| ACTIVIDAD / TEMA | Reunión de Líderes del grupo de identidad digital de la CODESI | Fecha | 05/09/2017 |
|---|---|---|---|
| LUGAR | Oficinas RENIEC | | |
| ASISTENTES: | | | |

| NOMBRES Y APELLIDOS | ROL/CARGO | E-MAIL | ENTIDAD |
|---|---|---|---|
| Ricardo Saavedra | Líder Público | | RENIEC |
| Javier Casas | Líder Sociedad Civil | | Suma Ciudadana |
| Jorge Cabrera | Líder Academia | | UPC |
| Ivan Otarola | Facilitador Técnico | | MTC |
| Tobías Aliaga | Gerente de Innovación | | RENIEC |
| Fernando Zapata | | | RENIEC |

## AGENDA DE LA REUNIÓN

- Revisión de objetivos y principios

## TEMAS TRATADOS Y ACUERDOS

Se hizo una recapitulación de lo realizado en cada una de las reuniones del grupo de trabajo de la CODESI, se explicó que en la última reunión se presentó el modelo de identidad para el sector público para tener una base de discusión, acordándose recibir comentarios al respecto hasta el día 1 de septiembre, hasta el momento sólo ha enviado sus comentarios la Cámara de Comercio de Lima.

Se explicó que el objetivo de esta reunión era tener una coordinación previa de los líderes para la reunión programada con todos los participantes para el 15 de septiembre, en la primera reunión se hizo un taller con los participantes formándose cuatro equipos de trabajo cada uno de los cuales definió los objetivos del grupo, luego de la reunión uno de los participantes acotó que, previamente a los objetivos del grupo, habría que definir los objetivos y principios de la identidad digital para el Perú, por ello es que se presentó, en la segunda reunión del grupo, ejemplos de objetivos y principios de un ecosistema de identidad digital para el Perú, como puntos o temas a discutir con los participantes.

Como primer punto de agenda se propuso revisar lo que desarrolló cada grupo en el taller, buscando identificar principios y tratando de clasificarlos de acuerdo a criterios comunes

En lo desarrollado por los grupos de trabajo se menciona lo siguiente:

Grupo 1:

- Planteamientos conceptuales
- Lineamientos
- Factibilidad técnica legal
- Protección de datos y transparencia

Grupo 2

- Principios y de acuerdo a ello un modelo de identidad digital,
- Modelo de estrategia y un marco regulatorio,
- Pruebas de concepto.

Grupo 3

- Conceptos. normativa recogida

- Sistema de identidad digital como parte del proyecto Perú digital
- Diagnóstico del estado del arte
- Principios, productores y consumidores de entidad digital
- Definir un glosario de términos.

Grupo 4

- Actores,
- Necesidades de cada actor
- Temas de protección de datos
- Concientización digital
- Confianza

Se observa que hay bastante concordancia en trabajar temas de principios, conceptos y lineamientos. Surge la pregunta sobre si existe formalmente una línea de base, que origine que este tema sea importante en la CODESI, El líder público plantea como base de discusión los diferentes contextos de actuación que tiene la identidad y su interacción en muchos niveles, por ejemplo en redes sociales. Sobre todo ello existe un concepto de identidad oficial, en el caso particular del Perú, se ha definido que la identidad oficial de las personas debe ser gestionada por una entidad constitucionalmente autónoma, que es el RENIEC que ha venido trabajando para otorgar credenciales a todos los peruanos.

A nivel de identidad el Perú es un caso de éxito pues se ha logrado incorporar al 99.3% de la población, y existe prácticamente un código único de identidad, que es la que se usa en diferentes entidades públicas y privadas, Pero existe otras identidades que pueden usarse en otros servicios como en las redes sociales. Suena lógico usar una sola identidad oficial pues facilitaría saber qué servicios se le brinda al ciudadano y con qué problemas se enfrenta en esos servicios. En el ámbito privado es diferente pues es a criterio y libre albedrio de las personas elegir su identidad.

