

**Declaración de Prácticas de la Autoridad que funge
como tercero Legalmente Autorizado para la
Digitalización de Documentos en Soporte Físico de
conformidad con la NOM 151-SCFI-2016**

OID: 2.16.484.101.10.316.100.5.1.6.2.1

**Versión 1.5
Mayo 2022**

Tabla de Contenidos

1. ADMINISTRACIÓN DE LA DOCUMENTACIÓN	8
I. MANEJO DE VERSIONES.....	8
II. CONTROL DE VERSIONES	8
III. LISTA DE DISTRIBUCIÓN.....	9
IV. CALENDARIO DE REVISIONES DEL DOCUMENTO.....	10
2. INTRODUCCIÓN.....	11
3. ALCANCE	11
4. REFERENCIAS.....	11
5. DEFINICIONES Y CONCEPTOS	11
6 IDENTIFICACIÓN DEL DOCUMENTO DE DECLARACIÓN DE PRÁCTICAS DE LA AUTORIDAD DE DIGITALIZACIÓN QUE FUNGE COMO TERCERO LEGALMENTE AUTORIZADO	13
7 ADMINISTRACIÓN DEL DOCUMENTO DECLARACIÓN DE PRÁCTICAS DE LA AUTORIDAD QUE FUNGE COMO TERCERO LEGALMENTE AUTORIZADO PARA LA DIGITALIZACIÓN DE DOCUMENTOS EN SOPORTE FÍSICO	14
7.1 DETERMINACIÓN DE CAMBIOS EN ESTA DECLARACION DE PRÁCTICAS DE AUTORIDAD QUE FUNGE COMO TERCERO LEGALMENTE AUTORIZADO PARA LA DIGITALIZACIÓN DE DOCUMENTOS EN SOPORTE FÍSICO Y SU PUBLICACIÓN.....	15
8 ESTRUCTURA JERÁRQUICA.....	15
8.1 PARTICIPANTES EN EL SERVICIO DE DIGITALIZACIÓN DE DOCUMENTOS EN SOPORTE FÍSICO FUNGIENDO COMO TERCERO LEGALMENTE AUTORIZADO DE CONFORMIDAD CON LA NOM 151 SCFI 2016	17
8.1.1 AUTORIDAD CERTIFICADORA SEGURIDATA	17
8.1.2 AUTORIDAD DE SELLOS DIGITALES DE TIEMPO	17
8.1.3 AUTORIDAD DE CONSTANCIAS DE CONSERVACIÓN DE MENSAJES DE DATOS NOM 151 SCFI 2016	17
8.1.4 SECRETARIA DE ECONOMÍA.....	17
8.1.5 AUTORIDAD QUE FUNGE COMO TERCERO LEGALMENTE AUTORIZADO EN EL PROCESO DE DIGITALIZACIÓN DE DOCUMENTOS EN SOPORTE FÍSICO DE CONFORMIDAD CON LA NOM 151 SCFI 2016	17

8.1.6	CLIENTES-USUARIOS COMERCIANTES.....	17
8.1.7	ADMINISTRADOR DEL SERVICIO DE DIGITALIZACIÓN DE DOCUMENTOS EN SOPORTE FÍSICO FUNGIENDO COMO TERCERO LEGALMENTE AUTORIZADO	18
9	OBLIGACIONES Y RESPONSABILIDADES	18
9.1	OBLIGACIONES DE LA AUTORIDAD QUE FUNGE COMO TERCERO LEGALMENTE AUTORIZADO PARA EL PROCESO DE DIGITALIZACIÓN DE DOCUMENTOS EN SOPORTE FÍSICO.....	18
9.2	OBLIGACIONES DEL COMERCIANTE.....	20
9.3	OBLIGACIONES DEL ADMINISTRADOR DEL SERVICIO	20
9.4	OBLIGACIONES DEL DIGITALIZADOR	20
9.5	RESPONSABILIDAD DE LA AUTORIDAD QUE FUNGE COMO TERCERO LEGALMENTE AUTORIZADO PARA LA DIGITALIZACIÓN DE DOCUMENTOS EN SOPORTE FÍSICO.....	21
9.6	RESPONSABILIDAD DEL CLIENTE- COMERCIANTE.....	22
9.7	RESPONSABILIDAD DEL ADMINISTRADOR	23
9.8	RESPONSABILIDAD DEL FEDATARIO	23
10	FECHA DE INICIO DE OPERACIONES COMO TLA	23
	UNA VEZ QUE LA SECRETARIA DE ECONOMÍA OTORGUE LA ACREDITACIÓN A SEGURIDATA PRIVADA, INICIARA SUS OPERACIONES COMO TLA EN CONJUNTO CON EL DIGITALIZADOR DEFINIDO.	23
11	PUBLICACIÓN Y CONSULTA DE INFORMACIÓN	23
11.1	CONSULTA DE INFORMACIÓN DEL SERVICIO DE DIGITALIZACIÓN DE DOCUMENTOS EN SOPORTE FÍSICO FUNGIENDO COMO TERCERO LEGALMENTE AUTORIZADO	23
11.2	PUBLICACIÓN DE CERTIFICADO DIGITAL DE LA AUTORIDAD QUE FUNGE COMO TERCERO LEGALMENTE AUTORIZADO PARA LA DIGITALIZACIÓN DE DOCUMENTOS EN SOPORTE FÍSICO	23
12	CICLO DE VIDA DE LA ADMINISTRACIÓN DE CLAVES DE LA AUTORIDAD QUE FUNGE COMO TERCERO LEGALMENTE AUTORIZADO PARA LA DIGITALIZACIÓN DE DOCUMENTOS EN SOPORTE FÍSICO	23
12.1	GENERACIÓN DE CLAVES DE LA AUTORIDAD QUE FUNGE COMO TERCERO LEGALMENTE AUTORIZADO PARA LA DIGITALIZACIÓN DE DOCUMENTOS EN SOPORTE FÍSICO DE SEGURIDATA PRIVADA.	24

12.2 PROTECCIÓN Y RESGUARDO DE LAS CLAVES PRIVADAS DE LA AUTORIDAD QUE FUNGE COMO TERCERO LEGALMENTE AUTORIZADO PARA LA DIGITALIZACIÓN DE DOCUMENTOS EN SOPORTE FÍSICO	24
12.3 DISTRIBUCIÓN DE LAS CLAVES PÚBLICAS DE LA AUTORIDAD QUE FUNGE COMO TERCERO LEGALMENTE AUTORIZADO PARA LA DIGITALIZACIÓN DE DOCUMENTOS EN SOPORTE FÍSICO	25
LA AUTORIDAD QUE FUNGE COMO TERCERO LEGALMENTE AUTORIZADO PARA LA DIGITALIZACIÓN DE DOCUMENTOS EN SOPORTE FÍSICO DE SEGURIDATA PRIVADA DEBE ASEGURAR QUE LA INTEGRIDAD Y LA AUTENTICIDAD DE LAS CLAVES DE VERIFICACIÓN DE FIRMA DE MENSAJES DE DATOS SE MANTIENEN SEGURAS DURANTE SU DISTRIBUCIÓN.....	25
12.4 RENOVACIÓN DE LAS CLAVES CRIPTOGRÁFICAS DE LA AUTORIDAD QUE FUNGE COMO TERCERO LEGALMENTE AUTORIZADO PARA LA DIGITALIZACIÓN DE DOCUMENTOS EN SOPORTE FÍSICO	26
12.5 FIN DEL CICLO DE VIDA DE LAS CLAVES DE LA AUTORIDAD QUE FUNGE COMO TERCERO LEGALMENTE AUTORIZADO PARA LA DIGITALIZACIÓN DE DOCUMENTOS EN SOPORTE FÍSICO	26
12.6 CICLO DE VIDA DEL MÓDULO CRIPTOGRÁFICO – AUTORIDAD QUE FUNGE COMO TERCERO LEGALMENTE AUTORIZADO PARA LA DIGITALIZACIÓN DE DOCUMENTOS EN SOPORTE FÍSICO DE SEGURIDATA PRIVADA.....	26
12.6.1 CICLO DE VIDA PRODUCTOS THALES	27
13. PROCESO PARA OTORGAR Y CONTRATAR EL SERVICIO DE DIGITALIZACIÓN DE DOCUMENTOS EN SOPORTE FÍSICO - GENERALIDADES	28
13.1 PROCESO PARA SOLICITAR UN SERVICIO DE DIGITALIZACIÓN CERTIFICADA. CONTRATACIÓN DEL SERVICIO DE DIGITALIZACIÓN	28
13.1.1	29
13.2 PROCESO DE RECEPCIÓN - RECOLECCIÓN DE DOCUMENTOS A DIGITALIZAR	31
13.3 RESGUARDO PARA LA PROTECCIÓN DE LA DOCUMENTACIÓN EN SOPORTE FÍSICO.....	34
13.3.1 MEDIDAS DE PROTECCIÓN DE LA DOCUMENTACIÓN EN SOPORTE FÍSICO.....	35
13.3.2 Restauración del documento en soporte Físico.....	35
13.4 PREPARACIÓN DE DOCUMENTOS.....	35
13.5 TRANSFERENCIA DE DOCUMENTOS EN SOPORTE FÍSICO A MENSAJE DE DATOS	39
13.6 DIGITALIZACIÓN	39
13.6.1 Revisión de la Muestra.....	40
13.6.2 Proceso de firma de documentos digitalizados	42
13.6.3 PROCESO DE ENTREGA O DESTRUCCIÓN DE DOCUMENTOS EN FÍSICO.....	46

14	TRAZABILIDAD DE REGISTRO DE FECHA Y HORA DE ACTIVIDADES DE DIGITALIZACIÓN	48
15	CONDICIONES QUE CUMPLE EL TLA PARA OFRECER EL SERVICIO DE DIGITALIZACIÓN FUNGIENDO COMO TLA	49
16	POLÍTICA DE DESHECHO – LIMITANTES.....	50
16.1	GRADO DE FIABILIDAD DE LOS MECANISMOS Y DISPOSITIVOS UTILIZADOS.....	51
	<i>Los puntos importantes para asegurar la fiabilidad de los mecanismos de firma electrónica avanzada, durante la digitalización son:.....</i>	<i>51</i>
16.2	SEGURIDAD EN EL ACCESO A LA AUTORIDAD QUE FUNGE COMO TERCERO LEGALMENTE AUTORIZADO PARA LA DIGITALIZACIÓN DE DOCUMENTOS EN SOPORTE FÍSICO	51
16.2.1	OTORGAMIENTO DEL SERVICIO	51
16.3	ADMINISTRACIÓN DE LA SEGURIDAD	52
16.4	CONTROLES DE SEGURIDAD FÍSICA	52
16.5	UBICACIÓN Y CONSTRUCCIÓN.....	52
16.5.1	ACCESO FÍSICO.....	53
16.5.2	ENERGÍA ELÉCTRICA Y AIRE ACONDICIONADO	54
16.5.3	RIESGOS POR INUNDACIONES.....	54
16.5.4	PREVENCIÓN DE INCENDIOS Y PROTECCIÓN	54
16.6	ALMACENAMIENTO DE MEDIOS	55
16.7	DESTRUCCIÓN DE DOCUMENTOS	55
16.8	COPIAS DE SEGURIDAD	55
16.9	PROCEDIMIENTOS DE CONTROL	56
16.10	ROLES DE CONFIANZA.....	56
16.10.1	NÚMERO DE PERSONAS REQUERIDAS POR TAREA	59
16.10.2	FUNCIONES QUE REQUIEREN SEPARACIÓN DE DEBERES	60
16.11	CONTROLES DE SEGURIDAD PERSONALES.....	60
16.11.1	REQUERIMIENTOS DE CALIFICACIÓN, EXPERIENCIA, CALIDAD Y FORMACIÓN	60
16.11.2	PROCEDIMIENTO DE COMPROBACIÓN	61
16.11.3	REQUISITOS DE PERSONAL EXTERNO	61
16.11.4	DOCUMENTACIÓN SUMINISTRADA AL PERSONAL	61

17	AUDITORÍA DE PROCEDIMIENTOS DE REGISTRO	62
17.1	<i>Tipos de Eventos Registrados</i>	62
17.1.1	FRECUENCIA DE REGISTRO.....	62
17.1.2	PERÍODO DE CONSERVACIÓN DE LOS REGISTROS DE AUDITORIA.....	63
17.1.3	PROTECCIÓN DE LOS REGISTROS DE AUDITORIA	63
17.1.4	NOTIFICACIÓN AL INDIVIDUO QUE GENERA UN SUCESO	63
17.1.5	EVALUACIONES DE VULNERABILIDAD	64
18.	BASE DE DATOS	64
18.1	RESPALDO DE BASE DE DATOS	64
18.1.1	POLÍTICA DE RESPALDOS	65
18.1.2	PROCEDIMIENTO DE RESPALDO	65
18.2	ARCHIVO DE REGISTROS.....	66
18.3	PERÍODO DE RETENCIÓN DE ARCHIVOS	66
18.3.1	PROTECCIÓN DE ARCHIVOS	66
18.3.2	PROCEDIMIENTOS DE ARCHIVO DE RESERVA.....	67
18.3.3	EXIGENCIAS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS	67
18.3.4	SISTEMA DE REGISTRO DE ARCHIVOS (INTERNO O EXTERNO)	67
18.4	RECUPERACIÓN ANTE DESASTRES Y LA REVELACIÓN DE CLAVES	67
18.5	PROCEDIMIENTO DE CONTINUIDAD DEL NEGOCIO TRAS UN DESASTRE.....	68
18.6	TERMINACIÓN – CESE DE LA AUTORIDAD DE TLA.....	68
18.6.1	SUSPENSIÓN TEMPORAL	68
18.6.2	SUSPENSIÓN DEFINITIVA.....	69
18.6.3	CLASIFICACIÓN Y ADMINISTRACIÓN DE ACTIVOS.....	69
19.	<i>Limitantes y Restricciones en el Uso de información</i>	70
19.1	LIMITACIÓN DE RESPONSABILIDAD	70
19.1.1	<i>Exclusión de Responsabilidad</i>	70
19.2	RESPONSABILIDADES ECONÓMICAS	71
20	ACTUALIZACIÓN DE LA DECLARACIÓN DE PRÁCTICAS DE LA AUTORIDAD DE TERCERO LEGALMENTE AUTORIZADO	71

20.1	REPOSITORIOS.....	71
20.1.1	Aspectos Opcionales	72
21	OT.....	72
21	ASUNTOS COMERCIALES Y ASUNTOS LEGALES	72
A.	TARIFAS.....	72
i.	Tarifas del Servicio de Digitalización certificada	72
ii.	Para consultar las tarifas favor de comunicarse a SeguriData Privada S.A. de C.V.	72
iii.	Tarifas por otros Servicios	72
iv.	Responsabilidad Financiera	72
v.	Otros Activos.....	73
vi.	Cobertura de Seguros o Garantías para Entidades Finales.....	73
vii.	Registros Financieros.....	73
B.	PROTECCIÓN DE CONFIDENCIALIDAD DE LA INFORMACIÓN.....	73
i.	Alcance de la Información Confidencial.....	74
ii.	Información No Confidencial	75
iii.	Revelación de Datos de Conformidad con un Proceso Judicial o Administrativo	75
iv.	Otras Circunstancias de Revelación de Información.....	75
C.	DERECHOS DE PROPIEDAD INTELECTUAL	75
i.	Licencias.....	75
D.	REPRESENTACIONES Y GARANTÍAS.....	76
E.	GARANTÍAS DEL TERCERO LEGALMENTE AUTORIZADO	76
i.	Garantías del Cliente	76
F.	LIMITACIONES DE RESPONSABILIDAD	76
G.	INDEMNIZACIONES.....	76
H.	ENTRADA EN VIGOR Y TERMINACIÓN	77
i.	Entrada en Vigor.....	77
ii.	Terminación	77
I.	AVISOS INDIVIDUALES Y COMUNICACIÓN CON LOS PARTICIPANTES	77
J.	MODIFICACIONES	77
K.	PROCEDIMIENTOS DE RESOLUCIÓN DE CONTROVERSIAS	77
L.	LEY DE ADMINISTRACIÓN	77
M.	CUMPLIMIENTO CON LA LEY APLICABLE	77
N.	DISPOSICIONES VARIAS	77
O.	OTRAS DISPOSICIONES.....	78
P.	OBLIGACIONES, POLÍTICAS Y PROCEDIMIENTOS APLICABLES A ORGANIZACIONES EXTERNAS.....	78
22	ANEXOS	79
22.1	ANEXO 1 CONTRATO MARCO COMERCIANTE – TLA.....	79

22.2	ANEXO 2 ANEXO CON ESPECIFICACIONES DE DIGITALIZACIÓN COMO PARTE DEL CONTRATO ENTRE TLA Y COMERCIANTE	80
22.3	ANEXO 3 CARTA USO EXCLUSIVO DE CERTIFICADO PSC	81
22.4	ANEXO 4 CONVENIO ALIANZA CON DIGITALIZADOR - CONTRATO DE SERVICIOS DIGITALIZADOR – TLA	82
22.5	ANEXO 5 PROCEDIMIENTO PARA LA GENERACIÓN DE CLAVES	83
22.6	ANEXO 6 REPORTE DE MUESTRA	84
22.7	ANEXO 7 REPORTE DE COTEJO	85
22.8	ANEXO 8 ACTA CIRCUNSTANCIADA	86
22.9	ANEXO 9 FORMATO DE RECEPCIÓN – ENTREGA DE DOCUMENTOS EN SOPORTE FÍSICO.....	87
22.10	ANEXO 10 FORMATO DE DEVOLUCIÓN DE DOCUMENTOS EN SOPORTE FÍSICO	88

1. Administración de la Documentación

I. Manejo de Versiones

El presente documento será considerado válido y con vigencia siempre que los cambios hayan sido autorizados y aprobados por los responsables definidos en la siguiente sección

El presente documento deberá ser revisado dos veces al año, lo cual no implica una actualización del mismo.

II. Control de Versiones

El manejo de versiones para la documentación sigue el cumplimiento de políticas definidas para la asignación de un número de versión, de acuerdo a:

Se incrementa un número entero cuando

- Un cambio o mejora grande ocurre en la documentación.
- Un conjunto de características, que han sido planeadas, han sido implementadas.
- La estructura del documento cambia.
- Si el contenido del documento cambia en un 40% será necesario incrementar el número de versión con un número entero.

Se incrementa con un decimal sobre la versión del documento cuando

Se incrementa para distinguir múltiples liberaciones de la actualización de la documentación.
Este número indica mejoras o cambios menores en el contenido de la documentación.
Si el contenido del documento cambia en un porcentaje menor al 40%, será necesario incrementar el número de versión con un número decimal.

VERSIÓN	FECHA DE	CAMBIO EN EL DOCUMENTO
1.0	17 NOVIEMBRE 2018	DOCUMENTO INICIAL
1.1	MAYO 2019	ACTUALIZACIÓN ISO/TR 13028
1.2	JULIO 2019	ACTUALIZACIÓN RECOMENDACIONES SECRETARÍA DE ECONOMÍA
1.3	AGOSTO 2019	ACTUALIZACION POR RECOMENDACIONES DE SECRETARÍA DE ECONOMÍA
1.4	OCTUBRE 22 2019	ACTUALIZACIÓN DE OID
1.5	MAYO 18 2022	SE ELIMINA UNA OBLIGACIÓN DEL DIGITALIZADOR DE ELABORAR CONTRATO ENTRE DIGITALIZADOR – CLIENTES, POR NO ESTAR CONSIDERADO EN LAS REGLAS Y NO CONSIDERARSE NECESARIO, SE ACTUALIZAN CONTRATOS EN FUNCIÓN DE RECOMENDACIONES DE SECRETARIA DE ECONOMÍA.

III. Lista de Distribución

Las copias en papel, medio magnético y electrónico de este documento están almacenadas en las siguientes localidades.

LOCALIDAD	DIRECCIÓN	RESPONSABLE	MEDIO DE ALMACENAMIENTO
D.F.	INSURGENTES SUR 2375	OLGA GARCIA	MAGNETICO Y PAPEL
D.F.	KIO INTERLOMAS	MOISES BAUTISTA	MAGNETICO Y PAPEL

IV. Calendario de Revisiones del Documento

El documento se revisará al menos una vez al año para verificar que el contenido sea aplicable y funcional a la Infraestructura de Tercero legalmente autorizado, lo que no implica una actualización del mismo.

FECHAS PROGRAMADAS DE FUTURAS REVISIONES
01/02/2019
01/02/2020
01/02/2021
01/02/2022
Por determinar

2. Introducción

SeguriData Privada S.A. de C.V. está acreditada para el servicio de emisión de certificados digitales para Firma electrónica avanzada, para la emisión de Sellos digitales de tiempo, para la emisión de Constancias de Conservación de Mensajes de Datos y para la Digitalización de documentos en soporte físico como tercero Legalmente autorizado de conformidad con la NOM-151-SCFI-2016, ante la Secretaria de Economía.

La presente Declaración contiene las políticas y prácticas que regirán el funcionamiento y operación para el servicio de Digitalización de Documentos en Soporte Físico, de acuerdo a la NOM-151-SCFI-2016, en su papel de fungir como Tercero Legalmente Autorizado.

3. Alcance

El ámbito de aplicación es para cualquier documento físico de carácter mercantil, de empresas y comerciantes, es decir, el universo es amplio, debido a esta amplitud y a los mecanismos de seguridad que se definen, tiene un uso universal para acreditar la inalterabilidad de cualquier documento físico de carácter mercantil, digitalizado.

4. Referencias

La estructura de esta declaración está basada en lo dispuesto por:

- Norma Oficial Mexicana NOM-151-SCFI-2016, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos, publicado en el DOF: 30/03//2017.
- Código de Comercio, CAPITULO 1 Bis “De la Digitalización” con los artículos 95 bis 1, 95 bis 2, 95 bis 3 95 bis 4, 95 bis 5 y 95 bis 6 : DOF: 07/04/2016.

5. Definiciones y Conceptos

TÉRMINO	DEFINICIÓN
Secretaría de Economía	Es un órgano de la Administración Pública Federal Centralizada que coordina y actúa como Autoridad Certificadora y Registradora, respecto de los Prestadores de Servicios de Certificación
Digitalización	Proceso que permite la migración de documentos impresos a mensajes de datos, conforme a lo establecido en el apéndice normativo B de la

TÉRMINO	DEFINICIÓN
	NOM 151 – SCFI 2016
Aceptación de autoría	A la propiedad de un algoritmo de firma digital que permite atribuir a una persona física o moral la autoría de un mensaje de datos inequívocamente
Acto de comercio	A todo acto que la legislación vigente considera como tal
Autenticación	Al proceso en virtud del cual se constata que una entidad es la que dice ser y que tal situación es demostrable ante terceros.
Archivo parcial	Al mensaje de datos representado en formato ASN.1, conforme al apéndice de la presente Norma Oficial Mexicana
Solicitante	Es la persona física o moral que inicia el trámite para obtener una constancia de conservación de mensajes de datos
Cliente	La persona física o moral que requiere el servicio proporcionado por la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico y que han aceptado explícita o implícitamente sus términos y condiciones.
ASN.1	A la versión 1 de Abstracts Syntax Notation (Notación Abstracta de Sintaxis).
Clave Publica	A la cadena de bits perteneciente a una entidad particular y susceptible de ser conocida públicamente, que se usa para verificar las firmas electrónicas de la entidad, la cual está matemáticamente asociada a su clave privada.
Clave privada	A la cadena de bits conocida únicamente por una entidad, que se usa en conjunto con un mensaje de datos para la creación de la firma digital, relacionada con ambos elementos.
Certificado Digital	Al mensaje de datos firmado electrónicamente que vincula a una entidad con una clave pública
Contrato	Al acuerdo de voluntades que crea o transfiere derechos y obligaciones
Convenio	Al acuerdo de voluntades que crea, transfiere, modifica o extingue derechos y obligaciones
Constancia	Al mensaje de datos representado en formato ASN.1
Criptografía	Al conjunto de técnicas matemáticas para cifrar información.
Destinatario	A aquella entidad a quien va dirigido un mensaje de datos
Emisor	A aquella entidad que genera y transmite un mensaje de datos
Entidad	A las personas físicas o morales.
Expediente electrónico	Al mensaje de datos representado en formato ASN.1,
Firma electrónica	A los datos en forma electrónica consignados en un mensaje de datos, o adjuntados, o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que dicho firmante aprueba la información recogida en el mensaje de

TÉRMINO	DEFINICIÓN
	datos. La firma electrónica establece la relación entre los datos y la identidad del firmante
Formato	A la secuencia claramente definida de caracteres, usada en el intercambio o generación de información
Legislación	A las normas jurídicas generales y abstractas emanadas del Congreso de la Unión, así como la normatividad emanada del Poder Ejecutivo.
Tamaño de la muestra	Es el número de mensajes de datos que compone la muestra extraída del total de mensajes de datos

6 Identificación del Documento de Declaración de Prácticas de la Autoridad de Digitalización que funge como Tercero Legalmente autorizado

Nombre del documento	Declaración de Prácticas de Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico de conformidad con la NOM 151-SCFI-2016
Versión del documento	1.4
Autor	SeguriData Privada S.A. de C.V.
Estado del documento	Autorizado
Fecha de emisión	27 agosto 2019
Fecha de inicio de uso	Sin determinar
Fecha de expiración	No es aplicable
Identificador Digital de Objetos – OID (Object Identifier Digital)	2.16.484.101.10.316.100.5.1.6.2.1

Localización (URL) de la Política de Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico	https://psc.seguridata.com/TLA
Declaración de Prácticas Asociada	Política de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico de conformidad con la NOM 151-SCFI-2016

El servicio de Digitalización de documentos en soporte físico, está disponible para personas físicas y morales (a través de un representante legal) que requieran digitalizar documentos en soporte físico bajo el cumplimiento del artículo 95 bis 1 del Código de Comercio

7 Administración del Documento Declaración de Prácticas de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico

Responsable de la Administración de la DECLARACION DE PRÁCTICAS de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico	
Nombre	SeguriData Privada S.A. de C.V.
Correo electrónico	autoridad-TLA@seguridata.com
Dirección	Insurgentes Sur 2375 Piso 3 Colonia Tizapán, Delegación Álvaro Obregón. C.P. 01000, México, Distrito Federal.
Teléfono	(55) 3098-0700
Fax	(55) 3098-0702

Persona de Contacto	
Nombre	Auxiliar informático de Seguridad
Correo electrónico	oficial.seguridad@seguridata.com
Dirección	Insurgentes Sur 2375 Piso 3 Colonia Tizapán, Delegación Álvaro Obregón. C.P. 01000, México, Distrito Federal.

7.1 Determinación de Cambios en esta DECLARACION DE PRÁCTICAS de Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico y su Publicación.

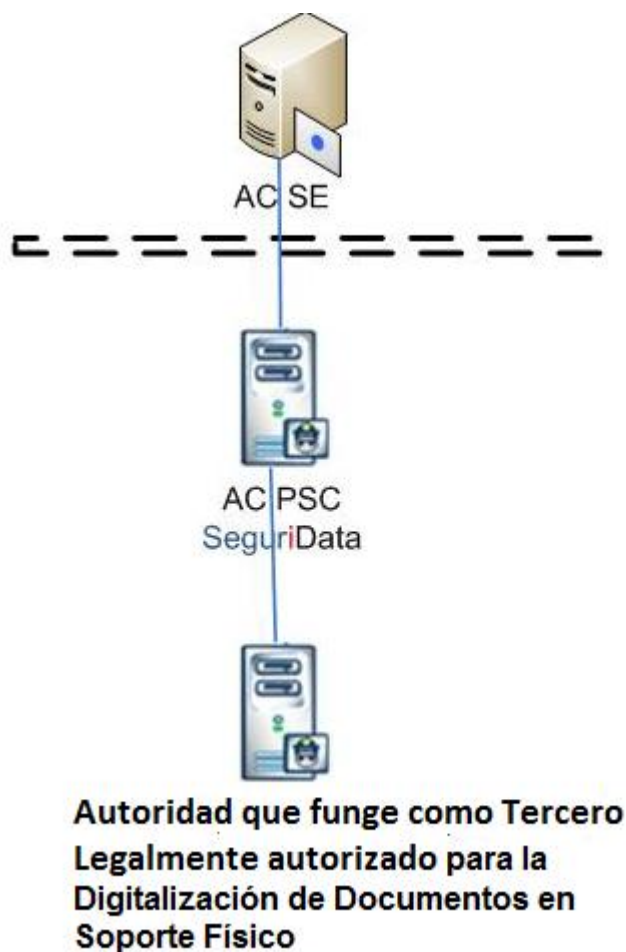
Las modificaciones propuestas o las nuevas aportaciones a incluir en esta DECLARACION DE PRÁCTICAS, deberán, previa a su aprobación, ser contrastadas con la Declaración definida, a fin de asegurar que sean soportados estos cambios.

No se podrán realizar cambios que no sean soportados por la Declaración de prácticas de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico. Deberá, en todo caso, contemplarse una actualización de dicha Declaración.

La presente Declaración de Prácticas de Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico se publica, en el sitio WEB del PSC SeguriData.

8 Estructura Jerárquica

La estructura Jerárquica está conformada por



La representación esquemática de los componentes involucrados en el servicio de Digitalización de documentos en soporte físico fungiendo como tercero legalmente autorizado de acuerdo a la NOM-151-SCFI-2016, se muestra a continuación:

8.1 Participantes en el Servicio de Digitalización de documentos en soporte físico fungiendo como Tercero Legalmente autorizado de conformidad con la NOM 151 SCFI 2016

8.1.1 Autoridad Certificadora SeguriData

Es la entidad acreditada por la Secretaría de Economía para ofrecer el servicio de Expedición de Certificados Digitales a las personas que lo requieran

8.1.2 Autoridad de Sellos Digitales de Tiempo

Es la entidad acreditada por la Secretaría de Economía para ofrecer el servicio de Sellos digitales de tiempo a las personas morales y/o físicas, que lo requieran

8.1.3 Autoridad de Constancias de Conservación de Mensajes de Datos NOM 151 SCFI 2016

Es la entidad acreditada por la Secretaría de Economía para ofrecer el servicio de emisión de Constancias de conservación de mensajes de datos a las personas morales y/o físicas, que lo requieran.

8.1.4 Secretaría de Economía

Es un órgano de la Administración Pública Federal Centralizada que coordina y actúa como Autoridad Certificadora y Registradora, respecto de los Prestadores de Servicios de Certificación.

