INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

“ELEMENTOS PARA UNA METODOLOGÍA DE GESTIÓN DE IDENTIDAD DIGITAL EN LA EMPRESA”

SOLUCIÓN ESTRATÉGICA EMPRESARIAL
Que para obtener el grado de MAESTRA EN GESTIÓN DE INNOVACIÓN EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Presenta:
Clemencia Erika Olivares Torrijos

Asesor:
Dr. Héctor Edgar Buenrostro Mercado

Ciudad de México, Enero de 2019.

Autorización de Impresión

C4

AUTORIZACIÓN DE IMPRESIÓN

Ciudad de México, 28 de enero de 2019

La Gerencia de Capital Humano/ Gerencia de Investigación hacen constar que el proyecto terminal titulado:

"Elementos para una metodología de gestión de Identidad digital en la empresa"

Desarrollada por el alumno

Nombre: **Clemencia Erika**

Apellido paterno: **Olivares**

Apellido materno: **Torrijos**

Desarrollado bajo la asesoría del:

Dr. Héctor Edgar Buenrostro Mercado

Ha sido revisado y aprobado por miembro del Núcleo Académico Básico (NAB).

Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

Vo. Bo.

Mtra. Gabriela García Acosta
Encargada de la Gerencia de Evaluación de Proyectos

***Anexar a la presente autorización al inicio de la versión impresa del proyecto integrado que ampara la misma.**

Agradecimientos

Empezó para mi este proyecto por mi amigo Felipe el “Bro” y el fue parte de esta decisión recuerdo que me dijo “esta maestría es para ti” y acepte jajaja, lo cual me encanto disfrute, viví, aprendí, implemente, tengo mucho que agradecer también a mi esposo Israel que me llevaba y traía, también aquí viví unos meses de mi embarazo de mi hermosa hija Nadia, yo creo que alrededor de estos años han ocurrido cosas trascendentales en mi forma de vida, mi mamá, mi hermana Penelope y mi cuñado Mad,también les preguntaba sobre tareas, recuerdo que también a Isaac cuñis le pedí apoyo en Arquitectura de procesos, mi papá físicamente estuvo un tiempo y por eso le dedico a mi Papi Sergio Olivares Muñoz esta tesis, que con tiempo y esfuerzo de parte también de mi asesor Héctor el cual me tuvo paciencia por fin llega a término.

Tabla de contenido

Índice de figuras

Índice de cuadros

Siglas y abreviaturas

TIC Tecnologías de la Información y Comunicación.

SSO *Single Sign On*.

SP Proveedor de servicio.

IdP Proveedor de identidad.

SSL/TLS *Secure Sockets Layer / Transport Layer Security*.

TLS *Transport Layer Security*.

SSL Secure Sockets Layer.

idM Administración de Identidad Digital.

UE Unión Europea.

Introducción

Elementos

En la actualidad, utilizar y estar en contacto con la tecnología de manera cotidiana es una actividad constante en nuestras vidas, ¿cuántas de esas actividades las realizamos conscientemente? En nuestro día a día conocemos nuevas personas, nos relacionamos con ellas, trabajamos alrededor de muchas personas, etcétera ¿Cuál es la diferencia de interacción entre una y otra relación? Según Goffman (1981) todo individuo posee ciertas características sociales y espera moralmente que otros lo valoren y enuncia que el individuo deberá ser en realidad lo que alega ser. "*Los otros descubren, entonces, que el individuo les ha informado acerca de lo que «es» y de lo que ellos deberían ver en ese*". (Goffman E, 1981;pag 31)

La identidad se conceptualiza desde el punto de vista del uso de la tecnología, por un lado, a través de elementos encargados de garantizar la unicidad de una persona física y, por otra parte, por elementos que son la expresión de la identidad humana en todos sus posibles aspectos. Tomando en cuenta los elementos legales, se establece "*que la identidad personal está formada, tradicionalmente, por el conjunto de datos resultantes de la unión de la información relativa a una persona presente en los registros públicos que va a permitir identificarla de forma unívoca*" (Sergio Sanchez, 2012). Para la generación de la Identidad Digital, la agregación de mayor cantidad de información sobre una persona, permite identificar de manera más específica a dicho individuo.

El concepto de Identidad Digital no requiere de toda la información referente al individuo, como por ejemplo, el estado civil o la profesión de la persona, que son consideradas por las diferentes legislaciones como datos superfluos, por estar demasiado ligados a la esfera privada del individuo. En este sentido, algunas directivas, tales como la propuesta por la Unión Europea sobre protección de datos, han sido desarrolladas con la finalidad de otorgar al sujeto el mayor control posible sobre su identidad y datos personales; planteando una serie de requisitos a cumplir por los receptores, controladores, procesadores y terceras partes a la hora de

manejarlos. El artículo 2, letra a), define datos personales de la siguiente manera: (Directiva Europea 95/46/CE)

"*Tiene como finalidad el otorgar al sujeto el mayor control posible sobre su identidad y datos personales, planteando una serie de requisitos a cumplir por los receptores, controladores, procesadores y terceras partes a la hora de manejarlos*".

El artículo 2, letra a) define datos personales de la siguiente manera:

*"«Datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social." (*Directiva Europea 95/46/CE*, pag. 34)*

Cuando los usuarios interactúan con servicios electrónicos, a menudo los personalizan de acuerdo a sus preferencias o necesidades, de manera que además de establecer unos datos de acceso como nombre de usuario y contraseña, se determinan otros parámetros tales como la información que desean que se les muestre, la disposición de los elementos en la página que ofrece el servicio o la forma de notificar los cambios en el mismo. Normalmente el establecimiento de una cuenta y la personalización de la misma se realizan por parte de los usuarios para cada uno de los proveedores de servicio a los que accede, de forma que el usuario suele utilizar varias cuentas diferentes con múltiples parámetros.

Es común que las personas utilicen y compartan información a través de servicios electrónicos de manera cotidiana. En el caso de las empresas y corporaciones, esto se da también a través de sus redes internas, lo que plantea la pregunta de cómo podría la empresa aprovechar las herramientas tecnológicas con las que cuenta para gestionar la información que los trabajadores comparten dentro de su red interna.

Las áreas en las que se han enfocado las grandes corporaciones para llevar a cabo cambios significativos en la cuestión de la identificación de los individuos, ha sido fundamentalmente; el seguimiento al personal. El "talento", es el área de seguimiento del personal, es donde surge la innovación para llevar a cabo la

Identidad Digital, buscando herramientas para que su trabajo se vea beneficiado y no consista únicamente en una identificación.

El objetivo de este trabajo es proponer una Identidad Digital que se aplique a las Pequeñas y Medianas Empresas (PYMES) mexicanas, incorporando los elementos técnicos y normativos aplicables al caso nacional, ya que las soluciones actuales no contemplan estos elementos.

La Identidad Digital puede adecuarse a los estándares internacionales proponiendo un enfoque de innovación en la gestión de la información, al apoyarse en el uso de tecnologías de información, a través de la revisión bibliográfica de los estudios de caso que se han realizado en México y otros países.

La propuesta está orientada a vincular a los individuos con una identidad digital en el sector privado para que ésta pueda ser aplicable a otros ámbitos como el sector público y de comercio.

La generación de una metodología de Identidad Digital en las empresas permitirá a los trabajadores de las mismas contar con una herramienta que los identifique y que muestre sus actividades dentro de su trabajo. Además, las empresas se beneficiarán al contar con información clave para introducir mejoras a sus áreas, así como apoyar a la gente que produce resultados en la empresa.

Sus fundamentos metodológicos estarán basados en situaciones específicas sobre Identidad Digital en el ámbito nacional e internacional que deben ser comprendidas y valoradas. Se revisarán una serie de hechos referentes al campo particular de conocimiento en Identidad Digital para llegar a un análisis de contenido partiendo de datos concretos que se tienen de Europa y América Latina, con el fin de generar esa metodología.

El presente trabajo se compone de tres capítulos. En el primero se presentan las consideraciones teóricas para analizar los desafíos que conlleva el concepto de Identidad Digital. En el segundo se desarrolla un análisis de las experiencias realizadas en materia de metodologías aplicadas de Identidad Digital en ambientes públicos y privados, mostrando las ventajas y desventajas de cada uno; se abordará adicionalmente la legislación referente a los datos personales en México. En el

tercer capítulo se propone la metodología a llevar a cabo en México, en empresas nacionales; y por último, se presentan las conclusiones y perspectivas.

Capítulo 1

La Identidad Digital como parte de la incorporación de las TICs en los entornos digitales

Capitulo 1. Elementos tecnológicos de la Identidad Digital

Para iniciar el trabajo, es fundamental establecer los elementos principales de la Identidad Digital. El objetivo del presente capítulo es identificar los elementos tecnológicos, la arquitectura básica y los elementos generales para el establecimiento de una Identidad Digital. Las Tecnologías de la Información y Comunicación (TIC) se han incorporado de manera acelerada en los distintos ámbitos sociales y económicos de las personas, las empresas y los gobiernos. Esto se refleja en el uso de estas herramientas como medio de interacción entre los distintos agentes, los cuales se reconocen entre sí a través de una Identidad Digital creada a partir de un conjunto de datos e información que se encuentra en la red.

Para la gestión de la identidad dentro de los sistemas de información, se debe partir de una serie de elementos que permitan identificar a cada una de las personas, empresas o instituciones que se encuentran relacionadas a través de internet desde distintas locaciones tales como su nombre, apellido, teléfono, correo electrónico, etcétera; formando parte del origen del individuo y de sus acciones dentro de los distintos ámbitos donde se desenvuelve (laboral, social, económico, entre otros).

En el mundo en línea se presenta una gran cantidad de oportunidades para hacer uso de la Identidad Digital como lo son transacciones de negocios o de datos de consecuencia significativa; en estos casos, la identidad es un componente clave para garantizar la seguridad, control de acceso, personalización e incluso el cumplimiento normativo.

En la actualidad, cada individuo cuenta con diferentes representaciones de Identidad Digital, que responden a los diferentes entornos digitales en que se desenvuelve; por lo general éstas se componen de una combinación de nombre de usuario-contraseña.

Desafortunadamente, en la práctica estas representaciones de información de identidad son independientes entre sí, por lo que su proliferación presenta un

problema tanto para la comodidad del usuario como para su seguridad. (Maler, 2005)

Por lo general, los desarrolladores de servicios en línea controlan todos los elementos dentro del dominio de su propia organización (por ejemplo, a través de una única empresa cuando se trata de servicios de negocio a los empleados), por lo que puede dictar el uso de un conjunto de la infraestructura de seguridad para la autenticación y autorización de usuarios, así como propagar sus atributos de identidad.

1.1 Conceptos de Identidad Digital

La Identidad Digital permite que los usuarios distribuyan de manera dinámica su información en distintos dominios de seguridad. Es el medio a través del cual las aplicaciones de Internet pueden ofrecer a los usuarios un acceso único en dominios cruzados (es decir, que nos permiten ir de un dominio a otro), también conocidos como "*Cross-Domain Single Sign-On*" (SSO), los cuales permiten autenticar su identidad una sola vez, para posteriormente tener acceso a recursos protegidos y a sitios Web, con el fin de utilizarlos dentro y fuera de la empresa. Sin embargo, a pesar de lo atractivo de estos beneficios, la Identidad Digital también implica ciertos costos, así como nuevos riesgos de seguridad y privacidad; esto porque comparte valiosa información con dominios que usan protocolos de red ligeramente acoplados. Tales riesgos requieren cierta mitigación, que puede abarcar, desde prevenir la repetición de mensajes, hasta obtener el consentimiento del usuario para compartir sus datos, tanto en línea como fuera de Internet.

Birch y Doyle (2011) mencionan que existen problemas en la administración de la Identidad Digital. Esta situación incrementa la cantidad de desafíos arquitectónicos nuevos, así como también involucra importantes problemas de seguridad y privacidad. De igual manera, hablan de los cambios físicos que, como seres humanos, tenemos a lo largo del tiempo –el envejecimiento natural–; así

como nuestro cuerpo, nuestra Identidad Digital cambia de una plataforma a otra como en el caso del correo electrónico o en redes sociales.

Con la administración digital se puede aumentar la portabilidad de la Identidad Digital con la que cuenta el usuario. La administración de la Identidad Digital es un conjunto de tecnologías y procesos que les permiten a los sistemas informáticos distribuir dinámicamente la información de identidad y delegar las tareas relacionadas a esa identidad a los dominios de seguridad. La Identidad Digital no solo sirve como un logueo de seguridad, también es útil para saber quién es la persona dentro de la historia viva de la empresa por lo cual entendemos que esta administración utilizará la información generada en apoyo de una mejora en la organización.

Los sitios Web y las aplicaciones consideran a las entidades como cuentas que ellos alojan en nombre de sus usuarios, los cuales acceden a su correo electrónico, a realizar compras en línea, o a participar en actividades sociales y actividades similares. Mientras que las aplicaciones Web manejan las cuentas de los usuarios de un modo similar a como lo hacen las empresas, los usuarios tienden a pensar en estas identidades como recursos personales que están bajo su propio mando. A diferencia de lo que ocurre en las empresas, los mayores problemas con las identidades en la Web son soportados por los usuarios: ellos deben crear y recordar sus nombres de usuario y sus contraseñas para cada sitio, completar cada uno de sus perfiles con sus mismos datos y recordar las reglas de cada sitio. La Identidad Digital ofrece soluciones a muchos problemas compartidos por ambos ambientes y, con frecuencia, el *Single Sign On* (SSO) suele ser la primera capacidad de identidad digital que las organizaciones incorporan. Este les ofrece una experiencia más amistosa a los usuarios Web, a través de un proceso de ingreso o acceso más consistente y menos frecuente, lo cual brinda a los empleados más tiempo para realizar las actividades correspondiente a su labor. (Stefanova, Kabakchieva y Nikolov, 2011)

La combinación de SSO con la vinculación de cuentas les permite a los portales Web unificar diversas interacciones en línea, esta característica puede permitirles a las iniciativas del gobierno electrónico presentar muchos sitios de

agencias diferentes como un todo unificado. Finalmente, SSO puede simplificar la arquitectura de cada sitio participante, ya que implica compartir información acerca de cuándo y cómo los usuarios confirman su autenticidad, usando una identidad particular. (Stefanova, Kabakchieva y Nikolov, 2011)

También podemos ver que estos accesos se pueden compartir en una sesión. Como usuarios se pueden compartir algunos atributos como los roles de un empleado y las direcciones de envío, esta información ayuda a que los sitios receptores puedan tomar sofisticadas decisiones de autorización, ya que podrían ver solo los recursos que ellos necesitan y presentar interfaces de usuario personalizadas, basadas en un solo atributo de la Identidad Digital, como la dimensión ergonómica.

1.2 Procesos y componentes de la Identidad Digital

La Identidad Digital es un fenómeno complejo que incorpora elementos provenientes de distintos ámbitos por lo que cualquier propuesta debe considerar una serie de componentes básicos que deben estar presentes para que ésta cumpla con el objetivo propuesto.

En este sentido, Maler (2014) establece cuatro componentes básicos que deben estar presentes en la formulación de la Identidad Digital:

- El usuario es una persona que asume una Identidad Digital particular para actuar recíprocamente con una aplicación de red en línea.
- El agente del usuario es un navegador u otra aplicación de software que se ejecuta en una PC, teléfono móvil, dispositivo médico, etcétera. Las interacciones en línea de un usuario siempre tienen lugar a través de un agente que permite, pasivamente, el flujo de información de identidad o actúa activamente como intermediario.
- El sitio del Proveedor de Servicio (SP) es una aplicación Web –como una aplicación de informe de gastos o una fuente comunitaria abierta– que descarga la autentificación a una tercera parte, que también podría enviarle algunos atributos

del usuario al SP. Como el SP suele basarse en información externa, a menudo se le llama una parte confiable.

• El Proveedor de Identidad (IdP) es un sitio Web al que ingresan los usuarios y que, en ocasiones, almacena atributos de común interés para compartir con varios SPs.

En este trabajo se ocuparán estos cuatro elementos ya que son las partes esenciales de las que se compone la Identidad Digital, las cuales se interrelacionan entre sí, tal como se muestra en la siguiente figura:

Figura 1. ***Diagrama Single Sign On***
Fuente: Elaboración propia de acuerdo a los elementos que integran el Single Sign On

Componentes básicos del diagrama *Single Sign On*:

El diagrama nos presenta el usuario como parte inicial de la que depende todo el demás funcionamiento. Al ingresar al sistema, tiene un nombre de usuario y contraseña / biométrico / credencial, o cualquier forma de ingreso que la empresa haya decidido ocupar para su Identidad Digital.

El Agente del Usuario (navegador o aplicación), nos va a dar la pauta de interrelación dentro del sistema que tenga la empresa, dando paso a la interacción de la información.

El sitio del Proveedor de Servicio (SP) es una aplicación Web que, de manera tradicional, se ocupa cuando entramos a un portal electrónico que sirve de apoyo en la administración de cada empresa que lo ocupe.

El proveedor de identidad (IdP) es un sitio Web que se encarga de guardar variables importantes para que el usuario tenga puntos de interés, pues al obtener estos datos, los ocupa para generar información adicional que puede ser de apoyo.

Compartir información personalmente identificable es una preocupación importante en la administración de la seguridad, la protección de los datos y en el cumplimiento de las normas o reglamentaciones. Sin embargo, con la Identidad Digital, compartir dicha información suele ser una meta clave, lo cual implica importantes problemas de seguridad. Por ejemplo, es posible que un sitio del proveedor de servicio conozca el único identificador digital de un usuario, de manera global, durante una sesión SSO, aun cuando no es necesario que conozca “quién es el usuario en realidad”.

