ENTREGABLE PARA LA INTEGRACIÓN DE PRESTADORES PRIVADOS AL SERVICIO DE AUTENTICACIÓN DIGITAL

Ministerio de Tecnologías de la Información y las Comunicaciones
Dirección de Gobierno Digital
Subdirección de Gobierno en Línea

Contenido

1. Certificación Cumplimiento Requisitos Técnicos

[Ciudad y fecha]

Señores:

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MINTIC)

Dirección de Gobierno Digital

Bogotá D.C. – Colombia

REFERENCIA: Certificación de cumplimiento de requisitos técnicos para la integración como prestador privado del servicio de AUTENTICACIÓN DIGITAL

[Nombre del representante legal del Solicitante], identificado como aparece al pie de mi firma, en mi calidad de representante legal de [nombre de la entidad solicitante], certifico en mi nombre y en nombre de [nombre de la entidad solicitante] que tengo y cumplo con los siguientes requisitos técnicos para la integración con el servicio de Autenticación Digital:

1. Cuento con los recursos técnicos, tecnológicos, humanos y financieros para el desarrollo de los requisitos técnicos y funcionales que permitan realizar modificaciones sobre el sistema en caso de ser actualizada la pasarela de servicios por parte de la Agencia Nacional Digital.

2. He adquirido el Dominio seguro [nombre del dominio] a nombre de [nombre de la entidad solicitante (el registrante debe ser la persona jurídica de derecho privado)] con [nombre de la entidad certificadora] con vigencia hasta [aaaa/mm/dd].

3. Cuento con la solución certificada por el consorcio OpenID Connect el cual se encuentra vigente hasta [aaaa/mm/dd].

4. Dispongo del recurso humano para realizar las pruebas de funcionamiento de las páginas y pruebas del consumo y exposición de los servicios. Este personal cuenta con los siguientes perfiles:

- Un Líder Técnico: Profesional en ingeniería de sistemas, con especialización en áreas afines y 46 meses de experiencia en actualización tecnológica de autenticación digital y mejoras en código fuente.

- Un Desarrollador Senior: Profesional en ingeniería de sistemas, multimedia o afines, con especialización en áreas afines o 24 meses de experiencia en autenticación digital con conocimientos en desarrollo front-end, creación de componentes web, implementación de responsive desing, metodologías ágiles (scrum), consumo de API, desarrollo de componentes en función de las historias de usuario, manejo de pruebas unitarias, código limpio y repositorio de código.

- Analista de Requerimientos y QA: Profesional en ingeniería de sistemas o afines, Especialización en áreas afines o 24 meses de experiencia adicional como analista de requerimientos y QA

5. He realizado y gestionado pruebas de seguridad aplicando metodologías y frameworks (OWASP, OSSTTM, EcCouncil, entre otros). Así mismo, cuento con el documento que evidencia la realización de dichas pruebas, así como el plan de mitigación o cierre de brechas.

6. Dispongo de políticas de protección de datos personales conforme al cumplimiento de la legislación vigente en esta materia en Colombia.

7. Dispongo de un plan de continuidad del negocio documentado, implementado y probado que soporta la disponibilidad de los servicios críticos

8. Cumplo con los requisitos técnicos y funcionales estipulados en la norma NIST 800-63v3.

9. Cumplo con los requisitos técnicos y funcionales de las recomendaciones de seguridad de AUTH 2.0 https://datatracker.ietf.org/doc/html/draft-ietf-oauth-security-topics

10. He realizado la implementación de OpenID Connect Back-Channel Logout 1.0 - draft 06, OpenID Connect Session Management 1.0 - draft 30 y OpenID Connect Front-Channel Logout 1.0

11. Los datos de usuarios se encuentran encriptados tanto en tránsito como en reposo.

12. Cuento con sistema de monitoreo que me permite controlar (# Número de Usuarios registrados por nivel de confianza, # Tiempo promedio de respuesta, # Número de Usuarios autenticados por ubicación geográfica, Disponibilidad del servicio) y he realizado pruebas funcionales para verificar su correcto funcionamiento.

En constancia de lo anterior firmo esta certificación a los [día] del mes de [mes] de 202[_].