8.1.5 Autoridad que funge como tercero Legalmente Autorizado en el proceso de Digitalización de Documentos en Soporte Físico de conformidad con la NOM 151 SCFI 2016

Autoridad acreditada por la Secretaría de Economía para fungir como Tercero Legalmente autorizado en el proceso de Digitalización de documentos en soporte físico de conformidad con la NOM 151 SCFI 2016

8.1.6 Clientes-Usuarios Comerciantes

A las personas físicas o morales que requieren los servicios proporcionados por la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico y que han aceptado explícita o implícitamente sus términos y condiciones.

8.1.7 Administrador del Servicio de Digitalización de documentos en soporte físico fungiendo como Tercero Legalmente autorizado

El administrador del servicio se ubica en las oficinas de SeguriData Privada S.A. de C.V. en Insurgentes Sur 2375 Piso 3, Colonia Tizapán, Delegación Álvaro Obregón, en México, Distrito Federal.

La misión del administrador es realizar las funciones de asistencia a la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico de SeguriData Privada SA de CV. en los procedimientos y trámites relacionados con los solicitantes para su identificación, registro y autenticación, de su identidad.

8.1.8 Digitalizador

Es el ente que realiza la digitalización de documentos en soporte físico, previamente auditado por el TLA en el cumplimiento de las reglas definidas en el título 8 de las reglas de PSC

8.1.9 Fedatario

Persona autorizada para dar fe sobre el proceso de digitalización, es opcional a petición del comerciante.

9 Obligaciones y Responsabilidades

9.1 Obligaciones de la Autoridad que funge como tercero Legalmente Autorizado para el proceso de Digitalización de Documentos en Soporte Físico

- El tercero legalmente autorizado, debe asegurar que todos los requerimientos están implementados de acuerdo a lo establecido en la NOM-151-scfi-2016, en lo concerniente a la Digitalización de documentos en soporte físico.
- La Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico debe proporcionar todos sus servicios en forma consistente y como lo establece la Declaración de prácticas de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico.
- La Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico debe atender las solicitudes de servicio de acuerdo a los términos y condiciones establecidas en el convenio suscrito por ambas partes, incluyendo los niveles de servicio, la disponibilidad y la exactitud de su servicio.
- La Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico debe verificar la identidad de los solicitantes del Servicio de Digitalización de documentos en soporte físico fungiendo como Tercero Legalmente

autorizado de acuerdo a lo establecido en la Declaración de prácticas de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico.

- Debe contar con la infraestructura necesaria que brinde disponibilidad y acceso permanente al servicio de Digitalización de documentos en soporte físico fungiendo como Tercero Legalmente autorizado.
- La Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico se compromete a guardar y cumplir estrictamente con la seguridad y confidencialidad de la información de los clientes, garantizando dicho cumplimiento por parte del personal que interviene en el servicio; de acuerdo a la fracción II del inciso A del artículo 102, fracción V y VII del artículo 104 del Código de Comercio, y último párrafo de la fracción III del Artículo 5, fracción VII y VIII del artículo 27 del reglamento del Código de Comercio en materia de Prestadores de Servicio.
- La Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico deberá controlar en todo momento el Proceso de Digitalización siendo responsable de la verificación respecto a la migración.
- La Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico, firmara un contrato con la Digitalizadora en el que se acuerden las responsabilidades y obligaciones, tanto de la autoridad como de la Digitalizadora y de los clientes, cada vez que se efectué un proceso de digitalización.
- La Autoridad que funge como tercero legalmente autorizado es responsable del proceso completo de Digitalización de documentos en soporte físico, para lo cual es responsable de auditar y validar que el Digitalizador cumple con lo necesario, especificado en el Título 8 de las reglas de PSC en materia de Digitalización de documentos en soporte Físico.
- Mantener y administrar los reportes de cotejo y las actas circunstanciadas de la digitalización de documentos en soporte físico, realizadas.
- Firmar con las llaves de TLA los documentos que se obtengan de la muestra definida
- Firmar un contrato con el Digitalizador, por cada digitalización que sea solicitada por un comerciante
- Someterse a las auditorías periódicas que se establezcan y en su caso cumplir con los requerimientos y recomendaciones que de ellas deriven.
- Seguir la política de privacidad descrita en la Declaración de Prácticas de Digitalización - TLA.
- Seguir las reglas específicas sobre el proceso de Digitalización

9.2 Obligaciones del Comerciante

- El Comerciante debe resguardar sus claves de acceso a usar en el servicio de Digitalización de documentos en soporte físico
- Verificar que el certificado no esté revocado.
- Participar de manera opcional en la Validación de la muestra en función de la determinación del tamaño y tipo de la muestra que permitan realizar un proceso de cotejo de los mensajes de datos resultantes de la digitalización contra los documentos en soporte físico.
- Firmar de manera electrónica los documentos digitalizados, usando el certificado emitido por el PSC para uso exclusivo de firma de documentos en el proceso de digitalización.

9.3 Obligaciones del Administrador del servicio

La Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico de SeguriData Privada S.A. de C.V. asigno a un Administrador para atender:

- Someterse a las auditorías periódicas que se establezcan y en su caso cumplir con los requerimientos y recomendaciones que de ellas deriven.
- Seguir una política de privacidad conforme a la Política de Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico de SeguriData Privada S.A. de C.V.

9.4 Obligaciones del Digitalizador

- Atender las solicitudes de digitalización
- Cumplir con el plan de gestión de calidad definido por el TLA
- Firmar el contrato con el TLA por cada servicio de digitalización
- Mantener la medida de seguridad definidas en la Política de seguridad

9.5 Responsabilidad de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico

La responsabilidad está limitada exclusivamente a proveer el Servicio de Digitalización de documentos en soporte físico fungiendo como Tercero Legalmente autorizado de acuerdo a lo establecido en la Declaración y en la Política de Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico.

La Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico no será responsable de manera enunciativa más no limitativa en los siguientes casos:

- Por cualquier tipo de daños y/o perjuicios que sufran sus clientes, siempre que éstos deriven de la indebida utilización de los servicios por parte de dichos clientes.
- Por cualquier tipo de daños y/o perjuicios que sufran sus clientes, siempre que estos deriven del incumplimiento de las obligaciones del cliente.
- Por los daños y/o perjuicios de la errónea interpretación, análisis, síntesis o conclusión a que los clientes del Servicio de Digitalización de documentos en soporte físico en el uso del servicio, sin que estas hayan sido confirmadas expresamente por la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico.
- Por los daños y/o perjuicios que se causen, si el cliente entrega datos y/o documentos falsos, para la obtención del servicio de Digitalización de documentos en soporte físico fungiendo como Tercero Legalmente autorizado
- Por la interrupción o alteración temporal del servicio por causas ajenas a la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico, como pueden ser de manera enunciativa más no limitativa, condiciones climatológicas adversas, sismos, inundaciones, fallas en la energía eléctrica, fuego, actos vandálicos, huelgas, cualquier otro motivo que afecte sus instalaciones o limiten la libertad en las comunicaciones.

Y la autoridad que funge como tercero legalmente autorizado, será responsable de:

- De la verificación que realice, respecto de la migración y firmara el mensaje de datos que resulte de dicho proceso, siempre y cuando constate que la migración se realizó de manera íntegra e inalterable tal y como se generó por primera vez en su forma definitiva.
- Por cada proceso de digitalización el Tercero legalmente autorizado deberá firmar un contrato con la Digitalizadora en el que se acordaran sus responsabilidades y obligaciones, así como los de la Digitalizadora y usuarios.
- Presentar y mantener el Modelo operacional y la Declaración de Prácticas de cada proceso de digitalización.
- Tiene la responsabilidad de notificar a Secretaría de Economía, en caso de que la muestra revisada no coincida con los documentos en soporte físico, y a la vez levantar un acta ante el Ministerio Público.

Es importante mencionar que, si la muestra es rechazada porque la calidad de la imagen no está dentro de la gestión de calidad, el proceso de digitalización se repite y no hay necesidad de notificar a Secretaría de Economía o de levantar un acta ante el Ministerio Público.

En general el TLA tiene la responsabilidad de validar el proceso completo de Digitalización:

- a) La contratación del servicio
- b) La recolección de documentos
- c) La digitalización de documentos: Preparación, digitalización, validación de muestra
- d) La firma de documentos digitalizados
- e) La emisión de la constancia de conservación de mensaje de datos
- f) La entrega al comerciante o destrucción de los documentos digitalizados

Todas las marcadas en el título 8 Digitalización de documentos en soporte físico como TLA de las reglas que deben cumplir los PSC.

9.6 Responsabilidad del Cliente- Comerciante

- Conservar los documentos digitalizados
- Usar el certificado PSC únicamente para firma de documentos digitalizados

9.7 Responsabilidad del Administrador

- Proporcionar el servicio para la contratación del Servicio de Digitalización de documentos en soporte físico fungiendo como Tercero Legalmente autorizado

9.8 Responsabilidad del Fedatario

- Validar la muestra obtenida de la digitalización de documentos y firmar

10 Fecha de Inicio de Operaciones como TLA

Una vez que la Secretaría de Economía otorgue la acreditación a SeguriData privada, iniciara sus operaciones como TLA en conjunto con el Digitalizador definido.

11 Publicación y Consulta de Información

11.1 Consulta de Información del Servicio de Digitalización de documentos en soporte físico fungiendo como tercero legalmente autorizado

La Autoridad, es responsable de poner a disposición del público en general, la información relacionada con el servicio de Digitalización de documentos en soporte físico fungiendo como Tercero Legalmente autorizado, a través del sitio WEB del PSC SeguriData.

11.2 Publicación de Certificado Digital de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico

El Certificado Digital de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico, se publica en el sitio WEB del PSC SeguriData y en el de la Secretaría de Economía, para que los clientes puedan verificar la integridad y la autenticidad de dicho certificado.

12 Ciclo de Vida de la Administración de Claves de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico

La Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico, cuenta con una clave pública y una clave privada, dichas claves tienen un ciclo de vida comprendido desde la generación, protección, resguardo y distribución, vigencia y renovación

12.1 Generación de Claves de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico de SeguriData Privada.

La Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico de SeguriData Privada debe asegurar que cualquier clave criptográfica esté generada bajo circunstancias controladas.

La generación de las claves de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico deben ser generadas en un ambiente físicamente seguro, por personal con roles de confianza.

La generación de las claves de firma de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico debe llevarse a cabo dentro de un módulo de seguridad de hardware criptográfico que cumpla con los requerimientos identificados en FIPS 140-2.

El algoritmo de la generación de las claves de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico, la longitud de la clave resultante y el algoritmo usado para firmar el mensaje de datos, deben ser aprobados por la Secretaría de Economía.

12.2 Protección y resguardo de las Claves Privadas de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico

La Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico de SeguriData Privada debe asegurar que se mantenga en todo momento la confidencialidad e integridad de sus claves privadas.

Las claves privadas de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico deben mantenerse y usarse dentro de un módulo criptográfico que cumpla con los requerimientos de estándar FIPS 140-2 nivel 3

El módulo criptográfico se debe mantener en instalaciones físicamente seguras y el acceso debe estar protegido por mecanismos de control de acceso.

Las claves privadas que sean respaldadas, deben ser almacenadas y recuperadas solamente por personal con roles de confianza, usando, el control mancomunado en un ambiente físicamente seguro.

El personal autorizado para llevar a cabo estas funciones debe cumplir con las actividades establecidas por las Prácticas de la Autoridad que funge como Tercero Legalmente autorizado. Las copias de respaldo de las claves privadas deben ser protegidas para asegurar su confidencialidad e integridad.

Las llaves con las que contara el TLA subordinadas a la autoridad de Secretaria de Economía, se encontraran resguardados en un **dispositivo HSM NSHIELD 500 DE USO EXCLUSIVO PARA EL Servicio de PSC como TLA.**

El anexo 5 presenta el procedimiento para la generación de nuevas claves. Para la generación de nuevas claves es necesario solicitarlo a la Secretaria de Economía con al menos 10 días de anticipación.

Responsabilidades:

Las actividades se llevan a cabo por el administrador de sistemas en conjunto con el operador de sistemas; participan los propietarios de las tarjetas definidas para el arranque y administración del HSM

Las medidas de seguridad para los accesos deben ser autorizadas y vigiladas por el profesional informático y el auxiliar de apoyo informático de SeguriData para el servicio de TLA.

12.3 Distribución de las Claves Públicas de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico

La Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico de SeguriData Privada debe asegurar que la integridad y la autenticidad de las claves de verificación de firma de Mensajes de Datos se mantienen seguras durante su distribución.

Los Certificados Digitales de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico SeguriData Privada se deben publicar en el sitio Web y de la Secretaría de Economía, para que los clientes puedan verificar la integridad y la autenticidad de los Tercero Legalmente Autorizado que emita la Tercero Legalmente Autorizado de SeguriData Privada

La Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico SeguriData Privada debe tener implementadas políticas y controles.

12.4 Renovación de las Claves Criptográficas de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico

El Certificado de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico, no debe ser utilizado más allá del período de tiempo que el algoritmo de firma y la longitud de la clave elegida se reconozca que siguen siendo confiables para firmar los mensajes de datos. De igual forma no debe ser utilizado más allá del periodo de vigencia del mismo

En cualquiera de estas condiciones se debe proceder a emitir nuevas claves de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico e incorporarlas al ambiente productivo, ya que SeguriData no usa ni recomienda la renovación.

12.5 Fin del Ciclo de Vida de las Claves de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico

La Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico de SeguriData Privada debe asegurar que sus claves privadas no puedan ser utilizadas después de su expiración o vigencia.

Se asegura que nuevas claves entren en operación cuando las claves de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico SeguriData Privada expiren

Se asegura la Expedición de nuevas claves antes de que éstas expiren, o cuando se vea comprometida su confidencialidad.

12.6 Ciclo de Vida del Módulo Criptográfico – Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico de SeguriData Privada

La Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico SeguriData Privada debe garantizar la seguridad del hardware criptográfico para la administración, almacenamiento y uso de su clave privada de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico, que se encuentra en el dispositivo nShield 500. Como parte de la administración del ciclo de vida de los dispositivos criptográficos.

El hardware criptográfico que firma los Mensajes de Datos de la digitalización de los mensajes en soporte físico, debe estar funcionando correctamente y bajo condiciones que garanticen la integridad de las claves privadas de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico.

12.6.1 Ciclo de Vida productos Thales

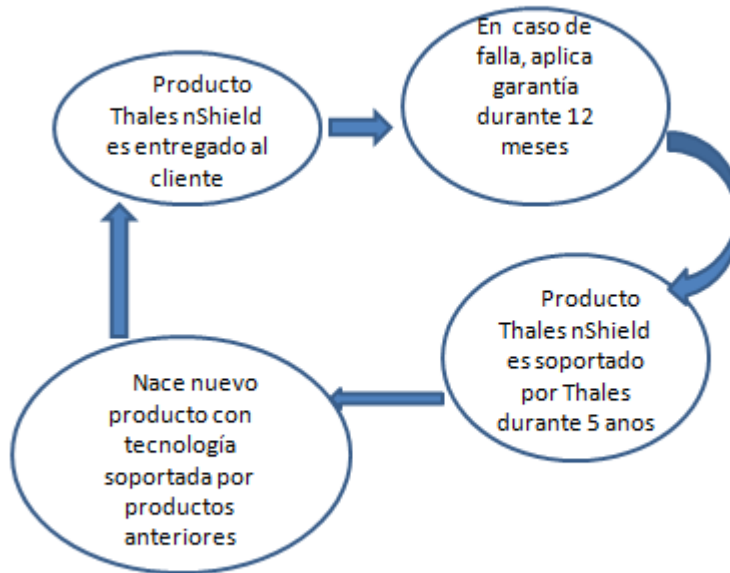
Thales garantiza que sus productos funcionarán sustancialmente. Dicha garantía es válida por un período de doce (12) meses a partir de la fecha de entrega en el caso de hardware. En caso de que la funcionalidad del producto sea materialmente deteriorada en virtud de los defectos de fabricación, THALES se obliga a reparar o reemplazar el producto afectado de forma inmediata, 1 semana como máximo.

El ciclo de vida de los productos se da en función del siguiente esquema de soporte



El ciclo de vida de los productos está en función del soporte de 5 años a partir de su lanzamiento, asegurando la compatibilidad con los nuevos modelos, para el caso del nShield, su ciclo de vida es al año 2023, con la garantía de que su funcionamiento se continúa soportando hacia los nuevos modelos.

CICLO DE VIDA PRODUCTOS DE THALES nShield



13. Proceso para otorgar y contratar el Servicio de Digitalización de documentos en soporte físico - Generalidades

13.1 Proceso para Solicitar un Servicio de Digitalización certificada. Contratación del Servicio de Digitalización

En función de la regla 176 de las reglas generales a las que están sujetos los Prestadores de Servicios de Certificación, por cada proceso de digitalización el Prestador de Servicios de Certificación deberá firmar un contrato con el comerciante, en el que se acordarán sus responsabilidades y obligaciones, así como los usuarios, lo anterior conforme al Modelo Operacional y la Declaración de Prácticas de cada proceso de digitalización.

Para dar cumplimiento a la regla anterior, se sigue un proceso para la contratación del servicio de Digitalización, mencionando como temas importantes la firma electrónica avanzada de los contratos del TLA con Digitalizador y de TLA con comerciante, o bien la firma autógrafa.

Para el esquema en que los contratos que se firmen con firma electrónica avanzada se realizará la emisión de un certificado PSC para el comerciante y para el Digitalizador, siguiendo lo indicado en

la Política de Certificación de SeguriData Privada como PSC, adicionando una carta donde se establezca la emisión del certificado únicamente para fines de firma en el Proceso de Digitalización.

Los contratos pueden ser firmados usando certificados del SAT por parte del comerciante y del Digitalizador, observando que estos certificados del SAT nunca están en resguardo del TLA, el comerciante y el digitalizador los usan para firmar el contrato una sola vez.

Los contratos antes mencionados, serán contratos tipo marco, definidos por el TLA donde únicamente se llenen las partes faltantes en función de los datos del comerciante y del digitalizador, así como las características de la Digitalización como:

1.- Tipo de documentos a digitalizar: se especifica si son originales, si son fotocopias simples o son copias certificadas, si son documentos vinculados, si alguno de los documentos requiere restauración, si algún documento requiere algún tratamiento especial como un plástico. Con esto se podrá identificar los documentos a digitalizar

2.- Volumen de documentos: Cantidad de documentos a digitalizar

3.- Tipo de muestreo definido (el Digitalizador está preparado con los 3 tipos de muestreo señalados en la regla 227 de las Reglas que deben cumplir los PSC título 8: Muestreo aleatorio simple, Muestreo aleatorio sistemático, Muestreo aleatorio estratificado)

3.- Sitio donde se recogen los documentos a digitalizar

4.- Opción de devolución de documentos o destrucción de los mismos y sitio de devolución en caso de optar por esta opción.

5.- Opción de incluir en el proceso de digitalización al Fedatario

6.- Opción de que el comerciante participe en la revisión de la muestra

7.- Periodo de inicio y finalización de la digitalización de documentos.

Los machotes del contrato se DEFINEN EN EL Modelo Operacional.

13.1 1 Proceso de: Contratación del Servicio de Digitalización

1.- El comerciante establece las necesidades de Digitalización en conjunto con el TLA y el Digitalizador (Tipo de documentos, volumen, identificador de documento, fechas, ubicación dónde se recogen documentos en físico, etc., documento **anexo 1 contrato marco**)

2.- El TLA como prestador de servicios de certificación, emite llaves PSC al comerciante para la firma de los documentos digitalizados, con una cláusula de uso exclusivo para el proceso de digitalización. **Anexo 3 carta de uso exclusivo de certificados PSC**

3.- El TLA formaliza el contrato con el comerciante, especificando el alcance del proyecto y las definiciones realizadas en el punto 1. Firmando el contrato, lo puede hacer con llaves de firma electrónica avanzada o bien de manera autógrafa, de acuerdo a la preferencia del comerciante.

4.-Si la firma es con firma electrónica avanzada:

a) El digitalizador ingresa al portal de firma del TLA y firma el contrato con las llaves PSC o con llaves del SAT, a continuación, el comerciante firma el contrato con las llaves PSC emitidas en el punto 2 de uso exclusivo para la digitalización certificada o con llaves del SAT., proporcionan tanto las llaves como el password al momento de la firma.

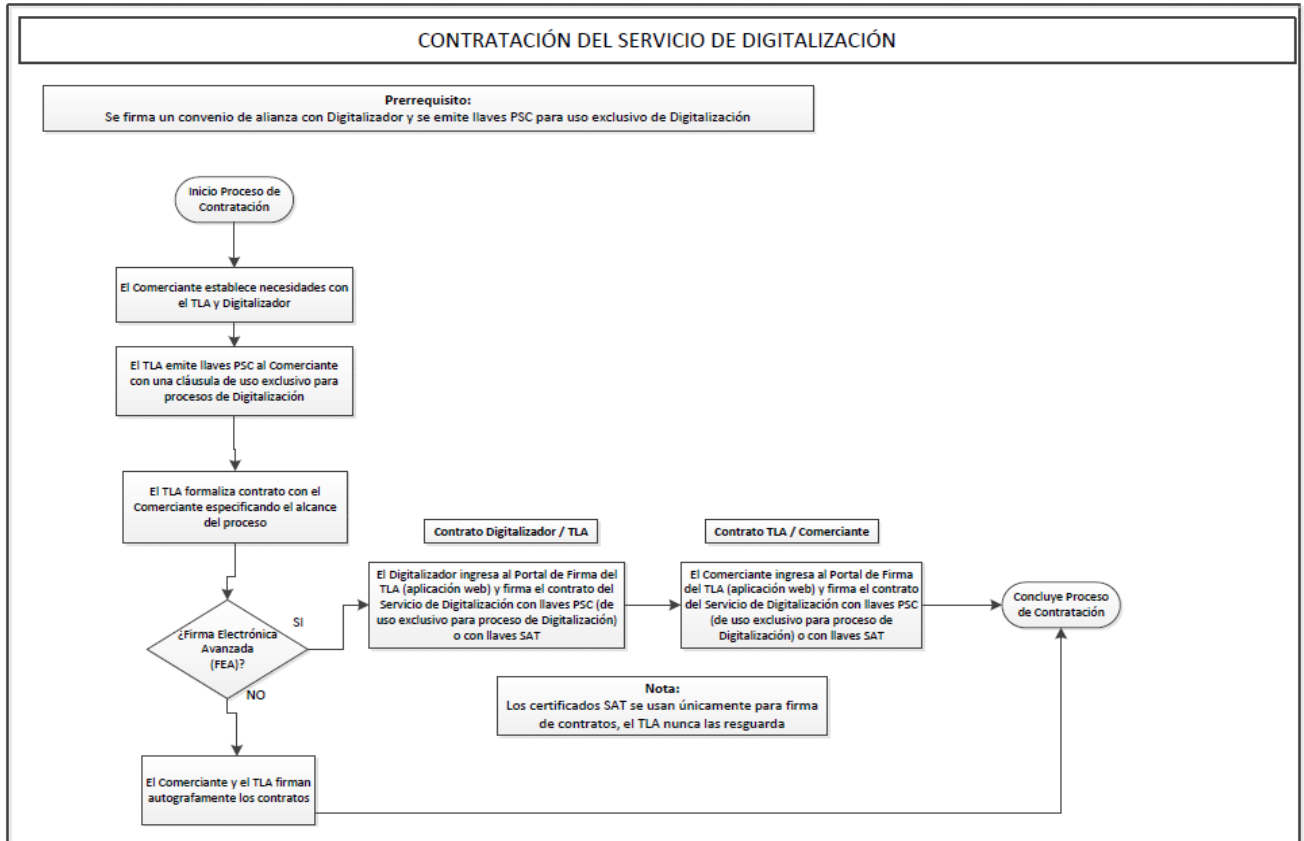
El digitalizador y el comerciante, mediante usuario y password ingresan a la plataforma del TLA para la firma de contrato.

El comerciante firma contrato de servicio de digitalización con el TLA, proporcionando su par de llaves y el password.

El digitalizador firma contrato de servicio con TLA. Proporcionando su par de llaves y el password.

TLA firma con sus llaves resguardadas en el HSM y proporciona su password

A continuación, el diagrama del proceso de Contratación del Servicio de Digitalización:



13.2 Proceso de Recepción - Recolección de documentos a digitalizar

En el contrato con el comerciante firmado con el TLA, el comerciante, especifica el sitio donde se recolectan los documentos a digitalizar, para ser llevados a las oficinas del Digitalizador.

Para la recolección de documentos, **se manejan elementos de seguridad** como:

- Formato de relación de documentos donde se relacionan los documentos a recolectar, asignando un control de los mismos. Ver formato **anexo 9**
- Bolsas de seguridad con cintas de seguridad
- Identificación de las bolsas de seguridad con datos del comerciante.
- Firma autógrafa del comerciante y del digitalizador de recepción y entrega de documentación.
- Firma autógrafa de la entrega de la bolsa de seguridad en las oficinas del digitalizador validando revisión de etiqueta de seguridad no violada a través de CCTV (Circuito cerrado de televisión)

f) Validación de documentos contra formato

En caso de alguna diferencia en la validación de documentos vs formato, se realiza la notificación al comerciante vía correo electrónico, esperando la respuesta de aprobación del comerciante para proseguir con el proceso de digitalización, considerando la diferencia de documentos reportada.

Si el comerciante no aprueba, se devuelven los documentos bajo el Proceso de devolución de documentos al comerciante y concluye el proceso.

A continuación, los pasos de este proceso:

1.- De acuerdo al contrato firmado en el proceso de contratación, se realiza la recolección de documentos en físico, en el lugar definido por el comerciante

2. El digitalizador acude con el comerciante al sitio indicado, llevando un formato (FormatoRecepcion-entrega.pdf) que indica el número de documentos a recolectar y la forma de control de los mismos.

3.- El digitalizador recibe los documentos y en presencia del comerciante los introduce en Bolsas de seguridad que son cerradas con cintas de seguridad. Identificando la bolsa con los datos del comerciante.

4.- El digitalizador y el comerciante firman de manera autógrafa la recepción de los documentos en físico.

5.- El digitalizador realiza el traslado de los documentos en físico a sus oficinas

6.- Al arribar a las oficinas del digitalizador, en el Centro de distribución se verifica que las bolsas de seguridad y/o valija con cintillo, tengan las cintas de seguridad y /o cintillo sin ser violadas, esto a la vista de un sistema de CCTV

7.- El centro de distribución sella de recibido el formato de recepción- entrega (anexo 9), lo introduce en una caja de plástico y lo entrega al área de control documental.

8.- El área de control documental revisa las bolsas y si detecta algún tipo de violación, realiza un reporte en Excel con los folios que presentan alguna anomalía e introduce en una bolsa etiquetada como ANOMALIAS LAS bolsas detectadas, y elabora un reporte en Excel con los folios de bolsas sin anomalía.

9.- Las bolsas las deposita en el contenedor de plástico y cierra el contenedor con un cintillo, además de agregar una etiqueta al contenedor que contiene los datos de:

Área de entrega: Digitalización de Documentos en soporte físico de conformidad con la NOM 151-SCFI 2016

Fecha

Número de lote

Numero de corte

Confidencial

SeguriData Privada S.A. de C.V.

Página 32 de 88

2022

Cantidad de documentos

Folio inicial del contenedor

Numero de entrega

Adicional se tiene una bitácora de envió, donde se tienen los datos para la distribución del contenedor, y se traslada al área de Mesa de Control en un vehículo.

En paralelo se envía vía correo electrónico en un archivo formato Zip encriptado con password, los reportes en Excel, al área de mesa de control.

10.- El contenedor llega a Mesa de control (cabe mencionar que por seguridad, existe un tiempo estimado entre la salida del contenedor de control documental y la llegada a mesa de control. Si excede el tiempo estimado, mesa de control se comunica a control documental para reportar).

9.- En caso de existir diferencias:

- a) El área de operaciones del digitalizador levanta acta de información incompleta y notifica a comerciante vía correo electrónico

Si el comerciante está de acuerdo con la diferencia reportada, se obtiene autorización y finaliza este proceso y continúa con el proceso de digitalización.

- b) En caso de que el comerciante no esté de acuerdo con la diferencia, el digitalizador devuelve los documentos al comerciante (proceso de devolución de documentos), y no se realiza la digitalización

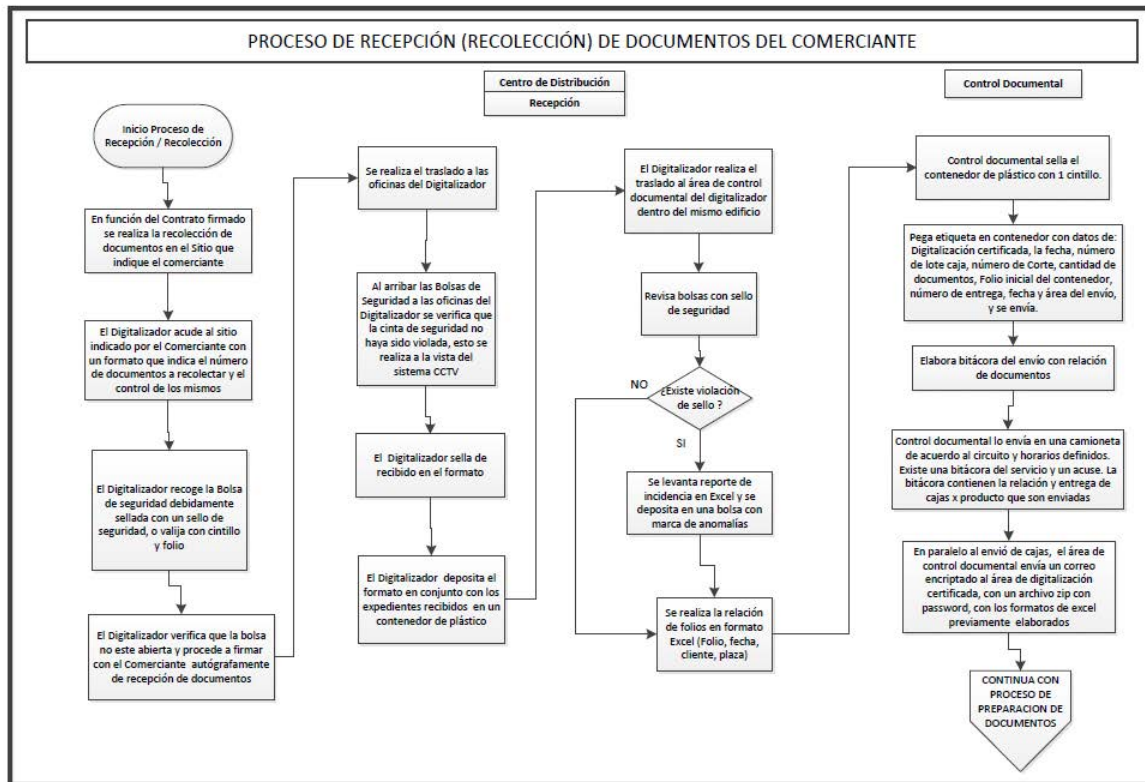
El formato de recepción entrega de documentos en soporte físico, se muestra en el **Anexo 9**

En este punto inicia la CADENA DE CUSTODIA DE LOS DOCUMENTOS EN SOPORTE FISICO.

