1. Planteamiento del Problema

En nuestro país existe un sistema de identidad digital que ha crecido de manera inorgánica, desconectado de las necesidades reales de los ciudadanos, y que no ha tomado en consideración algunos derechos importantes de las personas (naturales y jurídicas)

Ello se evidencia en una diversa problemática que el grupo de trabajo ha identificado

1.1. Crecimiento Inorgánico

- Falta de identificación de actores (personas naturales y jurídicas) en entornos digitales
- No se tienen claro los roles en el sistema actual de identidad digital
- El proceso de registro y actualización en los sistemas de identidad digital es lento
- Falta integración de los atributos de identidad digital
- Distintos estándares de manejo de identidad para diferentes actores. Ejemplo: A los ciudadanos residentes los atiende RENIEC de acuerdo a su normativa propia; la identidad oficial de los extranjeros es manejada por Superintendencia de Migraciones con sus propios esquemas.
- No existe un punto único de sesión para los diferentes servicios de identidad que ofrece el estado
- Cada entidad responsable de la identidad tiene sistemas heterogéneos y no se ha establecido un esquema homogéneo de interconexión entre estas entidades para manejar integradamente los servicios de identidad.
- No contamos con soluciones tecnológicas que puedan ser implementadas a gran escala. Principalmente las soluciones en el Estado son aplicables a pilotos.

1.2. Desconectados de las necesidades de los ciudadanos

- Los sistemas de identidad digital se han diseñado y funcionan pensando en un usuario urbano, que ya cuenta con dispositivos electrónicos para comunicarse, no se han pensado para un usuario de las regiones, que inclusive puede estar fuera de la economía formal y tiene necesidades de servicios distintos y específicos, que el estado debe proporcionar.
- Los atributos que conforman la identidad digital están desintegrados entre las diferentes entidades. En el caso de los servicios públicos, las distintas entidades del estado no se han puesto de acuerdo para

intercambiar, de forma automática, los datos absolutamente necesarios para brindar servicios, que le eviten al usuario hacer colas en diferentes entidades, el uso de papeles y realizar procedimientos engorrosos, y, todo ello, sin la seguridad de que esa información la maneje únicamente quién la necesite para brindar el servicio.

1.3. No considera derechos importantes de las personas

- Las personas no ejercen su derecho a ser identificadas y a controlar el acceso y uso de su información a través de medios digitales
- El sistema de identidad digital solo sirve para autenticar más no para que el ciudadano consienta el uso de su información, según los atributos usados para su autenticación, y según el nivel que este autorice.
- Falta delimitar el uso de los atributos que componen la identidad digital, es decir, no hay un uso racional que respete el principio de privacidad: La información de usuario sólo se expone a las entidades adecuadas en las circunstancias adecuadas

2. Requisitos para un nuevo modelo de identidad digital

Por otro lado, el grupo de trabajo ha establecido una serie de requisitos que, estimamos, deberían tomarse en cuenta en el desarrollo de un nuevo modelo de identidad digital:

- Los distintos proveedores de identidad deberían integrarse, sobre todo cuando manejan atributos comunes, para agilizar el registro y actualización de la identidad y la entrega de servicios.
- Las personas (naturales y jurídicas) deben ejercer su derecho a identificarse, manifestar su voluntad para controlar el acceso a su información personal (tributaria, financiera, de salud, etc.), al solicitar servicios y adquirir bienes por medios digitales.
- El modelo debe permitir que el ciudadano controle quién va a tener acceso a su información según el nivel que él le haya autorizado, y ofrecerle diferentes opciones de proveedores de identidad, con capacidad de emitir distintas credenciales, que lo autentiquen en función a las transacciones o servicios que él requiera.
- El sistema de identidad digital debe tener un punto único de inicio de sesión.
- Debe tener una alta escalabilidad, ser tolerante a fallos, con redundancia múltiple.
- El sistema de identidad digital debe estar interconectado con diferentes entidades como RENIEC, Migraciones y Registros Públicos para autenticar tanto a las personas naturales como jurídicas. Es necesario para ello tener un esquema de conexión homogéneo con todas estas entidades.
- La base de datos de los atributos que conforman la identidad debe estar validada para evitar suplantaciones o fraudes al momento de brindar servicios.
- El modelo debería tomar en cuenta los casos de éxito y las lecciones aprendidas de otros países que ya han avanzado en esta materia.
- Parte del modelo debe ser un glosario que permita un entendimiento común de todos los que participen en su desarrollo o uso.

3. Glosario

Atributo:

Una cualidad o característica atribuida a alguien o algo.

Autenticación:

Verificación de la identidad de un usuario, proceso o dispositivo, generalmente es un requisito previo para permitir el acceso a los recursos de un sistema.

Autenticación biométrica:

Es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para su autenticación.

Autorización:

Una decisión de conceder acceso, generalmente, en forma automática, mediante la evaluación de los atributos de un sujeto.

Autenticador:

Algo que caracteriza al usuario, como, por ejemplo, un rasgo biométrico, o que él conoce, como una contraseña, o que él posee, como un dispositivo criptográfico, y que utiliza para autenticar su identidad

Biometría:

Es el estudio para el reconocimiento inequívoco de personas basado en uno o más rasgos conductuales o físicos intrínsecos.

Credencial:

Es un objeto o estructura de datos que vincula documentadamente una identidad -a través de un identificador o identificadores- y (opcionalmente) atributos adicionales, a al menos un autenticador poseído y controlado por un usuario.
Generalmente se supone que el usuario mantiene la credencial, también se utilizará el término para referirse a los registros electrónicos mantenidos por el Proveedor de Servicios de Credenciales que establecen la vinculación entre el(los) autenticador(es) del suscriptor y la identidad.

Factor de autenticación:

Hay tres tipos de factores de autenticación: "algo que uno sabe", "algo que uno tiene" y "algo que uno es". En una autenticación se puede usar uno o más factores de autenticación.

Protocolo de autenticación

Una secuencia definida de mensajes entre un usuario y un verificador que demuestre que el usuario tiene posesión y control de uno o más autenticadores válidos para establecer su identidad y, opcionalmente, demostrar que el usuario se comunica con el verificador previsto.

Usuario:

Desde el punto de vista de la identidad digital, es un sujeto cuya identidad debe verificarse utilizando uno o más protocolos de autenticación.