Se menciona también que hay un punto a considerar, que es el ámbito de las personas jurídicas que normalmente no se contemplan en estos sistemas de identidad. Si hablamos de una personería jurídica, en el Perú hay un registro para ellas, que es administrado por la Superintendencia Nacional de los Registros Públicos SUNARP, también se maneja en la SUNAT una identificación de esas personas jurídicas a través del código RUC, sin embargo, hay un número RUC que se genera para las personas naturales, que son 1 millón de personas. Ese grupo representa una parte importante de la población activa. Hay un servicio de beneficios tributarios que ofrece la SUNAT, al cual se accede a través de una página web, pero solo está disponible para las persona jurídicas, permitiéndoles acceder a ellos a través de páginas web y esos mismos beneficios no se dan a las personas naturales allí registradas.

La consulta es, si además de las personas naturales, debemos considerar a las jurídicas o ¿quién más debe ser considerado dentro del modelo de identidad?. Se menciona que en la sociedad actual, dada la importancia creciente del Internet de las cosas, es necesario tener identificado a los activos o cosas, y se hace importante conocer alguno de sus atributos como la naturaleza del activo, el fabricante, sus propiedades, la naturaleza del activo.

Se pregunta cuál sería el fin de considerar los activos, dado que lo que se busca es definir los principios como por ejemplo garantizar la transparencia, la privacidad, la seguridad, etc. y el objetivo puede ser establecer los mecanismos, infraestructura y modelos de identidad.

La problemática de la persona natural y la persona jurídica tiene sus diferencias por el hecho de que hay, por ejemplo, varios representantes de una empresa que pueden tener diferentes roles y responsabilidades, y pueden variar con el tiempo, y una persona jurídica puede a su vez generar otra persona jurídica, hay empresas que piden que de una clave de sol madre se generen otras claves hijas, las cuales se entregan a diferentes personas.

Se menciona que en el caso de las empresas a veces no tienen una inactividad permanente como ocurre con las personas, que al fallecer su estado es irreversible; en el caso de una empresa esta puede estar inactiva temporalmente y luego reactivarse. Se menciona que las personas naturales intestadas pueden generar nuevos datos y atributos luego de fallecer, inclusive considerando su parentesco o relación con otras personas, por los temas de herencia.

Se pregunta cómo se hace cuando se instala un certificado digital en un servidor, se indica que lo primero que se busca es identificar a la persona natural que representa legalmente a la entidad donde se aloja el servidor y que se hace responsable del buen o mal uso del certificado, una vez identificada la persona responsable se identifica el servidor por una serie de atributos como la dirección MAC, la IP, etc. Y se

instala el certificado, se debe tener en cuenta los casos en los que un servidor puede suplantar a otro, lo cual ya tiene que ver con temas de seguridad.

Se indica que también se debe tener en cuenta a los extranjeros que residen en el país, hay un registro de los mismos que es contemplado por Migraciones

Resumiendo hasta el momento lo que se ha conversado; una tarea debe ser definir los diferentes actores; quiénes son los que deben ser identificados, para ello el grupo debe definir un modelo que no debe ser restrictivo, que defina roles que puedan ser ejecutados por diferentes entidades, públicas o privadas, con los diferentes mecanismos electrónicos y tecnológicos necesarios para realizar adecuadamente su función,

Uno de los líderes planteó como un principio que exista una única identidad digital, la tecnología que se va usar para obtenerla y usarla es un tema distinto, ese sería un principio: una identidad digital única tanto de las personas naturales como de las personas jurídicas. Se aclaró que esta identidad única sería para el ámbito público, es decir, para la interacción con el estado. En el ámbito privado hay un concepto que influye en el tema de identidad digital que es la confianza necesaria para dar un servicio, hay algunos privados a los que les basta una cuenta de Facebook o de correo electrónico para identificar a un usuario por la confianza o el poco riesgo del servicio, en otros casos se requiere, por el nivel de riesgo tener una identificación más exacta del usuario.

