



5ta. Sesión – Grupo de Trabajo de Identidad Digital

Viceministerio de Comunicaciones

Hacia un Perú Digital

Lima, Octubre 2017



1. Planteamiento del Problema
2. Objetivos, Alcances y Restricciones
3. Principios
4. Análisis de casos de éxito
5. Modelo de Identidad Digital
6. Glosario

¹ <https://definicion.de/problema/>

Agenda 5ta reunión grupo de trabajo identidad digital

1. Revisión de conclusiones del taller pasado y temas pendientes
2. Taller para el desarrollo de principios para un modelo de ecosistema de identidad digital

¹ <https://definicion.de/problema/>

Requisitos funcionales

2.1.1. Las personas deben ejercer su derecho a identificarse permitiendo que el ciudadano controle quién va a tener acceso a su información según el nivel que él le haya autorizado.

2.1.2. Las personas deben poder 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, definir sus atributos públicos y privados, establecer quién puede usar sus datos y consultar quién efectivamente los usa, se entiende que también habrán atributos obligatorios y opcionales

2.1.3. El modelo debe ofrecer 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.

2.1.4. El modelo debe permitir definir la forma en la que se accede a los atributos, si es directamente al dato en particular con todos su contenido (si puedo ver el nombre completo de la persona, o solo saber que es quien dice ser basado en el identificador que usó para autenticarse) o si es basado en preguntas que responden sí o no (en formato scoring, estas pueden ser compuestas o simples)

Requisitos funcionales

2.1.5. El sistema de identidad digital debe tener un punto único de acceso para los servicios públicos, a partir del cual pueda acceder a los diferentes proveedores de identidad como RENIEC, SUNAT, Migraciones, Registros Públicos, otras entidades públicas y privadas competentes.

2.1.6. Los distintos proveedores de identidad, que conforman el ecosistema de identidad digital, deben estar interconectados, a través de un esquema de conexión estándar y homogéneo entre todas las entidades, que permita la autenticación tanto de personas naturales y jurídicas, el compartir atributos comunes, agilizar el registro y actualización de su identidad y hacer eficiente la entrega de servicios.

2.1.7. El flujo de actualización de la información ha de ser inmediato, para tener disponibilidad de los atributos correctos en el menor tiempo posible, evitando fraudes, malos usos o confusiones, de igual forma, se debe definir un mecanismo de publicación de cambios, el responsable será el dueño del atributo

2.1.8. La biometría debería ser considerada dentro de las herramientas empleadas en identidad digital.

Requisitos de calidad

- 2.2.1. El modelo debería tomar en cuenta los casos de éxito y las lecciones aprendidas de otros países que ya han avanzado en esta materia
- 2.2.2. Debe existir un ente supervisor del desarrollo del ecosistema de la identidad digital. Preferiblemente un órgano autónomo dentro del Estado
- 2.2.3. Cada atributo de la identidad ha de tener un dueño, este dueño debe ser responsable de asegurar la autenticidad inicial del atributo y ser garante del mismo.
- 2.2.4. La base de datos de los atributos que conforman la identidad debe estar validada por los dueños para evitar suplantaciones o fraudes al momento de brindar servicios.
- 2.2.5. Se debe crear un canal de comunicación con el ciudadano y las empresas que permita difundir la información de la forma más adecuada (esto debería implicar un programa de gestión del cambio cultural), se ha de fomentar que el ciudadano este informado, esté donde esté y por diferentes mecanismos

Requisitos de calidad

- 2.2.6. El desarrollo del ecosistema de identidad digital debe estar basado en lineamientos estratégicos y un plan operativo que permita cumplir con sus objetivos.
- 2.2.7. Se ha de definir un plan de implantación progresivo (este plan se puede asociar a planes ya existentes que busquen mejorar las capacidades de las diferentes locaciones del Perú, ejemplo el despliegue de la red dorsal)
- 2.2.8. El sistema de identidad debe ser simple y fácil de usar
- 2.2.9. El modelo debe tener una alta escalabilidad
- 2.2.10. El modelo debe ser tolerante a fallos
- 2.2.11. El modelo debe contar con redundancia múltiple fuera de Lima

Limitantes externos

- 2.3.1. Se debe desarrollar una cultura digital y programas de concientización buscando promover la demanda,
- 2.3.2. Se requiere un trabajo normativo
- 2.3.3. Se ha de cumplir lo declarado en la ley de protección de datos personales (LPDP)