Atentamente,

_____

[Firma]
[Nombre del representante legal del Solicitante]
[Tipo y Número de documento del representante legal del Solicitante]
[Nombre de la entidad solicitante]
[Nit de la entidad solicitante]

Nota: Con la suscripción de la presente certificación, en forma voluntaria e irrevocable, ACEPTO en mi calidad de representante legal de [nombre de la entidad solicitante] que esta cumple con todas las condiciones técnicas solicitadas como requisito en el anexo técnico de la resolución N XXXX de 2021 y que el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MINTIC) y la Corporación Agencia Nacional de Gobierno Digital (AND) podrán solicitar copia y/o acceso a la información en cualquier etapa del proceso de los requisitos aquí mencionados para verificar su cumplimiento.

2. Lista de cumplimiento de requisitos norma NIST 800-63v3

Nro.	Descripción	Cumple	
Componente: General - Servicios de inscripción y / o prueba de identidad		**Si**	**No**
GEN-1	La prueba de identidad NO DEBE realizarse para determinar la idoneidad o el derecho a obtener acceso a servicios o beneficios		
GEN-2	La recopilación de PII DEBERÁ limitarse al mínimo necesario para resolver una identidad única en un contexto dado.		
GEN-3	El CSP DEBERÁ proporcionar un aviso explícito al solicitante en el momento de la recopilación con respecto al propósito de recopilar y mantener un registro de los atributos necesarios para la prueba de identidad, incluido si dichos atributos son voluntarios u obligatorios para completar el proceso de prueba de identidad, y las consecuencias para no proporcionar los atributos.		
GEN-4a	Si los CSP procesan atributos con fines distintos a la prueba de identidad, la autenticación o las afirmaciones de atributos (colectivamente, "servicio de identidad"), la mitigación del fraude relacionado o para cumplir con la ley o el proceso legal, entonces los CSP DEBERÁN implementar medidas para mantener la previsibilidad y la capacidad de gestión acordes con el riesgo de privacidad derivado del procesamiento adicional.		
GEN-4b	NO DEBERÁ hacer que el consentimiento para el procesamiento adicional sea una condición del servicio de identidad		
GEN-5a	El CSP DEBERÁ proporcionar mecanismos para la reparación de las quejas de los solicitantes o los problemas que surjan de la prueba de identidad.		
GEN-5b	El CSP DEBE evaluar los mecanismos de reparación para determinar su eficacia para lograr la resolución de quejas o problemas.		
GEN-6	Los procesos de prueba de identidad e inscripción DEBEN realizarse de acuerdo con una política escrita aplicable o * declaración de práctica * que especifique los pasos particulares que se toman para verificar las identidades.		
GEN-7	La * declaración de práctica * DEBERÁ incluir información de control que detalle cómo el CSP maneja los errores de revisión que dan como resultado que un solicitante no se inscriba con éxito		
GEN-8a	El CSP DEBE mantener un registro, incluidos los registros de auditoría, de todos los pasos tomados para verificar la identidad del solicitante.		
GEN-8b	Idealmente, el sistema de identidad del CSP incluye la capacidad de registrar y registrar de forma segura actividades específicas asociadas con el proceso de verificación de identidad.		
GEN-8c	El CSP DEBE llevar a cabo un proceso de gestión de riesgos, incluidas evaluaciones de los riesgos de privacidad y seguridad.		
GEN-9	Toda la PII recopilada como parte del proceso de inscripción DEBE estar protegida para garantizar la confidencialidad, integridad y atribución de la fuente de información.		