Esto evidencia que se debe tener en cuenta como principio: la seguridad y la confianza, el ciudadano debe de creer que su información está segura y se va a usar para los fines establecidos, en general tanto las personas naturales como jurídicas deben confiar en el modelo, se acota que también es importante la transparencia. Así como es importante que los usuarios confíen y sepan cómo se van a usar sus datos, debe de haber un nivel de transparencia para que el modelo en el ámbito público funcione, debe haber un equilibrio entre la confianza y la transparencia, ¿este concepto tiene que ver con el tema de la ley de protección de datos personales?, está relacionado porque no se puede pedir a las personas que tengan que validar el uso de sus datos personales para incorporarlos a fuentes de acceso público definidas por ley, por ejemplo no se le puede pedir a registros públicos que cada vez que alguien quiera una copia de tus escrituras públicas, te llame para autorizarla, es necesario identificar cuáles son estos registros públicos, que incluyen datos personales y que son necesarios para que funcione el sistema. Hay que identificar cuáles son las excepciones a la regla para pedir consentimiento sobre el uso de los datos; en ese sentido, hay una última excepción que incorpora la ley 29733, que indica que no se requiere el consentimiento previo para el tratamiento de tus datos cuando se persigue un interés público.

De este tema surgen varia preguntas, ¿Por qué tengo que dejar mi DNI en la recepción de una entidad privada o pública, cuando únicamente acudo a una reunión con personas de esa entidad? En el DNI hay datos personales importantes que no tendrían utilidad para autorizar una reunión de trabajo. Por ejemplo en el DNI aparece mi fecha de nacimiento, firma, mi dirección e inclusive mi huella digital, que con la tecnología actual podrían ser copiados fácilmente y mal utilizados, de ello surgen otras preguntas como ¿Por qué se muestra la impresión de la huella digital en el DNI? Los datos que se muestran en el DNI y su distribución han sido establecidos, en su momento, por leyes o normas, que probablemente deberían ser revisadas dado el avance actual de la tecnología. En general debería haber una racionalidad en el uso de los datos o atributos de las personas.

No se debería perder de vista que la identidad es un conjunto de atributos que caracterizan a una persona y cada entidad puede manejar los atributos que le corresponde. Por ejemplo el Reniec tiene la responsabilidad de acuerdo a ley de manejar los atributos definidos para lo que se denomina la identidad nacional, hay otras entidades que manejan otros atributos como las universidades, que guardan los records de estudios, inclusive información social de los estudiantes por lo temas de becas y subvenciones, los municipios también manejan datos como los predios que te pertenecen, los establecimientos de salud manejan tu historia clínica, etc. Para el gobierno hay una entidad que maneja los datos para definir un identidad nacional de las personas naturales como es el Reniec y hay otras entidades como la SUNARP y SUNAT que maneja la identidad de las personas jurídicas, cada una es un proveedor de esos atributos y juega un rol dentro del ecosistema, la identidad podría ser única pero no es la responsabilidad de uno solo, la identidad se va formando y debe ser contrastada con todos esos atributos; que no necesariamente son excluyentes y que pueden ser consolidados con fines de tener estadísticas nacionales.

Dentro de ese ecosistema existen también el rol de los prestadores de servicios de credenciales que son entidades que consideran que tienen la capacidad de poder entregar un set de credenciales que luego se utilicen para autenticar, RENIEC es un prestador de servicios de credenciales pero además maneja atributos como domicilio, estado civil, si eres o no un potencial donante de órganos, huellas dactilares, biometría facial, etc. no sería aconsejable que una persona siempre este cargando y mostrando todos sus atributos, lo ideal sería que hubiera un índice único, que a partir de él se pueda autenticar a una persona y

según ello darle acceso a otros atributos. Se acota que siempre hay que considerar que existe un proveedor de servicios que para darle acceso a sus usuarios, necesita autenticarlos y eso se puede hacer utilizando un factor, que no necesariamente es el DNI, podría ser la huella digital, un usuario y contraseña o mezcla de esos factores, que podrían usarse en el ámbito público como privado.

