ve comprometido, es posible invalidarlo y generar uno nuevo. Además, la implementación de procesos de autenticación biométricos, más allá del momento de enrolamiento, nos parece complicado desde un punto de vista funcional. ¿Acaso se van a distribuir lectores biométricos a la ciudadanía? ¿Cómo se instalarán y adaptarán a sus equipos? La biometría es un tema muy controversial en el mundo y los problemas y preocupaciones que introduce están bien documentadas. Sin embargo, el documento menciona estos problemas y preocupaciones muy superficialmente. Este es un tema poco desarrollado y no se analiza desde la óptica de los riesgos. Posiblemente esto se deba a que ni la autenticación ni la interoperabilidad son los ejes del documento. Sin embargo, esta ausencia es grave. Si bien en la reunión del 10 de octubre pasado se habló de que el enrolamiento, necesario para garantizar la autenticación estaba atada a todo el sistema de la Registraduría, lo cierto es que en el documento la opción de que la autenticación biométrica sea usada en otros momentos por el sistema está abierta. Es importante considerar que el uso de biometría en ese caso supondrá la protección de bases de datos con información que son datos personales sensibles y por tanto deben ser objeto de protecciones especiales de seguridad.
  Con la información que tenemos y por las razones descritas (privacidad, seguridad digital y funcionalidad), proponemos suprimir la posibilidad de autenticación por biometría y nos reservamos la oportunidad de comentar en particular sobre el proceso de enrolamiento cuando se tenga mayor información de carácter técnico para evaluar dicha fase.

- El documento insiste en que debe implementarse un sistema basado en neutralidad tecnológica. Sin embargo, esta neutralidad se considera desde la óptica de los

operadores pero se guarda silencio respecto de la ciudadanía. La ciudadanía debe poder acceder a los sistemas desde cualquiera que sea la opción tecnológica que haya escogido y esto debe garantizarse por el operador. En la actualidad hay ejemplos de organismos estatales (la DIAN, por ejemplo) en donde la ausencia de estas consideraciones suponen una verdadera negación de sus servicios para las personas que se ven obligadas a adquirir programas costosos y desactualizados (por tanto, inseguros) o incurrir en piratería. Ahora bien, como no conocemos la arquitectura del sistema propuesto ni su análisis de riesgos, no podemos controvertir la alegada neutralidad tecnológica en el documento que, como regla general, es un buen principio. Sin embargo, se conocen casos de políticas que exigen determinadas tecnologías en puntos concretos de esas arquitecturas – por razones de seguridad o privacidad – que en la medida en que son excepciones a la regla son perfectamente válidas, como la utilización de software libre para módulos que requieran acceso al código fuente para facilitar la tarea de control sobre su funcionamiento o facilitar procesos de interoperabilidad. Este punto no es posible desarrollarlo sin mayor información.

- En la reunión del 10 de octubre de 2016 se nos dijo que las consideraciones sobre neutralidad tecnológica necesarios para garantizar el acceso a los SDB por parte de la ciudadanía desde cualquier tipo de dispositivo y sistema operativo, se abordaba en el punto de accesibilidad. Al respecto, hacemos un llamado al Ministerio TIC, a utilizar la definición estándar. “Accesibilidad”, en su acepción más común en temas tecnológicos de “Accesibilidad web” se refiere a la necesidad de facilitar el acceso a los sistemas a la población con alguna discapacidad, algo que también está ausente en esta política y debería adoptarse como ya lo ha sido para otros proyectos del Ministerio.

- El documento no es claro sobre cuál es el ente regulador. En la reunión del 10 de octubre se mencionó que dependiendo del tópico son varios los entes reguladores. Ese detalle no aparece en ninguna parte en el documento ni forma parte del análisis de riesgo que establecería, como ya mencionamos, la inoperancia de la Procuraduría como autoridad que vigila el cumplimiento de la Ley de Protección de Datos para el sector público.