La responsabilidad de la custodia es en primera instancia es de:

- a) El cliente al realizar la entrega
- b) El digitalizador al recibir los documentos en soporte físico

El registro de la fecha y hora para esta etapa, se da con el formato de entrega y recepción de documentos donde se asienta de manera manual los datos de fecha y hora de la recepción y entrega de documentos en soporte físico.



13.3 Resguardo para la protección de la documentación en soporte físico

Una vez que los documentos son recibidos por el digitalizador en sus instalaciones, y que se validó lo entregado contra lo recibido, el resguardo y protección de los documentos en soporte físico a digitalizar, se da como sigue:

El Digitalizador resguarda los documentos en un lugar cerrado donde el acceso está limitado por dos niveles de control, uno en el acceso principal del digitalizador y otro en el acceso al área de trabajo de digitalización, los accesos se dan con tarjetas de proximidad solo proporcionadas al personal autorizado.

El personal con acceso al área de trabajo de digitalización, no pueden ingresar teléfonos celulares, ni alimentos, ni pertenencias personales, estos se resguardan en un locker antes de ingresar al área de trabajo de digitalización.

Los documentos a digitalizar, siempre están a la vista de los operadores que se encuentran ejecutando la función, con un supervisor de cada turno.

Los documentos que ya fueron escaneados son resguardados bajo llave, la llave está en resguardo del supervisor de cada turno, en tanto se concluye con la digitalización y son devueltos al comerciante o destruidos en caso de ser requerido de esta manera en el contrato de servicio.

Las medidas de seguridad para proteger la documentación de cualquier eventualidad como un incendio o algún riesgo de destrucción son mencionadas en el siguiente apartado.

13.3.1 Medidas de protección de la documentación en soporte físico

Las Medidas de protección a nivel seguridad son:

- 1) Control de acceso autorizado: El área donde se realiza el resguardo de documentos en soporte físico a digitalizar es un área cerrada con una puerta donde se accede con tarjetas de control en posesión exclusiva del personal que ahí labora. Previa a esta puerta existe otra puerta de acceso a las instalaciones donde se accede con una tarjeta de control.
- 2) Detectores de humo: Se tienen detectores de humo en el área de digitalización
- 3) Detectores de movimiento: Se tienen detectores de movimiento
- 4) Se tiene equipo cerrado de televisión, monitoreado las 24 horas
- 5) Se prohíbe el acceso de teléfonos celulares
- 6) Se prohíbe el acceso de alimentos
- 7) Resguardo de documentos bajo llave en archiveros

La CADENA DE CUSTODIA DE LOS DOCUMENTOS EN SOPORTE FISICO.CONTINUA CON:

- c) EL AREA DE OPERACIONES DEL DIGITALIZADOR RESGUARDA LOS DOCUMENTOS A DIGITALIZAR

El registro de la fecha y hora para esta etapa, se da con el formato de entrega y recepción de documentos en soporte físico al área de operaciones del Digitalizador quien anota en el formato la fecha y hora en que se ingresan los documentos.

13.3.2 Restauración del documento en soporte Físico

La restauración de documentos se realiza solo en caso de que el comerciante lo autorice y solicite en el contrato, y es solamente la obtención de una fotocopia del documento original, para que esta sea digitalizada, cumpliendo con el control de calidad y las medidas de seguridad establecidas, como lo es el metadato asociado.

13.4 Preparación de documentos

Las acciones para la preparación de los documentos incluyen:

- 1 Llegan los documentos en el contenedor con cintillo a la mesa de control
- 2 Mesa de control abre contenedor y valida que el sello no este violado,
- 3 Revisa folios contra la bitácora y contra el reporte en Excel enviado
- 4 Realiza entrega de bolsas al área de Digitalización de Documentos en soporte físico de conformidad con la NOM 151-SCFI 2016 junto con los reportes en Excel

Área de Digitalización de Documentos en soporte físico de conformidad con la NOM 151-SCFI 2016

- 1 Se valida que los folios coincidan
- 2 se procede a abrir las bolsas y a validar las que están violadas, realizando acta de hechos y reporta a TLA SeguriData
- 3 Se revisa de acuerdo a la especificación de digitalización el tipo de documentos y la calidad de los mismos
4. Si se detectan anomalías levanta acta de hechos y reporta a TLA SeguriData
5. Valida tipo de documento contra lo que se tiene. Para la evaluación de la calidad y capacidad del documento, se toman en cuenta:

- 1) Evaluación de la capacidad del documento original para soportar el proceso de digitalización como:

El digitalizador valido la calidad del papel, verificando si tiene:

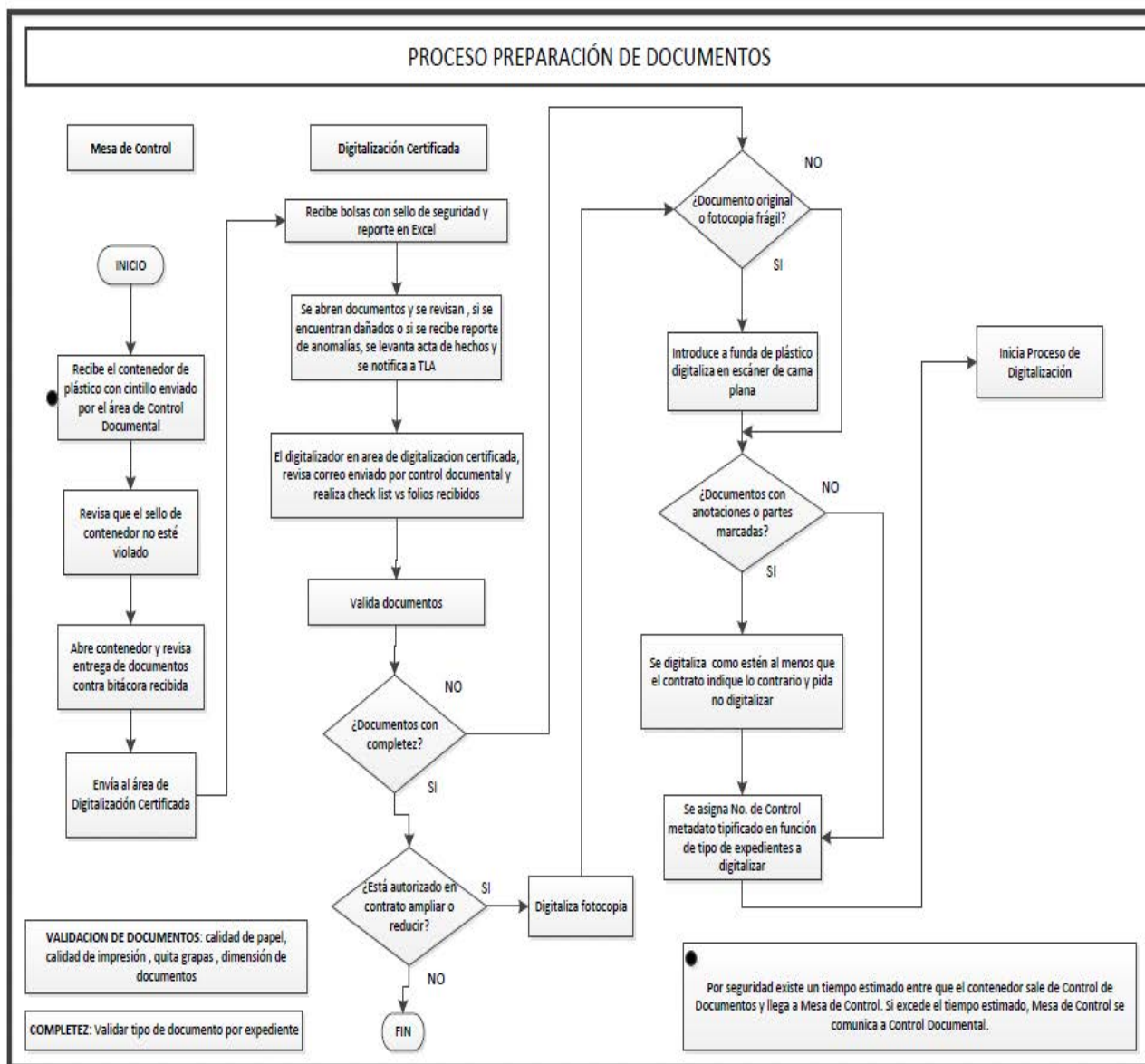
-arrugas

-Quita las grapas

-Verifica los atributos del contenido informativo: claridad de los gráficos

- 2) El digitalizador verifica las dimensiones no normalizadas , y en función de las necesidades especificadas en el contrato del servicio, procede a ampliar o reducir , digitalizando la fotocopia
- 3) El digitalizador valida si un documento original o fotocopia es frágil, lo introduce en una funda de plástico para salvaguardar el documento
- 4) Manejo de documentos originales que contengan anotaciones escritas a mano, pintura blanca opaca u otro tipo de líquido corrector, cinta, emblemas o áreas resaltadas
Este manejo, está de acuerdo al contrato con el cliente se valida el tratamiento: Escaneado tal como se presenta el documento, o bien, no se escanean y se separan de los documentos a escanear, marcándolos en el formato de recepción. FORMATO-RECEPCION-ENTREGA.PDF (ANEXO 9)
- 5) Distinguir entre documentos originales en papel y fotocopias
El manejo es a través de un número de control con una nomenclatura diferente para un documento original, una copia certificada y una fotocopia
- 6) La asignación de vínculos entre documentos asociados que vayan a contemplarse como un solo elemento, de modo que la imagen digitalizada pueda representar fielmente el documento original
 - Un documento y una nota autoadhesiva adherida;
 - Un documento con un adjunto,
 - Un documento impreso a ambas caras del papel o que contenga anotaciones al Dorso

- La asignación de un folio con una nomenclatura definida para este tipo de documentos
- 7) La asignación de vínculos entre el documento original y la copia digitalizada.
Mediante protocolos de identificación. Folio con una nomenclatura específica, el cual se define en el anexo del contrato, mostrado en el anexo 2, y se hace en función de las necesidades del cliente para realizar una identificación rápida de lo digitalizado, por ejemplo:
Para un expediente de crédito:
Este contenido por: ine, comprobante de domicilio, contrato firmado
Seria: nombre del cliente, tipo de documento, fecha
- 8) La comprobación y la verificación de que todos los documentos originales se han incluido en el proceso de digitalización; SE REALIZA MEDIANTE EL CONTROL DE FOLIOS, VALIDANDO EL NUMERO DE FOLIOS (número de control) de documentos en soporte físico contra los folios de los documentos digitalizados.
- 9) La definición de la clasificación de lotes o grupos de documentos originales aptos para su digitalización al mismo tiempo, se da por:
- Lotes por tamaño
 - Lotes por formato de documentos
 - Lotes por fecha



13.5 Transferencia de documentos en soporte físico a Mensaje de Datos

La imagen digital hereda y es gobernada por los metadatos que describen el proceso de negocio y los que describen las funciones para gestionar los documentos asociados a dicho proceso.

Estos metadatos cumplen el marco de la organización para la gestión de documentos digitales y son coherentes con la Norma ISO 23081-1:2017, y ayudan a la continuidad del negocio.

Los metadatos atribuidos o asociados a imágenes son un componente esencial en la gestión y la recuperación de imágenes.

En este proceso, se generan dos tipos de metadatos:

- a) Los metadatos específicos a la imagen particular y al proceso de creación de imágenes

Los metadatos antes descritos, se asocian de manera automática, (el software de digitalización tiene la función de asociarlos), se generan en el punto de captura digital directamente desde el equipo de digitalización, Y SE HEREDAN AL CONVERTIR LA IMAGEN A FORMATO PDF PARA LA FIRMA DIGITAL

Los metadatos a nivel de imagen incluyen:

- b) un identificador de imagen digital único;
- c) **la fecha y la hora de la digitalización;**
- d) el nombre del agente asociado con el proceso de digitalización; de acuerdo a definición puede ser las iniciales del operador o el nombre de la organización del comerciante
- e) el IDENTIFICADOR del dispositivo de captura (hardware y software); y
- f) la fecha de la última calibración (cuando sea posible, opcional).

El principal objetivo del metadato es el acceso al contenido, para lo cual se definen criterios de indexación y de búsqueda: por fecha, por identificador único, por organización.

13.6 Digitalización

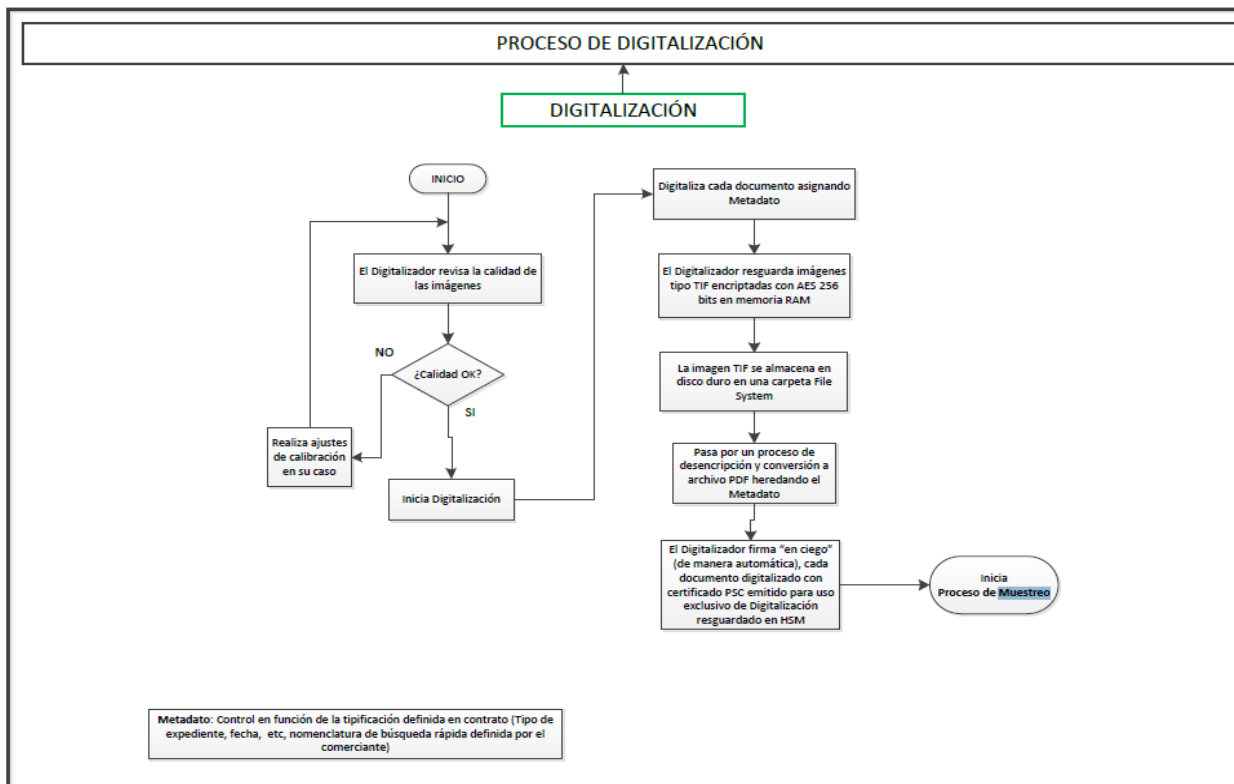
En este proceso se lleva a cabo el escaneo de los documentos previa conclusión de la preparación de los mismos y se cumple con la emisión automática de los metadatos, se procede a obtener la firma electrónica avanzada del Digitalizador, con sus llaves emitidas por un PSC (emitido para uso exclusivo de firma en Servicio de digitalización), resguardado en HSM del TLA, como medida de seguridad adicional al proceso

En este proceso de firma, se solicita una sola vez al digitalizador el password asociado a las llaves resguardadas en el HSM, y se activa el proceso de firma automático.

La firma incluye el sello digital de tiempo emitido por el PSC SeguriData.

- 1.- Digitaliza cada documento asignando un identificador único (folio) y la fecha y hora en que se está digitalizando
- 2.- El digitalizador resguarda cada imagen en formato tif encriptados con AES 256 bits, en memoria RAM
- 3.- La imagen TIF es almacenada en disco duro en una carpeta file system.
- 4.- La imagen TIF, pasa por un proceso de descripción y conversión a formato PDF
- 5.- El digitalizador firma cada documento digitalizado con el certificado PSC emitido para uso exclusivo de digitalización, resguardado en HSM. (En este proceso de firma, se solicita una sola vez al digitalizador su password asociado a las llaves resguardadas en el HSM, y se activa el proceso de firma automático)

La firma del digitalizador incluye un sello de tiempo y un registro en base de datos con la fecha y hora de la transacción.



13.6.1 Revisión de la Muestra

En este paso del proceso, se realiza el cotejo con la muestra a validar, tomando como base el

reporte de la muestra presentado en el **anexo 6**, intervienen el profesional jurídico y el profesional informático del TLA y el digitalizador de manera obligatoria, y de manera opcional un fedatario y el comerciante en caso de Así definirlo en los contratos firmados, como medida de seguridad adicional.

A continuación, se detallan los pasos del proceso de revisión de la Muestra:

1.- Una vez concluido el proceso de digitalización se procede a generar la compulsa con la muestra definida (en función de la regla 227 de las reglas generales a las que están sujetos los Prestadores de Servicio de Certificación), por el digitalizador y el TLA en conjunto con el comerciante.

2.- El digitalizador, el profesional informático y el profesional jurídico del TLA revisan la muestra contra los documentos físicos (Regla 228 de las reglas generales a las que están sujetos los Prestadores de Servicio de Certificación), en las oficinas del digitalizador, de manera opcional también acuden el comerciante y el fedatario.

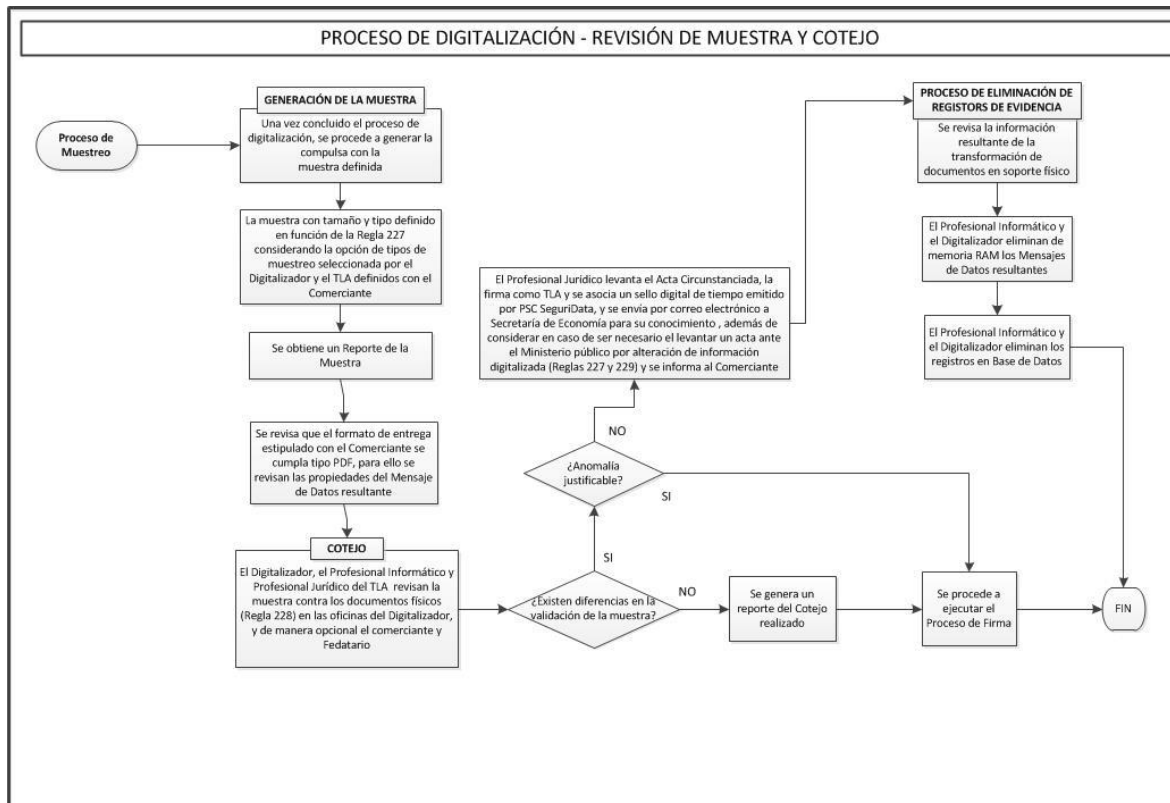
3.- Si los involucrados están de acuerdo, concluye este proceso e inicia el proceso de firma. **El registro de la fecha y hora se asienta** en el acta circunstanciada como registro de la actividad de inicio de revisión de muestreo y finalización de la misma

4.- En caso de diferencias en la validación de la muestra, se valida si es una anomalía justificable, y se procede a iniciar el proceso de firma.

Una anomalía justificable se define como la falta de nitidez de la imagen que se revisa, de manera que exista un criterio de aceptación de la nitidez y calidad de la imagen, o en su caso de rechace y se pida la digitalización nuevamente.

5.- Si la anomalía no es justificable: El profesional jurídico del TLA levanta acta circunstanciada, la firma como TLA asociando un sello digital de tiempo y se envía por correo electrónico a Secretaría de Economía para su conocimiento, además de considerar en caso de alteración grave de documentos identificado como “con dolo” levantar un acta ante el ministerio público (reglas 227 y 229 de las reglas generales a las que están sujetos los Prestadores de Servicio de Certificación), informando al comerciante. Concluye proceso y no se emiten firmas.

La anomalía no justificable, se define como la alteración de un documento digitalizado contra el original: puede ser que falte texto o que tenga un texto que no coincida por el documento original, donde existe presunción de actuación con “Dolo”.



Ver reportes de:

Anexo 6 Reporte de muestra

Anexo 7 Reporte de cotejo

Anexo 8 Acta circunstanciada con sus diferentes opciones en función del resultado de la Digitalización de documentos en soporte físico:

Acta circunstanciada sin diferencias

Acta circunstanciada con anomalías justificables, aceptada por el comerciante

Acta circunstanciada con anomalías justificables, no aceptadas por el comerciante

Acta circunstanciada con anomalías no justificables

13.6.2 Proceso de firma de documentos digitalizados

La firma se realizará sobre cada uno de los documentos digitalizados y el proceso solicitará una vez las llaves de los participantes y su password

TLA firma con las llaves resguardadas en el HSM

Comerciante y el Fedatario, en el caso de que sea incluido en el proceso de Digitalización, firman con sus llaves PSC, emitidas exclusivamente para el proceso de digitalización, **proporcionando las llaves y el password una sola vez**, al inicio del proceso de firma, previa aceptación de la Confidencial

SeguriData Privada S.A. de C.V.

Página **42** de **88**

muestra , de manera que el proceso se realiza de manera automática, firmando cada documento digitalizado que ya contiene la firma del digitalizador, la firma es bajo algoritmo SHA 256 CON LLAVES DE 4096, esto se actualizara en función de las necesidades de seguridad, (se refuerzan algoritmos y tamaño de llaves por seguridad), en función del tipo de llaves y firma emitidos por el PSC SeguriData bajo las reglas de los PSC.

Es importante mencionar que la FIRMA ELECTRONICA AVANZADA, incluye un sello digital de tiempo emitido por el PSC SeguriData en su Servicio de Sellos digitales de tiempo. Adicional al registro de la transacción en la base de datos que incluye la fecha y hora

Una vez firmado cada documento, se emite una Constancia de Conservación de mensaje de datos NOM 151 SCFI 2016, CON EL SERVICIO DE PSC DE SeguriData PARA CADA DOCUMENTO DIGITALIZADO Y FIRMADO. Adicional al registro de la transacción en la base de datos que incluye la fecha y hora

El mensaje de datos firmado por cada participante, se almacena y se conserva como PDF Signature por el TLA.

Y la constancia de conservación de mensaje de datos se almacena completa (incluye Hash), por cada documento digitalizado por el PSC en el Servicio de NOM 151 SCFI 2016.

Una vez concluido el proceso, el profesional jurídico en conjunto con el Profesional informático del TLA, elaboran el reporte de cotejo y el Acta circunstanciada.

El reporte de cotejo, contiene los datos que se mencionan en tabla que a continuación se presenta, y los datos del sello digital de tiempo asociado, se firma con las llaves del TLA y se deja disponible para consulta de la Secretaría de Economía, en la aplicación web publicada, con autenticación de usuario y password proporcionado a dicha secretaria.

El reporte de cotejo contiene la siguiente información:

No.	INFORMACIÓN
1	Nombre del comerciante que solicitó la digitalización, de su Representante Legal y su domicilio.
2	Nombre de la Digitalizadora.
3	Nombre del Tercero Legalmente Autorizado.
4	Nombres del Profesional Jurídico y del Informático.
5	Fechas en que se realizó la digitalización, el cotejo y el reporte.
6	Número de lote digitalizado (en su caso).
7	Número de documentos digitalizados.

8	Rango de folios de los documentos digitalizados.
9	Tamaño de la muestra(s), su nivel de confianza, límite de error de muestreo con el que se trabajó, y la desviación estándar estimada.
10	Listado de los números aleatorios generados por computadora y un sello digital de tiempo de este listado (emitido inmediatamente después generar el listado).
11	Lista de los folios de los mensajes de datos que forman parte de la muestra(s).
12	Técnica de muestreo probabilístico utilizada y las razones por las cuales se eligió.
13	Fracciones en los estratos (en su caso) y el criterio que se eligió.
14	En el caso de mensajes de datos extensos: los folios de los mensajes de datos, el tamaño de la muestra(s), los números de las hojas cotejadas y la técnica de muestreo utilizada.
15	Folios de los mensajes de datos digitalizados de la muestra que durante el cotejo se encontró con diferencias con los respectivos documentos en soporte físico.
16	En caso de no haber diferencias en el cotejo de la muestra se escribirá la leyenda "NO HUBO DIFERENCIAS EN LA MUESTRA".
17	El reporte será firmado electrónicamente por el Tercero Legalmente Autorizado.

Incluye además el registro de la fecha y hora de cada una de las actividades que se mostraron anteriormente, con la fecha de inicio y de finalización para contar con la trazabilidad de la custodia del documento en soporte físico desde que se recoge hasta que es entregado ya con su transformación a documento digital.

Cabe mencionar que estos procesos se realizan de manera automática a través de un software propiedad del digitalizador, que consume los servicios de SeguriData para la emisión de firma electrónica avanzada y los servicios de PSC SeguriData para la firma de TLA y la emisión de la NOM 151 SCFI 2016. Dicho software fue auditado por el TLA SeguriData como parte de las obligaciones de cumplimiento del mismo.

A continuación, la descripción de los pasos:

1.- La firma se realiza sobre cada documento digitalizado, solicitando una sola vez las llaves de los participantes y su password: TLA firma con llaves resguardadas en HSM, Comerciantes con archivos .cer y .key PSC, proporcionando su password una sola vez al inicio del proceso de firma, Si se optó por la firma de un fedatario, esta firma con llaves PSC en archivos .cer y .key proporcionando su password una sola vez al inicio del proceso de firma.

2.- Una vez que se dio el VoBo de la muestra, los participantes ingresan al portal proporcionan sus llaves y el password, y el proceso inicia firmando cada uno de los mensajes de datos de los documentos digitalizados con FIRMA PDF SHA 256. La firma incluye un sello de tiempo, emitido por un PSC autorizado, el orden de las firmas es primero TLA, seguido del comerciante. Y el fedatario en caso de ser requerido y la opción fue incluirlo.

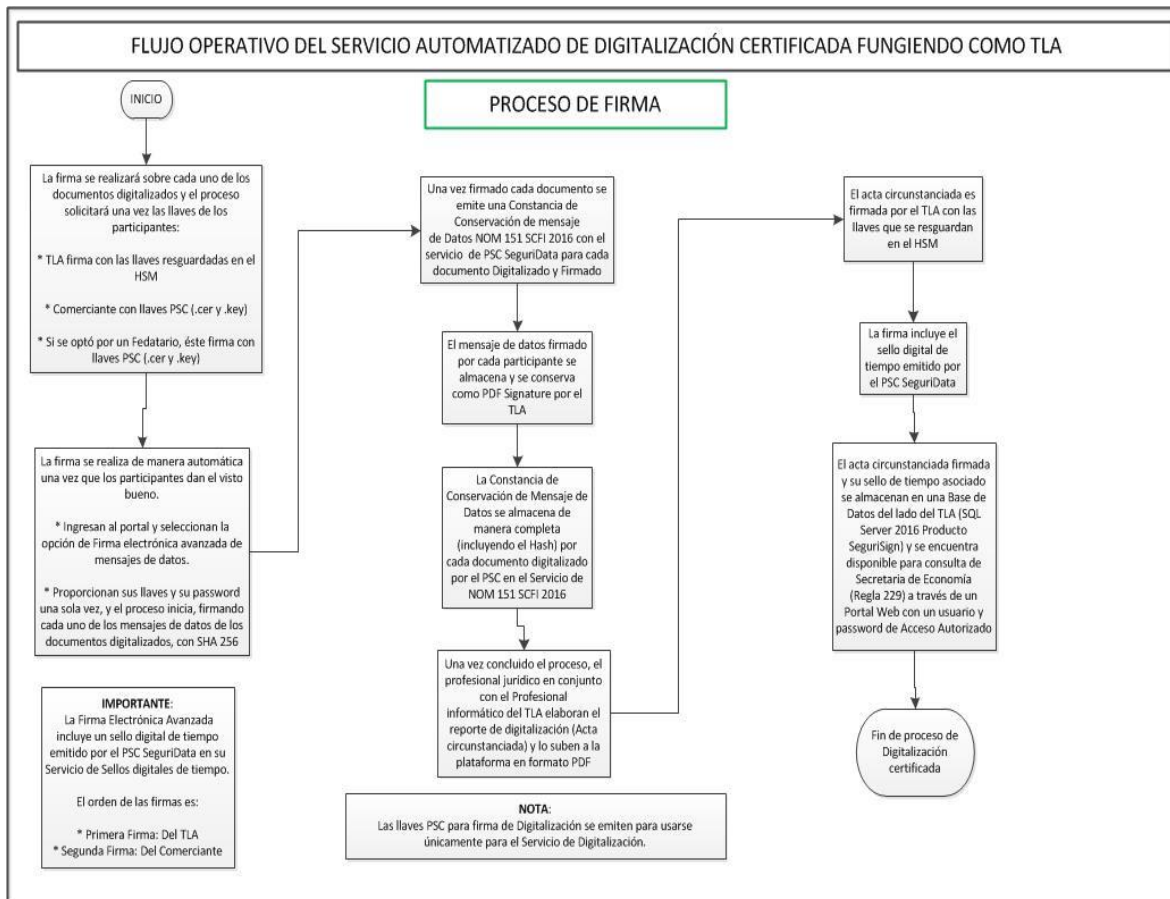
3.- Una vez firmado cada documento, se emite una constancia de conservación de mensaje de datos NOM 151 SCFI 2016, asociando la fecha y hora de emisión de la misma.