GEN-10	Toda la transacción de prueba, incluidas las transacciones que involucran a un tercero, DEBE ocurrir a través de canales protegidos autenticados.		
GEN-11	Si el CSP utiliza medidas de mitigación del fraude, entonces el CSP DEBE realizar una evaluación de riesgo de privacidad para estas medidas de mitigación.		
GEN-12	En caso de que un CSP deje de llevar a cabo los procesos de prueba de identidad e inscripción, entonces el CSP SERÁ responsable de eliminar o destruir por completo cualquier dato sensible, incluida la PII, o su protección contra el acceso no autorizado durante la duración de la retención.		
GEN-13	Independientemente de si el CSP es una agencia federal o una entidad no federal, los siguientes requisitos se aplican a la agencia federal que ofrece o utiliza el servicio de revisión		
GEN-14	Un código de inscripción DEBE estar compuesto por uno de los siguientes: 1. Como mínimo, una entropía alfanumérica aleatoria de seis caracteres o equivalente. Por ejemplo, un código generado usando un generador de números aleatorios aprobado o un número de serie para un autenticador de hardware físico; O 2. Una etiqueta óptica legible por máquina, como un código QR, que contiene datos de entropía similar o superior como un alfanumérico aleatorio de seis caracteres.		
GEN-15	Los requisitos de formación para el personal que valida la evidencia DEBEN basarse en las políticas, directrices o requisitos del CSP o RP		
GEN-16	Si el CSP proporciona pruebas de identidad y servicios de inscripción a menores (menores de 18 años), entonces el CSP DEBERÁ prestar especial consideración a las restricciones legales de interactuar con menores que no puedan cumplir con los requisitos de prueba de prueba de identidad [para garantizar el cumplimiento de la Ley de Protección de la Privacidad Infantil en Línea de 1998 (COPPA) y otras leyes.		
GEN-17	Si el CSP proporciona pruebas de identidad y servicios de inscripción a menores de 13 años, entonces ... los menores de 13 años requieren consideraciones especiales adicionales bajo COPPA y otras leyes, que el CSP DEBERÁ garantizar el cumplimiento, según corresponda.		
GEN-18	El CSP DEBE hacer que el operador vea la fuente biométrica (por ejemplo, dedos, cara) para detectar la presencia de materiales no naturales y realizar tales inspecciones como parte del proceso de prueba.		
GEN-19	El CSP DEBE recopilar datos biométricos de tal manera que garantice que los datos biométricos se recopilen del solicitante y no de otro sujeto. Se aplican todos los requisitos de rendimiento biométrico en SP 800-63B.		
Componente: IAL2 - Servicios de inscripción y / o prueba de identidad			
IAL2-1	El CSP DEBE admitir pruebas de identidad en persona o remota, o ambas.		
IAL2-2	El CSP DEBE recopilar lo siguiente del solicitante: 1. Una pieza de evidencia SUPERIOR o FUERTE si la fuente emisora de la evidencia, durante su evento de prueba de identidad, confirmó la identidad reclamada mediante la recopilación de dos o más formas de evidencia SUPERIOR o FUERTE y el CSP valida la evidencia directamente con la fuente emisora; O 2. Dos piezas de evidencia FUERTE; O 3. Una prueba FUERTE más dos pruebas FIRMAS		

IAL2-3	El CSP DEBERÁ validar cada pieza de evidencia con un proceso que pueda lograr la misma solidez que la evidencia presentada (ver IAL2-3 más arriba). Por ejemplo, si se presentan dos formas de evidencia de identidad FUERTE, cada pieza de evidencia se validará con una fuerza de FUERTE.		
IAL2-4a	El CSP DEBE verificar la evidencia de identidad de la siguiente manera: 1. Como mínimo, la vinculación del solicitante a la evidencia de identidad debe ser verificada por un proceso que pueda lograr una fuerza de FUERTE.		
IAL2-4b	La recopilación de características biométricas para fines físicos o comparación biométrica del solicitante con la prueba de identidad más sólida proporcionado para respaldar la identidad reclamada] realizado de forma remota DEBERÁ adherirse a todos los requisitos especificados en SP 800-63B		
IAL2-5	La verificación basada en conocimientos (KBV) NO DEBERÁ se utiliza para la verificación de identidad en persona (física o remota supervisada).		
IAL2-6a	El CSP DEBE confirmar la dirección de registro.		
IAL2-6b	Se DEBEN emitir registros válidos para confirmar la dirección fuente (s) o fuente (s) autorizada (s).		
IAL2-7	Si el CSP realiza pruebas en persona para IAL2 y proporciona un código de inscripción directamente al suscriptor para vincularlo a un autenticador en un momento posterior, luego el código de inscripción DEBERÁ ser válido para un máximo de 7 días.		
IAL2-8a	El CSP DEBE enviar un código de inscripción a una dirección de registro del solicitante		
IAL2-8b	El solicitante DEBE presentar un código de inscripción válido para completar el proceso de verificación de identidad.		
IAL2-8c	Los códigos de inscripción deberán tener el siguiente máximo validez: i. 10 días, cuando se envía a una dirección postal registrada dentro de Colombia; ii. 30 días, cuando se envía a una dirección postal registrada fuera de los Colombia; iii. 10 minutos, cuando se envía a un teléfono de registro (SMS o voz); iv. 24 horas, cuando se envía a una dirección de correo electrónico registrada.		
IAL2-8d	Si el código de inscripción enviado a la dirección confirmada de registro como parte del proceso de verificación de identidad remota en IAL2 también es pretende ser un factor de autenticación, entonces DEBERÁ restablecerse al primer uso.		
IAL2-8e	Si el CSP realiza pruebas remotas en IAL2 y opcionalmente envía notificación de prueba además de enviar el código de inscripción requerido, luego ... El CSP DEBE garantizar la inscripción el código y la notificación de verificación se envían a diferentes direcciones de registro.		
IAL2-9	El CSP DEBERÁ emplear controles de seguridad adaptados adecuadamente, para incluir Mejoras de control, desde la línea de base moderada o alta de los controles de seguridad. definido en SP 800-53 o equivalente federal (por ejemplo, FEDRAMP) o industria estándar.		