- Análisis de datos por algoritmos y prevención de discriminación (*Equal opportunity by design*): En el documento, se hace referencia al análisis de grandes volúmenes de datos (big data) (ver p. 28) como un escenario operacional consistente en la virtualización de datos en el campo de las operaciones que pueden desarrollar las entidades estatales como actores del sistema. En concreto, el documento dice:

> ***Virtualizar datos:*** *Permite a las entidades contar con una forma de recopilar grandes volúmenes de datos provenientes de diversas fuentes al interior de sus áreas funcionales y mostrarlos de forma centralizada para su posterior*

uso, facilitando y agilizando la provisión de información a los trámites y servicios que ofrecen a los usuarios [sic] con el fin de mejorar el rendimiento y hacer más oportuna la respuesta.

Este no es un tema marginal, pero es tratado como una pequeña parte del proyecto (como ya dijimos el eje del documento es la Carpeta Ciudadana y, en consecuencia, se excluyen las funciones de autenticación y de interoperabilidad). Si se hace el análisis desde PpD sobre todo el sistema y se amplía el perímetro del análisis de riesgo de protección de datos y seguridad digital a la interoperabilidad, este tema debería ser uno de los ejes centrales del documento. Entre las ausencias del análisis está que, si para big data se va a usar algoritmos que soportan los procesos de toma de decisiones individuales o colectivas, se recomienda usar principios de *equal opportunity by design* y transparencia frente a la ciudadanía como se plantea actualmente en Estados Unidos[3] y en Europa[4].

2.1. Sobre el análisis de riesgo

Respecto al análisis de riesgos (p 32-36 del documento), queremos hacer comentarios específicos en los puntos siguientes :

- Conformidad (ver p. 32): En la estrategia de mitigación se debe añadir cláusulas contractuales que, en particular, obliguen a cumplir estándares determinados y reglas que usualmente no se hacen extensibles a los particulares (por ejemplo, es el caso de estándares de seguridad, accesibilidad y usabilidad, pero no exclusivamente) y que les obligue a permitir auditorías y evaluaciones del Estado.

- Pérdida de información (p 33): Este punto no es claro, pues mezcla dos riesgos muy distintos sin diferenciarlos claramente:
    - Borrado o modificación de información por error, lo que se relaciona con el tema de las copias de seguridad;
    - La fuga de información, que tiene que involucra problemas técnicos como fallas en el cifrado y otras medidas de protección informáticas y problemas humanos como los provenientes de prácticas de ingeniería social o venta de datos personales e información privada o reservada por parte de empleados de los operadores con permisos de acceso.

[3] *Big Data : A report on algorithmic systems, oportunity and civil rights*, White House, May 2016 ; https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf

[4] El artículo 14-2-g del nuevo Reglamento Europeo de protección de datos menciona que el responsable de tratamiento facilite información sobre los procesos automatizados de decisión, su lógica y sus consecuencias. En la nueva ley francesa sobre una "República numérica" (artículo 4) menciona que "*Una decisión individual fundada en un algoritmo tiene que mencionarlo explícitamente, informando a la persona. Las reglas que definen este tratamiento, tanto como las principales características de su aplicación son comunicadas a la persona si ella lo pide*.".

- Robo de sesión: Quizás otra medida de mitigación fácil de implementar sería proveer en la misma interfaz visible a la persona usuaria la información de sus últimas conexiones (fechas y horas), de modo que, pueda establecer si alguien se conecta en su lugar y protocolos y mecanismos ágiles de respuesta antes tales situaciones.

- [Personas] usuarias con privilegios de acceso: No es clara la distinción entre los "usuarios-ciudadanos o usuarios-empresas" (los verdaderos usuarios del sistema) y los empleados del operador quienes tienen cuentas de acceso al "back-end" del sistema. Aquí parece que se trata del segundo caso ("*usuarios con elevados privilegios que no deberían tener acceso a los datos*"), pero se sigue empleando el mismo término "usuario", lo cual puede generar confusión.

- Recuperación (p 35): Esta parte tiene que ser más precisa en las exigencias. No se sabe si se habla solo de "recuperación" del sistema en un tiempo dado en caso de desastre (incendio, problema eléctrico grave, etcétera) o de garantizar un sistema de alta disponibilidad, lo que implica por lo menos dos equipos en configuración "activo-activo" ofertando el mismo servicio de forma tal que los clientes puedan conectarse a cualquiera de ellos indistintamente. Además, para la recuperación de datos y las copias de seguridad hay que definir tiempos aceptables de reestablecimiento de servicios en caso de fallos. Quizás estos detalles están en otros documentos. Este comentario está en concordancia con el siguiente (disponibilidad).