4.- El mensaje de datos firmado por cada participante, se almacena y se conserva como PDF Signature por el TLA

5.- La NOM 151 SCFI 2016, se almacena de manera completa, incluyendo el HASH por cada documento digitalizado, por el TLA con la fecha y hora de su emisión

6.- Una vez concluido el proceso de firma , el profesional jurídico en conjunto con el profesional informático del TLA , elaboran el acta circunstanciada y la suben a la plataforma en formato PDF , la firman con las llaves del TLA resguardadas en HSM , se asocia el sello de tiempo , resguardando esta acta del lado del TLA en una base de datos SQL 2016 en el producto SeguriSign , disponible para su consulta en un portal web, donde Secretaria de economía puede acceder a través de usuario y password para su consulta.

Concluye proceso de firma y de digitalización de documentos en soporte físico de conformidad con la NOM 151 SCFI 2016.



13.6.3 Proceso de entrega o destrucción de documentos en físico

En este proceso se define la forma en que los documentos se devuelven al comerciante, de así, definirlo o bien la forma en que se realiza la trituración de los documentos en caso de elegir la destrucción de los mismos.

De este proceso se destaca la participación opcional en la opción de destrucción de documentos del fedatario y del comerciante.

Para la opción de destrucción de documentos, se considera: Los documentos en soporte físico podrán ser destruidos según la naturaleza de la información de acuerdo con los ordenamientos legales aplicables. En todo caso, el proceso de digitalización realizado conforme a la NOM 151-scfi 2016, otorga integridad al mensaje de datos obtenido.

Los pasos del proceso son:

1.- Se valida si la petición del comerciante fue Destrucción de documentos

2.- Para el caso de no destrucción de documentos:

a) Se empaquetan los documentos ya digitalizados en bolsas de seguridad y se sellan con cintas de seguridad, elaborando el formato con la relación de los documentos, se presenta en el **Anexo 10**

b) El digitalizador transporta las bolsas hacia la ubicación física definida por el comerciante.

c) Realiza la entrega de los documentos al comerciante, el comerciante revisa que la cinta de seguridad no fue violada.

d) Si fue violada El comerciante envía correo electrónico al digitalizador y al TLA, estos levantan acta y aplican lo contundente definido en el contrato establecido y concluye el proceso

e) En caso de no violación: El comerciante abre bolsa de seguridad, revisa documentos contra el formato y firma de recibido. Concluye proceso

3.- Para el caso de destrucción de documentos:

a) Se elabora acta de destrucción en presencia del profesional jurídico y el profesional informático del TLA y el digitalizador, como opcional presencia de comerciante y fedatario.

b) Se trituran los documentos

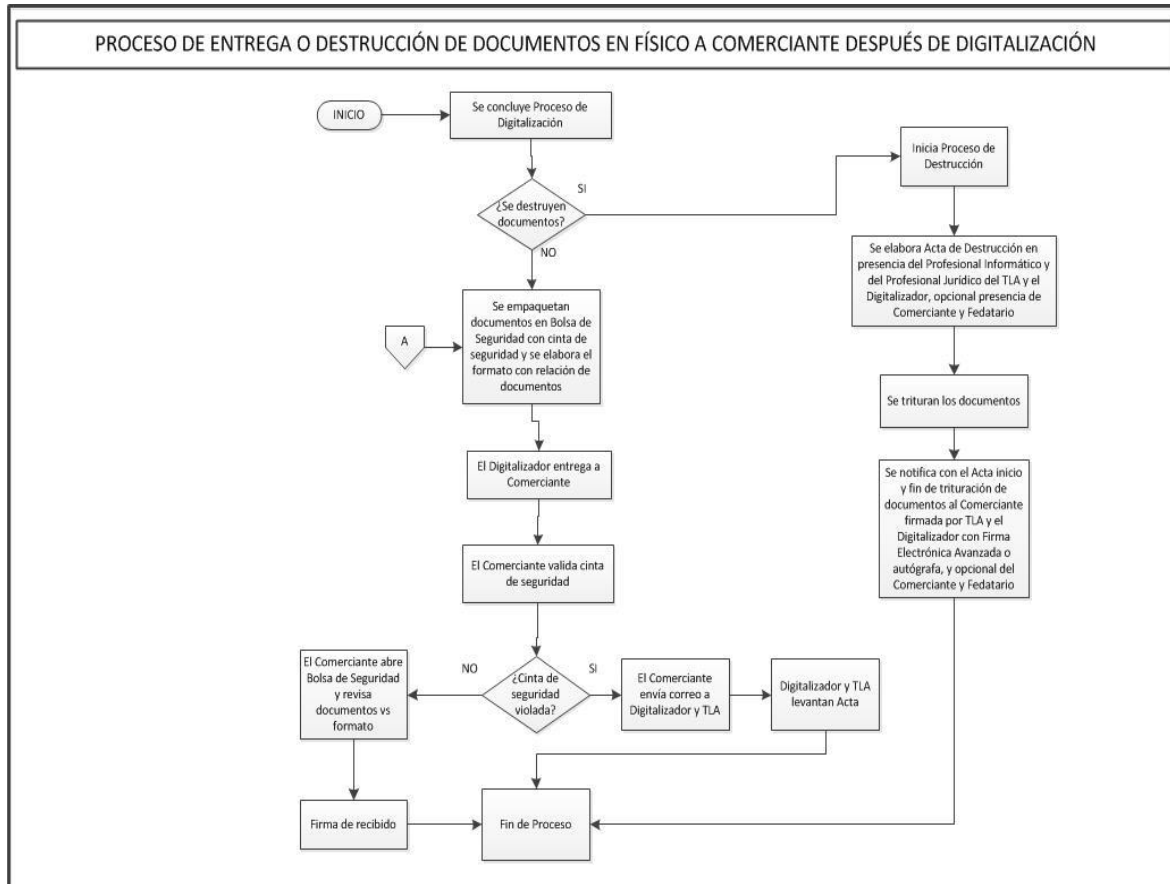
c) Se notifica acta de inicio y fin de trituración de documentos formada por el TLA y el digitalizador con FEA o firma autógrafa, y opcional la firma del comerciante y fedatario.

d) Concluye proceso

CADENA DE CUSTODIA

d) La cadena de custodia de los documentos en esta parte es del digitalizador al realizar la entrega al cliente

e) Y del cliente una vez que recibe los documentos en soporte físico y valida contra formato de entrega.



14 Trazabilidad de Registro de fecha y hora de actividades de Digitalización

Para la trazabilidad de las fechas y horas de las diferentes actividades, se lleva una bitácora con la información asociada a las actividades definidas, incluyendo la custodia en todo momento

Actividad	Fecha y hora de inicio	Fecha y hora fin	Custodia
1.- Firma de contrato			

2.- Recepción de documentos en soporte físico con el cliente			Digitalizador – Formato de recepción
3.- Traslado de documentos en soporte físico de oficinas de cliente a digitalizador			Digitalizador – Formato de recepción
4.- Recepción de documentos en área de operaciones de digitalizador			Digitalizador Formato de entrega
5.- Preparación de documentos para digitalizar			Digitalizador
6.- Inicio de Digitalización: -Transformación de documentos en soporte físico a Metadatos - Muestra de escaneo - Firma de documento digitalizado - Constancia NOM 151 de documento digitalizado			Digitalizador Base de datos
7.-Generación de acta circunstanciada			TLA
8.- Devolución de documentos en soporte físico			Digitalizador Formato de entrega

15 Condiciones que cumple el TLA para ofrecer el servicio de Digitalización fungiendo como TLA

Para ofrecer el Servicio de Digitalización de documentos en Soporte Físico, el TLA debe cumplir con lo estipulado en el Título 8 de las reglas de PSC en materia de Digitalización de documentos en soporte físico:

El Prestador de Servicios de Certificación interesado en actuar como Tercero Legalmente Autorizado, deberá cumplir con los elementos humanos y económicos establecidos en el presente TÍTULO y, con lo siguiente:

- 1) Contar con dos equipos HSM resguardado en un lugar seguro, compatibles como mínimo con el estándar FIPS 140-2 nivel 3 en sus elementos de seguridad e implantación de los algoritmos criptográficos estándares, donde se almacenan los Datos de Creación de Firma Electrónica del Certificado del Tercero Legalmente Autorizado.
- 2) Contar con las medidas de seguridad adoptadas para proteger los Datos de Creación de Firma Electrónica del Certificado del Tercero Legalmente Autorizado
- 3) Contar con un procedimiento en caso de robo de los Datos de Creación de Firma Electrónica del Certificado del Tercero Legalmente Autorizado.
- 4) El Tercero Legalmente Autorizado controla en todo momento el proceso de digitalización siendo responsable de la verificación que realice respecto de la migración y firmará el mensaje de datos que resulte de dicho proceso, siempre y cuando constate que la migración se realizó de manera íntegra e inalterablemente tal y como se generó por primera vez en su forma definitiva.
- 5) El Tercero Legalmente autorizado, por cada proceso de digitalización deberá firmar un contrato con la Digitalizadora, en el que se acordarán sus responsabilidades y obligaciones, así como los de la Digitalizadora y de los usuarios, lo anterior conforme al Modelo Operacional y la Declaración de Prácticas de cada proceso de digitalización.

16 Política de Deshecho – Limitantes

La Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico de SeguriData Privada debe:

Asegurar que después de la desincorporación de las claves de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico, estas no puedan ser accedidas ni usadas para ningún propósito diferente al menos que se requiera para aclaración de alguna controversia.

La Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico de SeguriData Privada, debe rechazar la muestra en caso de detectar diferencias entre lo digitalizado y el documento en soporte físico, y en caso de presuponer alguna anomalía por alteración en la digitalización, notificar a Secretaria de Economía por correo electrónico, con el acta circunstanciada correspondiente, y levantar un acta en el Ministerio Público.

Los certificados PSC emitidos por la Autoridad certificadora PSC para el comerciante y para el Digitalizador, tendrán una cláusula de uso exclusivo para la firma de documentos digitalizados

16.1 Grado de Fiabilidad de los Mecanismos y Dispositivos utilizados

Los puntos importantes para asegurar la fiabilidad de los mecanismos de firma electrónica avanzada, durante la digitalización son:

1. La seguridad que se da al acceso a la autoridad de que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico de SeguriData Privada
2. La seguridad que se da al software usado por el digitalizador y el software usado para la firma electrónica avanzada.
3. La confianza que se tiene en los algoritmos utilizados para la generación de las Firmas Electrónicas Avanzadas y para la definición del tipo y tamaño de la muestra a revisar.
4. La precisión y exactitud de la fuente de tiempo
5. La seguridad que se tiene al obtener la información de la fuente de tiempo
6. La disponibilidad que se tiene de la fuente de tiempo
7. La seguridad que se tiene al emitir una constancia de conservación por cada documento digitalizado

16.2 Seguridad en el acceso a la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico

La Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico del PSC se encuentra almacenada y custodiada en un módulo HSM que cumple con el FIPS 140-2 nivel 3. Las llaves se generan dentro del módulo y por las características del FIPS 140-2 nivel 3, éstas nunca abandonan el hardware en claro. Incluso, si el hardware fuera manipulado y se abriera, las llaves se eliminarían automáticamente en dicho intento.

16.2.1 Otorgamiento del Servicio

Para otorgar el Servicio, el cliente firma un contrato con el digitalizador y la autoridad de TLA con el Digitalizador, donde se especifica:

- El tipo de documento a digitalizar, puede ser original, copia simple o copia certificada, el digitalizador y el TLA actúan de buena fe, sin cuestionar la validez

16.3 Administración de la Seguridad

La administración de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico de SeguriData Privada debe proporcionar la información sobre la seguridad de la información, la cual se define en el documento Política de la Seguridad de la Información de Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico de SeguriData Privada, conteniendo obligaciones, sanciones, amenazas, plan de respuesta de incidencias y el procedimiento para dar a conocer dichas Políticas.

16.4 Controles de Seguridad Física

SeguriData Privada S.A. de C.V. gestiona y pone en práctica controles de seguridad apropiados para restringir el acceso al hardware y al software utilizado en relación con la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico de SeguriData Privada SA de CV.

SeguriData Privada S.A. de C.V. asegurará que el acceso físico a servicios críticos es controlado y que se tiene el análisis y la reducción de los riesgos físicos de sus activos.

Se ponen en práctica controles para evitar la pérdida, el robo, el daño o el compromiso de activos y la interrupción de la operación de la Infraestructura del TLA. También existen perímetros de seguridad claramente definidos.

Se ponen en marcha controles de seguridad físicos y ambientales para proteger los recursos en los que está alojada la Infraestructura de TLA, aplicando controles de acceso físico, controles de protección y recuperación ante desastres, controles de seguridad contra incendios e inundaciones y, controles de fallos en las instalaciones, suministros de energía, telecomunicaciones y, aire acondicionado, entre otros

16.5 Ubicación y Construcción

La ubicación de los servicios de la Infraestructura del TLA está en un centro de datos ambientalmente segura, ubicada en Interlomas como centro principal de operación, y un centro de datos alternativo ubicado en Tultitlan. Dichos centros de datos cumplen con las normas ISO siguientes:

- NMX-CC-9001-IMNC-2000/ISO 9001:2000, para los procesos de Administración de Cambios, Administración de Incidentes y Administración de las Configuraciones.
- ISO/IEC 20000-1:2005, para la administración de sistemas de Tecnologías de la Información.
- ISO/IEC 27001:2005, para la administración de sistemas de Tecnologías de la Información.

Todos los equipos relacionado con la Infraestructura de TLA cumplen con un conjunto de principios de seguridad mínimos que permiten proporcionar un servicio a prueba de fallos conforme al documento PSC-SEGURIDATA-POLITICAS DE SEGURIDAD-SITETULTITLAN-INTERLOMAS-VERSION1.0.doc, entregado a la Secretaría de Economía con motivo de la acreditación como Prestador de Servicios de Certificación, para el Servicio de Digitalización de documentos en soporte físico fungiendo como Tercero Legalmente autorizado de SeguriData Privada SA de CV.

16.5.1 Acceso Físico

El personal autorizado (roles de: oficial de seguridad, profesional jurídico, operador de sistemas, administrador de sistemas, administrador de base de datos, administrador de redes y, personal que realiza auditorías), para acceder a las áreas seguras donde está la Autoridad de TERCERO LEGALMENTE AUTORIZADO PARA DIGITALIZACION DE DOCUMENTOS EN SOPORTE FISICO, ya sea en el centro de datos principal o alterno, no podrá quedarse sólo, en los centros de datos, sin la supervisión de personal autorizado, y únicamente para realizar labores de actualización, mantenimiento, o auditoría. En la administración de la Autoridad de TERCERO LEGALMENTE AUTORIZADO PARA DIGITALIZACION DE DOCUMENTOS EN SOPORTE FISICO se protegen datos sensibles contra accesos no autorizados o modificaciones por red, la Autoridad de TERCERO LEGALMENTE AUTORIZADO PARA DIGITALIZACION DE DOCUMENTOS EN SOPORTE FISICO asegura que el acceso a la información y a las funciones de las aplicaciones del sistema están restringidos de acuerdo a la Política de Seguridad Física del Sitio de Interlomas y Tultitlan, incluyendo la separación de funciones de administración y operación.

El procedimiento para el Acceso Físico al site de Interlomas es:

El personal autorizado por parte de SeguriData debe enviar un correo electrónico a KIO solicitando el acceso de los visitantes, informando el motivo de la visita y el tiempo que permanecerán en las instalaciones, así como las áreas a las que se tendrá acceso, al menos con 24 hrs de anticipación

Si el visitante ingresa con auto, debe solicitarse la autorización para el estacionamiento, limitado a las políticas de espacio que en ese momento se tengan, la notificación debe ser vía correo electrónico por la persona autorizada por parte de SeguriData, con 24 horas de anticipación.

El visitante no podrá ingresar solo a las instalaciones del centro de datos, debe hacerlo forzosamente con personal autorizado por parte de KIO

Todo equipo de cómputo debe quedar registrado, anotando la marca y el número de serie
Queda prohibido introducir cajas de cartón, plástico y cualquier tipo de material inflamable, al centro de datos.

El cliente es responsable de llevarse todo el empaque de sus equipos que ingresan por la bodega

El cliente es responsable de avisar a KIO para que el custodio de la llave de SeguriData, abra la jaula o rack correspondiente.

El procedimiento para el Acceso Físico al site de Tultitlan es:

Si el visitante ingresa en auto, accede por el área de estacionamiento, donde el guardia solicita su nombre y la persona que visita, una vez que el guardia revisa si está en la lista de accesos, solicita su identificación y asigna el número de cajón que le corresponde, en caso contrario no se permite el acceso.

En la recepción, se solicita identificación y se anotan los datos en una bitácora electrónica, se toma una foto y se registra huella del dedo índice de la mano derecha, con esto se genera un gafete (etiqueta adherible).

En caso de traer equipo de cómputo el guardia de seguridad anota en una bitácora los datos del equipo a ingresar, número de serie, y marca

A continuación, el custodio de los visitantes, abre la puerta de cristal blindado, con una tarjeta de proximidad

Al pasar esta puerta se encuentra un arco sensor de metales y un guardia, el cual solicita al visitante o cliente se registre en la bitácora (nombre, fecha, hora de entrada, hora de salida, persona que guía al visitante, motivo de visita y firma), previa revisión de su autorización

El siguiente control es un control mediante huella digital y PIN, mediante el cual se abre una puerta de metal

Una vez que se accedió al centro de datos, se tiene un pasillo que conduce a otras puertas más, una de cristal y otra de malla de alambre las cuales abren con tarjetas de proximidad.

Continúan con una puerta adicional que abre con tarjetas de proximidad y conducen a los racks de SeguriData.

16.5.2 Energía Eléctrica y Aire acondicionado

El área segura de operaciones se encuentra conectada a una fuente de energía estándar. Los componentes críticos de la Infraestructura de TLA se encuentran conectados a la fuente de energía ininterrumpida (UPS). Para prevenir la interrupción del servicio en caso de interrupciones del suministro eléctrico, se cuenta con plantas de emergencia de generación de energía eléctrica y cuatro tanques de combustible para la misma, de 600, 100, 1500, y 6000 litros, que aseguran la continuidad en el servicio.

16.5.3 Riesgos por Inundaciones

La ubicación donde se encuentran los servicios de la Infraestructura de TLA proporciona protección contra las inundaciones, el detalle de encuentra en el documento PSC-SEGURIDATA-POLITICAS DE SEGURIDAD-SITETULTITLAN-INTERLOMAS-VERSION1.0.doc.

16.5.4 Prevención de Incendios y Protección

La ubicación donde se encuentran los servicios de la Infraestructura de TLA proporciona protección contra incendios, el detalle de encuentra en el documento PSC-SEGURIDATA-POLITICAS DE SEGURIDAD-SITETULTITLAN-INTERLOMAS-VERSION1.0.doc.

16.6 Almacenamiento de Medios

Todos los medios de comunicación magnéticos que contienen la información de la Infraestructura de TLA, incluyendo medios de comunicación de respaldos, son almacenados en gabinetes bajo llave bajo el resguardo de KIO con acceso exclusivo para el administrador de base de datos, el operador de sistemas y el administrador de sistemas, cumpliendo con la seguridad descrita tanto para el site de Interlomas como TULTITLAN.

Se conservan todos los registros de los usuarios y de la Autoridad de TLA, protegiéndolos contra destrucción y falsificación de acuerdo a la Política de Seguridad de la Información.

16.7 Destrucción de Documentos

Los documentos en papel y aquellos medios que contengan elementos sensibles de la Infraestructura de información comercialmente sensible serán eliminados, solo en caso de que la autoridad de TLA de SeguriData Privada SA de CV deje de existir, y será bajo las siguientes condiciones:

- Para información en medios magnéticos:
 - o Destrucción completa del mecanismo.
 - o El empleo de una herramienta aprobada para limpiar o sobrescribir medios magnéticos.
- Para información en material impreso
 - Trituración.

16.8 Copias de Seguridad

Se utilizarán elementos de almacenamiento en sitios externos para el resguardo y la retención de las copias de seguridad pertenecientes a la información relacionada con la Infraestructura de TLA, el software de reserva y datos relacionados con elementos críticos especificados en la Política de Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico de SeguriData Privada SA de CV.

El almacenamiento en sitio externo se tiene en el Site alterno ubicado en Santa Fe:

- Está disponible al personal autorizado 24 horas por día, 365 días del año con el fin de recuperar el software y datos;
- El lugar cuenta con los niveles apropiados de seguridad física.

Esto se detalla en el documento: PSC-SEGURIDATA-POLITICASDESEGURIDAD-SITETULTITLAN-INTERLOMAS-VERSION1.0.doc

16.9 Procedimientos de Control

SeguriData Privada S.A. de C.V. asegura que los procedimientos administrativos relacionados con el personal y exigencias procesales, mecanismos de seguridad físicos y tecnológicos, se mantienen conforme a esta Declaración de Prácticas de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico de SeguriData Privada SA de CV, la Política de Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico de SeguriData Privada SA de CV y otros documentos operacionales relevantes.

SeguriData Privada S.A. de C.V. asegura que sus sistemas son seguros y se gestionan correctamente, con un riesgo mínimo de fallo. Los perjuicios, incidentes de seguridad y mal funcionamiento serán reducidos al mínimo mediante el uso de sistemas de información de incidentes y procedimientos de respuesta.

SeguriData Privada S.A. de C.V. actuará de una manera oportuna y coordinada para responder rápidamente a los incidentes que puedan surgir.

El administrador de sistemas y el operador de sistemas de la autoridad de TLA, deben proporcionar información de los riesgos de la seguridad presentados durante la operación, al oficial de seguridad, como responsable de la Política de Seguridad de Información, mediante el registro de los eventos en la Bitácora definida.

16.10 Roles de Confianza

A fin y efecto de asegurar quien tiene acceso a qué parte del sistema, las responsabilidades se han diferido en varios roles y usuarios para asegurar que las personas actúan dentro de los límites de sus responsabilidades y dentro de la política de seguridad indicada.

Dicha diversificación se ha logrado creando roles separados con sus respectivas cuentas de usuario y certificados digitales, con límites establecidos de acuerdo a las funciones de cada rol.

A continuación la descripción de los roles, sus requisitos y responsabilidades:

Auxiliar de Apoyo informático de Seguridad:

Será el responsable de ejecutar el sistema de gestión, planes, políticas, procedimientos y prácticas de seguridad, este rol cumple con los requisitos definidos en la regla 180 del título octavo capítulo I de las Reglas de PSC

*Ser licenciado o ingeniero en área informática o afín, con título y cédula profesional expedidos por la Secretaría de Educación Pública o su equivalente

*Comprobar al menos dos años de experiencia en el área de seguridad informática

*Acreditar estudios en manejo de software o hardware relacionados con seguridad informática

*Contar con conocimientos comprobados de procesos de digitalización, y

*Declarar bajo protesta de decir verdad que no ha sido condenado por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo haya sido inhabilitado para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio.

Y en cumplimiento de la regla 183 del título octavo capítulo I de las Reglas de PSC, tiene las siguientes funciones y responsabilidades:

- a) Ejecutar el sistema de gestión, planes, políticas, procedimientos y prácticas para garantizar la autenticidad e integridad de los mensajes de datos resultantes de la Digitalización de Documentos en Soporte Físico;
- b) Llevar a cabo la ejecución de los procesos de Digitalización de Documentos en Soporte Físico, validar la calidad de las imágenes durante dicho proceso conforme a la fracción anterior y las pruebas de configuraciones;
- c) Determinar los requisitos de mejora de la imagen y/o grabaciones en audio o video;
- d) Monitorear y asegurar la correcta indexación y la calidad de las imágenes y sus metadatos;
- e) Llevar el control y reportes del proceso;
- f) Agregar los metadatos al mensaje de datos, y
- g) Comprobar la calidad de los mensajes de datos a la entrega de los archivos digitales y físicos

Profesional Jurídico:

Este rol cumple con los requisitos definidos en la regla 178 del título octavo capítulo I de las Reglas de PSC:

*Ser licenciado en derecho con título y cédula profesional expedidos por la Secretaría de Educación Pública o su equivalente;

*Demostrar al menos dos años de experiencia en materia notarial, correduría pública o derecho mercantil;

*Acreditar al menos un año de experiencia en derecho informático, y

*Declarar bajo protesta de decir verdad que no ha sido condenado por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo haya sido inhabilitado para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio.

Y tendrá las siguientes obligaciones, funciones y responsabilidades, definidas en la regla 181 de las reglas PSC

- a) Colaborar con el Profesional Informático en el tratamiento de los elementos jurídicos del sistema de gestión, planes, políticas, procedimientos y prácticas que se pudieran establecer, para garantizar la autenticidad e integridad de los mensajes de datos que resulten de la Digitalización de Documentos en Soporte Físico, los cuales deberá firmar y dar a conocer al personal involucrado en la digitalización;
- b) Supervisar las actividades de cotejo a que se refiere el artículo 95 bis 4 del Código de Comercio, y
- c) Elaborar el acta circunstanciada en la que se deje constancia de las actividades de cotejo de Digitalización de Documentos en Soporte Físico a que se refiere el artículo 95 bis 4 del Código de Comercio, la cual podrá ser generada de manera electrónica.

Profesional Informático:

Este rol cumple con los requisitos definidos en la regla 179 del título octavo capítulo I de las Reglas de PSC:

*Ser licenciado o ingeniero en área informática o afín, con título y cédula profesional expedidos por la Secretaría de Educación Pública o su equivalente;

*Comprobar al menos dos años de experiencia en el área de seguridad informática, y

*Comprobar estudios en seguridad informática y/o alguna certificación nacional o extranjera o su equivalente, en la misma materia. En caso de contar con experiencia en certificaciones, las mismas deberán contar con una vigencia de dos años como máximo.

Y tendrá por las siguientes obligaciones, funciones y responsabilidades, definidas en la regla 182 de las reglas PSC título octavo.

- a) Diseñar, implantar y dar cumplimiento al sistema de gestión, planes, políticas, procedimientos y prácticas para garantizar la autenticidad e integridad de los mensajes de datos que resulten de la Digitalización de Documentos en Soporte Físico, los cuales deberá firmar y dar a conocer al personal involucrado en la digitalización;
- b) Supervisar los equipos y suministros de Digitalización de Documentos en Soporte Físico;
- c) Supervisar el personal que lleva a cabo procesos de Digitalización de Documentos en Soporte Físico;
- d) Establecer el flujo de trabajo para el proceso de Digitalización de Documentos en Soporte Físico y asegurar su cumplimiento;
- e) Acordar el formato de la imagen con el comerciante;
- f) Seleccionar el hardware de digitalización y asegurar su cumplimiento;

- g) Estar presente en las actividades de cotejo a que se refiere el artículo 95 bis 4 del Código de Comercio;
- h) Asegurar que el proceso de Digitalización de Documentos en Soporte Físico incluye la Conservación de Mensaje de Datos resultante del proceso, y
- i) Supervisar pruebas de monitoreo.

Administrador.

Encargado de gestionar la Digitalización de documentos en soporte físico fungiendo como Tercero Legalmente autorizado de SeguriData Privada SA de CV, desde la contratación del servicio, hasta la expedición y entrega del mismo.

Administrador de Base de datos. Encargado de administrar la base de datos

Administradores del Sistema: Autorizados para instalar, configurar y mantener sistemas.

Los roles relevantes del personal serán formalmente designados por el Profesional Informático y el auxiliar de apoyo informático de Seguridad, asignados de manera formal mediante una reunión, y no podrán ejercerlos hasta que esto suceda.

Los procedimientos serán establecidos y puestos en práctica para todas las funciones que afecten a la Infraestructura de TLA

16.10.1 Número de Personas Requeridas por Tarea

El número de personas requeridas por tarea se da de acuerdo a la siguiente tabla:

Tarea	Personas requeridas
Contratación del servicio	Administrador
Digitalización de los documentos	Digitalizador
Revisión de muestra	Profesional jurídico, comerciante de manera opcional, digitalizador, y fedatario de manera opcional
Elaboración y firma de acta circunstanciada	Profesional informático Profesional jurídico
Administración de la base de datos	Administrador de base de datos

Administrar las comunicaciones	Auxiliar informático de redes de redes
Revisar procesos de auditoría y seguridad	Auxiliar informático de seguridad

Se llevarán a cabo prácticas para asegurar que una persona que actúa sola no pueda alterar las medidas de seguridad:

16.10.2 Funciones que Requieren Separación de Deberes

Las funciones que implican la administración de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico son separadas y asignadas a los roles comentados en el inciso 16.10.1

Todas las funciones que implican el mantenimiento de registros de auditoría son separadas y asignadas a los roles comentados en los puntos anteriores.

El personal (tanto temporal como permanente) tiene descripciones de trabajo definidas desde el punto de vista de separación de deberes y privilegios de acceso, determinando la sensibilidad de la posición con base en los deberes y niveles de acceso, los antecedentes, preparación y conocimientos del empleado, diferenciando funciones generales y específicas.

Para ello las descripciones de trabajo incluyen habilidades y requisitos de experiencia.