Componente: IAL3 - Servicios de inscripción y / o prueba de identidad			
IAL3-1	La recopilación de PII DEBERÁ limitarse al mínimo necesario para resolver un registro de identidad único		
IAL3-2	El CSP DEBE recopilar lo siguiente del solicitante: 1. Dos piezas de evidencia SUPERIOR; O 2. Una pieza de evidencia SUPERIOR y una pieza de evidencia FUERTE si la fuente emisora de la evidencia FUERTE, durante su evento de prueba de identidad, confirmó la identidad reclamada mediante la recopilación de dos o más formas de evidencia SUPERIOR o FUERTE y el CSP valida la evidencia directamente con la fuente emisora; O 3. Dos piezas de evidencia FUERTE más una pieza de evidencia JUSTA.		
IAL3-3	El CSP DEBE validar la evidencia de identidad de la siguiente manera: Cada pieza de evidencia debe ser validada con un proceso que pueda lograr la misma solidez que la evidencia presentada. Por ejemplo, si se presentan dos formas de evidencia de identidad FUERTE, cada pieza de evidencia se validará con una fuerza de FUERTE.		
IAL3-4	El CSP DEBE verificar la evidencia de identidad de la siguiente manera: 1. Como mínimo, la vinculación del solicitante con la evidencia de identidad debe ser verificada por un proceso que pueda lograr una fortaleza de SUPERIOR. 2. KBV NO DEBE utilizarse para la verificación de identidad en persona (física o remota supervisada)		
IAL3-5	El CSP DEBE realizar todos los pasos de verificación de identidad con el solicitante en persona.		
IAL3-6	El CSP DEBE confirmar la dirección de registro.		
IAL3-7	Se DEBERÁ enviar una notificación de prueba a la dirección de registro confirmada		
IAL3-8	Si el CSP proporciona un código de inscripción directamente al suscriptor (para vincularlo a un autenticador en un momento posterior). El código de inscripción DEBE ser válido por un máximo de 7 días.		
IAL3-9	El CSP DEBERÁ emplear controles de seguridad adaptados apropiadamente, para incluir mejoras de control, desde la línea de base alta de controles de seguridad definidos en SP 800-53 o equivalente federal.		
IAL3-10	El CSP DEBE recolectar y registrar una muestra biométrica en el momento de la revisión (por ejemplo, imagen facial, huellas dactilares) con el propósito de no repudio y revisión.		
Componente: Prueba de identidad remota supervisada			
SRP-1	Las transacciones de registro y prueba de identidad remotas supervisadas DEBEN cumplir con los siguientes requisitos, además de los requisitos de validación y verificación de IAL3 especificados en la Sección		
SRP-2	El CSP DEBERÁ monitorear toda la sesión de verificación de identidad, de la cual el solicitante NO DEBERÁ partir		
SRP-3	El CSP DEBE tener un operador en vivo que participe de forma remota con el solicitante durante la totalidad de la sesión de verificación de identidad.		
SRP-4	El CSP DEBE requerir que todas las acciones tomadas por el solicitante durante la sesión de prueba de identidad sean claramente visibles para el operador remoto.		