Teniendo esto en mente, debemos considerar la seguridad y un nivel mínimo de divulgación en un nivel fundamental, vale decir, a nivel de los identificadores, los cuales sirven como etiquetas de Identidad Digital. Con frecuencia, los sistemas de Identidad Digital manejan muchos tipos de identificadores asignados por diferentes IdPs, en diversos contextos. Tales identificadores pueden ser, de acuerdo con Birch y Doyle (2011):

- Absolutos (independientes del contexto y multidireccionales), o relativos (dependientes del contexto y unidireccionales);
- Valores únicos de una sola parte, segmentos jerárquicos, o claves acumuladas multiparte; raw, has, o encriptado; o anónimo, seudónimo, o “verónimo” (revelando totalmente la identidad real del usuario).

Los seudónimos son importantes para conservar la privacidad, principalmente cuando múltiples servicios Web cooperan para proporcionar un valor agregado a sus usuarios, lo que hace necesario compartir sus atributos. Si un IdP

se comunica con un SP de un usuario bajo un seudónimo único en la relación IdP-SP-Usuario –en lugar de utilizar, por poner un ejemplo, su número del seguro social o dirección de correo electrónico– impide que múltiples SPs correlacionen las actividades del usuario, y frustra a los indiscretos espías (a menos que usen sofisticado sistemas de ataques programados). Aun cuando los SPs conocen al usuario por su seudónimo, todavía tendría que compartir muchos atributos para identificarse parcial o totalmente ante un SP.

Por ejemplo, combinar algo tan pequeño como un código postal y una cifra de ingresos anuales, a menudo suelen ser unos datos personalmente identificables. En este caso, un sistema de consentimiento informado del usuario podría ayudar a resguardarle contra una divulgación de información excesiva. En el mundo real, se da el caso de que personas ajenas utilicen documentos de identificación de otras personas para diversos propósitos sin el conocimiento del emisor del documento; por ejemplo, una persona podría exhibir una licencia de conducir que no le pertenece para demostrar que tiene edad legal para beber. Para evitar una "desvinculación" similar, los protocolos de identidad digital deben aplicar flujos de datos especiales y una cuidadosa encriptación para evitar la visibilidad del IdP con respecto a las relaciones de un SP y un usuario.

1.3 Consideraciones de seguridad en Identidad Digital

Como en todo "*outsourcing*" (servicios prestado por terceros), la Identidad Digital administrada por personal externo a la organización puede ofrecer un mejor servicio a un costo más bajo; pero también trae consigo riesgos, por ejemplo, la Identidad Digital involucra el tema de la seguridad: idealmente, todas las partes deberían asegurar sus canales de comunicación contra los ataques de Replay, ataques Man-in-the-Middle (MitM), entre otros; en este último caso, el atacante tiene la habilidad para desviar o controlar las comunicaciones entre dos partes, por ejemplo, en el caso de una cuenta de correo electrónico, el perpetrador podría desviar todos los e-

mails a una dirección distinta a la de destino con el fin de leer y alterar toda la información antes de enviarla al destinatario correcto, también podría darse el secuestro de sesiones y otras amenazas que permiten el uso malicioso de la información del usuario o de los recursos Web. En un contexto HTTP, los arquitectos de seguridad tienen en cuenta los Secure Sockets Layer / Transport Layer Security (SSL / TLS), los cuales se refieren a los protocolos de seguridad, con la autentificación mutua como base de esa seguridad. Aun así, los desarrolladores de la aplicación, a menudo, los evitan, los pasan por alto o implementan este paso solo parcialmente. (Birch y Doyle, 2011)

Durante el proceso de autenticación del cliente y del servidor, hay un paso en que se requiere que se cifren los datos con una de las claves de un par de claves asimétricas, y que se descifren con la otra clave del par. Se utiliza un resumen de mensaje para proporcionar integridad. El protocolo TLS (Transport Layer Security) ha evolucionado a partir del protocolo SSL (Secure Sockets Layer); IBM® MQ da soporte tanto a SSL como a TLS. Los principales objetivos de ambos protocolos consisten en proporcionar confidencialidad (que a veces recibe el nombre de privacidad), integridad de datos, identificación y autenticación utilizando certificados digitales.

Los protocolos como el SSL están diseñados para permitir que las aplicaciones transmitan información de ida y de manera segura hacia atrás, por ello, las aplicaciones que lo utilizan dan y reciben claves de cifrado con otras aplicaciones, así como cifran y descifran los datos enviados entre los dos. La evolución la tenemos en TLS, dado que está basado en éste último certificado y funciona de manera muy similar, lo que hace es encriptar la información compartida. Actualmente, la mayoría de los sitios confían en los nombres de usuario y las contraseñas porque este método propone una carga de datos inicial menor, tanto para los usuarios como para los administradores del sitio.

Sin embargo, esto es notoriamente débil y susceptible a los ataques de tipo "*phishing*" o de suplantación de identidad (que implica intentar adquirir información confidencial de forma fraudulenta, por correo electrónico, en la web con transacciones o llamadas telefónicas). Para los SPs, la Identidad Digital es más

barata que implementar una infraestructura de autentificación de calidad superior, porque redirecciona la tarea de autentificación a un IdP. Sin embargo, los SSO basados en IdPs pueden magnificar los costos de una contraseña robada porque extienden el alcance de la actividad maliciosa. La mayoría de los protocolos SSO brindan maneras de mitigar este riesgo; por ejemplo, pueden limitar a un minuto o menos, la vida útil del "token" de seguridad que un IdP envía a los SPs. Algunos protocolos también brindan una única propiedad de desconexión que ofrece a los usuarios una desconexión casi simultánea de todos los sitios Web accedidos a través del SSO. Además, mientras que la mayoría de los protocolos les permiten a las partes de las identidades federadas de interacciones elegir el método de autentificación a usar, normalmente ofrecen una forma en que los IdPs describan el método que aplicaron en cada caso para que los SPs puedan tenerlo en cuenta al tomar decisiones de autorización. (Birch y Doyle, 2011)

1.4 Los desafíos en proveedores y los protocolos de la arquitectura de seguridad al compartir

La naturaleza ligera de acople es la relación que se establece al compartir publicaciones y eventos en redes sociales, lo cual plantea desafíos interesantes. Revelación del proveedor de identidad (IdP). Para proporcionar un SSO iniciado por un IdP, con el estilo de un portal, los administradores pueden, normalmente, configurar un IdP para avisar a sus sitios socios de SP, cuando un usuario quiere visitarlos. Pero con los SSO iniciados por SP, nos encontramos con el problema de la divulgación o revelación del IdP, por lo que hay que preguntarse: ¿cómo hace un SP para saber a dónde debe enviar su pedido de autentificación cuando un usuario visita el sitio y quiere un servicio basado en la identidad? Esto es lo mismo que decir "¿De dónde es usted?". Este problema tiene algunas soluciones posibles, que se detallan a continuación.

Si el SP forma parte de un acuerdo de IdP organizado de antemano (un “círculo de confianza” que a menudo involucra contratos comerciales y acuerdos de obligación legales), podemos configurarlo, estáticamente, con la ubicación del IdP. Si el SP debe escoger entre diferentes IdPs –entre múltiples IdPs, o si no tienen ninguna relación de IdP establecida, o si su círculo de confianza incluye múltiples IdPs, o si pertenece a varios círculos de confianza diferentes–, el usuario podría tener que ingresar al lugar de ubicación de su IdP. Esta situación es conocida como ingreso simplificado (en lugar de ingreso único). Aquí, el proceso no es continuo, lo que implica un costo significativo cuando la atención y la utilidad están en su punto máximo. Otra opción es darle un usuario, un agente de usuario que sea lo suficientemente inteligente como para conocer la respuesta. Conforme los navegadores Web tengan limitaciones más riesgosas y los dispositivos como los teléfonos inteligentes ganen popularidad, el rol de “los clientes inteligentes” aumenta significativamente.

Existen métodos de firma digital como XML Encryption, el cual es una recomendación del World Wide Web Consortium (W3C) que especifica un proceso para cifrar datos (no únicamente documentos XML) y presentar esa información cifrada en XML para que viaje por los medios de transmisión. Por ello XML-Sig y XML-Enc son estándares a ocupar en firmas digitales (url: https://www.w3c.es/). Estos dos estándares del W3C definen los métodos de firma digital y encriptación que son especialmente adecuados para las oportunidades y los desafíos presentados por XML como formato de datos. Permiten la firma y encriptación selectiva de subestructuras XML para la representación de contenido firmado y cifrado en forma de XML. Ambos son ampliamente utilizados ya que sustentan la seguridad de otras normas relacionadas con XML (url:bibin.us.es/capitulo7firmadigital).

En el siguiente diagrama se puede visualizar el proceso de autenticación y entrada al sitio web, en donde existe un proceso de cifrado si se ocupan servicios para enviar correos o datos entre navegadores o en el mismo navegador; de igual manera, conserva varios protocolos que utiliza para ligar a las redes sociales (que se explican mas adelante) como protocolos que se han ocupado en seguridad.

Figura 2. ***Diagrama autenticación en navegadores y redes sociales***

Fuente: Elaboración propia de acuerdo a el esquema de navegadores que ocupan los navegadores y redes sociales.

A continuación, se mencionan los protocolos para la gestión de datos, lo más conocido y probado en el mercado para redes sociales y navegadores:

- Gestión de Claves XML Especificación [XKMS]: Este estándar W3C define un conjunto de servicios web XML para registrar y buscar las claves criptográficas. Proporciona una capa de neutralidad tecnológica por encima de los sistemas PKI particulares, como son los más utilizados de acuerdo a las recomendaciones internacionales SPKI y PKIX, permiten a los dispositivos del cliente descargar las tareas de gestión de claves de un servicio externo.
- Service Provisioning Markup Language [SPML]: La norma OASIS (Advancing Open Standars for the Information Society) busca, como consorcio sin fines de lucro, reunir a las personas para acordar formas inteligentes de intercambiar información por medio de Internet y dentro de sus organizaciones. Permite un método independiente de la plataforma de aprovisionamiento de cuentas de usuario (http://www.oasis-open.org).
- Control de Acceso Extensible Markup Language [XACML]: La norma OASIS define una manera de expresar acceso para controlar las políticas en XML y proporciona un protocolo para interactuar con un punto de decisión política XACML con el fin de obtener decisiones de autorización (http://www.oasis-open.org).
- Lenguaje de Marcado de Aserción de Seguridad [SAML]: Esta norma proporciona formatos XML para la codificación de la información de identidad, protocolos XML para el intercambio de esa información y perfiles para lograr la

interoperabilidad en la realización de tareas de gestión de identidades comunes. Desarrollado por el Comité Técnico de Servicios de Seguridad [SSTC] de OASIS, SAML ha demostrado ser algo así como un "solvente universal" para la identidad y la información de seguridad. Está siendo adoptada como base para una serie de otras tecnologías modernas en este espacio. SAML versión 2.0 fue aprobada en marzo de 2005. SAML es el protocolo de identidades federadas más difundido entre las empresas, a las que permite lanzar credenciales de autenticación y autorización con validez más allá de los límites corporativos (http://www.oasis-open.org).

- Liberty Alliance [Liberty] Normas: El Proyecto Liberty Alliance es una alianza de más de 150 empresas sin fines de lucro y organizaciones gubernamentales de todo el mundo. En esta alianza se desarrollan estándares abiertos para la red federada de identidad, con énfasis en el apoyo a todos los dispositivos de red existentes y emergentes. Produce especificaciones de la tecnología, como la Federación de Identidades Marco [ID-FF] y la Identidad Web Services Framework [ID-WSF], junto con las directrices técnicas, comerciales y legales para su aprobación e implementación. También proporciona la interoperabilidad de servicios de ensayo y certificación (www.projectliberty.org).
- Servicios de Seguridad Web, SOAP de Message Security [WS-Security]: La norma OASIS y su serie de compañero "Perfiles de token de seguridad" (incluyendo uno que utiliza SAML [STP]) define la forma de aplicar la firma digital y el cifrado de mensajes SOAP de servicios Web para la protección de la seguridad de extremo a extremo.

Algunas empresas de Internet bien conocidas y de reconocido prestigio como Google, Yahoo! y MSN han estado utilizando durante años, soluciones de inicio de sesión único (SSO) y, recientemente, han empezado a actuar como *proveedores de identidad* para sitios de terceros. Además, el enorme crecimiento de popularidad de redes sociales como Twitter, Instagram y Facebook las han llevado a convertirse también en plataformas de identidad. Cada vez es más frecuente que los nuevos sitios web y servicios aprovechen estas plataformas existentes para autenticar a los usuarios dudosos de registrarse a nuevos servicios. El hecho de aprovechar estos servicios ha permitido a los usuarios acceder con un nombre familiar. Sin embargo,

es importante tener en cuenta que existen dos tipos diferentes de autenticación: *delegada* y *federada* (Google App Engine).

El sistema de Twitter es conocido como *autenticación delegada*. Muchos sitios web que han optado por no crear su propio sistema de autenticación, lo están externalizando o "delegando" de forma eficaz a entidades más reconocidas como es el caso de Twitter. El acceso a aplicaciones web vía Facebook Connect es otro ejemplo de delegación, aunque en este caso se trata de un sistema cerrado opuesto al "Acceso con Twitter" que utiliza OAuth, el cual es un sistema de autorización abierto, utilizado con regularidad en colaboración con la autenticación delegada. (MODINIS eIDM, 2011)

La autenticación delegada constituye un esfuerzo para hacer realidad el concepto de inicio de sesión único en Internet. Cuanto menor es el número de cuentas por las que los usuarios se tienen que preocupar por manejar y gestionar, mejor es el escalado de la web. Sin embargo, en este punto se presentan otros problemas: si se utiliza este tipo de autenticación, se requiere que los usuarios dispongan de cuentas de Twitter o de Facebook. No se trata del tipo de solución "crea una identidad en alguna parte y utilízala en cualquier lado" que nos podríamos imaginar, se trata de la *autenticación federada*, una solución que es mucho más cercana al verdadero inicio de sesión único de Internet.

Los proveedores con los que cuenta la Identidad Digital son variados y puede hacerse uso de ellos siempre que se tenga acceso a la Web, pues con el llenado de información que identifique al individuo, se le da un espacio y se le permite tener una identidad dentro de la instancia del proveedor, el cual le brinda los beneficios del que pueda ocupar en el lugar donde se haga sesión.

Existen dos tipos de proveedores: los *proveedores directos* como Google y Yahoo!, los cuales solo requieren una identidad digital genérica sin ningún nombre de usuario asociado. Se llaman *direcciones URL visibles libres* porque no están ligadas a ningún usuario determinado, en otras palabras, no existe información en la cadena de la URL de OpenID para identificar únicamente a los usuarios. Por el otro lado, Flickr, WordPress, Blogger y LiveJournal son conocidos como *proveedores con nombre de usuario* porque todos ellos requieren una URL

que cuente con dicho nombre de usuario; no es extraño que se conozcan como *direcciones URL visibles ligadas*, ya que cada una de estas direcciones URL contiene el nombre de usuario para poder asociarlo directamente con el usuario registrado con el proveedor.

Algunos proveedores funcionan con ambos sistemas, lo que significa que admiten tanto direcciones URL ligadas como libres: AOL, MyOpenID y MySpace son ejemplos de este tipo de proveedores. Independientemente del método que se escoja, asegúrese de que la interfaz conoce los requisitos y, si es necesario, de que los pida a los usuarios.

Un proveedor va a permitir a la empresa enlazar diferentes identidades entre sí, y así se garantiza la privacidad de los datos y se consigue desplegar servicios de forma segura y con SSO entre ellos.

Como lo mencionan los desarrolladores de las aplicaciones de Google: La magia de OpenID en App Engine reside en las invocaciones: son los métodos que se ocupan para create_login_url() o createLoginURL(), con el fin de generar el enlace al que los usuarios pueden hacer clic o en que la aplicación se redirecciona al proveedor adecuado para llevar a cabo la autenticación. Actualmente existen diferentes proveedores de OpenID entre los que los usuarios pueden escoger.

Conclusiones

La Identidad Digital se ha desarrollado a partir de reglas que pueden, en un principio, ser la base para realizar su actividad buscando que la seguridad y la arquitectura estén contemplados, y donde los protocolos pueden ser muy variados y tienden a buscar alternativas de acuerdo al lugar en que se vaya a aplicar el mismo.

Existen varias opciones en tecnología aplicada con alternativas comerciales y ambientes de gobierno, donde proveedores y protocolos a nivel comercial se ocupan para todas las transacciones dentro de la red. La seguridad es un tema que también se lleva a cabo de distintas formas, dependiendo el proveedor, los elementos que la componen no difieren de una a otra alternativa, todos los

componentes se repiten para cada opción y apoyan en la identificación del usuario o miembro que desea firmarse o reconocerse.

En el siguiente capítulo se revisarán aquellas iniciativas internacionales y nacionales que se han implementado, buscando componentes que favorecieran a cada objetivo del proyecto en los diferentes países. En el presente capítulo se mostraron los componentes de la Identidad Digital de manera general, en el siguiente, se sentarán las bases para mostrar los elementos que pueden apoyar a esta propuesta de trabajo.

Capítulo 2

Identidad Digital a nivel internacional y en México

Capítulo 2: Identidad Digital internacional y en México

La Identidad Digital abarca tanto la esfera pública como la privada, así como los ámbitos nacionales y transnacionales; debe darse especial atención a este tema, porque forma parte del día a día, tanto como operación, registro, trámite e investigación, ya que es necesario identificarse constantemente y con ello se tienen una serie de validaciones, propósitos, reglas y procedimientos que se deben llevar a cabo para que el proceso sea válido y finalmente se llegue al objetivo de protección de datos.