16.11 Controles de Seguridad Personales

Se realizan estudios e investigaciones sobre todas las personas seleccionadas para llevar a cabo un rol de confianza, de acuerdo a lo marcado en el procedimiento de selección y contratación en el documento PSC-SEGURIDATA-PROCEDIMIENTOSELECC-CONTRA- RH-VERSION1.0.doc, para asegurar su integridad, antes de iniciar sus funciones.

Sin restricción, SeguriData Privada S.A. de C.V. no será responsable de la conducta de un empleado más allá de sus deberes y sobre el que SeguriData Privada S.A. de C.V. carece de control, como los actos de espionaje, el sabotaje, la conducta criminal, o la mala fe.

SeguriData Privada S.A. de C.V. asegurará que las prácticas sobre el personal y la contratación del mismo, garanticen la validez de las operaciones realizadas dentro de la Infraestructura de TLA.

16.11.1 Requerimientos de Calificación, Experiencia, Calidad y Formación

SeguriData Privada S.A. de C.V. empleará personal que posea los conocimientos, experiencia y calificación necesaria para poder prestar los servicios que sean apropiados a su puesto de trabajo.

El personal directivo empleado poseerá conocimientos en tecnología de firma electrónica, así como en procedimientos de seguridad para el personal y experiencia en seguridad de la información y prevención de riesgos.

16.11.2 Procedimiento de Comprobación

Los procedimientos de comprobación incluyen, aunque no limitadamente, la comprobación y la confirmación de:

- Empleo anterior
- Referencias profesionales
- Referencias personales
- Formación académica
- Antecedentes penales
- Estatus e historial financiero y crediticio

SeguriData Privada S.A. de C.V. utilizará técnicas de investigación disponibles permitidas por la ley que proporcionen información similar.

SeguriData Privada S.A. de C.V. proveerá a su personal de formación interna y externa para mantener los niveles apropiados y requeridos de competencia para realizar su trabajo con el más alto nivel de calidad.

En caso de realización de cualquier tipo de acción no autorizada, se impondrá la sanción correspondiente, marcadas en el plan de continuidad del negocio y recuperación ante desastres, en función de la falta cometida, que va desde 3 llamadas de atención, hasta el despido.

16.11.3 Requisitos de Personal Externo

SeguriData Privada S.A. de C.V. no apoya el empleo de personal externo para la realización de funciones relevantes. La función de Digitalización será a través de un Digitalizador previamente auditado por SeguriData, y previa firma de un convenio de colaboración.

16.11.4 Documentación Suministrada al Personal

SeguriData Privada S.A. de C.V. proporciona a su personal todos los materiales de formación necesarios para realizar sus funciones de trabajo y sus tareas, manejando los casos de reemplazo de roles en caso de alguna ausencia en caso de enfermedad, u otro evento de acuerdo a lo definido en el Análisis y Evaluación de manejo de riesgos.

17 Auditoría de Procedimientos de Registro

En este subcomponente se describe el registro de eventos y la auditoría de sistemas, implementados con el fin de mantener un entorno seguro

17.1 Tipos de Eventos Registrados

Todos los actos relacionados con la Digitalización de documentos en soporte físico fungiendo como Tercero Legalmente autorizado son registrados. Esto incluye todos los datos de configuración usados en el proceso.

Los tipos de datos registrados incluyen, pero sin carácter limitativo:

- Todos los datos incluidos en cada proceso de Digitalización de documentos en soporte físico fungiendo como Tercero Legalmente autorizado serán registrados en la base de datos, para tener una referencia futura en caso de que su uso fuera necesario.
- Toda la documentación presentada para la solicitud de Digitalización de documentos en soporte físico fungiendo como Tercero Legalmente autorizado en conjunto con la propia solicitud y acuerdo firmados por el cliente, los cuales se encuentran en un sitio seguro de manera física almacenados en gavetas bajo llave
- Todos los metadatos y los archivos pdf resultado de la digitalización de documentos en soporte físico, son resguardados en la base de datos, para su futura consulta en caso de ser necesario.
- Todos los documentos en soporte físico son resguardados durante la digitalización y pueden ser sujetos de auditoría
- Todos los documentos digitalizados tienen asociada una NOM 151 SCFI 2016 para posteriores validaciones de auditoría de así requerirse y son resguardadas en base de datos.

17.1.1 Frecuencia de Registro

Comprobaciones de los registros son realizadas y contrastadas de manera mensual. Mediante el proceso de generación de reporte de auditoría, mientras que el registro de las transacciones es diario en función de su ocurrencia.

17.1.2 Período de Conservación de los Registros de Auditoria

Las transacciones son conservadas en la base de datos durante al menos 5 (cinco) años para posibles comprobaciones de auditoría, y al menos 5 (cinco) años para la información del mensaje de datos firmados. Las transacciones serán almacenadas al menos 5 (cinco) años después de que la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico cese sus operaciones.

17.1.3 Protección de los Registros de Auditoria

Los datos recogidos en la auditoria son revisados con regularidad para evitar cualquier tentativa de violar la integridad de cualquier elemento de la Infraestructura de TLA y del Digitalizador.

Solo el profesional informático y su auxiliar de Seguridad de la Infraestructura de TLA y del digitalizador y Auditores pueden ver los registros de auditoría en su totalidad. SeguriData Privada S.A. de C.V. decidirá si algún registro de auditoría en particular tiene que ser visto por un tercero y lo pondrá a su disposición.

SeguriData Privada S.A. de C.V. y el digitalizador realizan un respaldo de la base de datos que contiene las transacciones descritas, el cual se efectúa diariamente.

17.1.4 Notificación al Individuo que Genera un Suceso

Cuando se registra un suceso, al emitir el reporte de auditoría y recibir problemas en la integridad de los datos, el profesional informático y su auxiliar de seguridad que revisa dicho reporte, notifica al administrador de base de datos para que proceda a restaurar la base de datos con el respaldo correspondiente, de manera que no es necesario notificar del suceso, ya que no afecta a los clientes.

Se llevarán a cabo evaluaciones relativas al sistema de base, amenazas corrientes y riesgos de vulnerabilidad, que abarquen todos los apartados de la Infraestructura de TLA y del digitalizador incluyendo equipos, ubicación física, registros, datos, software, personal, procesos administrativos y comunicaciones. Los procedimientos de evaluación de vulnerabilidad tienen la intención de identificar amenazas y vulnerabilidades de la Infraestructura de TLA y del digitalizador, así como determinar un índice de riesgo en base a la existencia de protecciones y prácticas de control.

SeguriData Privada S.A. de C.V. realizará una evaluación de los riesgos de seguridad y determinará las exigencias y procedimientos operacionales necesarios.

SeguriData Privada S.A. de C.V. mantendrá un inventario de todos los activos, y de la información y asignará una clasificación a las exigencias de protección de tales activos, compatible con el análisis de riesgo.

Lo anterior, está definido en el documento de Análisis y Evaluación de manejo de riesgos para el Servicio de Digitalización de documentos en soporte físico actuando como TLA.

17.1.5 Evaluaciones de Vulnerabilidad

Se llevarán a cabo evaluaciones relativas al sistema de base, amenazas corrientes y riesgos de vulnerabilidad, que abarquen todos los apartados de la Infraestructura de TLA y del Digitalizador, incluyendo equipos, ubicación física, registros, datos, software, personal, procesos administrativos y comunicaciones. Los procedimientos de evaluación de vulnerabilidad tienen la intención de identificar amenazas y vulnerabilidades de la Infraestructura de TLA y del digitalizador, así como determinar un índice de riesgo en base a la existencia de protecciones y prácticas de control. Gracias a ello la dirección podrá llevar a cabo decisiones informadas, determinando como proporcionar un ambiente seguro en el que el riesgo se reduzca a un nivel y a un costo de gestión aceptables para dirección, clientes, y accionistas.

SeguriData Privada S.A. de C.V. realizará una evaluación de riesgo para evaluar los riesgos de seguridad y determinará las exigencias y procedimientos operacionales necesarios.

SeguriData Privada S.A. de C.V. mantendrá un inventario de todos los activos de la información y asignará una clasificación a las exigencias de protección de tales activos, compatible con el análisis de riesgo efectuado.

18. Base de Datos

18.1 Respaldo de base de datos

Para llevar a cabo los respaldos se manejará una infraestructura de almacenamiento en cinta de StorageTek a la cual se accede mediante herramientas especializadas, para ejecución y administración de respaldos de VERITAS / LEGATO con la suite de productos de Netbackup / Networker.

El esquema de respaldos a ejecutar sobre la base de datos es:

- El administrador de la base de datos realiza un respaldo de la base de datos a un archivo indicando en que carpeta se guarda para que este archivo cerrado se guarde en cinta.
- Se entregan 2 cintas. Una es la que se utiliza y reescribe diariamente en un respaldo incremental y la otra se resguarda en la cintoteca del centro de datos de KIO TULTITLAN site alterno como DRP donde se tiene un respaldo mensual, y se reutilizara cada mes

El esquema de respaldo a ejecutar sobre los archivos cerrados es de un respaldo completo los domingos y respaldos diarios incrementales con un histórico de una semana.

18.1.1 Política de Respaldos

La política contempla la ejecución de un respaldo completo cada 8 días y un respaldo incremental diario entre cada uno de los respaldos completos.

El servicio de respaldo tanto para el Site de Interlomas – principal como el de TULTITLAN – alterno, incluye:

- Respaldo completo semanal después de las 20:00 hrs los sábados
- Respaldo diario incremental después de las 20:00hrs
- Respaldo histórico de un mes, último día del mes después de las 20:00 hrs
- Resguardo histórico por mes, en instalaciones de siete de Santa Fe alterno

Se conservará una bitácora de los respaldos efectuados, marcando el servidor, la fecha de respaldo, el tipo de respaldo, la hora de respaldo y, el log de la información respaldada

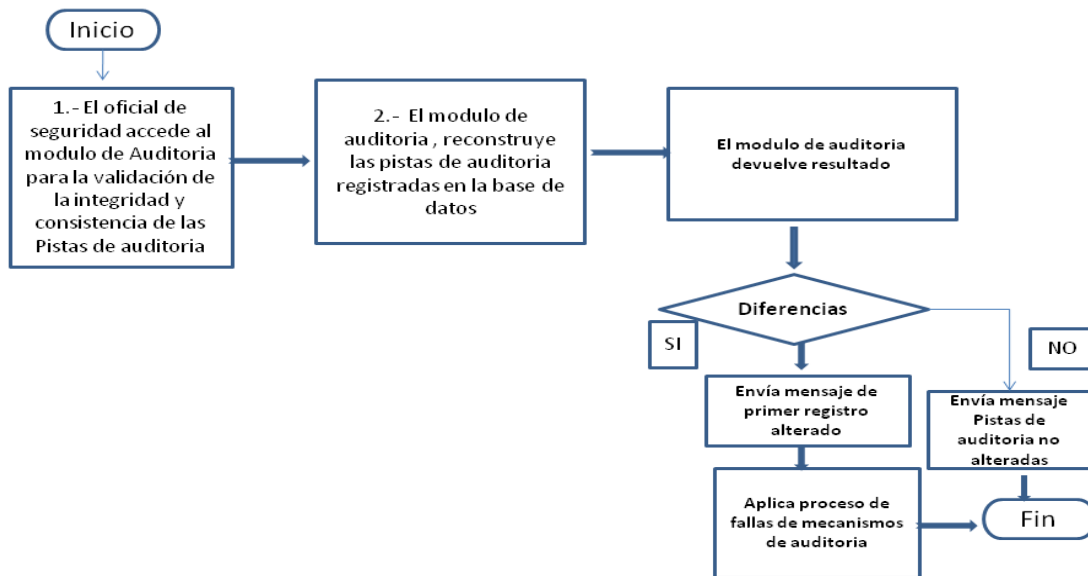
18.1.2 Procedimiento de Respaldo

El procedimiento se define de acuerdo a los eventos listados en los puntos anteriores, a partir del uso de los productos de software definidos. Software de digitalización, software de firma y manejador de base de datos SQL Server 20016.

Para los productos (aplicaciones) Software de digitalización y de firma, se audita a través de los logs (Bitácoras de errores), que son archivos de texto.

Y para el caso de documentación física se establece con relación al resguardo en un sitio seguro en una gaveta asegurada con llave.

A continuación, se muestra el procedimiento de registro de auditoria

PROCEDIMIENTO PARA REGISTRO DE AUDITORIA-EVENTOS**Validación de las Pistas de Auditoria****18.2 Archivo de Registros**

SeguriData Privada S.A. de C.V. asegurará que toda la información relevante acerca de la Infraestructura de Tercero Legalmente Autorizado sea registrada durante un período de tiempo de al menos 5 años, en particular con el objetivo de disponer de pruebas, relativas a los mensajes de datos firmados de los documentos digitalizados, que se puedan utilizar en procedimientos judiciales.

18.3 Período de Retención de Archivos

Los archivos de SeguriData Privada S.A. de C.V. serán conservados y protegidos contra la modificación o destrucción durante un plazo de al menos 5 (cinco) años.

18.3.1 Protección de Archivos

SeguriData Privada S.A. de C.V. asegurará que toda la información relevante acerca de la Infraestructura de TLA y del Digitalizador es registrada durante un período apropiado de tiempo, en particular con el objetivo de disponer de pruebas, relativas A LOS MENSAJES DE DATOS FIRMADOS, RESULTADO DE LA DIGITALIZACION POR CADA DOCUMENTO, que se puedan utilizar en procedimientos judiciales.

18.3.2 Procedimientos de Archivo de Reserva

Se aplicarán procedimientos de reserva adecuados, para que en caso de pérdida o destrucción de archivos primarios haya un juego completo de copias de reserva fácilmente disponible, a través de los respaldos de la base de datos que se hace diariamente y la replicación hacia el Site de TULTITLAN como DRP.

18.3.3 Exigencias para el Sellado de Tiempo de los Registros

Todas LAS firmas registradas dentro del Servicio de la Infraestructura de TLA, incluyen la fecha y la hora en el que el acontecimiento ocurrió, el sello de tiempo digital es solicitado a la Autoridad de Sellos Digitales de Tiempo, proporcionado por el Servidor TSA que se encuentra sincronizado con una fuente confiable d tiempo CENAM.

18.3.4 Sistema de Registro de Archivos (Interno o Externo)

El sistema de registro de archivos de SeguriData Privada S.A. de C.V. es interno.

18.4 Recuperación ante Desastres y la Revelación de Claves

SeguriData Privada S.A. de C.V. dispone de procedimientos para la recuperación después de desastres. El objetivo de estos es restaurar las actividades esenciales con la mayor rapidez posible cuando los sistemas y/o operaciones se han visto considerablemente afectados por incendios, huelgas, terremotos, inundaciones, etc.

SeguriData Privada S.A. de C.V. posee un Plan de Continuidad del negocio y Recuperación ante desastres apropiados, que asegura la continuación inmediata de los servicios en caso de una emergencia inesperada. SeguriData Privada S.A. de C.V. considera su Plan de Continuidad del negocio y Recuperación ante desastres como propio, y susceptible de contener información sensible o confidencial. En consecuencia, su contenido no es públicamente disponible, pero si entregado a Secretaria de Economía como parte de la acreditación en el Servicio de TLA.

SeguriData Privada S.A. de C.V. posee un plan frente a la revelación de claves apropiado que detalla sus actividades en caso de revelación de los Datos de Creación de Firma electrónica avanzada del TLA Tales proyectos incluyen procedimientos para:

- Notificación inmediata a todos los clientes del Servicio.
- En caso de revelación de claves de la Autoridad de TLA, SeguriData Privada S.A. de C.V. se compromete al menos a:
- Informar de la revelación de claves a todos los clientes, a la Secretaria de Economía, y otras entidades con las que tenga acuerdos u otro tipo de relaciones establecidas.

Lo anterior está definido en el documento PSC-SEGURIDATA-ANALISISY EVALUACION-DE-RIESGOSYAMENAZAS-TLAV1.0.doc y en el PSC-SEGURIDATA-PLANCONTINUIDADNEGOCIOYRECUPERACIONANTEDESASTRES-TLA V1.0.doc

18.5 Procedimiento de Continuidad del Negocio tras un Desastre

El Plan de Continuidad del Negocio de SeguriData Privada S.A. de C.V. es estrictamente confidencial y contiene:

- Procedimiento de resolución de incidentes y revelación de claves.
- Gestión de Recursos Informáticos, Software, y/o Datos Corrompidos.
- Capacidad de continuidad del negocio y procedimientos después de un desastre.

SeguriData Privada S.A. de C.V. asegurará en caso de un desastre, incluyendo la revelación de los Datos de Creación de Firma electrónica avanzada de TLA, que las operaciones serán restauradas cuanto antes.

El Plan de Continuidad del Negocio (o el Plan de Recuperación ante Desastres) tratará como un desastre la revelación o sospecha de revelación de los Datos de Creación de Firma electrónica avanzada de la Autoridad de TLA.

18.6 Terminación – Cese de la Autoridad de TLA

Las causas por las que puede ocurrir el cese de operaciones de TLA SeguriData Privada S.A. de C.V., como Prestador de Servicios, es que se hayan comprometido los Datos de Creación de Firma electrónica avanzada de la autoridad de TLA, o por toma de decisión de cese de actividades por parte de SeguriData Privada S.A. de C.V.

18.6.1 Suspensión Temporal

Este escenario se presenta cuando la Secretaría de Economía sancione a la autoridad de TLA de SeguriData Privada con la suspensión temporal por incumplir con alguna de las “reglas generales a las que deberá sujetarse un Prestador de Servicios de Certificación”.

Durante el periodo de tiempo definido por la Secretaría de Economía la autoridad de TLA de SeguriData Privada dejará de PROPORCIONAR EL SERVICIO DE DIGITALIZACION
En caso de una suspensión temporal se realizarán las siguientes actividades:

- Informar mediante el sitio WEB de la Suspensión temporal.
- Tratar de restablecer el servicio a la brevedad.
- Anunciar mediante el Sitio WEB, cuando se tenga fecha de restablecimiento del servicio.

18.6.2 Suspensión Definitiva

Si fuera necesario liquidar el servicio de TLA, el impacto de la liquidación será reducido al mínimo posible.

SeguriData Privada S.A. de C.V. define la política a seguir en caso de terminación total o parcial de su operación en cuanto al servicio de TLA:

- Asegurar que cualquier interrupción causada por la terminación de la Autoridad de TLA, es reducida al mínimo.
- Asegurar que los archivos de registro de la Autoridad de TLA son conservados.
- Asegurar que la terminación se notifica puntualmente a los clientes, y otras partes relevantes en la Infraestructura de TLA
- Notificar al gobierno competente y a los órganos de certificación relevantes, la terminación de operaciones, de acuerdo con la legislación vigente.

Antes de que la Autoridad de TLA, cese sus servicios ejecutará los siguientes procedimientos:

- Informará a todos los clientes, con las que mantenga acuerdos u otro tipo de relaciones vinculantes sobre el cese de los servicios.
- Terminará toda la autorización de subcontratistas para actuar de parte de SeguriData Privada S.A. de C.V. en el funcionamiento de cualesquiera funciones relacionadas con el proceso de TLA
- Destruirá o impedirá el uso de sus Datos de Creación de Firma Electrónica.

Se establece en la Declaración de prácticas de la autoridad de TLA y en la Política de la Autoridad de TLA las provisiones hechas para el cese del servicio. Esto incluirá:

- La notificación a las entidades afectadas.
- La transferencia de sus obligaciones a otras partes.

18.6.3 Clasificación y Administración de Activos

La autoridad de TLA de SeguriData Privada mantiene un inventario de todos los activos consistentes con el análisis del riesgo.

19. Limitantes y Restricciones en el Uso de información

La Autoridad de TLA de SeguriData Privada debe tomar las medidas técnicas y operativas apropiadas para mitigar el riesgo de procesamiento no autorizado o ilegal de datos personales y de la pérdida o destrucción accidental, o daño, de datos personales de sus clientes.

La Autoridad de TLA de SeguriData Privada utilizará la información proporcionada por el Cliente en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores.

La Autoridad de TLA de SeguriData Privada utilizará los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el Cliente y/o usuario, para lo cual deberá informar de las medidas de protección y confidencialidad.

19.1 Limitación de Responsabilidad

Las limitaciones de responsabilidad suponen la exclusión de responsabilidad por daños y perjuicios fortuitos o imprevistos directos o indirectos.

19.1.1 Exclusión de Responsabilidad

El TLA de SeguriData Privada S.A. de C.V. no asume ninguna responsabilidad cuando se encuentre ante cualquiera de estas circunstancias:

- Si Los documentos digitalizados bajo el control del reclamante fuera emitido como consecuencia de cualquier falsedad o falsificación de documentos.
- Si lo mensajes de datos firmados no coinciden con los documentos pdf en resguardo de los comerciantes
- Si se ha desarrollado hardware, software, o algoritmos matemáticos, que conviertan en insegura la criptografía de clave pública, siempre que el TLA de SeguriData Privada S.A. de C.V. haga uso de prácticas comercialmente razonables para protegerse contra incumplimientos en la seguridad que sean resultado de tal hardware, software, o algoritmos.
- Uno o más de los acontecimientos siguientes: Un desastre natural (incluyendo sin restricción, inundación, terremoto, u otra causa natural o meteorológica relacionada); huelga; guerra, insurrección u hostilidades militares abiertas; legislación adversa o acción gubernamental, prohibición, embargo, o boicot; revueltas o perturbaciones civiles; incendio

o explosión; epidemia catastrófica; embargo o restricción comercial; cualquier falta de disponibilidad de las telecomunicaciones o integridad; incluyendo obligaciones legales, sentencias de un tribunal competente al que el TLA de SeguriData Privada S.A. de C.V. sea, o pueda ser sujeta; y cualquier acontecimiento o circunstancia fuera del control de la TLA de SeguriData Privada S.A. de C.V.

19.2 Responsabilidades Económicas

Indemnización por Parte de los Clientes

Al grado permitido por la Declaración de Prácticas de Autoridad de TLA aplicables a la Digitalización de SeguriData Privada S.A. de C.V., los clientes indemnizarán a la Autoridad de TLA de SeguriData Privada S.A. de C.V. por:

- Falsedad o mala representación de información proporcionada en la solicitud de Digitalización.
- El uso de parte del cliente de un nombre (incluyendo sin limitación un nombre común, nombre de dominio, IP o correo electrónico) que infrinja los derechos de propiedad intelectual de un tercero.

20 Actualización de la Declaración de prácticas de la Autoridad de Tercero Legalmente Autorizado

La última versión autorizada de este documento de Declaración de prácticas de la Autoridad de Tercero Legalmente Autorizado de SeguriData Privada S.A. de C.V. está en todo momento disponible al público en general en la página <https://psc.seguridata.com/tla>

20.1 Repositorios

SeguriData Privada S.A. de C.V. es responsable de administrar el repositorio de la autoridad del tercero legalmente autorizado.

La Tercero Legalmente Autorizado de SeguriData Privada S.A. de C.V. no mantiene copias de los Datos de Creación de Firma electrónica avanzada asociados con las firmas de los mensajes de datos de los documentos digitalizados.

Disponibilidad del Servicio

El servicio de consulta de digitalización certificada estará disponible siempre que se establezca un contrato entre el digitalizador y el TLA. Y disponible para la validación de firmas el servicio de la autoridad del tercero confiable.

20.1.1 Aspectos Opcionales

Sin estipular.

21 Asuntos Comerciales y Asuntos Legales

La Autoridad de Tercero Legalmente Autorizado de SeguriData Privada S.A. de C.V. es una entidad legalmente constituida de acuerdo con la legislación aplicable.

Las partes de la Infraestructura implicadas en el Servicio de digitalización certificada serán independientes de otras organizaciones en sus decisiones que se relacionen con el establecimiento, aprovisionamiento, mantenimiento y suspensión de servicios; en particular su equipo directivo, el personal competente y el personal encargado de las funciones relevantes deben estar libres de presiones comerciales, financieras y otras que pudieran influir desfavorablemente en la confianza en los servicios que proporcionan.

a. Tarifas

El servicio de Digitalización certificada por parte de la Autoridad del tercero legalmente autorizado, harán disponible todas las tarifas aplicables por la solicitud. Para consultar las tarifas favor de comunicarse a SeguriData Privada S.A. de C.V.

i. Tarifas del Servicio de Digitalización certificada

ii. Para consultar las tarifas favor de comunicarse a SeguriData Privada S.A. de C.V.

iii. Tarifas por otros Servicios

Para consultar las tarifas favor de comunicarse a SeguriData Privada S.A. de C.V.

iv. Responsabilidad Financiera

La Autoridad del Tercero Legalmente Autorizado de SeguriData Privada S.A. de C.V., como Prestador de Servicios de Certificación dispone de recursos financieros para cubrir los daños que pudiesen surgir debido a su operación, de acuerdo a las disposiciones contenidas en el Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación y las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación.

La Tercero Legalmente Autorizado de SeguriData Privada S.A. de C.V. tiene la estabilidad financiera y recursos requeridos para funcionar conforme al documento “COMPROBACION DE CAPITAL PARA INVERSION EN PROYECTO PSC” entregado a la Secretaría de Economía para la acreditación como Prestador de Servicios.

v. Otros Activos

Las Tercero Legalmente Autorizado mantendrán los activos y recursos financieros necesarios para realizar sus deberes dentro de la Infraestructura del Tercero Legalmente Autorizado de SeguriData Privada S.A. de C.V. y serán razonablemente capaces de afrontar sus responsabilidades frente a los clientes.

La autoridad de Tercero Legalmente Autorizado de SeguriData Privada S.A. de C.V. posee los sistemas de calidad adecuados para conseguir la seguridad en la información acorde con los servicios que proporciona.

La Tercero Legalmente Autorizado de SeguriData Privada S.A. de C.V. emplea un número suficiente de personal que tiene, en relación con el tipo, gama y volumen de trabajo, la formación, conocimientos técnicos y experiencia necesarios para proporcionar servicios de Digitalización certificada de documentos en soporte físico.

vi. Cobertura de Seguros o Garantías para Entidades Finales

No estipulado.

vii. Registros Financieros

La autoridad de Tercero Legalmente Autorizado de SeguriData Privada S.A. de C.V. es responsable de mantener sus libros financieros y registros en una manera comercialmente razonable.

b. Protección de confidencialidad de la información

Este subcomponente contiene disposiciones relativas al tratamiento de la información, en nuestro caso de los documentos en soporte físico y posteriormente de la transformación dichos documentos a digital, esto en función de la Ley Federal de Protección de Datos personales en posesión de particulares.

Para ello, en los contratos del servicio que se establecen, se anexan cláusulas de protección de datos como sigue:

CLAUSULA DE PROTECCION DE DATOS EN EL CONTRATO:

“En caso de que con motivo de la Prestación de los Servicios objeto del presente contrato, se integre información que permita la posibilidad de identificar al titular de la misma, o las Partes tengan acceso a datos personales de personas físicas de aquella documentación que sea digitalizada, le son aplicables las disposiciones relacionadas con la protección de datos siempre que como se ha indicado sea posible identificar al titular de la misma, es decir los “Datos Personales”. Por lo anterior, las Partes en este acto se notifican respectivamente su responsabilidad respecto de tratamiento de los Datos Personales y de las medidas de seguridad física, administrativa y tecnológica para conservar la seguridad de los datos. Los Datos Personales serán utilizados por las Partes únicamente para el cumplimiento de lo contratado en el presente instrumento y en concordancia a los términos de sus respectivos Avisos de Privacidad, mismos que se obligan en este acto a respetar, sin perjuicio de la obligación de confidencialidad asumida en términos del presente Contrato.

Las Partes aceptan que es de su conocimiento que los Datos Personales únicamente podrán ser remitidos previo consentimiento de sus titulares y siempre garantizando la confidencialidad de los mismos conforme a las finalidades contenidas del Aviso de Privacidad correspondiente, así como de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y demás normatividad aplicable

La obligación de confidencialidad será vitalicia; sin embargo, a la terminación del presente Contrato y/o sus Anexos, las Partes inmediatamente procederán cuando fuere posible, a la destrucción de los Datos Personales de acuerdo a sus propias políticas y conforme a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares o de las leyes que los rijan dependiendo de la naturaleza de los datos obtenidos”

Adicional a las cláusulas anteriores, se tienen incluidas medidas de seguridad definidas en la Política de Seguridad, que incluyen la cadena de custodia de los documentos en soporte físico, así como la seguridad del resguardo de la digitalización resultante, en bases de datos protegidas mediante autenticación de usuario y password.

Se manejan también los acuerdos de confidencialidad aun después de concluida la relación laboral, con los recursos del TLA y del digitalizador, que intervienen en el proceso de digitalización de documentos en soporte físico.

i. Alcance de la Información Confidencial

Cualquier información personal o corporativa mantenida por el Tercero Legalmente Autorizado de SeguriData Privada S.A. de C.V. y relativa a un servicio de digitalización certificada, es considerada confidencial y no será divulgada sin el consentimiento previo del usuario afectado, a no ser que sea legalmente exigible, de acuerdo con los requisitos de esta Declaración de Prácticas.

Los registros que contengan información relevante serán protegidos de la pérdida, destrucción o falsificación. Algunos registros deben ser conservados para cumplir con las exigencias legales, o para asegurar actividades de negocio esenciales.

ii. Información No Confidencial

La Información incluida en el servicio de digitalización certificada de documentos en soporte físico, o almacenada en el repositorio no es considerada confidencial, a no ser que la legislación o acuerdos contractuales determinen lo contrario.

iii. Revelación de Datos de Conformidad con un Proceso Judicial o Administrativo

La información que los clientes aporten al Servicio de Tercero Legalmente Autorizado de SeguriData Privada S.A. de C.V. será totalmente protegida de su revelación salvo consentimiento del cliente, orden judicial u otra autorización legal.