SRP-5	El CSP DEBE requerir que toda la verificación digital de la evidencia sea realizada por escáneres y sensores integrados.		
SRP-6	El CSP DEBE requerir que los operadores se hayan sometido a un programa de capacitación para detectar posibles fraudes y realizar adecuadamente una sesión de prueba remota supervisada.		
SRP-7	El CSP DEBE emplear funciones de resistencia y detección de manipulación física adecuadas para el entorno en el que se encuentra.		
SRP-8	El CSP DEBE garantizar que todas las comunicaciones se realicen a través de un canal protegido mutuamente autenticado.		
Componente: Árbitros de confianza			
TRR-1	Si el CSP usa árbitros confiables, entonces El CSP DEBE establecer políticas y procedimientos escritos sobre cómo se determina un árbitro confiable y el ciclo de vida por el cual el árbitro confiable retiene su estatus como árbitro válido, para incluir cualquier restricción, así como cualquiera de los requisitos de revocación y suspensión.		
TRR-2	Si el CSP utiliza árbitros confiables, entonces el CSP DEBERÁ probar al árbitro confiable en el mismo IAL que el solicitante.		
TRR-3	Si el CSP utiliza árbitros confiables, el CSP DEBE determinar la evidencia mínima requerida para vincular la relación entre el árbitro confiable y el solicitante.		
Criterios de conformidad de verificación basados en conocimientos			
KBV-1	El CSP DEBERÁ adherirse a los requisitos de la Sección 5.3.2 si se utiliza KBV para verificar una identidad		
KBV-2	El CSP NO DEBE usar KBV para verificar la identidad de un solicitante con más de una pieza de evidencia de identidad validada.		
KBV-3	El CSP solo DEBE usar información que se espera que sea conocida solo por el solicitante y la fuente autorizada, para incluir cualquier información necesaria para comenzar el proceso KBV.		
KBV-4	NO SE DEBE utilizar información accesible libremente, por una tarifa en el dominio público o mediante el mercado negro.		
KBV-5	El CSP DEBERÁ permitir que una identidad resuelta y validada se excluya de KBV y aproveche otro proceso de verificación.		
KBV-6	El CSP DEBE asegurarse de que la información de la transacción tenga al menos 20 bits de entropía. Por ejemplo, para alcanzar los requisitos mínimos de entropía, el CSP podría pedirle al solicitante que verifique la (s) cantidad (s) y los números de transacción de un microdepósito (s) en una cuenta bancaria válida, siempre que el número total de dígitos es siete o más.		
KBV-7	El CSP PUEDE realizar KBV haciendo preguntas al solicitante para demostrar que es el propietario de la información reclamada.		
KBV-8	El CSP TIENE el tiempo de espera de las sesiones de KBV después de dos minutos de inactividad por pregunta. En los casos de tiempo de espera de la sesión, el CSP REINICIARÁ todo el proceso de KBV y considerará esto como un intento fallido.		
KBV-9	El CSP NO DEBERÁ presentar la mayoría de las preguntas de KBV de distracción.		

KBV-10	El CSP NO DEBE formular una pregunta de KBV que proporcione información que pueda ayudar a responder cualquier pregunta futura de KBV en una sola sesión o en una sesión posterior después de un intento fallido.		
KBV-11	El CSP NO DEBE utilizar preguntas KBV cuyas respuestas no cambien.		
KBV-12	El CSP DEBE asegurarse de que cualquier pregunta de KBV no sea que el solicitante no haya proporcionado, ni información personal que, cuando se combine con otra información en una sesión de KBV, pueda resultar en una identificación única.		

Nota: El detalle de cada uno de los requerimientos podrá ser consultado a través del siguiente enlace: https://www.nist.gov/system/files/documents/2020/07/02/800-63A%20Conformance%20Criteria_0620.pdf

3. Accesos

1. URL y credenciales de acceso a un ambiente QA para pruebas

   URL: [_____]
   Usuario: [_____]
   Contraseña: [_____]

2. URL y credenciales de acceso a ambiente Pre-productivo

   URL: [_____]
   Usuario: [_____]
   Contraseña: [_____]

3. URL y credenciales de acceso a ambiente Productivo.

   URL: [_____]
   Usuario: [_____]
   Contraseña: [_____]

4. Anexos

ANEXO 1 – ACUERDO DE CONFIDENCIALIDAD Y BUEN USO DE LA INFORMACIÓN

[Nombre del representante legal del Solicitante], identificado como aparece al pie de mi firma, en mi calidad de representante legal de [nombre de la entidad solicitante], certifico en mi nombre y en nombre de [nombre de la entidad solicitante] que tengo y cumplo con las siguientes cláusulas del acuerdo de confidencialidad y buen uso de la información, de la siguiente manera:

CONSIDERACIONES

1) Que la Parte Receptora cumple con los requisitos técnicos para la integración como prestador privado del servicio de **AUTENTICACIÓN DIGITAL**, en el marco del modelo de Servicios Ciudadanos Digitales.