En este capítulo se presenta una revisión de lo que se ha realizado internacionalmente en el tema de Identidad Digital, en cuanto a tecnología, procesos y aplicación, tanto en sectores públicos como privados. Se abordará también el caso de México a través de una muestra desde el inicio de su desarrollo.

2.1 Condiciones internacionales de la Identidad Digital

Entre los esfuerzos más relevantes para generar una Identidad Digital de múltiples usos se encuentra la desarrollada por la Unión Europea (UE). Las regulaciones en materia de identidad ciudadana –donde se encuentra de manera implícita la Identidad Digital– cambian de un país a otro, pero en el caso de la Unión Europea, existe un tratado que unifica este concepto en los Estados miembros, buscando mejorar los procedimientos que son ajenos entre países miembros, permitiendo que las tareas sean compartidas en coherencia y continuidad basándose en él. El Tratado de Lisboa es importante en el tema de la Identidad Digital a nivel del gobierno porque toma en consideración lo siguiente: un marco comunitario para la firma electrónica 1999/93/EC30 (aplicación del mercado interior como un objetivo principal de la Directiva, refiriéndose en específico al mercado interior de la firma electrónica y afines servicios); para el marco regulador de la UE en materia de electrónica en comunicaciones (que incluye la Directiva sobre la privacidad y las

comunicaciones electrónicas en la Directiva 2002/58/CE); como la base jurídica de la Directiva de Protección de Datos. En el artículo 16, se enuncia: "*Todo el mundo tiene el derecho a la protección de los datos personales que les conciernen*", permite la creación de un sistema general de protección de datos personales aplicables a todo el espectro de las políticas y los campos de acción de la UE.

En el mercado interno de la UE se presentan servicios, transacciones y actividades que cada vez requerirán la autenticación e identificación de los usuarios y ciudadanos. Además, y en relación con la adecuación de proponer al mercado interior como un espacio de competencia adecuado para la acción legal, en el campo de la identificación electrónica, se ha planteado que es importante plasmarlo en leyes básicas, como por ejemplo el articulo 9, el cual enuncia "*La Unión respetará en todas sus actividades el principio de la igualdad de sus ciudadanos, que se beneficiarán por igual de la atención de sus instituciones, órganos y organismos. Será ciudadano de la Unión toda persona que tenga la nacionalidad de un Estado miembro. La ciudadanía de la Unión se añade a la ciudadanía nacional sin sustituirla*." (Tratado UE, 1995:14)

Es importante señalar que el artículo 21 (en relación con el derecho de libre circulación y residencia de ciudadanos de la UE), considera la adopción de disposiciones relativas a los pasaportes, documentos de identidad, permisos de residencia o cualquier otro documento (o disposiciones sobre seguridad social o protección social). El tema de la identidad europea, y en particular de la identificación electrónica, se plasma en la promulgación de los derechos vinculados a dicha identidad europea, requerida para poder disfrutar de los derechos implícitos en ella y buscar generar un sistema mediante el cual todos los ciudadanos europeos puedan ser identificados como tales en cualquier Estado miembro en el que se encuentren.

Uno de los principales factores de bloqueo del desarrollo de sistemas de gestión de identidad interoperable en toda Europa y, como tal, del aprovechamiento de la construcción y realización del mercado único digital, es la diversidad –e incompatibilidad– de los enfoques legales a la protección y la gestión de identidades electrónicas. La necesidad de armonizar la gama amplia y diversa de las leyes

nacionales sobre Identidad Digital surge, por tanto, como un imperativo del mercado interior. (Nuno, *et al*., 2012)

Lo que muestran estas leyes es que la conexión entre protección de datos e identidad debería ser considerada como una base jurídica adecuada para la regulación de la identificación electrónica en la UE. De esta manera, y teniendo en cuenta que el derecho a la protección de datos debe abarcar no sólo la protección de la privacidad, sino también la protección de las identidades personales de los ciudadanos de la UE, la protección de datos (consagrado explícitamente en el Tratado de Lisboa como un derecho fundamental) emerge como la base jurídica más adecuada para la regulación de la identificación electrónica en Europa. (Nuno *et al*., 2012)

A partir de los elementos antes citados se derivaron los siguientes programas:

Programas y políticas para la generación de la identidad digital

a) Programas transnacionales

Los principales objetivos de las estrategias nacionales de Administración de Identidad Digital (IdM) son para darse cuenta de la importancia de la administración electrónica, fomentar la innovación en los servicios electrónicos públicos y privados, así como el fortalecimiento de la seguridad cibernética, buscando homologar las tecnologías que no se tienen entre uno y otro estado de la Unión Europea.

Para la mayoría de los países, el objetivo general o visión para el desarrollo de una estrategia nacional de IdM es la práctica de la administración electrónica; además de ésta, la mayoría de los países también tienen como objetivo fomentar la innovación en la economía de Internet, ya sea explícita o implícitamente; proyectándolo a mediano o largo plazo; sin embargo, la innovación, la administración electrónica y la ciberseguridad se pueden identificar en todo enfoque de los países. Las variaciones son esencialmente relacionadas con el nivel en que se abordan estas dimensiones (visión, estrategia o política).

Las estrategias nacionales de IdM apuntan a beneficiar a las empresas, los ciudadanos y el gobierno. Se espera que tengan beneficios económicos en términos de reducción de costos y aumento de la productividad en el sector público fomentando la capacidad de uso de servicios en línea, se busca de igual forma, un aumento de la confianza y seguridad acerca de las identidades en línea. (OECD, 2011).

Para lograr este objetivo, las estrategias de IdM se inclinan hacia la reducción o la limitación del número de credenciales digitales que los individuos tienen que utilizar en un gran número de servicios. Muchos países también ofrecen o planean ofrecer soluciones de inicio de sesión único para acceder a los servicios del sector público. En otras palabras, la mayoría de las estrategias pueden ser vistas como el objetivo de reducir uno o ambos enfoques donde el número de teclas digitales o credenciales de los usuarios de Internet tienen que gestionarse, así como el número de cerraduras digitales o puertas de enlace que se enfrentan cuando tratan de acceder a múltiples servicios de gobierno en línea. (OECD et al., 2011)

Las estrategias nacionales IdM generalmente adoptan un enfoque evolutivo basado en la normativa de identidad en línea existentes y buenas prácticas. Todos los gobiernos pueden automatizar y migrar sus procesos de negocio IdM existentes; las estrategias nacionales de IdM reflejan y respetan las culturas nacionales, estilos de gobierno y gestión de la identidad en línea con sus tradiciones. Por ejemplo, todos los países que respondieron que han lanzado una tarjeta nacional de identidad electrónica, en realidad lo que han realizado es la migración de sus actuales tarjetas nacionales basadas en papel. Los países que tienen una tradición de un registro nacional de población o un marco identificador nacional vigente lo están utilizando como base de su estrategia de gestión de la identidad digital, en ocasiones realizando el ajuste de las infraestructuras existentes para uso electrónico (por ejemplo, la creación de redes o la centralización de los registros de población existentes). No hay ningún ejemplo de un país que haya creado un documento nacional de identidad o el registro de la población, sin una tradición preexistente. (OECD et al., 2011)

En resumen, podemos apuntar que son proyectos públicos; la mayoría de ellos buscando apoyar la idea de unicidad como principal objetivo y estas metodologías o estrategias también podemos verlas en el ámbito privado, por ello enfocaremos el siguiente apartado para reflexionar sobre las alternativas que existen, sus ventajas y desventajas, obteniendo las mejores prácticas para la propuesta de metodología en México.

A partir de los esfuerzos por generar una Identidad Digital, se han establecido una serie de proyectos públicos para facilitar el uso de esta herramienta tecnológica. La Union Europea ha sido uno de los principales impulsores de proyectos transnacionales que facilitan la implementacion de una identidad de los ciudadanos de los países miembros. A continuación se presentan los principales proyectos públicos impulsados por la UE en materia de Identidad Digital.

2.1.1 Proyectos públicos

A continuación se enlistan proyectos que fueron establecidos en ambientes públicos, los cuales fueron implementados en la Unión Europea.

a) MODINIS eIDM Study

El plan de acción sobre administración electrónica 2010 (plan i2010), destacó como uno de los primeros proyectos cuyo objetivo era hacer más eficaces los servicios públicos, abordando problemas de interoperabilidad y necesidades futuras; además de considerar las diferencias en las prácticas legales y culturales apoyadas en el marco de protección de datos de la Unión Europea.

El proyecto MODINIS tiene como objetivo posibilitar proyectos en el ámbito de gobierno, lo que equivale a entrar a sistemas en el área legal y cultural; busca construir en base a la experiencia y las iniciativas de los Estados miembros de la UE para con ello avanzar hacia un enfoque coherente en la gestión de la identidad

electrónica en operaciones de carácter administrativo (electrónico) en la Unión Europea, donde se aborda lo siguiente: (Modinis eIDM, 2011)

- Apoyo a los servicios de administración electrónica transfronterizos e intersectoriales (registro de empresas, la contratación y la movilidad ciudadana);
- Análisis prospectivo de las posibles iniciativas y soluciones a nivel europeo;
- Proporcionar información sobre las tecnologías de identidad, la evolución del mercado y los requisitos técnicos correspondientes;
- Proponer una metodología para alimentar el marco descrito en el Marco de Buenas Prácticas.

Se procurará que los resultados del estudio se comuniquen a los Estados miembros y a la Comisión Europea mediante:

- Cinco talleres organizados en Bruselas, probablemente en los locales de la Comisión,
- Informes de gestión de identidad,
- Boletines periódicos, y
- Un grupo de trabajo de gestión de identidad de la administración electrónica.

Su principal aportación a la interoperabilidad es la definición de una infraestructura de alto nivel (disponibilidad y eficiencia), y un modelo o marco conceptual, llamado Modinis Conceptual Framework, el cual funge como un portal basado en federación que recoge las principales propuestas realizadas en el proyecto, en cuanto a organización general y principios básicos que deben regir una infraestructura eIDM a nivel paneuropeo.

La infraestructura se basa en un modelo federado que confía en una serie de portales de identidad en cada Estado miembro (al menos uno por estado, pero podrían ser más) los cuales son los responsables de la autenticación de una entidad a nivel nacional, así como de decidir el nivel de confianza que se otorga a los distintos procedimientos de autenticación realizados en cada Estado miembro. En

este modelo, los requisitos de autenticación para un servicio concreto, en un determinado Estado miembro, aceptarían como equivalentes los niveles de autenticación y los mecanismos empleados en otro Estado en base a un conjunto de criterios, de manera que no sería necesario establecer ninguna infraestructura específica a nivel europeo (Sánchez, Gómez, 2010).

Como podemos apreciar, el modelo presentado es para un Sistema Europeo de Gestión de Identidad basado en un conjunto específico de conceptos centrales específicamente pensados para aplicaciones de eGovernment y donde no se busca la homologación, sino una comunicación que al final arroje la información de cada Estado con sus herramientas.

b) TLS-Federation

Este proyecto se basa en el modelo Transport Layer Security (TLS), el cual consiste en la implementación de cualquier navegador y servidor web que se muestre inmune contra los "ataques web" comunes (base de datos, denegación de servicios, volumen de información, descifrar accesos, envío de script maliciosos, entre otros de acceso y consulta), con el objetivo principal de proporcionar un marco de trabajo regulatorio e interoperable para la gestión de identidad a nivel europeo. Esto puso el foco del proyecto en el uso de tecnologías y estándares conocidos, así como en la protección del usuario frente a posibles escenarios de robo de identidad.

El modelo TLS-Federation está basado en el uso de certificados que son ocupados durante el proceso de autenticación y está centrado en el usuario, ya que la identidad y los atributos de privacidad son gestionados directamente por él. Se puede utilizar dentro del mismo país o entre distintos países. (Bruegger, Hühnlein, Schwenk, 2012)

La tecnología se basa en una Autoridad de Identidad en TLS–Federation, lo que significa que los métodos de autenticación incluyen el uso de credenciales propias (certificados X.509 blandos o Tokens Seguros, I-Card –Information Card, es una colección de información de identidad de un usuario almacenada en un fichero–

, PKI (Public Key Infrastructure),[1] así como nombre de usuario / contraseña, contraseñas de única vez en el papel o creados por los tokens de hardware. Permite ocupar toda la tecnología de autenticación actual o futura pues es robusto y flexible en su desarrollo, lo que permite la compatibilidad. (inCommonFederation, 2014)

Es una solución que requiere poca instalación adicional y no hay necesidad de convertir las credenciales de sesión cuando se accede desde el dominio de cada Estado miembro al dominio europeo. Si se pone en marcha un sistema de autenticación, junto con el uso de proveedores de identidad gubernamentales basados en PKI, podría convertirse en un estándar en los Estados miembros europeos, por lo que TLS-Federation podría llegarse a utilizar para la autenticación a nivel europeo. Los componentes de esta tecnología ya existen y son soportados por la mayoría de los sistemas operativos, buscadores y servidores web existentes en el mercado actual. (Sánchez, Gómez, 2010)

Lo anterior muestra que esta solución procura seguridad para el usuario y una serie de protocolos que ya son comunes para los Estados miembros, así como la adaptación sencilla del conjunto de los mismos.

c) GUIDE

El objetivo principal en el proyecto GUIA (Creating a European Identity Management Architecture for eGovernment) fue definir una arquitectura que permitiera la integración de estas federaciones en un estado de confianza y seguridad con el fin de facilitar un entorno de identidad aparentemente sin fisuras a través del conjunto de Estados miembros de la UE. En este sentido, la investigación realizada concibe cómo proporcionar a la federación europea una Identidad Digital. Esto puede lograrse mediante la conexión de los proveedores de identidad existentes a una red de identidad o rejilla.

GUIDE utiliza un enfoque interdisciplinario innovador, orientado a cubrir toda la gama de procesos, políticas, cuestiones de gestión técnica de identidad jurídica

[1] Una infraestructura de clave pública –PKI (Public Key Infrastructure) en inglés– es una combinación de hardware y software, con políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

y social, buscando superar la fragmentación actual de las iniciativas de gestión de identidades definidas en su propósito principal, el cual desarrolla un enfoque coherente de la gestión de la identidad en toda la UE que permitirá a los Estados miembros acordar acerca de la identidad de una entidad (ciudadano o empresa), con el fin de permitir las aplicaciones sectoriales para realizar transacciones transfronterizas. El enfoque arquitectónico se basa en un modelo empresarial adoptado como marco para el desarrollo de la administración electrónica de la UE ya que la investigación reveló que los marcos de la administración electrónica se encuentran en estado de exploración para los Estados miembros.

La arquitectura se ha desarrollado como una Arquitectura Orientada a Servicios (SOA) implementada a través del modelo de servicios Web, satisfaciendo la independencia de la aplicación y la ubicación. El modelo conceptual de datos describe las entidades de datos clave que tienen que ser apoyadas por los servicios de identidad transfronteriza, así como también se han considerado los problemas de interoperabilidad. (Stefanova, Kabakchieva y Nikolov, 2011)

El principal problema es la definición de un marco lógico, técnico, institucional, político y legal, que sustente el apoyo al desarrollo de los servicios de gestión de identidad que integre los sistemas de gestión de identidades existentes y sea coherente con las condiciones jurídicas y reglamentarias vigentes en los Estados miembros. El objetivo refiere a la interoperabilidad entre sistemas y estructuras (procesos, cooperación, interfaces) nacionales dentro de las políticas legislativas y socioeconómicas.

En el nivel técnico, siendo una iniciativa pública, se acortan los presupuestos y se enfocan en algunas áreas; por el lado institucional se requiere que haya una adaptación de todas las áreas involucradas y que estén de acuerdo con la transferencia de apoyo mediante las identidades para finalizar en las áreas legal y política. Estas son reglas que se tienen por cada departamento, lo cual requeriría de un apoyo extra para la comprensión y empatía del proyecto.

La creación y el funcionamiento de la arquitectura GUÍA implican la administración pública así como la cooperación industrial, con el fin de desarrollar procesos interoperables, modelos de cooperación e interfaces. El operativo central

de GUÍA es aplicar una administración electrónica, la cual implica importantes transformaciones a lo largo de las líneas institucionales, políticas, legislativas y tecnológicas, lo cual se basa en un enfoque integrador, ya que trata de superar la fragmentación actual de las iniciativas que inhiben el funcionamiento continuo y eficaz de los servicios de administración electrónica que se han diseñado para facilitar el rediseño de las estructuras y procesos existentes, con el objetivo de mejorar la colaboración entre los diferentes departamentos del Gobierno, así como de la armonización de las prácticas de administración electrónica a nivel europeo como retos GUÍA. (Stefanova et al., 2011)

Queda claro en que esta propuesta busca hacer una integración que facilite la comunicación entre entes privados y públicos, lo cual hace a este un proyecto ambicioso en la obtención de estándares que los demás países están en proceso de realizar. Es por ello que es un prototipo para políticas que ayuden a la integración.

d) STORK (Secure idenTity acrOss boRders linKed)

Este proyecto desarrolla y prueba especificaciones comunes para un reconocimiento mutuo y seguro de las identidades electrónicas (eIDM) nacionales de los países participantes. Como objetivo tiene el de definir modelos y especificaciones comunes para el mutuo reconocimiento de eIDMs entre países, probando, en un entorno real, soluciones de eIDM seguras y fáciles de utilizar, tanto para ciudadanos como para empresas, y así interactuar con otras iniciativas de la Unión Europea para maximizar la utilidad de los servicios de eIDM.