Requisitos adicionales

- Considerar la gestión de riesgos en el modelo del ecosistema digital, en sus diferentes procesos como el registro de la identidad, la autenticación y el intercambio de atributos en las transacciones. Por ejemplo, no debería aplicarse el mismo proceso de autenticación para una consulta sobre el estado de un trámite, que para realizar un pago en línea
- Estar en cumplimiento con la ley de firmas y certificados digitales

Definición del enunciado del alcance

1. Objetivo del trabajo:

- A. Promover un ecosistema de identidad digital que mejore el acceso de los ciudadanos a todo tipo de servicios públicos y privados.
- B. Impulsar un ecosistema de identidad digital en el Perú que logre que más personas reciban mejores servicios, acrecentando el acceso, la asequibilidad, el ahorro de tiempo y la eco-eficiencia contribuyendo a la inclusión social, económica, financiera y cultural de los ciudadanos y procurando la formalización de la economía del país.

Definición del enunciado del alcance

1. Descripción del alcance:

Entregables

1. Modelo funcional

- a. Descomposición funcional y definición de procesos
- b. Diagrama de bloques funcionales (identificación, autenticación, autorización, transacción)
- c. Perfiles y atributos de las personas (naturales y jurídicas)
- d. Mapa de actores y de relaciones entre estos

2. Modelo técnico

- a. Estándares técnicos recomendados para el diseño, operación y mantenimiento del modelo
- b. Diseño del modelo para el manejo de la privacidad y el consentimiento
- c. Definición de niveles de servicio esperado (rendimiento, disponibilidad, continuidad, etc.)

Definición del enunciado del alcance

1. Descripción del alcance:

Entregables

3. Modelo financiero básico y gestión de riesgos
 - a. Supuestos generales de costos, del mercado y tributarios
 - b. Ingresos esperados
 - c. Costos, inversiones, fuentes de financiamiento
 - d. Identificar, definir y evaluar (probabilidad e impacto) los riesgos entre los actores del modelo
 - e. Definir una estrategia de manejo, monitoreo y mitigación de riesgos
 - f. Definir una matriz de riesgo con una propuesta de distribución de riesgo
4. Modelo organizacional
 - a. Diseñar el esquema de vigilancia y control de la operación del modelo de ecosistema de identidad digital
 - b. Mapa de actores y de relaciones para la administración del modelo

Definición del enunciado del alcance

1. Descripción del alcance:

Entregables

5. Modelo normativo
 - a. Identificación de las necesidades jurídicas y normativas mínimas para desarrollar el modelo
 - b. Análisis de cumplimiento de la ley de protección de datos personales y la ley de firmas y certificados digitales y el derecho a la identidad digital
6. Estrategia de implementación del modelo
 - a. Análisis de la estrategia
 - b. Mapa de ruta
 - c. Plan de comunicaciones, definición de los mensajes claves
7. Glosario

Principios Rectores

Definición

Son las razones fundamentales o causas primeras que enmarcan al modelo y deberían orientar la actuación de los distintos actores del ecosistema digital

Principios Rectores

Se han identificado varios principios en las listas de requisitos trabajadas en el taller anterior

1. El ecosistema de identidad digital debe estar centrado en el usuario
2. Debe propenderse a la neutralidad tecnológica (no emplear una sola tecnología sino varias)
3. El ecosistema de identidad digital debe tener un modelo de operación sostenible
4. El ecosistema de identidad digital debe considerar la accesibilidad de las personas (accesible a todo tipo de usuario, en diferentes condiciones físicas, en distintas localizaciones, tipos de conectividad y dispositivos) utilizando diversos tipos de autenticación
5. El modelo del ecosistema ha de ser abierto, utilizando estándares y no soluciones propietarias, permitiendo la integración en cualquier momento de otro actor al ecosistema y facilitando/actualizando/economizando la solución (opensource)
6. Ha de facilitar la inclusión (pero no ha de estar diseñado pensando solo en situaciones de falta de recursos (tecnológicos, comunicaciones etc,...) sino que cubra los diferentes aspectos de la población (conectados, no conectados, con acceso a banco o no, con acceso a telefónica o no, con acceso a los diferentes mecanismos de autenticación,...)



GRACIAS



Viceministerio de Comunicaciones

Preparado por: Iván Otárola

Revisado por: Alfredo Astudillo