2) Que, en virtud de lo acordado para la prestación del servicio de AUTENTICACIÓN DIGITAL en el marco del modelo de Servicios Ciudadanos Digitales, las partes firman el presente Acuerdo de Confidencialidad a fin de establecer los términos que rigen el uso, la protección y la no divulgación de la información que recíprocamente se intercambien, y

ACUERDAN

PRIMERO. [nombre de la entidad solicitante], quien para los efectos del presente documento se denominará PARTE RECEPTORA se obliga a no divulgar a terceras partes, la "Información confidencial", que reciba por parte de **MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA (MINTIC), DIRECCIÓN DE GOBIERNO DIGITA**L y/o la **CORPORACIÓN AGENCIA NACIONAL DE GOBIERNO DIGITAL – AND,** que para los efectos del presente

documento se denominarán PARTE REVELADORA y a darle a dicha información el mismo tratamiento que le darían a la información confidencial de su propiedad.

Parágrafo I: Para efectos del presente Acuerdo, "Información Confidencial" comprende toda la información divulgada por la PARTE REVELADORA, ya sea en forma verbal, visual, escrita, grabada en medios magnéticos o en cualquier otra forma tangible y que se encuentre claramente marcada como tal al ser entregada a la parte receptora. Tal información comprende, pero no está limitada a, información comercial, estratégica, contractual, operativa, planes de negocio, de desarrollo, información técnica, tecnológica, financiera, contable, legal, información sobre recursos humanos, planes de servicios, análisis y proyecciones, especificaciones, componentes de propiedad intelectual e industrial, know how, diseños, modelos, planos, procesos, equipos, software, proyectos e investigaciones de ciencias, tecnología e investigación, bases de datos, datos personales semiprivados, privados y/o sensibles, y cualquier otro aspecto que concierne a las actividades desarrolladas por la Parte Reveladora, aun cuando no estén marcadas o identificadas como confidenciales.

Parágrafo II: DE LA INFORMACIÓN NO CONFIDENCIAL. Se considera Información No Confidencial la siguiente:

a) Información de carácter público;

b) Información dada a conocer por un tercero que tenga el derecho de distribuirla o divulgarla sin ninguna restricción.

SEGUNDO. El presente Acuerdo de confidencialidad y no divulgación de la información, tiene por objeto señalar y especificar las políticas de confidencialidad que debe cumplir LA PARTE RECEPTORA, respecto del acceso, consulta y uso de la información confidencial que produce y administra LA PARTE REVELADORA. Por lo tanto, quien suscribe el presente documento se obliga a no revelar, divulgar, exhibir, mostrar, comunicar, utilizar y/o emplear la información conocida o entregada por la parte reveladora, para fines distintos al cumplimiento de la integración como prestador privado del servicio de AUTENTICACIÓN DIGITAL.

TERCERO. La parte receptora se obliga a mantener de manera confidencial la "Información confidencial" que reciba de la PARTE REVELADORA y a no darla a una tercera parte diferente de su equipo de trabajo y asesores que tengan la necesidad de conocer dicha información para los propósitos autorizados, y quienes deberán estar de acuerdo en mantener de manera confidencial dicha información.

CUARTO. REVELACIÓN PERMITIDA. La Parte Receptora podrá revelar Información Confidencial en los siguientes casos:

a) Por aprobación escrita de la Parte Reveladora;
b) A los trabajadores, contratistas, asesores o funcionarios de la Parte Reveladora, que tengan necesidad de conocerla en cumplimiento de sus obligaciones para la integración como prestador privado del servicio de **AUTENTICACIÓN DIGITAL**, si ello resulta necesario, para lo cual se deberá suscribir un acuerdo de confidencialidad;
c) Información que deba ser revelada o divulgada por requerimiento de decreto, reglamento, norma o entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial, previa notificación a la Parte Reveladora, para que ésta pueda tomar las medidas necesarias para proteger la información.