Sólo en el caso de que un Tribunal exija esta información, tal información será revelada si lo exige un procedimiento civil o administrativo.

iv. Otras Circunstancias de Revelación de Información

La autoridad de Tercero Legalmente Autorizado no tiene obligación alguna de revelar información al margen de una orden judicial legítima y acorde a la ley, que cumpla con las exigencias de esta Declaración de Prácticas de la autoridad del tercero legalmente autorizado.

c. Derechos de Propiedad Intelectual

Esta Declaración de Prácticas de la autoridad de Tercero Legalmente Autorizado y las Marcas y signos distintivos son propiedad de la Autoridad de Tercero Legalmente Autorizado de SeguriData Privada S.A. de C.V.

i. Licencias

El Tercero Legalmente Autorizado de SeguriData Privada S.A. de C.V. está en posesión de licencias de uso del hardware y el software utilizado en la Infraestructura de Tercero Legalmente Autorizado de SeguriData Privada S.A. de C.V., tal y como se especifica en esta Declaración de Prácticas de la autoridad de Tercero Legalmente Autorizado.

d. Representaciones y Garantías

Este subcomponente incluye representaciones y garantías de diversas entidades que se realizan en conformidad con la Política de la autoridad de Tercero Legalmente Autorizado o la Declaración de Prácticas de la autoridad del tercero legalmente autorizado.

e. Garantías del tercero legalmente autorizado

La autoridad de Tercero Legalmente Autorizado de SeguriData Privada S.A. de C.V. por la presente garantiza:

1. Que ha llevado a cabo los procedimientos necesarios para verificar que la información contenida en el mensaje de datos de cada documento digitalizado es exacta y veraz en el momento de su emisión, aunado a la constancia de conservación de mensaje de datos emitida por cada documento digitalizado.
2. Que el servicio de Tercero Legalmente Autorizado será suspendido si la autoridad de Tercero Legalmente Autorizado de SeguriData Privada S.A. de C.V. cree o se le ha notificado que el contenido de los mensajes de datos firmados d los documentos digitalizados son inexactos.

i. Garantías del Cliente

Al cliente se le garantiza que:

1. Toda la información que contiene la documentación digitalizada y el mensaje de datos firmado es verdadera y exacta.
2. El certificado usado para la firma del mensaje de datos del documento digitalizado, a ser usado para su objetivo intencionado, aprobado y legal compatible con esta Declaración de Prácticas de la autoridad de tercero legalmente autorizado.

f. Limitaciones de Responsabilidad

Este subcomponente puede incluir limitaciones de responsabilidad en la Política o en la Declaración de Prácticas de la autoridad de Tercero Legalmente Autorizado o limitaciones que aparecen o deben aparecer en un acuerdo asociado con la Política o en la Declaración de Prácticas de la autoridad de Tercero Legalmente autorizado, tales como una solicitud o un contrato de clientes

g. Indemnizaciones

No Aplica

h. Entrada en Vigor y Terminación

Este subcomponente incluye el período de tiempo en el que la Declaración de Prácticas de la autoridad de Tercero legalmente Autorizado, permanece en vigor desde el momento en que la Secretaría de Economía acredita a SeguriData privada SA de CV en el Servicio de Digitalización certificada como tercero legalmente Autorizado y termina cuando se deja de operar.

i. Entrada en Vigor

Esta Declaración de Prácticas de la autoridad del tercero legalmente autorizado, entra en vigor a partir de su Publicación en la página web <https://psc.seguridata.com/tla>, UNA VEZ QUE LA Secretaría de Economía otorgue la acreditación a la SeguriData Privada SA de CV

ii. Terminación

Esta Declaración de Prácticas de la autoridad de Tercero Legalmente Autorizado permanecerá en vigor hasta que sea modificada o substituida por una versión nueva.

i. Avisos Individuales y Comunicación con los participantes

Los Avisos Individuales y comunicaciones con los participantes se llevarán a cabo en la forma que el participante determinó en el contrato de servicios de Digitalización certificada de documentos en soporte físico.

j. Modificaciones

No Aplica

k. Procedimientos de Resolución de Controversias

Cualquier controversia o reclamación entre dos o más participantes en la Infraestructura de Tercero Legalmente Autorizado de SeguriData Privada S.A. de C.V. surgida con arreglo a esta Declaración de Prácticas de la autoridad de Tercero Legalmente Autorizado se someterá a un tribunal de arbitraje.

l. Ley de Administración

No Aplica

m. Cumplimiento con la Ley Aplicable

No Aplica

n. Disposiciones Varias

No Aplica

Confidencial

SeguriData Privada S.A. de C.V.
2022

Página 77 de 88

o. Otras Disposiciones

No Aplica

p. Obligaciones, Políticas y Procedimientos aplicables a Organizaciones Externas

Para el caso de Organizaciones Externas que apoyan el servicio de Digitalización certificada de documentos en soporte físico, se tiene el caso de KIO, las obligaciones se presentan en el documento de contrato y anexos al mismo, el cual hace referencia a los sitios de Interlomas como principal y Tultitlan como alterno contemplando infraestructura, enlaces y Firewall.

Los procedimientos para el caso de organizaciones externas se mencionan en el documento de Plan de Continuidad del Negocio y Recuperación ante Desastres, donde se menciona también como organización externa al proveedor DELL que maneja los equipos físicos que forman la infraestructura del servicio de digitalización certificada de documentos en soporte físico- figura de tercero legalmente autorizado, y al proveedor Thales para los dispositivos de seguridad

22 Anexos

22.1 Anexo 1 Contrato Marco Comerciante – TLA

CONTRATO DE PRESTACION DE SERVICIOS DE DIGITALIZACION DE DOCUMENTOS EN SOPORTE FÍSICO QUE CELEBRAN POR UNA PARTE, _____, A QUIEN EN LO SUCESIVO SE LE DENOMINARA COMO **"EL CLIENTE"**, REPRESENTADA EN ESTE ACTO POR _____, EN SU CARÁCTER DE REPRESENTANTE LEGAL, Y POR LA OTRA PARTE, **SEGURIDATA PRIVADA, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE**, REPRESENTADA EN ESTE ACTO POR EL SEÑOR JAVIER ALARCON IRIGOYEN, EN SU CARÁCTER DE REPRESENTANTE LEGAL, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ COMO **"SEGURIDATA"**, Y QUE CONJUNTAMENTE CON **"EL CLIENTE"** SE LES DENOMINARÁ COMO **"LAS PARTES"**, DE CONFORMIDAD CON LAS SIGUIENTES:

DECLARACIONES

I.- Declara "El Cliente", por conducto de su representante legal que:

I.1. Es una sociedad mercantil constituida de conformidad con la legislación mexicana, lo que acredita en términos de la Escritura Pública número _____ de fecha _____, otorgada ante la fe del Lic. _____, Notario Público No. de _____, e inscrita ante el Registro Público de la Propiedad y de Comercio de _____ bajo el Folio Mercantil No. _____.

I.2. Cuenta con las facultades suficientes y necesarias para obligar a su representada en los términos del presente instrumento, como lo acreditan con la Escritura Pública Número _____ de fecha _____, otorgada ante la fe del Lic. _____, Notario Público No. _____ de _____, e inscrita ante el Registro Público de la Propiedad y de Comercio de _____ bajo el Folio Mercantil No. _____, manifestando que dichas facultades no les han sido revocadas ni modificadas en forma alguna a esta fecha.

I.3. Tiene su domicilio para todo lo relacionado en el presente contrato en _____.

I.4. Su Registro Federal de Contribuyentes es: _____

I.5. Es su deseo celebrar el presente contrato de prestación de servicios de digitalización con SeguriData Privada S.A. de C.V.

II.- Declara "SEGURIDATA", por conducto de su representante que:

II.1. Su representada es una persona moral de nacionalidad mexicana, constituida bajo las leyes de los Estados Unidos Mexicanos, como consta en Escritura Pública número 29,170 de fecha 17 de diciembre de 1996, otorgada ante la fe del Notario Público Número 107 del Distrito Federal, Licenciado Maximiliano Pérez Salinas, e inscrita en el Registro Público de Comercio del Distrito Federal, bajo el folio mercantil número 218826.

II.2. Cuenta con facultades para celebrar el presente Contrato de Prestación de Servicios, como lo acredita en términos de la Escritura Pública número 35,187 de fecha 15 de noviembre de 2011, otorgada ante la fe del Notario Público Número 218 del Distrito Federal, Licenciado José Luis Villavicencio Castañeda. Manifestando bajo protesta de decir verdad, que dichas facultades no le han sido revocadas, limitadas, ni modificadas en forma alguna a esta fecha.

II.3. Tiene su domicilio en Insurgentes Sur, 2375, 3er piso, Colonia Tizapán San Ángel, C.P. 01000, Ciudad de México.

II.4 Su Registro Federal de Contribuyentes es: SPR961217 NK9

II.5 Que es un Prestador de Servicios de Certificación debidamente acreditado por la Secretaría de Economía para fungir como Tercero Legalmente Autorizado, acreditación que fue publicada en el Diario Oficial de la Federación el día 03 de diciembre de 2019.

III.- Declaran las Partes por conducto cada uno de sus respectivos representantes que:

III.1. Es interés de las Partes llevar a cabo la suscripción del presente Contrato de Prestación de Servicios en cumplimiento a lo señalado en la Regla 176 de las "Reglas a las que deberán sujetarse los Prestadores de Servicios de Certificación publicada en el Diario Oficial de la Federación, el 14 de mayo de 2018 a efecto de establecer las obligaciones y responsabilidades que tendrán cada una de las Partes en el proceso de digitalización de documentos en soporte físico

Expuesto lo anterior, ambas Partes de conformidad, acuerdan en celebrar el presente Contrato de Prestación de Servicios sujetándolo a las siguientes:

CLÁUSULAS

1. CONTRATANTES INDEPENDIENTES.

1.1. Las Partes convienen, que son dos (2) sociedades independientes y que nada de lo contenido en el presente Convenio les otorgará derecho a: (i) Tener cualquiera de las Partes, poder y control directo en las operaciones diarias de la otra Parte; (ii) Constituirse las Partes como accionistas y/o copropietarios de la otra Parte; (iii) Asumir alguna obligación en nombre de la otra Parte bajo ningún propósito; (iv) Todas las obligaciones financieras, laborales, de seguridad social o cualesquiera otras asociadas con los negocios de **El Cliente y SeguriData** son de la exclusiva responsabilidad de cada una de las Partes, según sea el caso.

2. OBJETO DEL CONTRATO

2.1. SeguriData mediante la firma del presente Contrato se obliga a prestar a **El Cliente** los servicios Digitalización de documentos en soporte físico de conformidad con la normatividad

y ordenamientos jurídicos que le son aplicables, enunciativa mas no limitativamente: (a) el Código de Comercio, (b) las Reglas a las que deberán sujetarse los Prestadores de Servicios de Certificación, (en lo sucesivo “Las Reglas”) (c) la Norma Oficial Mexicana NOM 151- SCFI 2016 “Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos” que para tal efecto ha emitido la Secretaría de Economía (en lo sucesivo NOM 151- SCFI 2016) publicada en el Diario Oficial de la Federación el 30 de marzo de 2017, o la que en su momento lasustituya y las Reglas.

2.2 Para efectos del presente Contrato se entenderá por digitalización lo señalado en el Código de Comercio:

“Migración de documentos impresos a mensaje de datos, de acuerdo con lo dispuesto en la Norma Oficial Mexicana sobre Digitalización y Conservación de mensajes de datos que para tal efecto emita la Secretaría”.

Así como lo dispuesto en el numeral 4.3 de la NOM-151:

“Proceso que permite la migración de documentos impresos a mensajes de datos, conforme a lo establecido en el Apéndice Normativo B de la presente Norma Oficial Mexicana”

2.3 El mensaje de datos resultante de la digitalización debe ser fiel al contenido original y garantizar su integridad por medio de la firma electrónica de SeguriData, del Digitalizador y de El Cliente.

El nivel de calidad mínimo para los mensajes de datos resultantes será de 200 píxeles por pulgada o superior para representaciones en blanco y negro, color o escala de grises

Se generará un mensaje de datos que permita asegurar la fidelidad e integridad conforme a los documentos amparados en soportes físicos. El mensaje de datos generado debe ser de alta calidad y se tratará con un intenso control de calidad, de manera que, si existe algún error en el proceso de captura, ésta deberá efectuarse una vez más.

El mensaje de datos será fiel al documento en soporte físico, para lo cual:

- a) Respetará la geometría o aspecto del origen en tamaños y proporciones;
- b) No contendrá caracteres o gráficos que no figurasen en el soporte físico, y
- c) El mensaje de datos generado a partir del proceso de digitalización, deberá permanecer no disponible para su modificación o consulta por parte de El Cliente, mientras se genere la constancia de conservación de mensajes de datos.
- d) Su generación atenderá en todo momento a lo establecido en las Reglas y en la NOM-151- SCFI-2016, al igual que los parámetros definidos, para el cotejo con el algoritmo aplicado para la obtención de la muestra a revisar

3.- OBLIGACIONES Y RESPONSABILIDADES DE LAS PARTES:

SeguriData mediante la firma del presente Contrato se obliga a prestar los servicios que a continuación se relacionan con motivo de los servicios de Digitalización de documentos en soporte físico que se prestarán en favor de El Cliente:

3.1 De SeguriData:

3.1.1. SeguriData fungirá como Tercero Legalmente Autorizado (TLA) y controlará la digitalización de documentos impresos de El Cliente, en los términos que se establezcan en el Código de Comercio, en las “Reglas” y en la NOM 151-SCFI-2016 o la que en su momento la sustituya, incluida la expedición de certificados digitales de firma electrónica para los participantes en el proceso de digitalización, la emisión de constancias de conservación de mensajes de datos y sellos digitales de tiempo a partir de los mensajes de datos resultantes del proceso de digitalización.

SeguriData incluirá su Firma Electrónica Avanzada como Tercero Legalmente Autorizado de la muestra de los documentos y posteriormente de la totalidad de documentos digitalizados, y solicitará al Cliente la aceptación de la muestra, y posteriormente del total de documentos digitalizados, plasmando su firma electrónica, para embeberlos en el archivo digital resultante de la digitalización certificada de cada documento, agregando un sello digital de tiempo y una constancia de conservación.

3.1.2 SeguriData mantendrá y administrará los reportes de cotejo y las actas circunstanciadas de la digitalización de documentos en soporte físico realizadas.

3.1.3 SeguriData entregará al Cliente los certificados de firma electrónica avanzada de uso exclusivo para firma de los mensajes de datos resultantes del proceso de digitalización.

3.1.4. La responsabilidad está limitada exclusivamente a proveer los servicios que le corresponden en términos del presente Contrato, de acuerdo con lo establecido en su propia Declaración de Prácticas de Digitalización de Documentos en soporte físico, y la Política de Digitalización de Documentos en soporte físico, acordes a la normatividad aplicable.

SeguriData estará exenta de toda responsabilidad en los casos que enunciativa, pero no limitativamente se señalan a continuación:

- a) Por cualquier actividad no prestada directamente por SeguriData al Cliente
- b) Por los daños y/o perjuicios que se causen, si El Cliente entrega datos y/o documentos falsos o alterados, para la obtención de los servicios de digitalización objeto del presente Contrato.
- c) Por cualquier tipo de daños y/o perjuicios que sufra El Cliente, siempre que éstos deriven de la indebida utilización de los servicios por parte de El Cliente.
- d) Por los daños y/o perjuicios que se causen al Cliente por la errónea interpretación, análisis, síntesis o conclusión respecto de los servicios por parte o del propio Cliente, sin que estas hayan sido confirmadas expresamente por SeguriData.
- e) Por la interrupción o alteración temporal del servicio por causas ajenas a SeguriData que afecte sus instalaciones o limiten la libertad en las comunicaciones.

3.2 De El Cliente:

3.2.1. El Cliente deberá definir los documentos que desea digitalizar y solicitar los servicios de digitalización a SeguriData.

3.2.2 El Cliente deberá definir formato de la imagen resultante del proceso de digitalización certificada, ya sea para su entrega o para su resguardo según el alcance del servicio contratado por El Cliente, como se define en el ANEXO 1 del presente contrato.

3.2.3 El Cliente deberá definir el tipo de envase de recolección de los documentos en soporte físico.

3.2.4 El Cliente deberá firmar el formato de recepción con el detalle de dichos documentos.

3.2.5 Definir el Método de Control documental relacionando principalmente la cantidad y el tipo de documentación que recibe, definiendo esencialmente si es original, copia simple o copia certificada, y cualquier otro elemento que permita identificarlos.

3.2.6 El Cliente en conjunto con el TLA y el Digitalizador definen el tipo de muestreo que usará para la verificación de la Digitalización, así como el tamaño de la muestra, posterior a ello, deberá aceptar el total de documentos digitalizados, plasmando su firma electrónica avanzada, para embeberlos en el archivo digital resultante de la digitalización certificada de cada documento, agregando un sello y una constancia de conservación. El certificado de firma electrónica avanzada será de uso exclusivo para firma de los archivos resultantes del proceso de digitalización.

3.2.7 El Cliente deberá resguardar sus claves de acceso en el servicio de Digitalización de Documentos en soporte físico.

3.2.8 El Cliente deberá verificar que el certificado no esté revocado.

3.2.9 El Cliente podrá participar de manera opcional en la Validación de la muestra en función de la determinación del tamaño y tipo de muestra que permitan realizar un proceso de cotejo de los mensajes de datos resultantes de la digitalización contra los documentos en soporte físico.

3.2.10 En caso de devolución al Cliente de los documentos a digitalizar se deberá generar un acta de entrega con el detalle de los documentos que se devuelven la cual deberá ser firmada por El Cliente.

3.2.8. En caso de destrucción se deberá generar un acta de destrucción que también deberá firmar El Cliente.

3.2.9. Si el Cliente requiere del resguardo de sus archivos digitales, SeguriData se encargará de ofrecer el espacio de almacenamiento y los esquemas de consulta de estos.

3.2.10 Se definirá junto con SeguriData el lapso del servicio y el esquema de entrega de información al terminar el servicio contratado.

4. CARACTERÍSTICAS DEL SERVICIO

4.1 Con base en la cláusula que antecede, Las Partes señalan que las características específicas de los servicios de digitalización objeto del presente contrato serán las que se señalan

en el ANEXO 1 que se adjunta al presente y que firmado por ambas partes forma parte integrante del mismo.

5. CONTRAPRESTACIÓN

5.1. Para efectos del presente contrato, El Cliente pagará a SeguriData por los servicios objeto del presente Contrato las cantidades que se determinan en el Anexo 1, en la forma que en el mismo se establecen, el cual debidamente firmado por las Partes forma parte integrante del mismo.

6. CONFIDENCIALIDAD

6.1. SeguriData garantiza a El Cliente que cuenta con los elementos humanos, materiales, económicos y tecnológicos requerido para prestar los servicios de digitalización objeto del presente contrato y su confidencialidad.

6.2. Las Partes en este acto se obligan a guardar y mantener la confidencialidad de cualquier información que sea recibida, proporcionada o dada a conocer por la otra Parte y/o cualquiera de sus subsidiarias o filiales, incluyendo de manera enunciativa más no limitativa, toda aquella información relativa a sus operaciones, ruta crítica, negocios, productos, servicios, métodos, procesos, procedimientos, información de sistemas, contratos, convenios, descubrimientos, ideas, diseños, dibujos, programas, "know-how", información financiera, información técnica, listas de clientes actuales o potenciales, bases de datos, planes, proyectos y políticas de negocio, métodos de mercadeo, estrategias, costos, o cualquier otra información aun cuando dicha información conste en cualquier clase de documento, archivo, material, medio magnético y/o electrónico, así como las conversaciones y pláticas que sean grabadas o conservadas en cualquier medio magnético y/o electrónico, documento, archivo y/o material en donde se haga constar la citada información (en lo sucesivo la "Información Confidencial").

7. PROTECCION DE DATOS PERSONALES

7.1. En caso de que con motivo de la Prestación de los Servicios objeto del presente contrato, se integre información que permita la posibilidad de identificar al titular de la misma, o las Partes tengan acceso a datos personales de personas físicas de aquella documentación que sea digitalizada, le son aplicables las disposiciones relacionadas con la protección de datos siempre que como se ha indicado sea posible identificar al titular de la misma, es decir los "Datos Personales". Por lo anterior, las Partes en este acto se notifican respectivamente su responsabilidad respecto de tratamiento de los Datos Personales y de las medidas de seguridad físicas, administrativas y tecnológicas para conservar la seguridad de los datos. Los Datos Personales serán utilizados por las Partes únicamente para el cumplimiento de lo contratado en el presente instrumento y en concordancia a los términos de sus respectivos Avisos de Privacidad, mismos que se obligan en este acto a respetar, sin perjuicio de la obligación de confidencialidad asumida en términos del presente Contrato.

7.2 Las Partes aceptan que es de su conocimiento que los Datos Personales únicamente podrán ser remitidos previo consentimiento de sus titulares y siempre garantizando la confidencialidad de los mismos conforme a las finalidades contenidas del Aviso de Privacidad correspondiente, así como de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y demás normatividad aplicable

7.3 La obligación de confidencialidad será vitalicia; sin embargo, a la terminación del presente Contrato y/o sus Anexos, las Partes inmediatamente procederán cuando fuere posible, a la destrucción de los Datos Personales de acuerdo a sus propias políticas y conforme a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares o de las leyes que los rijan dependiendo de la naturaleza de los datos obtenidos.

8. PROPIEDAD INDUSTRIAL Y/O INTELECTUAL.

8.1 SeguriData garantiza a El Cliente haber obtenido de los titulares respectivos, los derechos de propiedad industrial e intelectual, que resulten necesarios para la aportación de los Bienes, Software y/o Servicios requeridos por El Cliente y, por lo tanto, garantiza que no se vulnera disposición legal, convenio, derecho o propiedad intelectual de terceros, ni de ningún modo constituye competencia desleal.

8.2 SeguriData garantiza que los Bienes, Software y/o Servicios aportados y que forman parte del presente instrumento, no violan disposición gubernamental, ley o reglamento vigente alguno, ni tampoco derechos de propiedad industrial o intelectual de terceros, por lo que, en caso de que cualquier tercero iniciara en contra El Cliente alguna denuncia, querella, demanda, requerimiento extrajudicial, juicio o procedimiento judicial o administrativo relacionado de manera directa o indirecta con derechos de propiedad industrial o intelectual de terceros, Las Partes se compromete a su cargo y costa a poner en paz y a salvo los intereses de El Cliente dejando a El Cliente, libre de cualquier responsabilidad.

9. VIGENCIA Y TERMINACION.

9.1. El presente Contrato tendrá una vigencia indefinida, sin embargo cada proceso de digitalización tendrá la vigencia que se señale particularmente en la Cláusula Cuarta.

10. GENERALES.

10.1. Ninguna de las estipulaciones del presente Contrato podrá ser cedida o transferida por las Partes a terceros sin el consentimiento previo y por escrito de cada una de ellas.

10.2. En virtud de lo estipulado en el párrafo anterior, cada una de las Partes se obligan a mantener, indemnizar y a sacar en paz y a salvo a la otra, en contra de cualquier demanda o reclamación que se le hiciere por parte de alguno de sus trabajadores o prestadores de servicios, así como en contra de cualquier reclamación de parte de alguna autoridad derivada del cumplimiento o incumplimiento de obligaciones patronales o de seguridad social a cargo de la parte de que se trate.

10.3. Las Partes se comprometen a partir de la fecha de firma del presente Contrato y hasta doce (12) meses posteriores a la fecha de su terminación cualquiera que fuera la causa, a no ofrecer propuestas de trabajo o contratar de manera directa al personal de la otra sin que medie autorización escrita para ello.

En caso de incumplimiento a la obligación objeto de este apartado, la parte que incumpla

pagará a la parte afectada, una pena convencional equivalente al cien por ciento (100%) de los salarios o contraprestación pagada a la persona de que se trate durante los doce (12) meses anteriores a la fecha de terminación de su relación con la parte afectada.

10.4. La no utilización de algún derecho por alguna de las Partes no implicará la renuncia al ejercicio de dicho derecho.

10.5. El presente Contrato y sus Anexos constituyen la totalidad del acuerdo al que han llegado las Partes, cancelando cualquier aviso o comunicación que al efecto hayan celebrado con anterioridad y sólo podrá ser modificado mediante la celebración de un Contrato o Contrato diverso entre las Partes, debidamente firmado por sus representantes legales.

10.6. Ninguna de las Partes será responsable frente a la otra por incumplimiento o demora en relación con las estipulaciones del presente Contrato, cuando éstos se deban por causas de caso fortuito o fuerza mayor, en tanto que dicha causa sea subsanable en un periodo razonable de tiempo.

10.7. Todos los avisos o notificaciones legales que se dirijan las Partes deberán efectuarse por mensajero con acuse de recibo o mediante correo certificado a los domicilios señalados por cada una de ellas.

10.8. Todos los impuestos que se generen con motivo del cumplimiento del presente Contrato y/o del Contrato de Prestación de Servicios y sus Anexos, si los hubiera, serán pagados por la Parte a quien le correspondan, de conformidad con las disposiciones legales aplicables.

11. DISPUTAS.

11.1. Las Partes están de acuerdo en:

- a) Resolución Administrativa de Disputas. Las Partes acuerdan reunirse y debatir de buena fe cualesquiera asuntos controvertidos, reclamados o disputados que surjan en relación con este Contrato. Si dichos asuntos no pudieran resolverse entre los contactos técnicos y/o contractuales de las Partes, cada una de ellas podrá someter dichos asuntos a sus respectivos Representantes Legales, durante un plazo de 10 (diez) días, mediante notificación por escrito que explique la Disputa con razonable detalle, a fin de darle solución a la misma.
- b) Resolución Judicial. En caso de que las Partes no puedan resolver de manera Administrativa cualquier asunto controvertido, reclamado o disputado, se resolverá de manera definitiva en base a la legislación y tribunales competentes de la Ciudad de México.

12. SITUACIONES NO PREVISTAS.

12.1. Las Partes convienen en que intentarán resolver de común acuerdo aquellas situaciones no previstas en el presente Contrato, quedando entendido que las resoluciones que se adopten deberán constar por escrito y serán firmadas por ambas Partes.

13. DOMICILIOS PARA NOTIFICACIONES.

13.1. Cualquier aviso o notificación que se dirijan LAS PARTES deberán efectuarse por mensajero o correo certificado a los domicilios señalados por cada una de ellas en el Capítulo de Declaraciones. Por lo que cualquier notificación, documentación o aviso enviado por Las Partes al domicilio señalado, surtirá todos los efectos legales a que haya lugar, en

tanto no sea notificado por escrito con acuse de recibo cualquier cambio de domicilio, con por lo menos 5 (cinco) días de anticipación.

14 DISPOSICIONES LEGALES.

14.1. Cualquier término o disposición del presente Contrato que contravenga a las leyes o disposiciones de los Estados Unidos Mexicanos, se considerará reformada de tal manera que se observe el cumplimiento de dichas leyes o disposiciones, sin perjuicio de que los términos y condiciones acordes con dicha legislación no sufrirán modificación alguna y continuarán vigentes para todos los efectos legales derivados del presente instrumento.

15. JURISDICCIÓN.

15.1. Para la interpretación y cumplimiento del presente Contrato, las Partes se someten a la jurisdicción y competencia de los tribunales de la Ciudad de México, renunciando a cualquier otro fuero que por razón de su domicilio presente o futuro o que por cualquier otra causa pudiere corresponderles.

ENTERADAS LAS PARTES DEL CONTENIDO Y ALCANCE LEGAL DE ESTE CONTRATO, PROCEDEN A FIRMARLO POR DUPLICADO EN LA CIUDAD DE MEXICO, CON FECHA _____ DEL 20__.

"EL CLIENTE"	"SEGURIDATA"
	SEGURIDATA PRIVADA, S.A. DE C.V.
REPRESENTANTE LEGAL	LIC. JAVIER ALARCON IRIGOYEN. REPRESENTANTE LEGAL

ANEXO 1

DEL CONTRATO DE PRESTACION DE SERVICIOS DE DIGITALIZACIÓN DE DOCUMENTOS
EN SOPORTE FÍSICO CELEBRADO ENTRE
_____, A QUIEN EN LO SUCESIVO SE LE
DENOMINARA COMO “EL CLIENTE”, Y SEGURIDATA PRIVADA, SOCIEDAD ANÓNIMA
DE CAPITAL VARIABLE, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ COMO “SEGURIDATA”,
Y CONJUNTAMENTE SE LES DENOMINARÁ COMO “LAS PARTES”

CARACTERÍSTICAS DEL SERVICIO:

1. Tipo de envase para recolección documentos:

El Cliente deberá elegir el tipo de envase para la recolección de documentos, la cual podrá ser:

- a) Bolsa plástica de seguridad
- b) Valija con cintillo de seguridad con folio
- c) Ambas

2. Fecha y domicilio en la que se recogerán los documentos:

3. Tipo de Expediente:

El Cliente deberá señalar el tipo de documentos de que se trata, por ejemplo, contratos, órdenes de compra, identificaciones, comprobantes de domicilio, estados financieros, etc.

4. Tipo de documento:

Se deberá señalar si los documentos se entregan en original, copia o copia certificada:

5. Cantidad de documentos:

La digitalización se lleva a cabo considerando la legibilidad, calidad de papel y completez de los documentos entregados por el Cliente reflejándose fielmente tal y como se entregaron. En caso de tener algún requerimiento especial para la digitalización, El Cliente deberá señalarlo:

[illegible][illegible]

9. Tipo de técnica de muestreo elegido:

El Cliente con apoyo del TLA y del Digitalizador deberá elegir una técnica de muestreo en términos de la regla 226 de Las "Reglas":

- a) Muestreo aleatorio simple.
- b) Muestreo aleatorio sistemático.
- c) Muestreo aleatorio estratificado desproporcionado.
- d) Muestreo por grupos

10. Forma en que se entregarán al Cliente los mensajes de datos una vez realizada la digitalización:

11. El Cliente señala que es su deseo que una vez que sean digitalizados los documentos:

- a) Sean destruidos
- b) Le sean devueltos

El Cliente declara que los datos asentados son ciertos y serán los que rijan los servicios de digitalización de documentos en soporte físico objeto del presente Anexo.

ENTERADAS LAS PARTES DEL CONTENIDO Y ALCANCE LEGAL DE ESTE ANEXO, PROCEDEN A FIRMARLO POR DUPLICADO EN LA CIUDAD DE MEXICO, CON FECHA _____ DEL 20__.

"EL CLIENTE"	"SEGURIDATA"
	SEGURIDATA PRIVADA, S.A. DE C.V.
REPRESENTANTE LEGAL	LIC. JAVIER ALARCON IRIGOYEN. REPRESENTANTE LEGAL

CONTRATO DE PRESTACION DE SERVICIOS DE DIGITALIZACION DE DOCUMENTOS EN SOPORTE FÍSICO QUE CELEBRAN, POR UNA PARTE, _____, POR SU PROPIO DERECHO, _____, A QUIEN EN LO SUCESIVO SE LE DENOMINARA COMO “**EL CLIENTE**”, Y POR LA OTRA PARTE, **SEGURIDATA PRIVADA, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE**, REPRESENTADA EN ESTE ACTO POR EL SEÑOR JAVIER ALARCON IRIGOYEN, EN SU CARÁCTER DE REPRESENTANTE LEGAL, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ COMO “**SEGURIDATA**”, Y QUE CONJUNTAMENTE CON “**EL CLIENTE**” SE LES DENOMINARÁ COMO “**LAS PARTES**”, DE CONFORMIDAD CON LAS SIGUIENTES:

DECLARACIONES

I.- Declara “El Cliente”, por su propio derecho, que:

- I.1.** Es mayor de edad, con plena capacidad para celebrar y obligarse en términos del presente contrato.
- I.2.** Tiene su domicilio para todo lo relacionado en el presente contrato en _____.
- I.3.** Su Registro Federal de Contribuyentes es: _____
- I.4.** Es su deseo celebrar el presente contrato de prestación de servicios de digitalización con SeguriData Privada S.A. de C.V.
- I.5.** Es su deseo celebrar el presente contrato de prestación de servicios de digitalización con SeguriData Privada S.A. de C.V.