Es un modelo federado para interoperabilidad, tecnológicamente flexible-adaptable y que soporta múltiples niveles de autenticación. Concretamente, se presenta un modelo que confía en un proxy y requiere de la creación de proveedores de identidad a nivel nacional (al menos uno por país). Este sistema de proveedores de identidad se une en STORK a una red de proxys proveedores de servicios denominados PEPS (Pan European Proxy Services). Estos proxys serán creados a nivel nacional, aunque el modelo también contempla la posibilidad de que exista un proxy europeo centralizado o incluso un modelo mixto; de tal modo que ciertos

países confían en un PEPS nacional, mientras que otros lo hacen en un PEPS europeo. Los PEPS sirven básicamente para superar el problema técnico que se presenta cuando aparece un conjunto amplio de soluciones de identificación / autorización, como es el caso del escenario europeo. Por ejemplo, en algunos casos, un ciudadano querrá utilizar una combinación nombre de usuario–contraseña para acceder a un servicio, mientras que otro preferirá utilizar su tarjeta de identificación electrónica. Suponiendo que el dueño de la aplicación dé por buenos ambos métodos de identificación, la infraestructura técnica debe ser capaz de soportar ambas soluciones. Es aquí donde entra en escena el PEPS, cuya principal función es la de conectar a los proveedores de servicios con los proveedores de identidad adecuados en cada país y validar la confianza y la seguridad de la información de identidad enviada por los proveedores de identidad.

En lo referente al marco tecnológico elegido para interconectar las soluciones o el modelo conceptual detrás del marco de trabajo, las decisiones no se han hecho públicas aún. Sin embargo, dentro de las intenciones del proyecto STORK se encuentra el ser lo más tecnológicamente transparente posible y así asegurar soluciones interoperables con los sistemas nacionales de eIDM existentes. Así mismo, STORK intenta confiar, tanto como sea posible, en estándares abiertos. (Sánchez, Gómez .et al., 2010)

Esta idea nos lleva a la posibilidad de tener una herramienta que recibe las diferentes tecnologías de los Estados miembros permitiendo una comunicación sin que esta intervenga en su solución por país.

El siguiente cuadro muestra los elementos importantes de cada metodología, no perdiendo de vista sus limitaciones y similitudes, considerando que vienen del sector gobierno europeo, se puede notar que cumplen con los estándares propios de sus países; lo interesante es lo que propone cada metodología y su resultado final.

Cuadro de Metodologías	
Público	

Nombre de proyecto	Consiste en	Limitaciones
MODINIS eIDM	- Interoperabilidad - Servicios transfronterizos e intersectoriales - Análisis de iniciativas y soluciones a nivel europeo - Proponer metodología - Buenas prácticas - Talleres - Boletines - Seguridad	- Conjunto específico de conceptos centrales específicamente pensados para aplicaciones de eGovernment
GUIDE	- Interoperabilidad - Servicios transfronterizos e intersectoriales - Análisis de iniciativas y soluciones a nivel europeo - Proponer metodología - Buenas prácticas - SAML como protocolo de comunicación y utilización de certificados X.509 - SOA - Análisis de procesos actuales - Seguridad	- Falta un marco lógico, técnico, institucional y político / legal, el cual sustente el apoyo al desarrollo de los servicios de gestión de identidad, que integra los sistemas de gestión de identidades existentes y sea coherente con las condiciones jurídicas y reglamentarias vigentes en los Estados miembros (Unión Europea)
TLS-Federation	- Interoperabilidad - Servicios transfronterizos e intersectoriales - Análisis de iniciativas y soluciones a nivel europeo - Proponer metodología	- Podría ser un estándar en los Estados miembros europeos, pero tendría que convertirlo en un estándar legal para que todos formen parte de la iniciativa.

	- Buenas prácticas - Fácil instalación - Seguridad - certificados X.509	
STORK	- Interoperabilidad - Servicios transfronterizos e intersectoriales - Análisis de iniciativas y soluciones a nivel europeo - Proponer metodología - Buenas prácticas	- Lo referente al marco tecnológico elegido para interconectar las soluciones o el modelo conceptual detrás del marco de trabajo, las decisiones no se han hecho públicas aún

Cuadro 1. ***Resumen de Metodologías Públicas UE***

Fuente: Elaboración propia de acuerdo a las metodologías utilizadas en EU

2.1.2 Proyectos privados

Los esfuerzos privados se han desarrollado poniendo atención a los proyectos que se realizan a partir de proyectos nacionales, programas que se presentaron en la sección anterior. El uso continuo en instituciones que día a día contribuyen a una notable serie de operaciones, logra abrir el panorama para producirlos en diferentes ámbitos fuera de un ambiente controlado.

Los proyectos que se mencionaron anteriormente constituyen una base tecnológica, pero no conforman todo el panorama, a continuación, se enlistarán diferentes tecnologías siempre enfocadas a la seguridad y a las circunstancias propias de cada entidad, por ello es importante ver cuáles son los ámbitos en los que se dará su aplicación y así actuar en consecuencia con la tecnología más idónea, tomando en cuenta la independencia de las mismas.

a) Ecosistema digital

Su objetivo es multidisciplinario, enfocado a que diferentes áreas dentro de la empresa puedan tener empatía, ya que cada uno de ellos tienen una forma diferente de administrar los datos, de identificar a su personal y a sus sistemas propios o herramientas cotidianas con lo que apoyaría a homogeneizar el ecosistema digital.

Este proyecto se basa en ambientes heterogéneos, en los que tanto infraestructura como plataformas son diferentes, por lo que pueden llegar a adaptarse en diversas tecnologías. Los proveedores de identidad local, así como de sitios web son distintos, pero incluyen siempre un lenguaje en común para sus mensajes y metadatos que fluyen en la red XML, así como del protocolo SAML, el cual es un estándar utilizado de manera internacional con certificados X509.

Un problema con estos ecosistemas es que a pesar de que cubren gran variedad de herramientas, su autenticación sigue siendo dispersa y no existe una administración centralizada, por lo que la respuesta de autenticación se vuelve lenta y no forma parte de una idea a gran escala; tal vez dentro de ciertas organizaciones, este método de autenticación entre sistemas tenga un buen recibimiento.

b) Administración cliente / servidor

Su objetivo es tener control punto a punto dentro de la misma organización, que no exista un tercero en la administración de datos colocando la información de manera transparente para quien lleve la gestión y explotación de reportes del servicio que se estará dando.

Cuando se cuenta con una plataforma cliente / servidor, la administración de una identidad se realiza a partir de servicios con un proveedor determinado y estos son regulados en esta administración por medio de un acceso controlado, ya que se manejan una serie de roles para ejecutar el ingreso de cada usuario.

Estos servicios son totalmente comerciales pues cuentan con ciclos de vida para el uso de servicio, pueden componerse de la Identidad Digital adecuada, solo que proporcionada por un servicio externo que tiene un tiempo para presentar el servicio y se tiene que acoplar a un servicio bajo las condiciones que determine el proveedor.

c) Modelo de algoritmos para optimizar la comunicación y seguridad en la transmisión de información

Aquí el objetivo se basa en la rapidez y optimización de colocar el mensaje de manera y tiempo correcto para los involucrados. A través de nuestra Identidad Digital podemos transmitir mensajes, gustos o emociones, los cuales deseamos que lleguen inmediatamente al destinatario, siendo esto seguro y de apoyo para el destinatario.

Buscando una optimización tecnológica, el manejo de algoritmos posibilitaría una mejor respuesta y optimización de la serie de datos que han sido generados en la comunicación, esto podría ser aplicado a cualquier ambiente de trabajo puesto que pretende mantener la relación de transmision de datos donde sea fluida y sin interrupciones en los mensajes que hayan sido transmitidos.

El manejo de estas mejoras estaría limitado a plataformas iguales dentro de un ambiente controlado, y a primera instancia se manejaría como un experimento de unidades (hardware) cercanas con medidas de optimización de nodos. Esta alternativa muestra que la generación de mejoras a los sistemas actuales es posible bajo medidas condicionadas, lo cual deberá tener un estándar y ampliarse a multiplataformas para que esto pueda ser adaptado en diferentes lugares.

d) Proyecto en Estados Unidos, Australia y Canadá

Al igual que la Unión Europea, en América existen avances y proyectos con el fin de llevar una mejor empatía con respecto a servicios de Identidad Digital en los gobiernos, se ha buscado que las normas sean apoyadas en estos procesos –como comentaremos mas adelante– dejando claro que estas iniciativas, al igual que en Europa, buscan seguir una serie de pasos enfocados en la mejora.

En Australia se está implementando un servicio de verificación de documentos para que las dependencias de gobierno lleven a cabo comprobaciones en tiempo real sobre la validez de los documentos presentados por los clientes como prueba de agencias de identidad. El gobierno también anima a seguir un marco de autenticación electrónica que promueve la reutilización de los procesos y las prácticas existentes para mejorar la seguridad, facilidad de uso y eficiencia de costos. Estos enfoques respetan la tradición descentralizada del estilo de gobierno de Australia, al tiempo que permite un sistema de gestión de identidad más sólida, ya que es el objetivo principal de la estrategia australiana. (OECD et al., 2011)

En países como Australia, Canadá y los Estados Unidos se pueden observar tres cosas en atención a la tabla de los principales componentes para IdM: (OECD et al., 2011)

- Australia, Canadá y los Estados Unidos tienen el mayor territorio y la densidad de población más baja de todos los encuestados. Además, los tres son ejemplos de países con un sistema de gobierno federal y están a favor de un enfoque descentralizado de la gestión de la Identidad Digital.
- En general, las tarjetas ciudadanas o tarjetas de servicio son adoptadas por los países que no tienen una tradición de un documento nacional de identidad obligatorio, pero sí tienen una tradición de un registro o identificador nacional de población.
- Un enfoque migratorio es probable que implique retos adicionales a los que existían en el entorno preexistente. Por ejemplo, los desafíos transfronterizos que existían con la gestión de la identidad en línea no se resolverán simplemente mediante la migración de la gestión de la identidad en línea.

País	***Enfoque***
Australia	• Normas de registro, matrícula, seguridad para la prueba de los documentos de identidad, Integridad de Datos de identidad, autenticación

	electrónica y biométrica de Interoperabilidad ● Documento Nacional de Servicio de Verificación (DVS) ● Inicio de sesión único a los servicios de gobierno electrónico
Estados Unidos	● Un marco amplio del ecosistema de identidad ● Una infraestructura de identidad interoperable alineada con el marco del ecosistema de identidad
Canadá	● Elementos fundamentales para definir conceptos clave (por ejemplo, modelos de seguridad, código de privacidad, la confianza en el modelo), ● Un marco de la definición de una estructura de alto nivel y la arquitectura, así como de los ámbitos legal, de privacidad, y seguridad, ● La confianza de identificación y requisitos de experiencia de servicio, ● Un componente de prestación de servicio de identificación de proyectos piloto, ● Normas y directrices, así como un componente de apoyo

Cuadro 2. ***Enfoque de los Proyectos.***
Fuente: Elaboración propia de acuerdo a proyectos en América

Como conclusión podemos decir que las estrategias nacionales e internacionales llevan a cabo procesos de migración donde a menudo requiere de ajustes y cambios evolutivos. A veces, los componentes innovadores tienen que ser diseñados para abordar los desafíos específicos planteados por el mundo digital o para aprovechar el contexto digital. La brecha de intereses y tecnología cambia de un lugar a otro, así que estas iniciativas, tanto nacionales como internacionales,

deben plantearse en pequeñas etapas y ver los resultados de éxito, evaluando fortalezas y debilidades para afinar cada proyecto iniciado, así como ser claro en fechas y los resultados que se quiere obtener, pues difícilmente obtendrás resultados exitosos implantando la tecnología sin una planeación adecuada.

Resumen de metodologías privadas

El siguiente cuadro de metodologias privadas muestra a continuación, que si bien pueden compartir protocolos propios de la tecnología tambien es cierto que cambiarán los resultados para lo cual busca cada organización y que los métodos en que serán implantados muestran diferencias y adaptaciones propias de cada lugar, algunas buscan empezar a implantar estos métodos, otros buscan economizarlos y otros más buscan lo mejor de cada cual y montarlos como algo cotidiano y certero en toda la operación.

Cuadro de Metodologías		
Privado		
Nombre de proyecto	Consiste en	Limitaciones
Ecosistema Digital	- Las entidades varían, pueden ser colaborativas y a veces competitivas, - Con ambientes tecnológicamente heterogéneos, diferentes tipos de plataformas e infraestructuras, - Proveedores de identidad local o sitios web de confianza,	- No hay autenticación centralizada, - La administración tendría que ser centralizada para tomar en cuenta las diferentes plataformas e infraestructuras, - Limites en propuesta de tiempo

	- Utiliza XML para mensajes y metadatos, - Usa un protocolo SAML como estándar internacional, utilización de certificados X.509	
Administración cliente / servidor	- Consta de usuarios, - Proveedores de servicio para la administración de la identidad, - Proveedor del servicio, - Tarjeta de servicio (servicios subscritos), cambiar servicios utilizando al proveedor, - Perfiles y filtros de información, - Cuenta con un ciclo de vida de administración: subscripción al modelo de servicio, modelo de uso del servicio, modelo de cancelación del servicio.	- Es un servicio tradicional con límites de servicio, - El proveedor es el administrador de la identidad, - Falta de multiplataforma,
Modelo de algoritmos para optimizar la comunicación y seguridad en la transmisión de información	Manejo de un algoritmo que busca optimizar el flujo de información, así como su seguridad y consiste en la clasificación de los nodos en un anillo con una distancia métrica aplicada a sus identificadores: - Paso 1. Primera optimización que adiciona una tabla de vecinos con los otros nodos que se pueden alcanzar en un solo hop. - Paso 2. Segunda optimización que construye una tabla de enrutamiento en cada nodo que insta a que envíe todos los	- Falta de multiplataforma

	mensajes a su router, a menos que se trata de uno de sus vecinos. - Paso 3. Tercera optimización, en la cual se insta a cada nodo a mantener nodos de búsqueda en dos tablas de los nodos, que apunta de modo distante como agujas del reloj, y uno nuevo que apunta a nodos distantes en sentido contrario a las manecillas del reloj.	

Cuadro 3. ***Metodologías privadas***

Fuente: Elaboración propia de acuerdo a metodologías privadas

Consideraciones de los proyectos públicos y privados

En la práctica, estos proyectos muestran que pueden llegar a ser muy generales pero tambien tener una dosis de multidisciplinariedad, esto porque mientras que unos son muy cerrados en el ámbito público ya que su demanda y estatutos dificultan en ocasiones lo que se puede llegar hacer, en otros casos pueden existir procesos que bajo el esquema de Identidad Digital gestionarían el propósito de la institución.

En el caso de los privados, pueden ser más cerrados que los públicos, esto nos lleva a identificar sus desventajas, ya que buscan no ser centralizados o en el afán de ser tan focalizado a su ambiente, pierden el foco de lo que puede brindar la tecnología. El tema de las licencias se vuelve un problema al querer implantar algo en cada una de ellas; los administradores de estas herramientas para empresas privadas muchas veces son un tercero mientras que en las públicas buscan mantener un control dentro de sus instalaciones.

Tanto en los ámbitos públicos como privados se presenta la multidisciplinariedad, ya que son varias las áreas donde se implantará la Identidad

Digital, el reto está en cómo se combinan para encontrar una situación homogénea que sea incluyente y se obtengan los resultados más favorables sin escatimar en seguridad e intercambio de información; pues qué sería de esta herramienta sin la información previa y la que alimentará la vida de ésta en donde se aplique. Más que una herramienta, buscamos un apoyo, un lugar centralizado e información que ayude y apoye para generar mayor certidumbre de los siguientes pasos y del por qué se utilizó cierta tecnología y no otra.

Como resultado de los proyectos, observamos que varios de los elementos que usaron para cada una de sus ejecuciones son compartidos, en ocasiones se utilizan bajo el contexto en que se están implementando, donde es lo más adecuado para llegar a los resultados que se requerían en su momento, por ello utilizaremos las mejores prácticas para dar el enfoque general de los elementos que debe llevar una metodología para la Identidad Digital.

Se implementaron estas herramientas de un país a otro en apoyo a sus gobiernos, buscando que se adaptaran a las necesidades de cada institución. Los elementos compartidos fueron los de la infraestructura, donde un proveedor les implementaba la gestión de Identidad Digital y posteriormente se da una gestión interna en la que se buscaba hacer el trámite propio del órgano gobernado.

Al conocer las propuestas de gobierno que son presentadas en el ámbito público, se habla de establecer tecnologías que buscan interoperabilidad, pues las tecnologías con las que cuentan los diferentes gobiernos no son las mismas, ni el tamaño de población de los diferentes países miembros de la Unión Europea.

Los proyectos dan solución e implantación de nuevas tecnologías, pero de lo que adolescen estas prácticas es de algo que sustente su desarrollo, las reglas, políticas y empezar a integrar esa solución para ver resultados, pues queda la incógnita de la implantación en dos o mas países, dado que lo han pensado y argumentado de manera individual.

Actualmente, las soluciones de tipo privado comprometen un servicio que involucra a proveedores externos y la utilización de tecnologías estables y la infraestructura no está definida para varias plataformas, pues viéndolo del punto de vista privado, las empresas podrían ser y comportarse como un estado autónomo

que solo ocupa un tipo de tecnología, es por ello es una buena alternativa para adoptar.