QUINTO. OBLIGACIONES DE CONFIDENCIALIDAD. La Parte Receptora se obliga a:

a) Guardar bajo absoluta reserva la Información Confidencial;
b) Cuidar la información a la que tenga acceso, evitando su deterioro, destrucción y/o utilización indebida, ejerciendo sobre ésta el mismo grado de cuidado y diligencia que utiliza para proteger información confidencial de su propiedad;
c) Utilizar la Información Confidencial únicamente para el desarrollo de sus obligaciones y actividades estipuladas para la integración como prestador privado del servicio de **AUTENTICACIÓN DIGITAL**;
d) Asegurar que las personas a las que se les revele Información Confidencial, por autorización de la Parte Reveladora, mantengan dicha Información Confidencial privada y confidencial, y no la revelen ni divulguen a ninguna otra persona no autorizada;

e) No obtener, compilar, sustraer, ofrecer, vender, intercambiar, enviar, comprar, interceptar, divulgar, modificar y/o emplear Información Confidencial que pertenezca a/u obtenga de la Parte Reveladora, o de información que maneje con ocasión de las actividades o que le sea dada a conocer con ocasión a la integración como prestador privado del servicio de AUTENTICACIÓN DIGITAL, ya sea de forma total o parcial, en provecho personal o de un tercero, directo o indirecto, sin estar facultada para ello;

f) No suministrar a persona alguna la(s) clave(s) de acceso a los sistemas de la Parte Reveladora que le haya(n) sido asignada(s), o dar acceso o exhibir expedientes, documentos o archivos a personas no autorizadas;

g) Efectuar una adecuada custodia y reserva de la información y gestión -es decir tratamiento- de los datos suministrados por la PARTE REVELADORA al interior de las redes y bases de datos (físicas y/o electrónicas) en donde se realice su recepción y tratamiento en general;

h) Para el caso del manejo de información que incluya datos personales, la PARTE RECEPTORA dará estricto cumplimiento a las disposiciones constitucionales y legales sobre la protección del derecho fundamental de habeas data, en particular lo dispuesto en el artículo 15 de la Constitución; Política y la ley 1581 de 2012 y las disposiciones internas de la entidad;

i) No utilizar la Información Confidencial en detrimento de la Parte Reveladora.

SEXTO. INCUMPLIMIENTO DE LA CONFIDENCIALIDAD. El incumplimiento de la confidencialidad o el uso indebido de la Información Confidencial dará derecho a la Parte Reveladora a solicitar indemnización por los daños y perjuicios ocasionados, y tendrá la facultad de interponer las acciones legales correspondientes tendientes a restringir el uso y/o divulgación de la Información Confidencial y a obtener el resarcimiento de los daños y perjuicios ocasionados.

SÉPTIMO. LEY APLICABLE Y RESOLUCIÓN DE DISPUTAS. El presente Acuerdo se regirá por ley colombiana. Toda controversia o diferencia relativa a este Acuerdo se resolverá a través del procedimiento de conciliación, transacción, amigable composición o arreglo directo entre las Partes, en un término no mayor a cinco (05) días hábiles a partir de la fecha en que cualquiera de las Partes comunique por

escrito a la otra la existencia de una diferencia. En el caso en que estos mecanismos no sean efectivos, se someterá a la jurisdicción contencioso-administrativa.

OCTAVO. CESIÓN. Ninguna de las Partes podrá ceder el presente Acuerdo salvo autorización previa y por escrito de la otra Parte.

NOVENO. VIGENCIA. La vigencia del presente Acuerdo será indefinida y permanecerá vigente mientras exista relación receptora, se hará acreedora a la Pena Convencional establecida en la Cláusula Sexta del presente Acuerdo.

En constancia de lo anterior firmo esta certificación a los [día] del mes de [mes] de 202[_].

Atentamente,

_____

[Firma]

[Nombre del representante legal del Solicitante]

[Tipo y Número de documento del representante legal del Solicitante]

[Nombre de la entidad solicitante]

[Nit de la entidad solicitante]

ANEXO 2 - POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES, HABEAS DATA Y TÉRMINOS Y CONDICIONES DEL USO DEL SERVICIO.

[Incluir el texto]