II.- Declara “SEGURIDATA”, por conducto de su representante que:

- II.1.** Su representada es una persona moral de nacionalidad mexicana, constituida bajo las leyes de los Estados Unidos Mexicanos, como consta en Escritura Pública número 29,170 de fecha 17 de diciembre de 1996, otorgada ante la fe del Notario Público Número 107 del Distrito Federal, Licenciado Maximiliano Pérez Salinas, e inscrita en el Registro Público de Comercio del Distrito Federal, bajo el folio mercantil número 218826.
- II.2.** Cuenta con facultades para celebrar el presente Contrato de Prestación de Servicios, como lo acredita en términos de la Escritura Pública número 35,187 de fecha 15 de noviembre de 2011, otorgada ante la fe del Notario Público Número 218 del Distrito Federal, Licenciado José Luis Villavicencio Castañeda. Manifestando bajo protesta de decir verdad, que dichas facultades no le han sido revocadas, limitadas, ni modificadas en forma alguna a esta fecha.
- II.3.** Tiene su domicilio en Insurgentes Sur, 2375, 3er piso, Colonia Tizapán San Ángel, C.P. 01000, Ciudad de México.

II.4 Su Registro Federal de Contribuyentes es: SPR961217 NK9

II.5 Que es un Prestador de Servicios de Certificación debidamente acreditado por la Secretaría de Economía para fungir como Tercero Legalmente Autorizado, acreditación que fue publicada en el Diario Oficial de la Federación el día 03 de diciembre de 2019.

III.- Declaran las Partes que:

III.1. Es interés de las Partes llevar a cabo la suscripción del presente Contrato de Prestación de Servicios en cumplimiento a lo señalado en la Regla 176 de las "Reglas a las que deberán sujetarse los Prestadores de Servicios de Certificación publicada en el Diario Oficial de la Federación, el 14 de mayo de 2018 a efecto de establecer las obligaciones y responsabilidades que tendrán cada una de las Partes en el proceso de digitalización de documentos en soporte físico

Expuesto lo anterior, ambas Partes de conformidad, acuerdan en celebrar el presente Contrato de Prestación de Servicios sujetándolo a las siguientes:

CLÁUSULAS

1. CONTRATANTES INDEPENDIENTES.

1.1. Las Partes convienen, que son dos (2) partes independientes y que nada de lo contenido en el presente Convenio les otorgará derecho a: (i) Tener cualquiera de las Partes, poder y control directo en las operaciones diarias de la otra Parte; (ii) Constituirse las Partes como accionistas y/o copropietarios de la otra Parte; (iii) Asumir alguna obligación en nombre de la otra Parte bajo ningún propósito; (iv) Todas las obligaciones financieras, laborales, de seguridad social o cualesquiera otras asociadas con los negocios de **El Cliente y SeguriData** son de la exclusiva responsabilidad de cada una de las Partes, según sea el caso.

2. OBJETO DEL CONTRATO

2.1. SeguriData mediante la firma del presente Contrato se obliga a prestar a **El Cliente** los servicios Digitalización de documentos en soporte físico de conformidad con la normatividad y ordenamientos jurídicos que le son aplicables, enunciativa mas no limitativamente: (a) el Código de Comercio, (b) las Reglas a las que deberán sujetarse los Prestadores de Servicios de Certificación, (en lo sucesivo "Las Reglas") (c) la Norma Oficial Mexicana NOM 151- SCFI 2016 "Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos" que para tal efecto ha emitido la Secretaría de Economía (en lo sucesivo NOM 151- SCFI 2016) publicada en el Diario Oficial de la Federación el 30 de marzo de 2017, o la que en su momento lasustituya y las Reglas.

2.2 Para efectos del presente Contrato se entenderá por digitalización lo señalado en el Código de Comercio:

“Migración de documentos impresos a mensaje de datos, de acuerdo con lo dispuesto en la Norma Oficial Mexicana sobre Digitalización y Conservación de mensajes de datos que para tal efecto emita la Secretaría”.

Así como lo dispuesto en el numeral 4.3 de la NOM-151:

“Proceso que permite la migración de documentos impresos a mensajes de datos, conforme a lo establecido en el Apéndice Normativo B de la presente Norma Oficial Mexicana”

2.3 El mensaje de datos resultante de la digitalización debe ser fiel al contenido original y garantizar su integridad por medio de la firma electrónica de SeguriData, del Digitalizador y de El Cliente.

El nivel de calidad mínimo para los mensajes de datos resultantes será de 200 píxeles por pulgada o superior para representaciones en blanco y negro, color o escala de grises

Se generará un mensaje de datos que permita asegurar la fidelidad e integridad conforme a los documentos amparados en soportes físicos. El mensaje de datos generado debe ser de alta calidad y se tratará con un intenso control de calidad, de manera que, si existe algún error en el proceso de captura, ésta deberá efectuarse una vez más.

El mensaje de datos será fiel al documento en soporte físico, para lo cual:

- a) Respetará la geometría o aspecto del origen en tamaños y proporciones;
- b) No contendrá caracteres o gráficos que no figurasen en el soporte físico, y
- c) El mensaje de datos generado a partir del proceso de digitalización, deberá permanecer no disponible para su modificación o consulta por parte de El Cliente, mientras se genere la constancia de conservación de mensajes de datos.
- d) Su generación atenderá en todo momento a lo establecido en las Reglas y en la NOM-151- SCFI-2016, al igual que los parámetros definidos, para el cotejo con el algoritmo aplicado para la obtención de la muestra a revisar

3.- OBLIGACIONES Y RESPONSABILIDADES DE LAS PARTES:

SeguriData mediante la firma del presente Contrato se obliga a prestar los servicios que a continuación se relacionan con motivo de los servicios de Digitalización de documentos en soporte físico que se prestarán en favor de El Cliente:

3.1 De SeguriData:

3.1.1. SeguriData fungirá como Tercero Legalmente Autorizado (TLA) y controlará la digitalización de documentos impresos de El Cliente, en los términos que se establezcan en el Código de Comercio, en las “Reglas” y en la NOM 151-SCFI-2016 o la que en su momento la sustituya, incluida la expedición de certificados digitales de firma electrónica para los participantes en el proceso de digitalización, la emisión de constancias de conservación de mensajes de datos y sellos digitales de tiempo a partir de los mensajes de datos resultantes del proceso de digitalización.

SeguriData incluirá su Firma Electrónica Avanzada como Tercero Legalmente Autorizado de la muestra de los documentos y posteriormente de la totalidad de documentos digitalizados, y solicitará al Cliente la aceptación de la muestra, y posteriormente del total de documentos digitalizados, plasmando su firma electrónica, para embeberlos en el archivo digital resultante de la digitalización certificada de cada documento, agregando un sello digital de tiempo y una constancia de conservación.

3.1.2 SeguriData mantendrá y administrará los reportes de cotejo y las actas circunstanciadas de la digitalización de documentos en soporte físico realizadas.

3.1.3 SeguriData entregará al Cliente los certificados de firma electrónica avanzada de uso exclusivo para firma de los mensajes de datos resultantes del proceso de digitalización.

3.1.4. La responsabilidad está limitada exclusivamente a proveer los servicios que le corresponden en términos del presente Contrato, de acuerdo con lo establecido en su propia Declaración de Prácticas de Digitalización de Documentos en soporte físico, y la Política de Digitalización de Documentos en soporte físico, acordes a la normatividad aplicable.

SeguriData estará exenta de toda responsabilidad en los casos que enunciativa, pero no limitativamente se señalan a continuación:

- a) Por cualquier actividad no prestada directamente por SeguriData al Cliente
- b) Por los daños y/o perjuicios que se causen, si El Cliente entrega datos y/o documentos falsos o alterados, para la obtención de los servicios de digitalización objeto del presente Contrato.
- c) Por cualquier tipo de daños y/o perjuicios que sufra El Cliente, siempre que éstos deriven de la indebida utilización de los servicios por parte de El Cliente.
- d) Por los daños y/o perjuicios que se causen al Cliente por la errónea interpretación, análisis, síntesis o conclusión respecto de los servicios por parte o del propio Cliente, sin que estas hayan sido confirmadas expresamente por SeguriData.
- e) Por la interrupción o alteración temporal del servicio por causas ajenas a SeguriData que afecte sus instalaciones o limiten la libertad en las comunicaciones.

3.2 De El Cliente:

3.2.1. El Cliente deberá definir los documentos que desea digitalizar y solicitar los servicios de digitalización a SeguriData.

3.2.2 El Cliente deberá definir formato de la imagen resultante del proceso de digitalización certificada, ya sea para su entrega o para su resguardo según el alcance del servicio contratado por El Cliente, como se define en el ANEXO 1 del presente contrato.

3.2.3 El Cliente deberá definir el tipo de envase de recolección de los documentos en soporte físico.

3.2.4 El Cliente deberá firmar el formato de recepción con el detalle de dichos documentos.

3.2.5 Definir el Método de Control documental relacionando principalmente la cantidad y el tipo de documentación que recibe, definiendo esencialmente si es original, copia

simple o copia certificada, y cualquier otro elemento que permita identificarlos.

3.2.6 El Cliente en conjunto con el TLA y el Digitalizador definen el tipo de muestreo que usará para la verificación de la Digitalización, así como el tamaño de la muestra, posterior a ello, deberá aceptar el total de documentos digitalizados, plasmando su firma electrónica avanzada, para embeberlos en el archivo digital resultante de la digitalización certificada de cada documento, agregando un sello y una constancia de conservación. El certificado de firma electrónica avanzada será de uso exclusivo para firma de los archivos resultantes del proceso de digitalización.

3.2.7 El Cliente deberá resguardar sus claves de acceso en el servicio de Digitalización de Documentos en soporte físico.

3.2.8 El Cliente deberá verificar que el certificado no esté revocado.

3.2.63.2.9 El Cliente podrá participar de manera opcional en la Validación de la muestra en función de la determinación del tamaño y tipo de muestra que permitan realizar un proceso de cotejo de los mensajes de datos resultantes de la digitalización contra los documentos en soporte físico.

3.2.73.2.10 En caso de devolución al Cliente de los documentos a digitalizar se deberá generar un acta de entrega con el detalle de los documentos que se devuelven la cual deberá ser firmada por El Cliente.

3.2.8. En caso de destrucción se deberá generar un acta de destrucción que también deberá firmar El Cliente.

3.2.9. Si el Cliente requiere del resguardo de sus archivos digitales, SeguriData se encargará de ofrecer el espacio de almacenamiento y los esquemas de consulta de estos.

3.2.10 Se definirá junto con SeguriData el lapso del servicio y el esquema de entrega de información al terminar el servicio contratado.

4. CARACTERÍSTICAS DEL SERVICIO

4.1 Con base en la cláusula que antecede, Las Partes señalan que las características específicas de los servicios de digitalización objeto del presente contrato serán las que se señalan en el ANEXO 1 que se adjunta al presente y que firmado por ambas partes forma parte integrante del mismo.

5. CONTRAPRESTACIÓN

5.1. Para efectos del presente contrato, El Cliente pagará a SeguriData por los servicios objeto del presente Contrato las cantidades que se determinan en el Anexo 1, en la forma que en el mismo se establecen, el cual debidamente firmado por las Partes forma parte integrante del mismo.

6. CONFIDENCIALIDAD

6.1. SeguriData garantiza a El Cliente que cuenta con los elementos humanos, materiales, económicos y tecnológicos requerido para prestar los servicios de digitalización objeto del presente contrato y su confidencialidad.

6.2. Las Partes en este acto se obligan a guardar y mantener la confidencialidad de cualquier información que sea recibida, proporcionada o dada a conocer por la otra Parte y/o cualquiera de sus subsidiarias o filiales, incluyendo de manera enunciativa más no limitativa, toda aquella información relativa a sus operaciones, ruta crítica, negocios, productos, servicios, métodos, procesos, procedimientos, información de sistemas, contratos, convenios, descubrimientos, ideas, diseños, dibujos, programas, "know-how", información financiera, información técnica, listas de clientes actuales o potenciales, bases de datos, planes, proyectos y políticas de negocio, métodos de mercadeo, estrategias, costos, o cualquier otra información aun cuando dicha información conste en cualquier clase de documento, archivo, material, medio magnético y/o electrónico, así como las conversaciones y pláticas que sean grabadas o conservadas en cualquier medio magnético y/o electrónico, documento, archivo y/o material en donde se haga constar la citada información (en lo sucesivo la "Información Confidencial").

7. PROTECCION DE DATOS PERSONALES

7.1. En caso de que con motivo de la Prestación de los Servicios objeto del presente contrato, se integre información que permita la posibilidad de identificar al titular de la misma, o las Partes tengan acceso a datos personales de personas físicas de aquella documentación que sea digitalizada, le son aplicables las disposiciones relacionadas con la protección de datos siempre que como se ha indicado sea posible identificar al titular de la misma, es decir los "Datos Personales". Por lo anterior, las Partes en este acto se notifican respectivamente su responsabilidad respecto de tratamiento de los Datos Personales y de las medidas de seguridad físicas, administrativas y tecnológicas para conservar la seguridad de los datos. Los Datos Personales serán utilizados por las Partes únicamente para el cumplimiento de lo contratado en el presente instrumento y en concordancia a los términos de sus respectivos Avisos de Privacidad, mismos que se obligan en este acto a respetar, sin perjuicio de la obligación de confidencialidad asumida en términos del presente Contrato.

7.2 Las Partes aceptan que es de su conocimiento que los Datos Personales únicamente podrán ser remitidos previo consentimiento de sus titulares y siempre garantizando la confidencialidad de los mismos conforme a las finalidades contenidas del Aviso de Privacidad correspondiente, así como de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y demás normatividad aplicable

7.3 La obligación de confidencialidad será vitalicia; sin embargo, a la terminación del presente Contrato y/o sus Anexos, las Partes inmediatamente procederán cuando fuere posible, a la destrucción de los Datos Personales de acuerdo a sus propias políticas y conforme a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares o de las leyes que los rijan dependiendo de la naturaleza de los datos obtenidos.

8. PROPIEDAD INDUSTRIAL Y/O INTELECTUAL.

8.1 SeguriData garantiza a El Cliente haber obtenido de los titulares respectivos, los derechos de propiedad industrial e intelectual, que resulten necesarios para la aportación de los Bienes, Software y/o Servicios requeridos por El Cliente y, por lo tanto, garantiza que no se vulnera disposición legal, convenio, derecho o propiedad intelectual de terceros, ni de ningún modo constituye competencia desleal.

8.2 SeguriData garantiza que los Bienes, Software y/o Servicios aportados y que forman parte del presente instrumento, no violan disposición gubernamental, ley o reglamento vigente alguno, ni tampoco derechos de propiedad industrial o intelectual de terceros, por lo que, en caso de que cualquier tercero iniciara en contra El Cliente alguna denuncia, querella, demanda, requerimiento extrajudicial, juicio o procedimiento judicial o administrativo relacionado de manera directa o indirecta con derechos de propiedad industrial o intelectual de terceros, Las Partes se compromete a su cargo y costa a poner en paz y a salvo los intereses de El Cliente dejando a El Cliente, libre de cualquier responsabilidad.

9. VIGENCIA Y TERMINACION.

9.1. El presente Contrato tendrá una vigencia indefinida, sin embargo cada proceso de digitalización tendrá la vigencia que se señale particularmente en la Cláusula Cuarta.

10. GENERALES.

10.1. Ninguna de las estipulaciones del presente Contrato podrá ser cedida o transferida por las Partes a terceros sin el consentimiento previo y por escrito de cada una de ellas.

10.2. En virtud de lo estipulado en el párrafo anterior, cada una de las Partes se obligan a mantener, indemnizar y a sacar en paz y a salvo a la otra, en contra de cualquier demanda o reclamación que se le hiciere por parte de alguno de sus trabajadores o prestadores de servicios, así como en contra de cualquier reclamación de parte de alguna autoridad derivada del cumplimiento o incumplimiento de obligaciones patronales o de seguridad social a cargo de la parte de que se trate.

10.3. Las Partes se comprometen a partir de la fecha de firma del presente Contrato y hasta doce (12) meses posteriores a la fecha de su terminación cualquiera que fuera la causa, a no ofrecer propuestas de trabajo o contratar de manera directa al personal de la otra sin que medie autorización escrita para ello.

En caso de incumplimiento a la obligación objeto de este apartado, la parte que incumpla pagará a la parte afectada, una pena convencional equivalente al cien por ciento (100%) de los salarios o contraprestación pagada a la persona de que se trate durante los doce (12) meses anteriores a la fecha de terminación de su relación con la parte afectada.

10.4. La no utilización de algún derecho por alguna de las Partes no implicará la renuncia al ejercicio de dicho derecho.

10.5. El presente Contrato y sus Anexos constituyen la totalidad del acuerdo al que han llegado las Partes, cancelando cualquier aviso o comunicación que al efecto hayan celebrado con anterioridad y sólo podrá ser modificado mediante la celebración de un Contrato o Contrato diverso entre las Partes, debidamente firmado por sus representantes legales.

10.6. Ninguna de las Partes será responsable frente a la otra por incumplimiento o demora en relación con las estipulaciones del presente Contrato, cuando éstos se deban por causas de caso fortuito o fuerza mayor, en tanto que dicha causa sea subsanable en un periodo razonable de tiempo.

10.7. Todos los avisos o notificaciones legales que se dirijan las Partes deberán efectuarse por mensajero con acuse de recibo o mediante correo certificado a los domicilios señalados por cada una de ellas.

10.8. Todos los impuestos que se generen con motivo del cumplimiento del presente Contrato y/o del Contrato de Prestación de Servicios y sus Anexos, si los hubiera, serán pagados por la Parte a quien le correspondan, de conformidad con las disposiciones legales aplicables.

11. DISPUTAS.

11.1. Las Partes están de acuerdo en:

- a) Resolución Administrativa de Disputas. Las Partes acuerdan reunirse y debatir de buena fe cualesquiera asuntos controvertidos, reclamados o disputados que surjan en relación con este Contrato. Si dichos asuntos no pudieran resolverse entre los contactos técnicos y/o contractuales de las Partes, cada una de ellas podrá someter dichos asuntos a sus respectivos Representantes Legales, durante un plazo de 10 (diez) días, mediante notificación por escrito que explique la Disputa con razonable detalle, a fin de darle solución a la misma.
- b) Resolución Judicial. En caso de que las Partes no puedan resolver de manera Administrativa cualquier asunto controvertido, reclamado o disputado, se resolverá de manera definitiva en base a la legislación y tribunales competentes de la Ciudad de México.

12. SITUACIONES NO PREVISTAS.

12.1. Las Partes convienen en que intentarán resolver de común acuerdo aquellas situaciones no previstas en el presente Contrato, quedando entendido que las resoluciones que se adopten deberán constar por escrito y serán firmadas por ambas Partes.

13. DOMICILIOS PARA NOTIFICACIONES.

13.1. Cualquier aviso o notificación que se dirijan LAS PARTES deberán efectuarse por mensajero o correo certificado a los domicilios señalados por cada una de ellas en el Capítulo de Declaraciones. Por lo que cualquier notificación, documentación o aviso enviado por Las Partes al domicilio señalado, surtirá todos los efectos legales a que haya lugar, en

tanto no sea notificado por escrito con acuse de recibo cualquier cambio de domicilio, con por lo menos 5 (cinco) días de anticipación.

14 DISPOSICIONES LEGALES.

14.1. Cualquier término o disposición del presente Contrato que contravenga a las leyes o disposiciones de los Estados Unidos Mexicanos, se considerará reformada de tal manera que se observe el cumplimiento de dichas leyes o disposiciones, sin perjuicio de que los términos y condiciones acordes con dicha legislación no sufrirán modificación alguna y continuarán vigentes para todos los efectos legales derivados del presente instrumento.

15. JURISDICCIÓN.

15.1. Para la interpretación y cumplimiento del presente Contrato, las Partes se someten a la jurisdicción y competencia de los tribunales de la Ciudad de México, renunciando a cualquier otro fuero que por razón de su domicilio presente o futuro o que por cualquier otra causa pudiere corresponderles.

ENTERADAS LAS PARTES DEL CONTENIDO Y ALCANCE LEGAL DE ESTE CONTRATO, PROCEDEN A FIRMARLO POR DUPLICADO EN LA CIUDAD DE MEXICO, CON FECHA _____ DEL 20____.

"EL CLIENTE"	"SEGURIDATA"
XXXXXXXXXXXXXXXXXXXXXXXXXXXX	SEGURIDATA PRIVADA, S.A. DE C.V.
XXXXXXXXXXXXXXXXXXXXXXXXXXXX	LIC. JAVIER ALARCON IRIGOYEN. REPRESENTANTE LEGAL

ANEXO 1

DEL CONTRATO DE PRESTACION DE SERVICIOS DE DIGITALIZACIÓN DE DOCUMENTOS
EN SOPORTE FÍSICO _____ **CELEBRADO ENTRE**
 _____ **POR SU PROPIO DERECHO , A QUIEN EN LO**
SUCESIVO SE LE DENOMINARA COMO “EL CLIENTE”, Y SEGURIDATA PRIVADA,
SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ
COMO “SEGURIDATA”, Y CONJUNTAMENTE SE LES DENOMINARÁ COMO “LAS PARTES”

CARACTERÍSTICAS DEL SERVICIO:

1. Tipo de envase para recolección documentos:

El Cliente deberá elegir el tipo de envase para la recolección de documentos, la cual podrá ser:

- a) Bolsa plástica de seguridad
- b) Valija con cintillo de seguridad con folio
- c) Ambas

2. Fecha y domicilio en la que se recogerán los documentos:

3. Tipo de Expediente:

El Cliente deberá señalar el tipo de documentos de que se trata, por ejemplo, contratos, órdenes de compra, identificaciones, comprobantes de domicilio, estados financieros, etc.

4. Tipo de documento:

Se deberá señalar si los documentos se entregan en original, copia o copia certificada:

5. Cantidad de documentos:

6. Lote de los documentos (cuando aplique):

7. Requerimientos Especiales:

La digitalización se lleva a cabo considerando la legibilidad, calidad de papel y completez de los documentos entregados por el Cliente reflejándose fielmente tal y como se entregaron. En caso de tener algún requerimiento especial para la digitalización, El Cliente deberá señalarlo:

8. Metadato elegido por el Cliente:

9. Tipo de técnica de muestreo elegido:

El Cliente con apoyo del TLA y del Digitalizador deberá elegir una técnica de muestreo en términos de la regla 226 de Las "Reglas":

- a) Muestreo aleatorio simple.
- b) Muestreo aleatorio sistemático.
- c) Muestreo aleatorio estratificado desproporcionado.
- d) Muestreo por grupos

10. Forma en que se entregarán al Cliente los mensajes de datos una vez realizada la digitalización:

11. El Cliente señala que es su deseo que una vez que sean digitalizados los documentos:

- a) Sean destruidos
- b) Le sean devueltos

El Cliente declara que los datos asentados son ciertos y serán los que rijan los servicios de digitalización de documentos en soporte físico objeto del presente Anexo.

ENTERADAS LAS PARTES DEL CONTENIDO Y ALCANCE LEGAL DE ESTE ANEXO, PROCEDEN A FIRMARLO POR DUPLICADO EN LA CIUDAD DE MEXICO, CON FECHA _____ DEL 20__.

"EL CLIENTE"	"SEGURIDATA"
XXXXXXXXXXXXXXXXXXXXX	SEGURIDATA PRIVADA, S.A. DE C.V.
XXXXXXXXXXXXXXXXXXXXX	LIC. JAVIER ALARCON IRIGOYEN. REPRESENTANTE LEGAL

22.2 Anexo 2 Anexo con especificaciones de Digitalización como parte del Contrato entre TLA y comerciante

ANEXO 1

DEL CONTRATO DE PRESTACION DE SERVICIOS DE DIGITALIZACIÓN DE DOCUMENTOS
EN SOPORTE FÍSICO CELEBRADO ENTRE
_____, A QUIEN EN LO SUCESIVO SE LE
DENOMINARA COMO “EL CLIENTE”, Y SEGURIDATA PRIVADA, SOCIEDAD ANÓNIMA
DE CAPITAL VARIABLE, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ COMO “SEGURIDATA”,
Y CONJUNTAMENTE SE LES DENOMINARÁ COMO “LAS PARTES”

CARACTERÍSTICAS DEL SERVICIO:

1. Tipo de envase para recolección documentos:

El Cliente deberá elegir el tipo de envase para la recolección de documentos, la cual podrá ser:

- a) Bolsa plástica de seguridad
- b) Valija con cintillo de seguridad con folio
- c) Ambas

2. Fecha y domicilio en la que se recogerán los documentos:

3. Tipo de Expediente:

El Cliente deberá señalar el tipo de documentos de que se trata, por ejemplo, contratos, órdenes de compra, identificaciones, comprobantes de domicilio, estados financieros, etc.

4. Tipo de documento:

Se deberá señalar si los documentos se entregan en original, copia o copia certificada:

5. Cantidad de documentos:

[illegible]

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins, text, or other markings on the paper.

9. Tipo de técnica de muestreo elegido:

El Cliente con apoyo del TLA y del Digitalizador deberá elegir una técnica de muestreo en términos de la regla 226 de Las "Reglas":

- a) Muestreo aleatorio simple.
- b) Muestreo aleatorio sistemático.
- c) Muestreo aleatorio estratificado desproporcionado.
- d) Muestreo por grupos

10. Forma en que se entregarán al Cliente los mensajes de datos una vez realizada la digitalización:

11. El Cliente señala que es su deseo que una vez que sean digitalizados los documentos:

- a) Sean destruidos
- b) Le sean devueltos

El Cliente declara que los datos asentados son ciertos y serán los que rijan los servicios de digitalización de documentos en soporte físico objeto del presente Anexo.

ENTERADAS LAS PARTES DEL CONTENIDO Y ALCANCE LEGAL DE ESTE ANEXO, PROCEDEN A FIRMARLO POR DUPLICADO EN LA CIUDAD DE MEXICO, CON FECHA _____ DEL 2019.

"EL CLIENTE"	"SEGURIDATA"
	SEGURIDATA PRIVADA, S.A. DE C.V.
REPRESENTANTE LEGAL	LIC. JAVIER ALARCON IRIGOYEN. REPRESENTANTE LEGAL

22.3 Anexo 3 Carta uso exclusivo de certificado PSC

Ciudad de México, a ____ de _____ de _____

CARTA RESPONSIVA Y ACUERDO DE RESGUARDO

El que suscribe _____ en nombre y representación de _____, en lo sucesivo "El Cliente"; en mi carácter de usuario del certificado para firmas electrónicas emitido por SeguriData Privada S.A. de C.V., en su carácter de Prestador de Servicios de Certificación y TLA, por medio de la presente manifiesto mi conocimiento y aceptación a los términos y condiciones para la obtención, uso y manejo de Firma electrónica y certificado digital, mismos que utilizarán única y exclusivamente para el firmado de los archivos digitales resultantes del proceso de Digitalización de los documentos de El Cliente, en términos de la Norma Oficial Mexicana NOM-SCFI-151-2016, "Requisitos que deben observarse para la Conservación de mensajes de datos y digitalización de documentos".

En este acto manifiesto de manera expresa mi consentimiento entiendo y asumo mi responsabilidad respecto del uso adecuado del Certificado digital de firma electrónica así como de las llaves que para tales efectos se generen, y que me sean entregadas por SeguriData.

De igual manera manifiesto de manera expresa mi consentimiento para que SeguriData resguarde las llaves que para efectos del uso del certificado me sean generadas.

Por su parte SeguriData se obliga a la guarda y debida custodia de las llaves, así como de la confidencialidad de los datos de mis datos personales, en términos de su Aviso de Privacidad.

Atentamente

NOMBRE DEL CLIENTE

Representado por:

22.4 Anexo 4 Convenio alianza con digitalizador - Contrato de servicios digitalizador – TLA

CONVENIO DE ALIANZA ESTRATEGICA QUE CELEBRAN POR UNA PARTE, "**Colocar nombre de digitalizador**", A QUIEN EN LO SUCESIVO SE LE DENOMINARA COMO **“NOMBRE DE DIGITALIZADOR”** , REPRESENTADA EN ESTE ACTO POR EL _____, EN SU CARÁCTER DE REPRESENTANTE LEGAL, Y POR LA OTRA PARTE, **SEGURIDATA PRIVADA, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE**, REPRESENTADA EN ESTE ACTO POR EL SEÑOR JAVIER ALARCON IRIGOYEN, EN SU CARÁCTER DE REPRESENTANTE LEGAL, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ COMO **“SEGURIDATA”**, Y QUE CONJUNTAMENTE CON **“NOMBRE DE DIGITALIZADOR”** SE LES DENOMINARÁ COMO **“LAS PARTES”**, DE CONFORMIDAD CON LAS SIGUIENTES:

DECLARACIONES

I.- Declara **“NOMBRE DE DIGITALIZADOR”** , por conducto de su representante legal que:

I.1. Es una sociedad mercantil constituida de conformidad con la legislación mexicana, lo que acredita en términos de la Escritura Pública número _____ de fecha _____, otorgada ante la fe del _____, Notario Público No. _____ de la Ciudad _____, e inscrita ante el Registro Público de la Propiedad y de Comercio de la Ciudad de México, bajo el Folio Mercantil _____ de fecha _____.

I.2. Cuenta con las facultades suficientes y necesarias para obligar a su representada en los términos del presente instrumento, como lo acredita con la Escritura Pública Número _____ de fecha _____, otorgada ante la fe del Notario Público Número _____ del _____, Lic. _____, manifestando que dichas facultades no les han sido revocadas ni modificadas en forma alguna a esta fecha.