2.2 Condición de la Identidad Digital en México

En este apartado se expone cuál es la reglamentación y las políticas con respecto a Identidad Digital a nivel nacional. México ha buscado generar una serie de elementos legales y temas de seguridad presentes en la legislación debido a que conllevan importantes acciones en el Derecho a la Identidad y han tomado los elementos tecnológicos que existen.

En la legislación, existe la Reforma Constitucional con respecto al Derecho a la Identidad que está contenida en el Artículo 4 de la Constitución Política de los Estados Unidos Mexicanos; donde se implica que toda persona tiene derecho a la identidad y a ser registrado de manera inmediata a su nacimiento. Los estados siempre garantizarán el cumplimiento de estos derechos de identidad. De igual manera, las autoridades competentes expedirán gratuitamente la primera copia certificada del acta de registro de nacimiento.

La identificación, con el carácter de ciudadano mexicano, así como del estado al que pertenece, consiste en la acreditación de las copias certificadas que se obtinen en el Registro Civil, que nos son expedidas para comprobar nuestra nacionalidad y edad.

2.2.1 Condiciones tecnológicas de la Identidad Digital en México

Existe el Registro Nacional de Población en México (RENAPO) en el que se estructura la identidad en los siguientes rubros: (renapo.gob.mx, sf)

- Identidad legal
- Identidad vivencial
- Identidad física
- Identidad digital

En términos de la Ley General de Población: "*Las actividades de la RENAPO se refieren al registro y la acreditación de la identidad de todas las personas residentes en el país y de los nacionales que residan en el extranjero. Y están reflejados en los artículos 85 y 86 de nuestra ley*". (https://www.gob.mx/segob/renapo)

Esto implica un amplio registro en cuatro ámbitos de la identidad de un ciudadano, formulando, por lo tanto, cuatro campos importantes de identificación donde existe un acuerdo mediante el cual se da a conocer el Programa para el Establecimiento del Registro Nacional de Ciudadanos y la expedición de la Cédula de Identidad Ciudadana. El Registro Nacional de Población tiene como finalidad inscribir a cada una de las personas que comprenden la población del país mediante datos que permitan certificar y acreditar fehacientemente su identidad.

El Registro Civil es la base de nuestra identidad legal (RENAPO) y a partir de ahí, todos los mexicanos tenemos la posibilidad de ejercer los derechos que nuestras leyes nos otorgan y los tratados internacionales reconocen. Por ello se incorpora a las organizaciones como un registro importante para identificar al personal que labora en ella, estos datos están contenidos en la credencial de elector.

La credencial de elector es un documento de identidad legal que es expedida a través del Instituto Nacional Electoral, el cual indica que: "*es una identificación oficial que avala la ciudadanía mexicana y que emplean millones de personas para ejercer su derecho al voto en México y en el extranjero*". (https://www.ine.mx/credencial)

La CURP se incorpora como identidad vivencial, y se acredita mediante la Clave Única de Registro de Población, un trámite que se lleva a cabo desde diciembre de 2005, y que se puede consultar e imprimir a través de internet en www.renapo.gob.mx y www.segob.gob.mx. Un dato sobre este proceso es que en el 2013 se realizaban 72.9 millones de consultas a través de internet en los meses de enero a julio, esto es, en promedio 344 mil consultas diarias. Este es un ejemplo de registro único ciudadano y de consulta electrónica del mismo.

La identidad física consiste en acreditar la identidad mediante la información biométrica de las personas (huellas digitales, reconocimiento de iris, reconocimiento de rostro). La biometría se basa en la premisa de que cada individuo es único y posee rasgos físicos distintivos (rostro, huellas dactilares, iris de los ojos, etcétera) que pueden ser utilizados para su identificación inequívoca. Biometría es el conjunto de métodos automatizados de autenticación (identificación y verificación) de la identidad de una persona, basados en una característica fisiológica o de comportamiento. La metodología aplicada para el reconocimiento de biométricos está dividida en dos procesos claramente diferenciados: 1) Verificación que valide que es el individuo correcto el que está haciendo la petición y 2) Identificación cuando se validan todas las características biométricas guardadas. Esto se puede incorporar a toda organización pues ya la entrada a espacios laborales puede ser por medio de, por ejemplo, huellas dactilares.

Como se entiende en la RENAPO, la Identidad Digital consiste en la Firma Electrónica, la cual da posibilidad de realizar trámites sin tener que trasladarse a las oficinas de la dependencia, ni ceñirse a horarios para el cumplimiento de una obligación. Y esto se puede incorporar dando la posibilidad de automatizar nuevos trámites y servicios que permitan obtener un mayor control de la información que ingresa a la dependencia para la toma oportuna de decisiones e identificar a los usuarios que realicen transacciones electrónicas con la dependencia, reconociendo la autoría y voluntad jurídica de dichas transacciones. Eliminando además, los formatos impresos, con la reducción en el uso de papel que esto implica.

La Identidad Digital en las organizaciones

La identidad es importante en las organizaciones pues representa el origen de cada persona en la organización, la oportunidad de reconocerle, y también de recuperar la autonomía de sus propios datos, pues la gente los produce y los comparte creando valor para las empresas a través de la cocreación y compartiendo sus datos. En la medida en que el Usuario / Trabajador / Talento lo permita, estos datos se pueden actualizar y podrían ser ampliados basándose en el aprendizaje

automático, integrado y predictivo, donde también pueden pertenecer a proveedores de terceros de confianza (como por ejemplo bancos, empresas desarrolladoras de software) para prestar proactivamente servicios. Inclusive, estas identidades digitales a partir del uso de metadatos y valores de atributos que les permiten diseñar su propio registro de datos personales y facilitar las experiencias que el talento puede vivir dentro de la empresa.

Al tener la oportunidad de ocupar estas herramientas de identidad en las empresas, pueden llevar a cabo un mejor uso de los datos y obtener metadatos de la información, como ahora se busca en plataformas como Identidad Digital 3.0 (Digital Economy, 2017), donde a partir de la identificación del talento dentro de las organizaciones y de sus actividades, permite que obtengamos información adicional para generar iniciativas que se traducen en KPIs (Key Performance Indicator), que es una medida del nivel de desempeño de un proceso. Como ejemplo de esto, BBVA Bancomer ocupa disciplinas como Workplace que busca dar una gestión de valor, u otra disciplina Advanced Middleware, que busca un mayor entendimiento entre las necesidades de la organización, la cual va detrás del cliente y no al revés. Se buscan las formas de dar eficiencia a lo que se tiene, creando mejores interacciones mediante sus identidades digitales.

2.2.2 La legislación de la Identidad Digital

La Ley Federal de Transparencia y Acceso a la Información Pública determina los procesos de ingreso y acceso a los procesos de la información pública, y determina los procesos básicos para acceder a ella. En el capítulo quinto de esta ley –en los artículos 121, 124 y 144–, se enuncian los procedimientos para el acceso a la información, las solicitudes que habrá de apoyar al solicitante y mediante qué plataforma o lugar se podrá obtener lo que se requiere así como lo que se obtendrá desde su folio para seguimiento o acuse de recibo. Todo aquello que se le proporcione al solicitante es público y será recibido por medios remotos o locales de comunicación electrónica.

Elementos de la legislación en materia de Identidad Digital en México

Derecho a la protección de los datos personales en México. En México contamos con una ley que protege los derechos en relación a los datos personales (Ley Federal de Protección de Datos Personales en Posesión de los Particulares 2010), estas leyes buscan ser cumplidas en función del ciudadano y las particularidades de cada una de ellas, hablando de datos sensibles los que abarcan desde discriminación o amerite un riesgo mayor al ciudadano, así también, de consentimiento a través de firma electrónica o en papel donde se permite la utilización de los mismos.

Al hablar de Tratamiento de Datos Personales (TDP), hay medidas de seguridad, técnicas y físicas donde el articulo 19 es puntual al enunciar *"… proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo, se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.*" Dejando claro que si ello ocurriera la ley colabora y adopta medidas para servicio de los intereses del involucrado.

Cuando hablamos de una empresa, y la información que ella maneja del empleado, coloca al usuario de los sistemas en un ambiente donde se manejan datos comunes que van desde nombre, usuario, contraseña, área, domicilio, edad, sexo, hasta algunos de confidencialidad, donde el usuario firma de común acuerdo estas estipulaciones. Esto se vuelve un contrato de confianza, un artículo en donde se habla que esta relación puede continuar es el Artículo 21: "El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable."

La información que proveemos en las empresas en las que somos contratados están cuidadas al abordarse la ley TDP; no tocan la parte digital en la ley como tal, pero deja claro de la oportunidad de abrir una brecha de artículos sobre ello y eso también los vemos en el Artículo 27: "*El titular tendrá derecho en todo momento y por causa legítima a oponerse al tratamiento de sus datos. De resultar procedente, el responsable no podrá tratar los datos relativos al titular.*" Este apoya la labor de oposición de la información que proporcionó.

La base jurídica de la identificación electrónica debe corresponderse con el derecho a la protección de datos personales para entender la importancia de la protección de los datos personales de identificación electrónica, así como el vínculo íntimo entre la identidad y los datos protección.

a) Ejemplo de un proyecto bajo consideraciones de seguridad en México

Existe un proyecto que empezó el 1 de octubre 2010 y finalizo al 31 de octubre de 2012: el proyecto SECURE-ID, el cual tiene como meta la creación de una plataforma que fue un marco de trabajo confiable, capaz de proporcionar funcionalidades de identificación segura mediante certificados digitales, tarjetas de identificación electrónicas y protocolos de Identidad Digital. A través de los elementos de desarrollo libre y usando infraestructura que puede utilizar el software libre, una forma de gestionar de manera práctica la información digital e identidad que podría adaptarse a cualquier ambiente. Esta funcionalidad podrá ser utilizada por muchas aplicaciones y/o servicios que las necesiten.

Es por ello es que el proyecto SECURE-ID lo ocuparemos como una muestra de la obtención de una Identidad Digital confiable en México, en donde se ocuparon protocolos que ayudaron a que los servicios fueran confiables y que permiten ver cómo es que podría aplicarse de manera segura la Identidad Digital.

Este proyecto de innovación ha sido financiado por CDTI en el marco del Programa de Cooperación Interempresas Nacional, tras la obtención de la etiqueta Iberoeka. Los involucrados son INDRA, creativIT (Innovando en soluciones IT), DMS (Desarrollo – Medio – Sistemas) y un consorcio mexicano (Moviquity), así

como la Universidad del Tecnológico de Monterrey. El papel de Indra es el de coordinador del proyecto y centrará su trabajo investigador en los siguientes demostradores:

- Enviar documentación firmada a través de la red Lexnet de la Administración de Justicia española a partir de su integración con el DNIe.
- Procesos Electorales: Uso del documento de identidad electrónico en procesos electorales.
- Servicios preelectorales.
- Servicios electorales.
- Servicios postelectorales.

Los objetivos de investigación y tecnológicos pretenden impulsar la modernización de la e-Administración, mediante la utilización de las TIC, para conseguir la integración de administraciones y transacciones. Se desarrollarán cuatro servicios demostradores en México y/o España basados en la plataforma desarrollada, que utilicen tecnologías de certificación y el DNIe en un marco de Identidad Digital.

Estos servicios se orientan a los escenarios:

- Enviar documentación firmada.
- Sistema de votaciones, consultas, referéndum, etc.
- Descarga de información sensible.
- Pagos y facturación electrónica para e-Administración.

Las novedades tecnológicas de SECURE-ID se resumen:

- Sistemas de gestión de identidad basados en estándares abiertos, facilitando interoperabilidad y competencia justa.
- Hard y Soft compatible con especificaciones de Liberty Alliance y OASIS para implementar las infraestructuras de los COTs.
- Entorno IDM seguro: Implementación de Liberty IDM y OASIS considerando la seguridad y privacidad como aspectos clave para la aceptación por el usuario final, y teniendo en cuenta los requisitos de usuario y la regulación europea y mexicana para controlar el envío de datos personales de usuarios.

- Documento de identidad electrónico: implementación de un sistema de gestión de identidad basado en documento de identidad electrónico, desarrollado con tecnología interoperable a partir de Liberty y OASIS, para ofrecer funciones de servicios como gestión de privacidad, seguridad y servicios web.
- Claves en mano: Uso de tarjetas inteligentes como almacén de claves, en lugar de en un ordenador de donde podrían ser extraídas.
- Integración del certificado del DNIe con redes concretas de envío de documentos firmados electrónicamente: Por su trascendencia en procesos electorales, se plantea su integración con la red Lexnet de la administración de justicia, accediendo a partir de diferentes plataformas tecnológicas: Vbasic, .net, servicios web.
- Demostradores de documentación de identidad electrónica cuya finalidad es tener una visión clara de las posibilidades y ventajas de la implantación del documento de identidad electrónico.
- Firma electrónica de cualquier información: creación de un sistema capaz de firmar electrónicamente con la identidad real del usuario (DNIe), cualquier documento o archivo electrónico.
- Innovaciones en gestión documental: Definición del esquema de meta-datos (contexto, jerarquización y clasificación, búsqueda y recuperación, y trazabilidad de los procesos). Permitirá separar el contenido y contenedor, con conversores a XML y renditions. Integración del sistema de gestión documental con la red Lexnet.
- Creada la infraestructura de identidad digital, se desarrollarán servicios específicos para demostrar diversos escenarios en entornos reales, con el fin de validar y medir la satisfacción del usuario.
- Enviar documentación firmada: desarrollo de una aplicación basada en Liberty y OASIS en las infraestructuras PKI capaces de firmar un archivo con el documento de Identidad Digital del usuario, así el usuario enviará un documento firmado digitalmente a un servicio que validará la información del

usuario y aceptará el archivo con la misma validez y confianza que si hubiera sido firmado con puño y letra.

- Procesos electorales y consultas: Se demostrará el uso del documento de identidad electrónico en procesos electorales.
- Servicios preelectorales: Presentación de candidaturas, solicitud de voto por correo, etcétera. Viabilidad de la gestión electrónica de las tareas, asegurada la identidad de los agentes y la autenticidad de la documentación electrónica.
- Servicios electorales: Voto electrónico. Recoger y validar la identidad del elector con DNIe y entorno de Identidad Digital, previo a seleccionar y enviar el voto electrónico.
- Post-electorales: Viabilidad de la gestión de actas electorales generadas, enviadas y custodiadas en formato electrónico.
- Descarga de información sensible: Demostrar la facilidad de integrar un servicio en un entorno federado y utilizarlo. Un usuario podría, por un lado, consultar información personal, como su vida laboral, multas, etcétara, y por el otro, descargar información de la administración. (controlando quién accede a esa información).
- Pagos y facturación electrónica para e-Administración: El servicio alcanzará las interacciones del usuario (ciudadanos, empresas, administraciones) con la administración electrónica para realizar micropagos, pagos, facturación electrónica, etcétera.

Las tecnologías utilizadas en este desarrollo son:

Tecnologías utilizadas	
Tecnologías libres	Descripción
Liberty Alliance y OASIS (Organización para el Avance de las Normas de Información Estructurada).	• Organización formada en septiembre de 2001 para establecer normas, directrices y mejores prácticas para la gestión

	de la identidad en sistemas informáticos • Software de código abierto
Identidad federada.	Es una de las soluciones para abordar la gestión de identidad en los sistemas de información. El valor añadido adicional, respecto a otras soluciones, es la gestión de identidad interdependiente entre compañías, lo que se denomina Federated Identity Management.
Infraestructuras PKI.	Permite a los usuarios autenticarse frente a otros y usar la información de los certificados de identidad (por ejemplo, las claves públicas de otros usuarios) para cifrar y descifrar mensajes, firmar digitalmente información, garantizar el no repudio de un envío, entre otros usos.
DNIe (autenticación y firma electrónica).	El certificado tiene dos claves, una pública –que es la única que "viaja" en las transacciones telemáticas– y otra privada que nunca sale de la tarjeta en la que se encuentra. La primera de ellas permite autentificar la identidad de un ciudadano, mientras que la segunda se utiliza para ejecutar el procedimiento de la firma electrónica.
Lexnet (envío seguro de documentos).	Envía documentos firmados electrónicamente, se ha convertido en un instrumento de trabajo seguro.

Cuadro 4*. Tecnologías utilizadas*

Fuente: Elaboración propia de acuerdo a Tecnologías que se utilizaron en el proyecto

Los elementos centrales de este proyecto se basan en procedimientos internacionales de seguridad y aportan a la idea de que todo puede ser implementado dado un procedimiento que pueda adecuarse *ad hoc* al lugar en el que vivirá e indudablemente puede llevarse a cabo un procedimiento de identidad digital transparente utilizando las tecnologías de información adecuadas de manera libre.

Se menciona este proyecto ya que es diferente al resto por su alto contenido tecnológico, el cual cubre toda la cadena de valor, desde el análisis previo del servicio, hasta su desarrollo y validación por parte de usuarios finales y abona procesos de identidad que podrán ocupar, tanto instituciones públicas como privadas. Es por ello que este proyecto representa una propuesta que contiene tecnologías de uso libre, pero cimentadas en recomendaciones internacionales y que cubren una serie de análisis para adecuar los servicios, así como un piloto de usuarios finales.