Es necesario acotar el alcance del grupo de trabajo, lo que se busca es tener claro principios como los de seguridad y confianza con una identidad digital para las relaciones entre las personas naturales y jurídicas con el estado, eso es lo que nos va regir y en ese ámbito se va a trabajar, Se sugiere que también tengamos como principio el tema de facilidad de uso, se plantea que ya hablar de digital es ir a un tema tecnológico y el problema de tecnología es que es excluyente de las personas, porque la tecnología de por si no es inclusiva, por eso no podría garantizarse la facilidad de uso porque implica tecnología y la tecnología no es inclusiva. Se plantea una posición distinta respecto a que la tecnología debe ser orientada porque según ello puede ser exclusiva o inclusiva, eso depende del modelo o esquema que se quiera implantar. Se señala que debemos considerar en ese esquema a los ciudadanos más alejados del país, como los aguarunas, por ejemplo; las tecnologías que ellos requieren son por ejemplo paneles solares, para que puedan cargar las baterías, que van a proveer de energía a los dispositivos para que puedan hacer uso de la identidad digital, y ese es un costo que no todos pueden asumir. De qué sirve definir una identidad digital que no se va a poder usar, se menciona que el concepto de facilidad de uso puede ser un concepto muy relativo con respecto al usuario, porque para algunos una tecnología puede ser fácil y para otros no, el tema del costo puede superarse, sin embargo el tema cultural subsiste, Luego se acota que se podría utilizar el término de experiencia usuaria, en donde básicamente nos centramos en el ciudadano y, en base a su experiencia o necesidad, él dice como requiere el servicio, la facilidad de uso es un concepto, el concepto tiene una percepción y una definición propia de quien lo percibe, como todo concepto varia en su interpretación para alguno la facilidad de uso es una cosa y para otro es otra cosa diferente, la seguridad y la transparencia también pueden ser relativas, por eso también deben tener esas precisiones, por eso hay que referirnos a los conceptos en base a una norma o ley o alguna referencia concreta, el acceso en cambio es más asumible porque todos van a tener su número.

Si hablamos de facilidad de uso estamos hablando de tecnología y la tecnología nos es inclusiva, y estaríamos desvirtuando nuestra labor, Se plantea una posición distinta respecto a que debemos considerar que estamos enfocándonos en la identidad digital y lo digital involucra definitivamente tecnología, significa en nuestro caso un cambio por la transformación digital necesaria para nuestro desarrollo, y la tecnología en si no es inclusiva ni exclusiva, esto dependerá de las políticas, de su implementación y de cómo la usamos, pues es una herramienta que puede servir para dársela a algunos cuantos y no distribuírsela a otros, y ser exclusiva en ese sentido, o hacer que se masifique y ayudar a la gente, por lo menos a un gran mayoría.

Concluyendo; es un avance acotar el ámbito en el sentido de definir que nuestro trabajo se limita a la identidad digital de las personas naturales y jurídicas en su interacción con la administración pública, es importante también definir el concepto de seguridad, y el concepto de relación de confianza, que debe ser la base de los principios. Buscamos una identidad digital que cuando la porten o la usen genere la confianza de que será bien usada, que hay transparencia, que los atributos van a ser entregados de forma racional, y que todo el mundo puede ser actor en este modelo.

Existen diferentes niveles de confianza para el proveedor de credenciales que contempla diferentes factores para autenticar. El uso de uno o más de estos factores depende del nivel de confianza que se está dispuesto a aceptar, en donde deberían haber mínimos requeridos para cada nivel de confianza. Pero más que regular los mínimos, deberíamos decir que existen esos mínimos en el estado de acuerdo a distintos niveles de confianza.

Los líderes consideran importante presentar estos temas de discusión en la reunión general del grupo. Por ello la reunión del 15 debe enfocarse más que a la revisión del modelo de identidad público a establecer los principios del modelo.