- Disponibilidad: Véase los comentarios del punto anterior sobre recuperación. "*[L]as operaciones críticas se pueden reanudar inmediatamente y todo el resto de operaciones, en un tiempo prudente*". Si esto implica una redundancia con sistemas "activos-activos" para estas operaciones críticas. Es necesario mencionarlo explícitamente.

- Respuesta a incidentes (p 35): La primera columna no es la expresión de un riesgo, son medidas para protegerse del riesgo de "incidentes no detectados".

- Órdenes judiciales: "*Revelación de datos a partes no deseadas por incautación de hardware físico a raíz de una orden judicial de las autoridades*". En este punto, ¿se refieren a "incautación" de equipos de la ciudadanía o de los operadores? Esto no es claro y quizás por eso la estrategia de mitigación que se propone "*Cumplimiento de políticas que en la materia sean definidas por el Ente Regulador en el marco de la legislación vigente*" es tan vaga. Cabe preguntarse cuáles son estas "*políticas en la materia*".

- Conclusión de la tabla (p 36)**:** En cuanto a "integridad, confidencialidad y disponibilidad", es importante añadir el "no repudio" en este contexto (diligencias en línea).

- El enlace de la nota 52 relacionado con el modelo de seguridad habilitado por el ministerio TIC no está disponible http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_Seguridad.pdf.

3. Recomendaciones

Debido al corto tiempo para analizar el documento y al hecho de que al momento de preparar los comentarios no se conocen los detalles técnicos, creemos que es conveniente mejorar el esquema de participación que hasta ahora ha seguido el Ministerio TIC para que el proyecto pueda ser desarrollado teniendo en cuenta las miradas de los diferentes sectores interesados. Por ahora no tenemos una lista completa de recomendaciones, pues no contamos con la información suficiente. Esperamos, sin embargo, que las que se encuentran repartidas en el documento les sean útiles y en todo caso recopilamos algunas.

En suma, sin pretender ser exhaustivos, reconociendo los límites establecidos por la imposibilidad de estudiar a fondo el anexo técnico y la ausencia de algunos de los documentos de soporte, y los problemas de tiempo mencionados al comienzo del documento, recomendamos

- Poner a disposición los documentos técnicos relacionados con el proyecto con tiempo suficiente para hacer comentarios relevantes. Igualmente ofrecer acceso a la documentación de las fases anteriores de los proyectos.
- Realizar más encuentros entre el Ministerio y cada sector, además de permitir que estos espacios también reúnan diversos sectores.
- Desarrollar a profundidad cada uno de los tres servicios que integran el proyecto y realizar una nueva socialización del documento. De hecho es importante que evalúen hasta qué punto en realidad el modelo propuesto integra tres servicios diferentes, y considera las necesidades y particularidades de cada uno y no es simplemente la respuesta a uno de ellos, el proyecto de Carpeta Ciudadana. En ese sentido lo más importante es que se debe considerar la conveniencia, necesidad y riesgos en todo nivel de implementación de un modelo donde varios operadores serán intermediarios en la comunicación entre entidades estatales y en la autenticación de la identidad de las personas que hacen uso de servicios estatales.
- Realizar un análisis de impacto de privacidad de todo el sistema y de cada una de sus partes. Mencionamos como deseable medir el impacto de las potenciales personas usuarias de los servicios a partir del propio diseño de la política en su totalidad y no solo de cada uno de sus elementos. Hasta ahora, como se explicó, solo parece haber un análisis de Carpeta Ciudadana.
- Ampliar el perímetro del análisis de riesgos a la protección de datos y a la seguridad digital para incluir los demás actores, además de los operadores, y las conexiones entre los sistemas.
- Considerar una implementación de cifrado de los documentos almacenados en la Carpeta Ciudadana, concebido de tal forma que solo el ciudadano y las entidades con las que decidió compartir los datos pudieran descifrar los documentos, con la consiguiente aplicación de un descifrado al nivel del “cliente”.

- Eliminar la biometría dentro de las posibilidades para la autenticación. En todo caso debe considerarse la necesidad e idoneidad de involucrar la información biométrica de las personas usuarias en los diferentes puntos del sistema.