Si quisiéramos comparar este proyecto con lo anteriormente observado en este capítulo, la similitud que se presenta en los tres es que los sistemas tienen siempre ese toque "*ad hoc*" y esto es porque, aunque cada uno tiene protocolos, estándares o mejores prácticas, siempre llega un momento que se tiene que adaptar a la organización, y es ahí donde el universo de posibilidades se reduce a lo que da valor y es útil. La tecnología comparte servicios, orden y la parte de gobierno, ya que siendo este un proyecto con miras a usarse en asuntos publicos como son autenticación de usuarios con credencial de elector, pagos, facturas y bajar información; esto se da bajo una buena administración. Esto es algo que tambien se buscó en todos los proyectos públicos y metodologías que anteriormente se mencionaron.

La diferencia con los privados es la inversión, ya que muchas de esas metodologías causan un costo por licenciamiento, mientras que este proyecto es libre, incluso algunos proyectos como los públicos también tienen ese costo de licencias, lo que trae como consecuencia que no sean herramientas para todos, sino para unos cuantos, con limitaciones adicionales como la existencia de terceros en

su ejecución e, incluso, en su administración; lo que no es el objetivo de este proyecto que lo que busca es que todo ciudadano lo pueda utilizar.

Otro punto a tratar es cómo buscan utilizar lo más actualizado en los proyectos con miras a obtener resultados que sean confiables, pues la identidad digital en este proyecto busca ser administrada por ellos mismos y desarrollada allí mismo, y porque se dió énfasis en ello ya que los proyectos que se mencionaron como publicos y privados siempre tienen algo externo que complementa la funcionalidad, la ventaja de haberlo desarrrollado en casa es que indudablemente se sabe en qué se puede mejorar o localizar el error con mayor certeza si algo llega a fallar, cosa que con un tercero implica esperar a que se busque y focalice el lugar que está ocasionando el error; el riesgo de lo anterior es que ese tercero se convierte en juez y parte, por lo que debería agregarse a este proyecto un equipo de control de calidad ajeno que dedicara su esfuerzo a buscar esos puntos débiles de la herramienta y proponer nuevas mejoras.

Conclusiones

La Unión Europea ha mostrado interés en un tema tan importante como lo es la Identidad Digital, poniendo en marcha varias iniciativas públicas y privadas que han permitido dar un panomara de lo que podría llegar a alcanzarse en el ámbito de seguridad y administración de datos. Existen limitaciones que compartimos, ya que homogeneizar y tener algo centralizado no es algo que hayan considerado en seguridad como una realidad en estos países. Por otro lado, en America también existen iniciativas que contemplan la Identidad Digital, si bien estas están más enfocadas a temas de gobierno, junto con distintas tecnologías, apoyan el mismo principio de la UE buscando tener sistemas mayormente robustos en el tema de Identidad Digital, brindando un mejor servicio y transparencia a quien se ocupe de los sistemas.

Los esfuerzos en la Unión Europea que hemos mencionado a lo largo de este escrito, muestran que nacionalmente cada país está ocupando sus esfuerzos para tener en cuenta la Identidad Digital única para cada individuo, muchos de ellos han

sido pilotos o se han implantado en secretarías de gobierno o entidades donde su funcionamiento indica, no solo un rápido acceso, sino la oportunidad de contener en un solo lugar la información relevante del individuo que se identifica, por supuesto, la base jurídica en cada sistema que se implantó es parte de su realización y la oportunidad de tener la protección de datos con la seguridad de que estos solo aportan una mejora en cada ocupación del método.

El proyecto enfocado a la referencia por tener una plataforma que contenga tanto arquitectura como medios tecnológicos a la mano y con costos bajos, convirtió esta iniciativa en algo que apoya la idea de que bajo el contenido de elementos adecuado puede desarrollarse de manera transparente y con buenos resultados un proyecto en base a la Identidad Digital, pues todo ello, bajo un análisis adecuado y estableciendo objetivos, logran obtener un lenguaje común para todos; ejemplo de ello es la implantación en otro país.

De igual manera, el proyecto tuvo un alcance enfocado con un planteamento específico, por lo que el objetivo se logró; la meta era tener una administración en cuestiones de instituciones gubernamentales en materia de documentación digital para el gobierno español en interacción con los usuarios.

A continuación, en el siguiente capítulo se abordarán las buenas prácticas obtenidas en éste; aquellos elementos que podrán ayudar en la metodología para utilizar una Identidad Digital en las empresas.

Capítulo 3

Propuesta de elementos para generar una metodología en Identidad Digital

Capítulo 3: Propuesta de elementos para generar una metodología en Identidad Digital

En el capítulo anterior se revisaron las iniciativas de identidad tanto nacionales como internacionales, las cuales permiten accesos a servicios de banca en línea como comercio eléctrico, entrada a la bancanet de un banco, o una llave para la entrada al trabajo, esta posibilidad de un único acceso nos permite ser libres dentro del ámbito en el que nos desenvolvemos; de igual manera, tiene su historia en el ámbito de gobierno donde también somos identificados en pagos y procesos que nos permiten, de manera digital, ser identificados como individuos.

La problemática radica en que a nivel empresarial no se cuenta con una metodología que se emplee de manera multidisciplinaria, siendo cada una de las utilizadas y mencionadas en el capítulo anterior acotadas a lo que se requería *in situ,* sin tomar en cuenta la usabilidad y buscando que fuese multiplataforma, por lo que con este planteamiento buscamos que se ocupen los recursos en donde se instalarán y que los procesos en los que se introduzca esta gestión puedan incluir el ámbito normativo adecuado, así como la oportunidad de crecimiento en los estatutos.

Encontramos también que las metodologías no se adaptan a diferentes entornos, por lo que las empresas coartarían su instalación, lo cual dificultaría su correcta operación, pues la operabilidad seria única –exclusiva– cuando esto se convierte en especifico, solo está pensado para ambientes particulares, como vimos en capítulos anteriores, en el caso de metodologías instaladas en entidades de gobierno. Otro tema es el tiempo que les lleva su desarrollo, por lo que tienen pocas posibilidades de crecer o tener una mejor administración, perdiendo la oportunidad de obtener información importante para su utilización.

Por ejemplo, los esfuerzos que se han dado en eventos europeos, se muestran en la conferencia europea E-Identity Management en Londres, que se llevó a cabo del 9 al 10 de junio 2010. Alexander Hanff, jefe de redes éticas de privacidad internacional, tomó nota de los cambios significativos que han ocurrido

en Reino Unido derivado de la abolición de la tarjeta de identificación, resaltando que había sido algo positivo y esperaba que llegaran nuevos usos, resaltando la transparencia como elemento clave en el nuevo paisaje de identidad y confianza. De igual manera, apuntó que la mayoría de las empresas están preparadas para un impacto de regulación de las telecomunicaciones europeas.

En este mismo ejercicio, en la identidad hacia el interior de las empresas, podemos ver que la transparencia permitiría que siendo esto parte de la aplicación de la privacidad en datos y en encomienda de identificación, es ya una opción clave. En el mismo foro intervino Kevin Fraser, jefe de protección de datos del Ministerio de Justicia. El describió los ocho principios fundamentales de la protección de datos. En el punto de vista técnico, Kim Cameron, arquitecto principal en temas de identidad y acceso en Microsoft, estableció algunos de los controladores de *cloud computing* y algunos de los desafíos que enfrentaba. Mencionó algunos problemas de sincronización, como ejemplo de ello tenemos Microsoft Exchange y Outlook, abogó por un modelo de notificaciones en la nube enfocado a Identidad Digital, lo cual es una idea de notificación continua y en tiempo real.

El fundador y CEO de Facebook Mark Zuckerberg, comentó en esta reunión "*los días de tener una imagen diferente para su compañeros de trabajo y para otras personas, probablemente están llegando a su fin. Tener dos identidades por sí mismo es un ejemplo de la falta de integridad*". Las identidades en las redes sociales no pierden valor y en cada red social el comportamiento de cada individuo se encamina hacia algún rumbo, por ejemplo, mientras en Linkedln puedes tener interacciones relacionadas con el trabajo, en Facebook son meramente de amistad. Una misma persona presenta diferentes facetas y diferentes identidades que anclan diferentes relaciones.

La base de datos de un individuo representa la colección de información definida para cada lugar donde se habrá de implementar y refleja los datos de una narrativa continua sobre un individuo para los fines que se requieran. La identidad en la base de datos determina la reputación de un individuo, pues registra cómo está considerado por las autoridades, así como las alertas y notas incluidas en el sistema.

Cuando se trata de entornos “cerrados”, es posible aprovechar nuevas tecnologías de gestión de conexión, desconexión e identidad más rápidamente porque se puede experimentar previamente con un pequeño grupo de prueba. Un artículo sobre “*The Laws of Identity*” menciona que las empresas, por ejemplo, ven a sus relaciones con los clientes y empleados como un activo clave y son muy celosos de ellos. No es razonable esperar que restrinjan sus propias decisiones o cedan el control sobre cómo crear y representar sus relaciones digitalmente. Tampoco ningún enfoque único surgido que podría servir como una motivación evidente para hacerlo. Los diferentes contextos de empresas discretas conducen a un requisito de que sean libres de adoptar diferentes tipos de soluciones. Incluso identidades *ad hoc* singulares son mejores que un marco de identidad que estaría fuera de su control.

3.1 Nueva metodología de Identidad Digital

En los capítulos anteriores hemos visto que los aspectos legales son una parte esencial en cuestión de identidad pues abarcan derechos de los que el personal que labora goza y es algo que siempre se pide para entrar a un lugar o establecimiento, pues se manejan tarjetas electrónicas de acceso. Esta metodología contempla esto, pues hemos visto que una de las debilidades es la falta de marco institucional y político para la aplicación de la Identidad Digital donde, dentro del marco institucional, tenemos las disposiciones o procedimientos para facilitar el uso compartido de datos para las diferentes áreas dentro de la empresa que las ocupen, lo que permitirá que la coordinación de los datos sea la manera de unión y distribución correcta de los mismos, lo que se traduce en la unicidad institucional. Aquí entra en juego la parte política, donde influyen en la empresa aquellas normas que permiten la armonía entre las áreas, manteniendo un ambiente adecuado a lo que necesitan.

En cuestiones técnicas, se ha observado que se pierde entre lo nuevo o lo más barato; la propuesta es que sea escalable, así como adaptable para la empresa en las que se desarrolle, con miras a un mantenimiento continuo y usable que mantenga las cuestiones de seguridad apropiadas, algo que ya hemos visto en los otros capítulos, los cuales se aplicarían, pues cada uno de los ejemplos lo contemplaron de igual forma, fue algo en lo que todos tuvieron punto de encuentro, por lo que la gestión de identidades existentes podrán ser coherentes con las condiciones políticas y reglamentarias de la empresa.

Del mismo modo, en temas de conexión, proponemos que las soluciones en cuestiones de usabilidad y aplicación, faciliten un mejor marco de trabajo que esté apegado a lo más práctico con calidad para un mejor resultado del manejo de la información; uno de los huecos que se localizan en las metodologías mencionadas en el capítulo anterior fue, por ejemplo, que no hay autenticación centralizada, lo cual no permite que la aplicación de la solución sea apegada a un mejor resultado de calidad con el usuario, sino que interpone información que puede corromperse en el trayecto, debido al mal uso de datos, por ello la administración tendría que ser centralizada.

3.1.1 Elementos de una nueva metodología de Identidad Digital

Un elemento fundamental de la metodología, es que debe servir en diferentes plataformas. Es importante ocuparse en el tema de la falta de multiplataforma pues, al cerrar sus proyectos a circunstancias de moda o de costos, cohartan la posibilidad de ser escalable y actualizable, lo que hace que cualquier aplicación llegue a un punto en donde será reemplazada, lo cual no es adecuado, se busca que la continuidad de los datos sea una constante en cada resultado.

Los elementos importantes para la ejecución en una empresa deben ser los siguientes:

- **Legal**, el cual llevará los principios que la compañía considere en sus prácticas para protección de datos, para la identificación de todo el personal que se encuentra registrado en la empresa.
- **Técnico,** donde los elementos serán escalables y utilizarán estándares para su ejecución, la tecnología a ocupar estará dada por la que mejores resultados le lleve en el desarrollo y mantenimiento de la gestión de datos en la Identidad Digital.
- **Seguridad,** refiere a todo aquello que cumplirá con los requisitos que la empresa esta conformando en materia de protección de información, lo cual se traduce en que los estatutos que tiene la empresa son los que se ocuparán.
- **Usabilidad,** se busca sea amigable para el usuario y el administrador de la información que se genera en la Identidad Digital.

En este sentido, en el presente trabajo solo la propuesta de identidad digital para las empresas se basará en los elementos técnicos, lo cual se ha identificado como un hueco que se requiere y necesita en el proceso de Identidad Digital.

Es importante considerar que hablar de Identidad Digital tiene ciertas limitaciones como lo muestra la literatura recabada en esta investigación, tomando en consideración la aplicación en el ámbito del gobierno, se cierra a circunstancias de cada estado en el que se esté proponiendo dicha aplicación, esto encierra en un solo plano los servicios de gestión de identidad. Los estados forman parte de países que llevan una estructura de gobierno bien sustentada en transacciones comerciales entre los integrantes de la propuesta, la mayoría de ellos son del primer mundo y muchos de ellos cuentan con un número de población pequeño, lo cual permite una instalación de la infraestructura tecnológica adecuada para la implantación. Esto también deja claro que entre más ordenada y administrada esté una empresa, esto hará que los objetivos digitales se lleven a cabo.

La resistencia al cambio genera limitantes que en la forma tradicional de muchas empresas envuelve criterios que requieren modificarse, ejemplo de ello es la forma de acceder en el horario laboral desde una tarjeta electrónica hasta dispositivos de retina o dactilar.

A partir de la revisión que se realizó en el primer capítulo, donde se revisan los elementos básicos de la Identidad Digital, los cuales son el usuario, un navegador u otra aplicación de software que se ejecuta en una PC o teléfono móvil, una computadora (el agente del usuario), el sitio del proveedor de servicio (SP) y el proveedor de identidad (IdP) es un sitio Web.

Para hablar de lo que conlleva la metodología, veremos en el siguiente cuadro los elementos que podemos abordar y aclararemos su relación, así como su contribución a la propuesta que considera lo siguiente:

Metodología		
Propuesta – Características		
Empresas - Usuarios	Usos tecnológicos	Nuevas características

Todo es un ecosistema con información que sirve para tomar decisiones, los usuarios son parte de la empresa y su opinión se ocupa mediante encuestas del servicio en tecnologías de información al proporcionar los datos en las empresas que laboran, como se basa en un ambiente	- Técnicos
	  - Interoperabilidad
	  - SAML como protocolo de comunicación y utilización de certificados X.509,
	  - SOA
	  - Multiplataformas
	  - Utiliza XML para mensajes y metadatos
	  - Administración centralizada
	- Usabilidad
	  - Buenas prácticas
	  - Análisis de procesos actuales
	- Seguridad
	  - Autenticación centralizada
		- Existe un marco lógico, técnico e institucional que tendrá el desarrollo de los servicios de gestión de identidad y considerará los reglamentos
		- El uso de información que ofrece su estadía en la empresa, permitirá abrir mayor empatía en los sistemas de identidad ocupados, así como de la información que servirá a una área de Talento y Cultura en la empresa.
		- La tecnología que se ocupará, será escalable por lo que podrá evolucionar con las necesidades que se arrojen de los datos

controlado por cada empresa	- Legal - Cumplimiento de los reglamentos que la empresa tiene como parte de los estatutos que la originan	obtenidos en los procesos de identidad. - Existira una BD la cual contendrá información que recorra las áreas por las que el usuario transcurre en sus labores.

Cuadro 5. ***Elementos y usos tecnológicos principales.***

Fuente: Elaboración propia de acuerdo a características tecnológicas de la metodología

Los elementos que podemos enlistar se ejemplifican en la siguiente figura, la cual muestra que las relaciones entre los usos tecnológicos, lo cuales son multidisciplinarios, pues uno se complementa del otro, todos suman y apoyan a los resultados que se requieren para completar su labor; en el área de la tecnología siempre existen relaciones cruzadas, así como lo ejemplificamos a continuación:

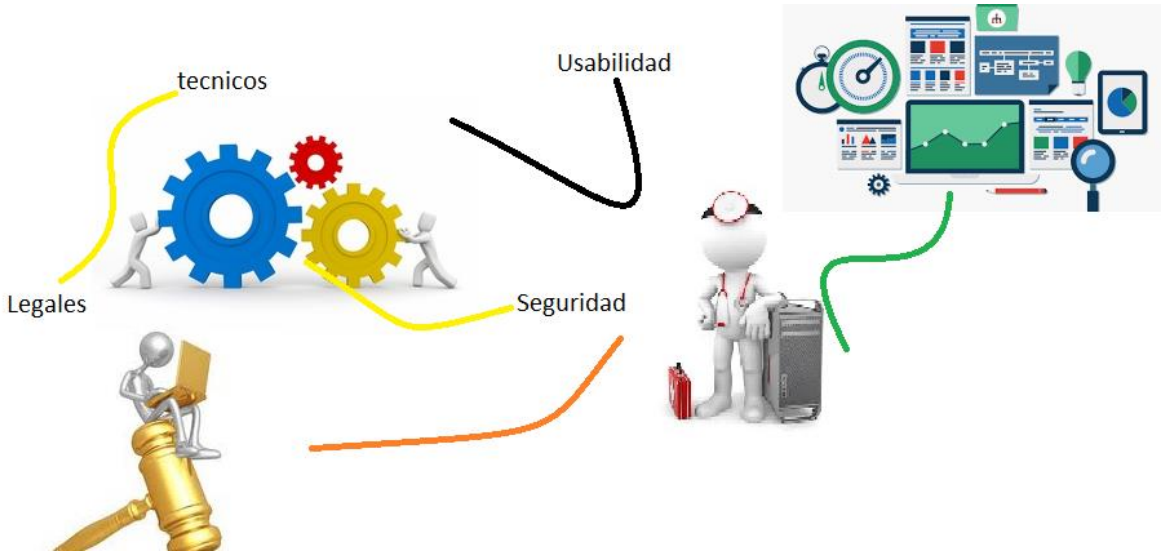

Figura 3. ***La relación entre los elementos en la Identidad Digital.***

Fuente: Elaboración propia de acuerdo a los elementos que se han tocado en el documento

3.1.2 Técnicos, seguridad, legales y usabilidad

En el marco técnico, las operaciones de interoperabilidad se van a basar en el desarrollo de software libre, ya que este permite reducir costos y tener mejor

interoperabilidad en el manejo de datos con la libertad de estudiar la manera de evolucionarlo y seguir en cualquier adaptación para las futuras necesidades, pues ha demostrado ser una de las mejores maneras para tener actualizadas las versiones. Como protocolo de comunicación tenemos SAML, el cual ha sido utilizado tanto nacional como internacionalmente, lo cual permite que los miembros se conecten a través del proveedor de identidad que se elija en la empresa; con la utilización del certificado X.509 se colabora en una autenticación básica para los clientes que entren. Un cliente que tenga este certificado podrá acceder de manera segura, la cual se habrá de habilitar para la autenticación de certificados de cliente. La modalidad de autenticación X.509, además de su valor predeterminado en una autenticación básica, la cual consiste en la autenticación de inicio de sesión con un ID de conexión, una contraseña y después pedirá que se den los certificados X.509.

Utilizando certificados X.509, el administrador de gestión digital debe asegurarse de que existe un certificado de cliente, lo que lleva al proceso de reconocimiento del certificado de servidor e instalarlo en el navegador correspondiente que será determinado por la empresa en la que se encuentra. De esta manera, el administrador se puede conectar. Esto necesariamente aborda el tema de seguridad pues se buscará de manera eficaz la autenticación que asegure, tanto la identidad de los usuarios, como de las aplicaciones para que su acceso a la aplicación e instalaciones sea la más placentera y segura. Con lo que se podrá proteger la información sensible a lo largo de los procesos que pase o las áreas que abarcará. Entonces después de esta conexión, el administrador accede por primera vez a la ventana de conexión de la consola de administración, se crea un registro de cliente certificado y se emite una cookie de cliente, de forma similar a cuando un cliente normal accede a un URL seguro.

Con respecto al tema de seguridad, la protección de datos en la Identidad Digital adaptará soluciones de autenticación multifactorial, pues hemos indicado que el sistema será heterogéneo, ya que la estrategia se conforma de capas que integren una seguridad completa y que se refieren a el cifrado que tendrá mediante el certificado de autenticación, de igual manera usuario y contraseña, seguridad de

la red de la empresa, y un entorno que mediante huella digital sea una autenticación fuerte.

En el tema legal, al cumplir con los requerimientos de la Ley del Registro Civil es cuando obtenemos el registro único e irrepetible para identificar a los usuarios en cada organización, y mediante una credencial de elector, la cual los identifica como ciudadanos, esta credencial de elector también genera información de la ubicación del usuario, junto con su domicilio. De igual forma, utilizaremos los reglamentos que la empresa tiene como parte de los estatutos que la originan. Para ello también usaremos en la parte técnica los lectores de huella que se ocuparán para leer los datos de cada identificación de identidad y concretará esa fiabilidad como firma electrónica única, la cual validará cada acceso y dará información del evento en el proceso que se encuentre. Al combinar la seguridad de la firma con autenticación y claves de un solo uso, así como el certificado que se ocupa, eliminará el riesgo de manipulación de datos o de pérdida, robo o pirateo de contraseñas con lo que se reduce el riesgo de robo de identidad, pues los perfiles que tenemos por usuarios son únicos e irrepetibles.

Se propone un área responsable en tecnología para establecer una gestión y supervisión, así como buscar buenas prácticas para evitar los riesgos de seguridad. De igual manera, servirá para encontrar mejoras en los flujos de datos en el crecimiento de la misma para cubrir las presentes y futuras condiciones en la gestión de la Identidad Digital. La metodología toma en consideración los reglamentos que rigen a la empresa a la que se establezca la metodología de Identidad Digital, pues de ello deriva el principio de entrada a las instalaciones que gestionaremos bajo estos principios la Identidad Digital en el sistema.

Para la cuestión de usabilidad, y buscando que la herramienta tenga facilidad de uso y ya que se accede a partir de diferentes multiplataformas, se propone un diseño más intuitivo, FAQs que se utilicen y permitan ser más amigable a lo largo de la administración y utilización de la herramienta por parte del usuario. Se propone a nivel técnico, que bajo esta gestión de autenticación de Identidad Digital, se centralice para múltiples puntos de acceso, donde tendremos diferentes tipos de usuarios que tendrán una autenticación personalizada para todos los casos; existen

empresas que no solo de manera interna entran a diferentes lugares, sino que tienen diferentes sedes, los cuales tienen diferentes puntos para usar en el sistema.

En cuestión de gestión de información, utilizaremos un enfoque de Arquitectura Orientada para los Servicios (Service Oriented Architecture o SOA en inglés), el cual es un marco de trabajo conceptual que establece una estructura de diseño para crear y usar procesos de negocio que se ocuparán para la gestión en cuanto a flexibilidad de integración con sistemas ligados y alineación directa a los procesos de negocio, con la infraestructura de TI con la que cuente la empresa, por ello utilizarla permite la reducción de costos en implementación y adaptación ágil ante cambios, ya que combinan fácilmente las nuevas tecnologías con aplicaciones independientes, permitiendo que los componentes del proceso se integren y coordinen de manera efectiva, pues ocupan para los servicios Web un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones.

Permitirá también la intercomunicación entre sistemas de cualquier plataforma, lo cual está enfocado a servicios de mayor utilización de la empresa a la que sea instalada, por ello la multiplataforma es muy importante para llevar acabo la instalación pues las circunstancias de software para cada sitio serán adecuadas, por ello es que se propone la utilización de herramientas de software libre. El énfasis en la usabilidad de la aplicación siempre nos ayudará a que sea rápido su acceso, sencillo para desarrollar las tareas que deriven, tanto para el administrador, como para el usuario final que lo ocupará.

Se utilizarán formatos XML (lenguaje Extensible Markup Language) para mensajes y metadatos, lo cual denota un lenguaje de fácil acceso y que la gestión de información logre una mejor traducción así como una utilización oportuna, siendo ello la consecuencia de una administración centralizada donde los reportes se ocuparán de darnos visibilidad de lo que necesitamos entender para llevar una mejor gestión y apoyo, tanto al equipo de trabajo de Identidad Digital, como a los usuarios de ella, pues utiliza formatos de mensaje para comunicación entre aplicaciones, ayudará a publicar e intercambiar contenidos de bases de datos y la descripción para los metadatos que tengamos e introduzcamos para asegurar obtener información valiosa para otros procesos de la empresa, fomentando así

también la autodocumentación. Los metadatos siempre nos apoyarán en un mejor reporting de a la información.

La seguridad que nos proporciona la utilización del software libre nos ayudará a reducir costos, como ya se indicó. Mediante la organización de datos con gestión centralizada, junto con los controles de perfiles y autenticación a través de contraseñas y lector de huella, se mejorará la visión de datos a utilizar.

El usuario podrá contar con un tiempo perfecto de uno a dos días para aprender a usar bien la herramienta facilitando las operaciones que necesite realizar, pues es diariamente que se está utilizando; por lo que la interfaz será sencilla y práctica. La información que presenta solo es de identificación, pues todo se carga en Base de Datos, lo cual solo será vista táctil en el dispositivo que se requiera para la identificación del usuario.

Sera fácil de recordar el funcionamiento de la herramienta, con lo que se pondrá la utilización completa en el desarrollo del trabajo. La frecuencia de uso, como ya se mencionó es cotidiana pues es nuestra entrada y salida como identidad digital a lo largo de procesos dentro de la empresa. Existirá un apoyo para cualquier error que enfrente el usuario, el sistema siempre buscara el envió de apoyo físico y tecnológico mediante un correo o con una llamada a tu celular.

De acuerdo a la simplicidad de uso que tendrá en el usuario y administración del sistema, podremos obtener también satisfacción subjetiva que nos será brindada por el uso de la herramienta a lo largo de los primeros meses de vida y esto será una suma de las buenas prácticas aplicadas al sistema.

A continuación mostramos los esquemas de la metodología compuestos por tres etapas, comenzando por un esquema general que muestra los elementos que estarán presentes en las siguientes tres etapas, los usuarios, el ingreso al sistema, las validaciones de seguridad, la gestión y administración de los datos, así como el resultado de la explotación de la información.

3.1.3 Esquema general

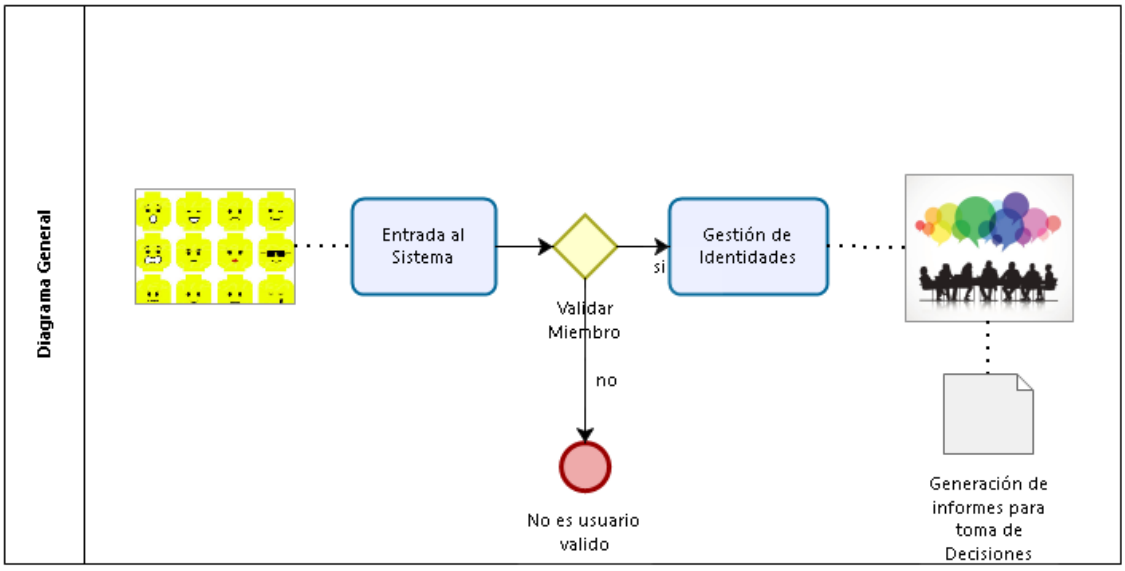

Figura 4. ***Diagrama general de gestión de identidades digitales*****.**
Fuente: Elaboración propia de acuerdo al esquema general que a manejado la propuesta de desarrollo.

En esta figura se muestra el flujo general, en el cual el ingreso de los usuarios posibilita el ingreso de la información y validación para darles entrada, desde el ingreso a las instalaciones hasta la utilización de herramientas propias de la empresa tales como correo, programas y sistemas que sean utilizados, todo esto mediante una sola validación inicial donde ya tienen contenida la información validada mediante los protocolos de seguridad que ya se han mencionado.

De igual manera, se muestra el área de gestión de información, donde se podrá apoyar para generar información relevante que permita tomar acción en las diferentes áreas, todo en apoyo de la empresa y del empleado, la gestión de Identidad Digital no solo se manifiesta como un acceso a un sistema, sino como la posibilidad de ocupar los datos y manejar un conocimiento que dé valor a los

siguientes pasos para cambios que vayan presentándose a lo largo de la administración. A continuación, se presentan los siguientes pasos para las etapas que constituyen la metodología:

Etapa 0

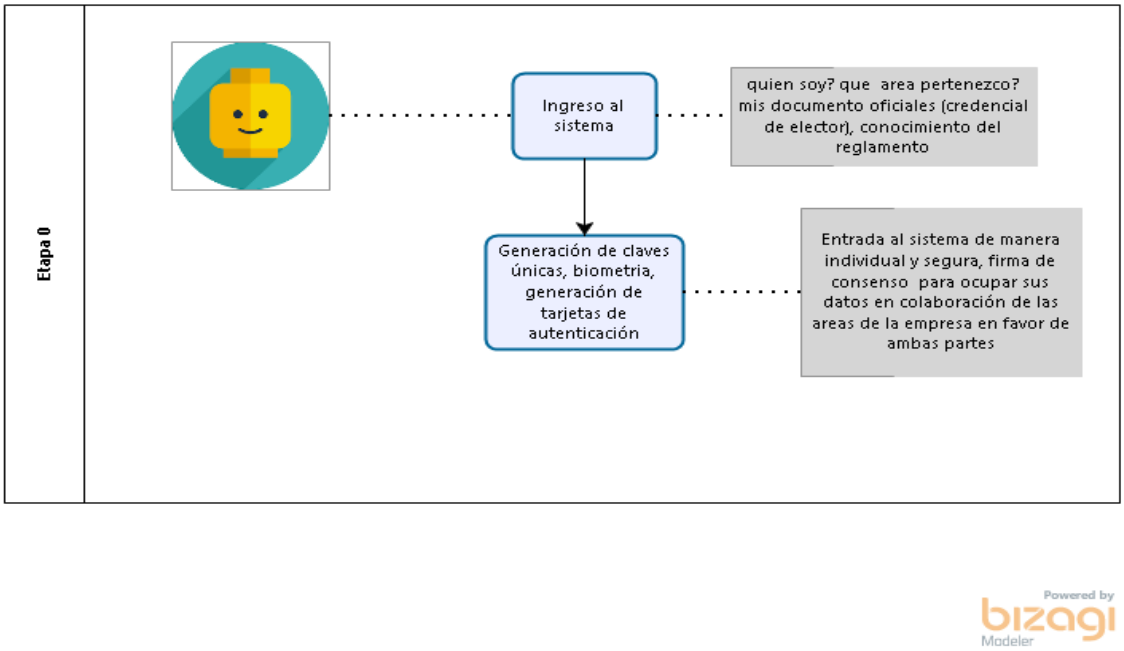

Figura 5. ***Ingreso al sistema, identificación inicial.***

Fuente: Elaboración propia de acuerdo a la etapa cero que esta considerado para los elementos a utilizar en el modelo de elaboración.

Se considera a esta como Etapa 0, pues debe de desarrollarse antes de iniciar el proyecto. De ella depende el inicio de los datos que componen la generación de claves de autenticación y equivale al inicio de las actividades dentro de la empresa, pues identifica al usuario como un colaborador dentro de los sistemas en las cuales estará involucrado.

Se muestra en el esquema general como una entrada al sistema pues es el proceso inicial para identificar de manera segura al usuario el cual es identificado

mediante huella o credencial desde la entrada a las instituciones y su ingreso a los sistemas en los que tendrá participación.

El ingreso al sistema se hace a partir de la administración de la información que entrega el usuario y que se integra a la empresa, pues el medio de obtenerla es bajo la información que se entregará bajo los documentos oficiales y firmas de contrato y procedimientos legales que tengan a bien establecerse en el convenio trabajador–empleado.

A partir de los documentos oficiales y de su ingreso, se realiza la gestión de datos al sistema así como su Identidad Digital, la cual le permitirá ingresar a las instalaciones y también ocupar los programas e información que se le comparta a lo largo de su trayecto en la empresa, esto conlleva la implementación de candados de identidad individual, la generación de certificados y la seguridad de que los datos proporcionados serán solo de índole laboral de acuerdo al acuerdo que celebren ambas partes.

Los elementos que lo constituyen son:

- Usuario
- Proceso de ingreso al sistema
- Seguridad que conlleva la creación de sus claves únicas

El usuario contará con las credenciales de identificación para entrar al sistema, ocupando el lugar de acuerdo a los privilegios que le fueron otorgados y parte inicial en el sistema, la cual nos otorgará datos a partir de su comportamiento para planear mejoras en las áreas donde se encuentra.

Etapa 1

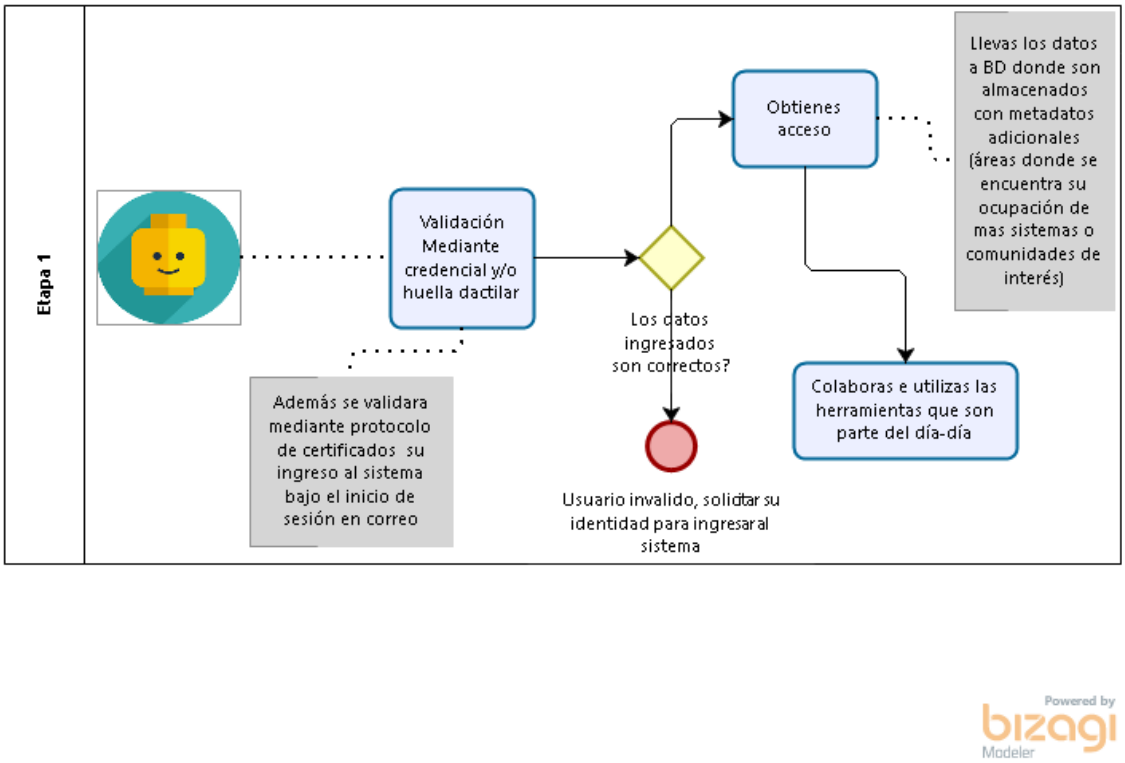

Figura 6. ***Validación del usuario y entrada al sistema.***
Fuente: Elaboración propia de acuerdo a la validación que se realiza en la primer etapa.

En el esquema general ubicamos esta etapa en la validación de datos, aquí entra seguridad en el acceso utilizando la gestión de datos iniciales que tiene el sistema para la Identidad Digital de los usuarios que ya han entrado al sistema, donde busca su propia historia a lo largo de su estancia en los sistemas a los que puede tener acceso.

Esta etapa genera la experiencia del usuario desde su entrada a las instalaciones, así como su acceso a su correo y a los diferentes sistemas que ocupa para la colaboración que realiza día a día en sus labores; los datos son tratados e identificados como válidos, lo cual permite validar o invalidar la solicitud de acceso

al momento de ingresar al sistema, ocupándose de ello el sistema de gestión de Identidad Digital.

Al colaborar con la información, el usuario acepta que ésta sea utilizada en apoyar a las áreas en que labora así como en soporte a sus operaciones, pues la identidad contribuye a contar con un mejor lugar de trabajo, mejores condiciones para los sistemas, así como la seguridad de que no se viola ninguna directriz en el sistema y se maneja la seguridad de que los datos del usuario–sistema se respetan.

Los elementos que lo constituyen son:

- Usuario
- Validación
- Accesos
- Colaboración

De manera individual, este proceso habla de la Identidad Digital del **usuario** como primera instancia apoyada en la base de la información que ya fue recabada para su identificación dentro de los sistemas de la empresa, con miras de contribuir a que sea simple su acceso y conlleve las reglas de seguridad necesarias para un correcto flujo de datos.

Validación recapitula las reglas de seguridad que ya hemos mencionado en este capítulo y muestra las reglas y parámetros que se necesitarán como filtro de inicio en la validación, se ocupará de que a nivel usuario no presente detalles inesperados, sino un correcto uso de la información.

Acceso es el alcance que puede darse dados los permisos de seguridad asignado para ese usuario en particular y mostrara el acceso correcto así como

identificación con nombre y avatar si es que se proporcionó, dado que el sistema también se alimenta de lo que cada usuario en particular realice en su día a día con ello la consulta de los diferentes datos si es que entra a comunidades.

Colaboración representa el set de herramientas, portales, comunidades del grupo al que pertenezcan, los cuales son parte de los permisos que el usuario ha convenido por contrato en el trabajo, lo que conviene para fines de información adicional, son los metadatos, los cuales darán oportunidad de generar información de valor.

Etapa 2

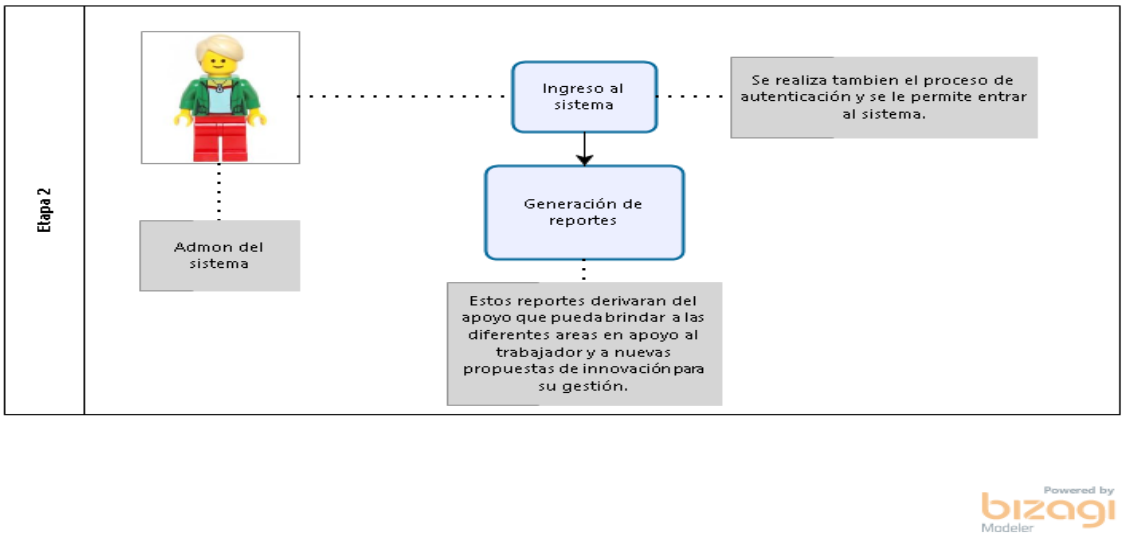

Figura 7. ***Administración y generación de reportes de la Identidad Digital.***

Fuente: Elaboración propia de acuerdo a la administración que se esta apreciando para el proyecto.

El esquema general ubica esto en la parte de administrar el sistema como tal para generar los informes a través del mecanismo de metadatos que se obtendrá de los accesos de cada uno de los usuarios. La finalidad de la Identidad Digital también es que vaya más allá de un usuario y contraseña, más bien ese es el inicio de una

gestión que brindará mejores servicios, mejor tiempo de respuesta a cuestiones que de otro modo tardarían más tiempo, el aporte de valor en cada una de las etapas.

Como segunda etapa está la generación de reportes, dado lo que se ha ingresado al sistema y la vida que ha llevado a lo largo de su realización al compartir datos; ocupar sistemas le da la oportunidad de generar metadatos que serán compartidos y utilizados bajo el administrador del sistema de gestión de Identidades Digitales. Utilizar esa información generará valor a las actividades del usuario pues no solo forma parte de un lugar, sino de toda la organización.

Elementos que lo constituyen:

- Administrador de la herramienta
- Ingreso al sistema
- Generación de reportes

El **administrador** de los datos debe ser alguien que colabore con sus conocimientos para una correcta y sencilla administración de la información arrojada en las diferentes etapas de la herramienta, todo ello deriva en valor. Corresponde al administrador dar seguimiento a las quejas y sugerencias que se presenten a lo largo de la vida de la herramienta.

El **ingreso al sistema** se realizará como un usuario individual, lo cual identitifica al usuario mediante su Identidad Digital, el progreso continuo puede ser de entrada y salida, pues podrá monitoriar aquellas herramientas cuyo propósito sea informativo, se pedirá de su cooperación y la información formará parte de la confidencialidad de la empresa–trabajador.

Conclusiones

Conclusiones

La relevancia que ha tomado la Identidad Digital dentro del ámbito tecnológico es un tema recursivo lleno de alternativas que no se reduce solo a obtener una contraseña y un nombre de usuario; ya no solo forma parte del apoyo de información o de la ejecución de operaciones digitales en los diferentes sistemas a los que pertenecen, donde se genera una historia de las entradas y salidas, esto es rastreable lo cual muestra que podemos hacer uso de los datos y convertirlos en conocimiento, explotando la información que está siendo generada.

Los aspectos de seguridad y legales, por un lado, técnicos y de usabilidad por el otro, constituyen los dos ejes decisivos sobre los que se consolida la Identidad Digital, pues apoyan en todo el desarrollo de la sinergia de la información, esta serie de elementos nos ayudan a generar un enfoque holístico y multidimensional de lo que representa la Identidad Digital.

En la Identidad Digital hay una dimensión inmediata que se da a través de un acceso a un servicio, y otra mediata en la que, de acuerdo a las necesidades que se tengan o de las tecnologías que se puedan ocupar, será la manera de actuar a lo largo de la utilización del sistema, cosa que pudimos constatar con los esfuerzos de la Unión Europea y lo que se ha alcanzado también en América.

Se han realizado, a distintos niveles, esfuerzos para llevar a cabo un tratamiento integral buscando que la tecnología empatice, pero estos no se ocupan de lo que el objetivo de todo grupo hoy en día busca, que es la empatía multidisciplinaria. Las bases de este trabajo se vertebra en torno a los aciertos y errores que surgen en el desarrollo de las nuevas tecnologías en cuanto a Identidad Digital se refiere. Es por ello que buscamos que estos elementos sumen y completen los alcances enfocados de cada organización.

En el presente trabajo hay una propuesta de los elementos para utilizar en una metodología para el desarrollo de la Identidad Digital que pueda ser usada en diferentes ámbitos dado que cada empresa encuentra su propia identidad, la cual se refleja en cómo administra sus datos y a los integrantes de las mismas. Se

presenta una propuesta capaz de integrar en el concepto de Identidad Digital a la esfera de multidisciplinariedad, por lo que el futuro del sistema se plantea como algo que continuará y conducirá a una mejor administración.

Los alcances que se proponen abarcan la interoperabilidad, colocando los elementos Técnicos, Seguridad, Usabilidad y Legal, donde busca abarcar lo que institucionalmente ocupan las empresas, respetando sus lineamientos y las necesidades que requiera cada una de ellas; la empatía entre los sistemas es clave en esta propuesta, pues de ello depende la usabilidad y derivará en la escabilidad que puedan llevar a cabo los diferentes procesos en la empresa y se reflejen en la administración del sistema. La oportunidad de llevar estos elementos a una empresa con la tecnología que se adapte a las necesidades, no limita a un desarrollo de software cerrado, pues la apertura en el desarrollo de software libre es cada ves mejor, la constante en el mercado es el cambio y la identidad digital pronto será mucha más ágil, practica y permitirá obtener información real, oportuna y segura. El nivel de adaptación de los elementos propuestos procura el sentido humano y el tecnológico para que, de la mano, lleven este propósito de integración en Identidad Digital.

Las limitaciones dependerán de la implementación y de las tecnologías que decidan ocupar, pues esta propuesta busca brindar las bases a través de los elementos listados, y la forma en que las etapas pueden plantearse a lo largo de su implementación, lo que dará sentido al trato electrónico y se vuelve un valor viviente para ayudar e identificar nuevas oportunidades de cambio y de gestión de información y talento.

La participación de los integrantes de una organización puede generar, además de su ingreso a las instalaciones, información que está contemplando los elementos que justificamos en el documento presente formando parte del valor que muestra las actividades a lo largo de sus funciones dentro de las áreas que se tocan en la organización, la Identidad Digital forma parte del día a día pues brinda la oportunidad de llevar una gestión ágil con miras a brindar una administración basada en la cultura y enfoque de valor para la empresa, buscando la seguridad de

los datos que son tratados a lo largo de los procesos que pueden llegar a ser utilizados.

A lo largo de las etapas expuestas como propuesta de elementos para generar una metodología propia de cada cultura organizacional a la que se desee implementar, están dados los pasos que serán un inicio para su adecuación, pues reflejan un *pipeline* que se puede ocupar en cualquier organización, teniendo como consecuencia que sea un enfoque sencillo y práctico que satisface el objetivo de mantener una identidad digital de valor, lo que se dará en una adecuada gestión de identidades.

Siendo estos elementos la base para la columna vertebral de la metodología a ocuparse en cualquier organización, proponemos que se ocupe para aprovechar la mayor ventaja de acuerdo a lo que se desee, todo pensado con el fin último de que la organización obtenga información útil con la que se forme una sinergia ganar–ganar talento–organización, pues al no ser elementos que se destaquen de manera prioritaria –talento u organización–, podemos tener mejores resultados.

Bibliografía

Álvarez, J. (2003). Cómo hacer investigación cualitativa, fundamentos y metodología: Paidós Mexicana, S.A. de C.V. México.

Area Manuel, Tic, identidad digital y educación. Cuatro reflexiones Reencuentro, num. 62, diciembre, Universidad Autonoma Metropolitana Unidad Xochimilco, 2011, pp. 97-99.

Birch, D., Doyle A. (2011). Digital Identity Reader 2011. (Digital Identity Readers): United Kingdom, England.

Bruegger, B., Hühnlein, D., Schwenk, J. (2012). TLS-Federation – a Secure and Relying-Party-Friendly Approach for Federated Identity Management, Ruhr Universität Bochum, Germany.

Camenisch, J., y Pfitzmann, B. (2007). Federated Identity Management. IBM Zurich Research Laboratory, Switzerland.

Directiva Europea 95/46/CE url: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV%3Al14012

Diario Oficial de la Federación, http://www.dof.gob.mx/nota_detalle.php?codigo=4885577&fecha=30/06/199

Digital Identity 3.0. The Platform for People Working. Paper No. 2, Edit Chair in Digital Economy, 2015.http://europa.eu/pol/pdf/qc3209190esc_002.pdf

García Gil Ramón J., Mariscal Judith, Ramírez Fernando, Gobierno electrónico en México. Centro de Investigación y Docencia Económicas. num 214, noviembre 2008,

Gaytan Sánchez Patricia. Calle, Cuerpo y Género. La identidad como proceso en la ciudad de México, Acta Sociológica núm. 55, mayo-agosto de 2011, pp. 37-53.

Gestión de Identidad en las Administraciones Públicas: Interoperabilidad pan-Europea, Sergio Sánchez García, Ana Gómez Oliva, DIATEL – EUITT – Universidad Politécnica de Madrid, Ctra. Valencia Km.7, 28031, Madrid, Spain.

Goffman, E. (1961). Encounters: Two Studies in the Sociology of Interaction - Fun in Games & Role Distance. Indianapolis, Bobbs-Merrill.

Goffman, E. (1981). Forms of Talk. Philadelphia, University of Pennsylvania Press.

Google App Engine, Uso de autenticación federada mediante OpenID en App Engine. http://europa.eu/pol/pdf/qc3209190esc_002.pdf

Identity Cards Act, The Australian and the United Kingdom schemes.

InCFederation/X.509 Certificates in Metadata https://spaces.internet2.edu/display/InCFederation/X.509+Certificates+in+Metadata

Josep María Rosanas, En busca de la identidad empresarial perdida. Revista: Istmo Liderazgo con valores. Edición:331, Sección: Alta Dirección, Galería principal, Portada Web Articulo http://www.redalyc.org/articulo.oa?id=199520908018#

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Nueva Ley DOF 05-07-2010.

López Jimenez Ilia E. El impacto de la tecnología en la comunicación empresarial: reflexiones y análisis, Revista Electrónica en América Latina Especializada en Comunicación, número 79 mayo - julio 2012.

Maler, E. (2005). Federated Identity Management. An Overview of Concepts and Standards.

Maler, E., Reed D., (2006). Administración de identidades - El Diagrama de Venn de la Identidad, Opciones y Problemas en la Administración de la Identidad Digital.

MODINIS eIDM, 2011. Recuperado de: https://www.cosic.esat.kuleuven.be/modinis-idm/

Nuno Gomes de Andrade, N. Regulating electronic identity in the European Union: An analysis of the Lisbon Treaty's competences and legal basis for eID, Elsevier.

OECD (2011), "National Strategies and Policies for Digital Identity Management in OECD Countries", OECD Digital Economy Papers, No. 177, OECD Publishing, 2011.

Parlamento Europeo y Consejo de la Unión Europea: Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Diario Oficial de la Comunidad Europea, vol. L, 281, pp. 31-50. Luxemburgo: Unión Europea (23 de Noviembre de 1995).

Proyecto SECUREID Mexico-España, localizada en la liga: http://www.indracompany.com/sostenibilidad-e-innovacion/proyectos-innovacion/secureid-creacion-de-un-entorno-seguro-de-servicios

Sánchez García, S., Gómez Oliva, A. (2012). Gestión de Identidad en las Administraciones Públicas: Interoperabilidad pan-Europea DIATEL – EUITT. Universidad Politécnica de Madrid, Ctra. Valencia Madrid, Spain.

Secretaría de Gobernación. Ley Federal de Transparencia y Acceso a aa Información Pública. http://www.dof.gob.mx/avisos/2493/SG_090516/SG_090516.html

Stefanova, K., Kabakchieva, D., y Nikolov, R. (2011). Design Principles of Identity Management Architecture Development for Cross-Border eGovernment Services. University of National and World Economy, Sofia, Bulgaria.

Tratado de la Unión Europea. http://europa.eu/pol/pdf/qc3209190esc_002.pdf

https://www.oasis-open.org/standards#wssprofilesv1.0.

https://www.w3c.es/

http://bibing.us.es/proyectos/abreproy/11314/fichero/MEMORIA_FIRMA_DIGITAL_XML%252FCap%C3%ADtulo+7+Firma+digital+XML

http://portal.ine.mx/credencial/