I.3. Tiene su domicilio en _____

I.4. Su Registro Federal de Contribuyentes es: _____

I.5. Ha decidido celebrar el presente Convenio de Alianza con **“SEGURIDATA”**, ya que ésta cuenta con la experiencia e infraestructura administrativa, organizacional y operativa apropiada, así como los recursos humanos, técnicos y financieros necesarios para desarrollar los servicios referidos en el presente Convenio.

II.- Declara **"SEGURIDATA"**, por conducto de su representante que:

II.1. Su representada es una persona moral de nacionalidad mexicana, constituida bajo las leyes de los Estados Unidos Mexicanos, como consta en Escritura Pública número 29,170 de fecha 17 de diciembre de 1996, otorgada ante la fe del Notario Público Número 107 del Distrito Federal, Licenciado Maximiliano Pérez Salinas, e inscrita en el Registro Público de Comercio del Distrito Federal, bajo el folio mercantil número 218826.

II.2. Cuenta con facultades para celebrar el presente Convenio, como lo acredita en términos de la Escritura Pública número 35,187 de fecha 15 de noviembre de 2011, otorgada ante la fe del Notario Público Número 218 del Distrito Federal, Licenciado José Luis Villavicencio Castañeda. Manifestando bajo protesta de decir verdad, que dichas facultades no le han sido revocadas, limitadas, ni modificadas en forma alguna a esta fecha.

II.3. Tiene su domicilio en Insurgentes Sur, 2375, 3er piso, Colonia Tizapán San Ángel, C.P. 01000, Ciudad de México.

II.4. Que es un Prestador de Servicios de Certificación debidamente acreditado por la Secretaría de Economía para fungir como Tercero Legalmente Autorizado, acreditación que fue publicada en el Diario Oficial de la Federación el día 03 de diciembre de 2019.

II.5 Ha decidido celebrar el presente Convenio de Alianza con **“NOMBRE DE DIGITALIZADOR”**, ya que éste cuenta con la experiencia e infraestructura administrativa, organizacional y operativa apropiada, así como los recursos humanos, técnicos y financieros necesarios para desarrollar los servicios referidos en el presente Convenio.

II.6 Su Registro Federal de Contribuyentes es: SPR961217 NK9

III.- Declaran las Partes por conducto cada uno de sus respectivos representantes que:

III.1. Es interés de las Partes promover la suscripción del presente Convenio de Alianza Estratégica, para aprovechar recíprocamente las fortalezas y experiencias de servicios, a efecto de ofrecer y proporcionar a los Clientes de ambas partes (a los que para efectos del presente Convenio podrá denominárseles individualmente como “El Cliente”) los siguientes servicios:

Por parte de “NOMBRE DE DIGITALIZADOR”:

- La digitalización de documentos en soporte físico, en los términos que se establezca en la Norma Oficial Mexicana “Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos” que para tal efecto ha emitido la Secretaría de Economía (en lo sucesivo NOM 151- SCFI 2016) publicada en el Diario Oficial de la Federación el 30 de marzo de 2017, o la que en su momento la sustituya.

Para efectos del presente Contrato se entenderá por digitalización lo señalado en el Código de Comercio:

“Digitalización: Migración de documentos impresos a mensaje de datos, de acuerdo con lo dispuesto en la Norma Oficial Mexicana sobre Digitalización y Conservación de mensajes de datos que para tal efecto emita la Secretaría”.

Así como lo dispuesto en el numeral 4.3 de la NOM-151-SCFI-2016: “Digitalización: Proceso que permite la migración de documentos impresos a mensajes de datos, conforme a lo establecido en el Apéndice Normativo B de la presente Norma Oficial Mexicana”

Por parte de SEGURIDATA

- Servicios relacionados con firmas electrónicas,
- Expedición de certificados digitales de firma electrónica,
- Prestar servicios relacionados con la firma electrónica como la conservación de mensajes de datos y sellos digitales de tiempo
- Fungir en calidad de tercero legalmente autorizado

III.2. Cada una de las Partes asume las obligaciones y responsabilidades inherentes a las actividades que a cada uno compete y que son descritas en el presente contrato, lo anterior,

de conformidad con la normatividad y ordenamientos jurídicos que le son aplicables, enunciativa mas no limitativamente: el Código de Comercio, las Reglas a las que deberán sujetarse los Prestadores de Servicios de Certificación, la Norma Oficial Mexicana 151-SCFI-2016 “Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos” que para tal efecto ha emitido la Secretaría de Economía (en lo sucesivo NOM 151- SCFI-2016) publicada en el Diario Oficial de la Federación el 30 de marzo de 2017, o la que en su momento la sustituya.

Expuesto lo anterior, ambas Partes de conformidad, acuerdan en celebrar el presente Convenio sujetándolo a las siguientes:

CLÁUSULAS

1. CONTRATANTES INDEPENDIENTES.

1.1. Las Partes convienen, que son dos (2) sociedades independientes y que nada de lo contenido en el presente Convenio les otorgará derecho a: (i) Tener cualquiera de las Partes, poder y control directo en las operaciones diarias de la otra Parte; (ii) Constituirse las Partes como accionistas y/o copropietarios de la otra Parte; (iii) Asumir alguna obligación en nombre de la otra Parte bajo ningún propósito; (iv) Todas las obligaciones financieras, laborales, de seguridad social o cualesquiera otras asociadas con los negocios de “NOMBRE DE DIGITALIZADOR” y “**SEGURIDATA**” son de la exclusiva responsabilidad de cada una de las Partes, según sea el caso.

2. ACUERDOS GENERALES DE LA ALIANZA.

2.1. Las Partes mediante la firma del presente Convenio constituyen una alianza estratégica con el objeto de unir esfuerzos para desarrollar o buscar oportunidades de negocios sobre los productos y servicios relacionados en **la Declaración III.1** que antecede.

2.2. El objetivo del Convenio de Alianza Estratégica entre “NOMBRE DE DIGITALIZADOR” y “**SEGURIDATA**” se circunscribirá a:

Por parte de **SEGURIDATA**:

Servicios relacionados con firmas electrónicas, expedición de certificados digitales de firma, o prestar servicios relacionados como la emisión de constancias de conservación de mensajes de datos, el sellado digital de tiempo y fungir en calidad de tercero legalmente autorizado (TLA),

Por parte de “**NOMBRE DE DIGITALIZADOR**”:

La digitalización de documentos impresos, en los términos que se establezca en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos (en lo sucesivo NOM 151-SCFI 2016) o la que en su momento la sustituya.

2.3. El servicio para el Cliente final estará conformado por 2 (dos) componentes que se complementan perfectamente entre sí, uno aportado por “**NOMBRE DE DIGITALIZADOR**” y otro aportado por “**SEGURIDATA**”:

2.3.1. “SEGURIDATA” es responsable de:

- 1.- Proporcionar a **“NOMBRE DE DIGITALIZADOR”** en su carácter de Digitalizador los elementos técnicos necesarios para integrar las funcionalidades de Firma Electrónica Avanzada en los documentos digitalizados, como TLA en función de la NOM 151-SCFI-2016
- 2.- Atender la solicitud de **“NOMBRE DE DIGITALIZADOR”** para la generación de constancias de conservación de mensaje de datos y sellos digitales de tiempo a partir de los archivos electrónicos resultante del proceso de digitalización.
- 3.- La responsabilidad está limitada exclusivamente a proveer los servicios que le corresponden en términos del presente Convenio, de acuerdo con lo establecido en sus propias Declaraciones y Políticas, acordes a la normatividad aplicable.
- 4.- SeguriData Privada S.A. de C.V. estará exenta de toda responsabilidad en los casos que enunciativa, pero no limitativamente se señalan a continuación:
 - a) Por cualquier actividad no prestada directamente por SeguriData y que corresponda a **“NOMBRE DE DIGITALIZADOR”**
 - b) Por los daños y/o perjuicios que se causen, si el cliente entrega datos y/o documentos falsos o alterados, para la obtención de los servicios objeto del presente convenio.
 - c) Por cualquier tipo de daños y/o perjuicios que sufran sus Clientes, siempre que éstos deriven de la indebida utilización de los servicios por parte de dichos Clientes.
 - d) Por los daños y/o perjuicios que se causen al Cliente por la errónea interpretación, análisis, síntesis o conclusión respecto de los Servicios por parte de **“NOMBRE DE DIGITALIZADOR”** o del propio Cliente, sin que estas hayan sido confirmadas expresamente por SeguriData.
 - e) Por la interrupción o alteración temporal del servicio por causas ajenas a SeguriData que afecte sus instalaciones o limiten la libertad en las comunicaciones.
5. **SEGURIDATA** tiene la obligación y es responsable de mantener y administrar los reportes de cotejo y las actas circunstanciadas de la digitalización de documentos en soporte físico realizadas

2.3.2. “NOMBRE DE DIGITALIZADOR” aportará y desarrollará todas las tareas operativas asociadas a los servicios siguientes:

a) Firma de contrato con SeguriData como TLA

“NOMBRE DE DIGITALIZADOR” firmará con SeguriData un contrato de prestación de servicios previo a la Digitalización de documentos en soporte físico, este contrato debe firmarse por cada proceso de digitalización que se realice.

b) Preparación para digitalización:

- “NOMBRE DE DIGITALIZADOR” recibirá o trasladará a sus instalaciones, los documentos físicos a ser digitalizados, generando un acta de recepción con el detalle de dichos documentos la cual deberá ser firmada por el Cliente.
- Una vez con los documentos a digitalizar en sus instalaciones y de acuerdo con el alcance del servicio con el Cliente, se podrán clasificar, reordenar, validar contra una lista de comprobación, para su acomodo previo a su digitalización.
- De igual forma se debe validar que los documentos no contengan grapas, clips u otro tipo de objetos que impidan su adecuada digitalización.
- Los documentos ya ordenados, indexados o clasificados quedaran listos para su digitalización por parte de “NOMBRE DE DIGITALIZADOR”.
- Definirá en conjunto con el Cliente el Método de Control como ID.

c) Digitalización de documentos:

- Los documentos se digitalizarán en el scanner definido por “NOMBRE DE DIGITALIZADOR” para el proceso en el área correspondiente.
- Durante su digitalización no deberán alterarse, ni desordenarse, para que al terminar el proceso vuelva a quedar integrado de acuerdo con lo convenido en el Contrato que celebre con SeguriData
- Los documentos físicos se deberán resguardar para su devolución al Cliente o para su destrucción según el alcance del servicio convenido en el contrato correspondiente.
- En caso de devolución al Cliente se deberá generar un acta de entrega con el detalle de los documentos entregados la cual deberá ser firmada por el Cliente.
- En caso de destrucción se deberá generar un acta de destrucción.

d) Archivos de imágenes certificadas:

- Durante el proceso de digitalización, “NOMBRE DE DIGITALIZADOR” solicitará vía web services a “SEGURIDATA” la firma como Tercero Legalmente Autorizado, de la muestra y posteriormente de la totalidad de documentos digitalizados, y al Cliente le solicitará la aceptación de la muestra , y posteriormente del total de documentos digitalizados, plasmando su firma (y en caso opcional según lo establece la Norma NOM 151-SCFI-2016, la firma de un Fedatario), para embeberlos en el archivo digital resultante de la digitalización certificada, de cada documento , agregando un sello y una constancia de conservación.
- “SEGURIDATA” deberá tener habilitados sus servicios de certificados digitales, estampillas de tiempo y constancias de la NOM-151 para el servicio, así como el de TLA:
- Como resultado del proceso de digitalización certificada se obtendrán los archivos digitales en el formato definido para el Cliente, ya sea para su entrega o resguardo según el alcance del servicio

e) Resguardo de imágenes certificadas:

- Si el Cliente requiere del resguardo de sus archivos digitales, “NOMBRE DE DIGITALIZADOR” se encargará de ofrecer el espacio de almacenamiento y los esquemas de consulta de estos.
- Se definirá el lapso del servicio y el esquema de entrega de información al terminar la vigencia del contrato del servicio.
- De igual forma se podría definir que al término del ciclo de vida de la información,

los archivos digitales puedan ser eliminados tomando en cuenta la legislación aplicable para cada tipo de documento.

f) Niveles de calidad

- El mensaje de datos resultante de la digitalización debe ser fiel al contenido original y garantizar su integridad por medio de la firma electrónica de SeguriData como TLA, "NOMBRE DE DIGITALIZADOR" como Digitalizador y la del Cliente; y de manera opcional de así solicitarlo el cliente, la firma de algún fedatario público.
- El nivel de calidad mínimo para los mensajes de datos resultantes será de 200 píxeles por pulgada o superior para representaciones en blanco y negro, color o escala de grises
- Se generará un mensaje de datos que permita asegurar la fidelidad e integridad conforme a los documentos amparados en soportes físicos; el mensaje de datos generado debe ser de alta calidad y se tratará con un intenso control de calidad, de manera que, si existe algún error en el proceso de captura, ésta deberá efectuarse una vez más.
- El mensaje de datos será fiel al documento en soporte físico, para lo cual:
 - a) Respetará la geometría o aspecto del origen en tamaños y proporciones;
 - b) No contendrá caracteres o gráficos que no figurasen en el soporte físico, y
 - c) El mensaje de datos generado a partir del proceso de digitalización, deberá permanecer no disponible para su modificación o consulta por parte del solicitante del servicio, mientras se genere la constancia de conservación de mensajes de datos.
 - d) Su generación atenderá en todo momento a lo establecido en la NOM-151-SCFI-2016, al igual que los parámetros definidos, para la compulsa con el algoritmo aplicado para la obtención de la muestra a revisar
- "NOMBRE DE DIGITALIZADOR" atenderá las revisiones que SeguriData requiera realizar a "NOMBRE DE DIGITALIZADOR", en función a lo referido en la NOM 151-SCFI-2016, en cuanto a Hardware, Software y documentación relacionada al servicio de Digitalización en soporte físico de documentos, siendo en todo momento responsabilidad de "NOMBRE DE DIGITALIZADOR" el proceso de digitalización

Asimismo, "NOMBRE DE DIGITALIZADOR" definirá a su sola discreción el precio final que ésta última cobrará a sus Clientes.

2.3.3 Será obligación de "NOMBRE DE DIGITALIZADOR" :

- Cumplir con el Plan de Gestión de Calidad definido por SeguriData
- Mantener las medidas de seguridad definidas en la Política de Seguridad por SeguriData

2.3.4. Responsabilidades de "NOMBRE DE DIGITALIZADOR" :

"NOMBRE DE DIGITALIZADOR" será responsable por cualquier error, falla u omisión en el proceso de digitalización o preparación para la digitalización, debiendo sacar y mantener en paz a SeguriData de cualquier reclamación por parte del Cliente., siendo SeguriData como TLA la responsable directa frente al Cliente del proceso completo de Digitalización de documentos en soporte físico

“NOMBRE DE DIGITALIZADOR” tiene la obligación y será responsable de cumplir con el Plan de Gestión de Calidad definido por SeguriData Privada S.A. de C.V., así como cumplir y mantener las medidas de seguridad definidas en la Política de Seguridad de SeguriData Privada S.A. de C.V.

2.3.5. Cada una de las Partes actuará bajo su propio nombre ante sus respectivos Clientes, desarrollando las siguientes acciones:

a) Determinarán los precios, los porcentajes de comisión, clase de servicio, fecha de entrega de los productos y servicios, condiciones comerciales y los aspectos técnicos del proyecto de que se trate, los que se establecerán en un Contrato de Prestación de Servicios y en su caso en sus Anexos respectivos, los que deberán estar firmados por los representantes legales de cada una de las Partes, mismos que se numerarán progresivamente conforme las Partes lo celebren en cada proyecto.

b) Cada proyecto deberá registrarse ante la Parte que presente al Cliente, conforme al procedimiento señalado en la cláusula 3.

c) “NOMBRE DE DIGITALIZADOR” y “SEGURIDATA” actuarán como aliados comerciales exclusivos cuando detecten con alguno de sus Clientes, proyectos relacionados con los servicios respaldados por cualquiera de las Partes, dando aviso a la Parte interesada para presentar sus respectivos servicios, siendo responsable la Parte interesada de toda la labor técnica respectiva.

d) “NOMBRE DE DIGITALIZADOR” podrá prestar servicios, entre otros de consultoría, a clientes de “SEGURIDATA”, cuando ésta última le invite a prestar dichos servicios. “NOMBRE DE DIGITALIZADOR” será responsable de la prestación de dichos servicios, de conformidad con los términos y condiciones que se establezcan por escrito para tales efectos.

e) Las Partes en este acto se obligan a llevar a cabo los Servicios de acuerdo a las fechas comprometidas con El Cliente.

2.4. Las Partes podrán realizar los actos a que se refiere esta cláusula en toda la República Mexicana y en cualquier otro lugar que estimen conveniente, previa la firma del acuerdo respectivo.

2.5. Las Partes se obligan a ejecutar de manera coordinada todas las actividades relativas a demostraciones, prototipos, propuestas, etc. y en general, para llevar a cabo todas las acciones necesarias concernientes a los proyectos que resulten conforme a este Convenio.

2.6. Las Partes convienen y aceptan que cada una de ellas asume de manera independiente cualquier responsabilidad, reclamación o demanda que pudieran instaurar una en contra de la otra; o incluso los Clientes en contra de una u otra, en virtud de la prestación de los servicios que cada una realice.

3. REGISTRO DE PROYECTOS.

3.1. “NOMBRE DE DIGITALIZADOR” y “SEGURIDATA” registrarán en forma escrita (correo electrónico y/o cualquier otro medio), los proyectos de sus Clientes en los que se

pretendan introducir sus productos y servicios conjuntos, con el fin de evitar conflictos con otras alianzas o socios de negocios de las Partes, o por proyectos independientes. Cualquiera de las Partes podrá rechazar el registro de alguno de esos proyectos, si estos ya han sido registrados de manera independiente precisamente por alguna de las Partes, o por algún otro Socio de Negocios y el proyecto está considerado como probable o activo.

3.2. En el caso de que se generen nuevos proyectos con un mismo Cliente o prospecto, las Partes también deberán registrarlos de acuerdo con el procedimiento mencionado en el primer párrafo de esta cláusula

4. CONFIDENCIALIDAD.

4.1. Las Partes en este acto se obligan a guardar y mantener la confidencialidad de cualquier información que sea recibida, proporcionada o dada a conocer por la otra Parte y/o cualquiera de sus subsidiarias o filiales, incluyendo de manera enunciativa más no limitativa, toda aquella información relativa a sus operaciones, ruta crítica, negocios, productos, servicios, métodos, procesos, procedimientos, información de sistemas, contratos, convenios, descubrimientos, ideas, diseños, dibujos, programas, "know-how", información financiera, información técnica, listas de clientes actuales o potenciales, bases de datos, planes, proyectos y políticas de negocio, métodos de mercadeo, estrategias, costos, o cualquier otra información aun cuando dicha información conste en cualquier clase de documento, archivo, material, medio magnético y/o electrónico, así como las conversaciones y pláticas que sean grabadas o conservadas en cualquier medio magnético y/o electrónico, documento, archivo y/o material en donde se haga constar la citada información (en lo sucesivo la "Información Confidencial").

4.1.1. Las Partes se obligan de manera enunciativa, más no limitativa a:

a) No revelar, divulgar y/o transmitir la Información Confidencial (i) a terceros; o (ii) a consejeros, funcionarios, empleados, representantes, asesores, subcontratistas o agentes a quienes no sea indispensable revelarles la Información Confidencial. Asimismo, las Partes harán que sus consejeros, funcionarios, empleados, representantes, asesores, subcontratistas o agentes que tengan acceso o conocimiento de la Información Confidencial, la guarden y mantengan bajo dicho carácter, cumpliendo con las obligaciones de confidencialidad que aquí se estipulan. Lo anterior, en el entendido de que las Partes deberán, en caso de ser necesario, celebrar todos aquellos Contratos o convenios de confidencialidad a fin de que sus consejeros, funcionarios, empleados, representantes, asesores, subcontratistas o agentes protejan la Información Confidencial. Asimismo, cada una de las Partes deberá capacitar a sus consejeros, funcionarios, empleados, representantes, asesores, subcontratistas o agentes en relación con el uso y cuidado que deben guardar respecto de la Información Confidencial, así como darles a conocer los alcances de las obligaciones de confidencialidad contenidas en el presente Convenio.

b) Proteger la Información Confidencial que les haya sido revelada, con el mismo grado de cuidado, pero nunca en grado menor, al que emplean para proteger su propia Información Confidencial.

c) No utilizar en beneficio propio y/o de terceros la Información Confidencial que les sea de alguna manera revelada por alguna de las Partes, en el entendido de que las mismas solo la utilizarán conforme a lo previsto en el presente Convenio.

Las Partes aceptan que el término “Información Confidencial” de ninguna manera incluirá: (i) toda aquella información que de manera indubitable las Partes hubiesen poseído con anterioridad a la fecha de celebración del presente Convenio; (ii) toda aquella información que hayan obtenido legalmente de un tercero, sin que dicho tercero haya tenido la obligación de mantenerla bajo dicho carácter de confidencial; (iii) toda aquella información que sea del dominio público; (iv) toda aquella información que sea revelada por una de las Partes con previa autorización por escrito de la otra Parte para llevar a cabo dicha revelación; y (v) toda aquella información que requiera ser reportada o divulgada a las autoridades judiciales o administrativas en cumplimiento de alguna ley, reglamento o decreto que resulte aplicable a la Parte que la divulgue, o bien que dicho requerimiento de divulgación sea resultado de una orden, sentencia o laudo que sea obligatorio para una de las Partes, situación en la cual la Parte que tenga la obligación de divulgar o revelar la Información Confidencial deberá inmediatamente informar sobre dicha obligación a la otra Parte.

4.2. En caso de violación a la obligación antes mencionada por alguna de las Partes, la otra Parte podrá ejercer las acciones penales, civiles y administrativas a que el hecho de lugar, así como rescindir el presente Convenio, ello sin perjuicio de exigir el pago de los daños y perjuicios que conforme a derecho le correspondan.

4.3. Al término de este Convenio, las Partes seguirán obligadas a no divulgar o usar la Información Confidencial y a devolverse de inmediato todos los documentos y materiales de su propiedad que contengan la citada Información Confidencial que, con motivo de la celebración y ejecución del presente Convenio, haya sido comunicada o entregada.

4.4. Las estipulaciones de la presente cláusula continuarán vigentes después de la terminación de este Convenio y aún después de concluidas, por el término de diez (10) años.

4.5. Ningún intercambio de información se podrá interpretar como que alguna de las Partes otorga o confiere a la otra, cualquier derecho, licencia o potestad en relación con la información intercambiada, ya que cada una de las Partes es propietaria de su información, misma que eventualmente podrá ser intercambiada en los términos y condiciones del presente Convenio, por lo que bajo ninguna circunstancia, la otra parte tiene algún derecho sobre ésta, salvo lo expresamente pactado en este instrumento.

4.6. Ambas partes manifiestan que tienen conocimiento de que tanto “**SEGURIDATA**” como “**nombre del Digitalizador**”, en cumplimiento de lo dispuesto por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, han emitido y hecho del conocimiento de sus clientes el Aviso de Privacidad a que se refiere dicha Ley, habiéndolo publicado respectivamente como les resulta conveniente, por lo anterior, ambas Partes se obligan en este acto a respetar los términos del Aviso de Privacidad referido en el presente párrafo, sin perjuicio de la obligación de confidencialidad asumida en términos del presente Convenio.

5. PROTECCION DE DATOS PERSONALES

5.1 En caso de que con motivo de la Prestación de los Servicios objeto del presente contrato, se integre información que permita la posibilidad de identificar al titular de la misma, o las Partes tengan acceso a datos personales de personas físicas de aquella documentación que sea digitalizada, le son aplicables las disposiciones relacionadas con la protección de datos siempre que como se ha indicado sea posible identificar al titular de la

misma, es decir los “Datos Personales”. Por lo anterior, las Partes en este acto se notifican respectivamente su responsabilidad respecto de tratamiento de los Datos Personales y de las medidas de seguridad físicas, administrativas y tecnológicas para conservar la seguridad de los datos. Los Datos Personales serán utilizados por las Partes únicamente para el cumplimiento de lo contratado en el presente instrumento y en concordancia a los términos de sus respectivos Avisos de Privacidad, mismos que se obligan en este acto a respetar, sin perjuicio de la obligación de confidencialidad asumida en términos del presente Contrato.

5.2 Las Partes aceptan que es de su conocimiento que los Datos Personales únicamente podrán ser remitidos previo consentimiento de sus titulares y siempre garantizando la confidencialidad de los mismos conforme a las finalidades contenidas del Aviso de Privacidad correspondiente, así como de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y demás normatividad aplicable

5.3 La obligación de confidencialidad será vitalicia; sin embargo, a la terminación del presente Contrato y/o sus Anexos, las Partes inmediatamente procederán cuando fuere posible, a la destrucción de los Datos Personales de acuerdo a sus propias políticas y conforme a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares o de las leyes que los rijan dependiendo de la naturaleza de los datos obtenidos.

5.4 Ambas partes manifiestan que tienen conocimiento de que tanto SeguriData como “NOMBRE DE DIGITALIZADOR”, en cumplimiento de lo dispuesto por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, han emitido y ponen a disposición de sus clientes el Aviso de Privacidad a que se refiere dicha Ley, habiéndolo publicado respectivamente como les resulta conveniente, por lo anterior, ambas Partes se obligan en este acto a respetar los términos del Aviso de Privacidad referido en el presente párrafo, sin perjuicio de la obligación de confidencialidad asumida en términos del presente Contrato

6. MARCAS DE LOS PRODUCTOS Y SERVICIOS.

6.1. Las Partes reconocen y aceptan que todas las marcas, nombres comerciales, emblemas y demás palabras o símbolos que identifiquen a los productos y servicios que cada una de ellas comercializa son y serán en todo momento propiedad de sus licenciantes respectivos.

7. PROPIEDAD INDUSTRIAL Y/O INTELECTUAL.

7.1. LAS PARTES se reconocen la propiedad o licencia respecto de los derechos de propiedad industrial y/o intelectual que usarán o se proporcionarán para o durante la prestación de los Servicios materia del presente Convenio (la “PROPIEDAD INDUSTRIAL / INTELECTUAL”), ya sea que se encuentren o no registrados, e incluyendo de manera enunciativa pero no limitativa, los programas de cómputo, sistemas, manuales, marcas y/o diseños.

7.2. Cada una de LAS PARTES también está de acuerdo en que el hecho de aprovechar los beneficios de la PROPIEDAD INDUSTRIAL / INTELECTUAL propiedad de o licenciada a la otra PARTE, no constituye, ni le otorga derecho alguno al respecto, diverso de los expresamente

establecidos en el presente Convenio. Por lo anterior, cada una de LAS PARTES deberá abstenerse de usar o aprovechar los derechos de la PROPIEDAD INDUSTRIAL / INTELECTUAL propiedad de o licenciados a la otra para fines que no tenga expresamente permitidos.

7.3. Cada una de LAS PARTES conviene dejar de usar cualquier derecho de la PROPIEDAD INDUSTRIAL / INTELECTUAL propiedad de o licenciado la otra, a la terminación o vencimiento del presente Convenio, inclusive en caso de que ocurra la terminación del presente sin necesidad de previa resolución judicial, en los términos que más adelante se establecen.

7.4. A la terminación o vencimiento del presente Convenio, cada una de LAS PARTES deberá discontinuar cualquier uso de cualquier derecho de la PROPIEDAD INDUSTRIAL / INTELECTUAL propiedad de o licenciado a la otra y arreglará todo para disponer de aquellos documentos, folletos, materiales publicitarios y programas de cómputo que le haya proporcionado o permitido la otra PARTE, de conformidad con las instrucciones de esta última. En todo caso, LAS PARTES deberán devolverse recíprocamente, dentro de los 10 (diez) días siguientes a la terminación o vencimiento del presente Convenio, el material que, por cualquier medio, contenga o implique cualquier derecho de la PROPIEDAD INDUSTRIAL / INTELECTUAL.

7.5. Cada una de LAS PARTES deberá abstenerse de modificar, desensamblar, descompilar, transferir, someter a procesos de ingeniería de reversa en forma total o parcial, los programas de cómputo que le hubiera proporcionado o licenciado la otra (por sí o por cuenta de un tercero), sin el consentimiento previo expreso y por escrito de esta última. Asimismo, cada una de LAS PARTES conviene que no deberá reproducir o copiar los programas de cómputo que le hubiera proporcionado la otra total o parcialmente, salvo en caso de que fuera necesario para tener un respaldo de información, en cuyo caso la copia estará sujeta a la misma protección que el original.

7.6. Las protecciones y derechos previstos a favor de LAS PARTES en términos de esta Cláusula seguirán vigentes, aunque haya concluido la prestación de los Servicios.

8. VIGENCIA Y TERMINACION.

8.1. El presente Convenio tendrá una vigencia indefinida, sin embargo, cada proceso de digitalización tendrá la vigencia que se señale particularmente en cada contrato de servicios que se firme con SeguriData.

8.2. Las Partes convienen que podrán dar por terminado el presente Convenio, así como el (los) Contrato (s) de Prestación de Servicios y sus Anexos respectivos, (si los hubiera), en forma anticipada, sin causa para ello, debiendo en tal caso notificar a la otra parte, de su voluntad en tal sentido por escrito y con treinta (30) días naturales de anticipación a la fecha deseada de terminación anticipada.

En caso de que cualquiera de las Partes decida dar por terminado el Convenio, las Partes acuerdan expresamente para todos los efectos a que haya lugar, que los Convenios de proyectos específicos con los Clientes que no se hayan concluido, deberán ser cumplidos a cabalidad en cuanto a sus términos y condiciones particulares

8.3. Las Partes convienen y aceptan que, a la terminación del presente Convenio, ninguna de ellas tendrá derecho a percibir indemnización alguna por el simple hecho de la

terminación misma, salvo que exista una causa plena y justificada para tal determinación que derive precisamente de algún incumplimiento de la otra Parte.

9. GENERALES.

9.1. Ninguna de las estipulaciones del presente Convenio podrá ser cedida o transferida por las Partes a terceros sin el consentimiento previo y por escrito de cada una de ellas.

9.2. En virtud de lo estipulado en el párrafo anterior, cada una de las Partes se obliga a mantener, indemnizar y a sacar en paz y a salvo a la otra, en contra de cualquier demanda o reclamación que se le hiciere por parte de alguno de sus trabajadores o prestadores de servicios, así como en contra de cualquier reclamación de parte de alguna autoridad derivada del cumplimiento o incumplimiento de obligaciones patronales o de seguridad social a cargo de la parte de que se trate.

9.3. Las Partes se comprometen a partir de la fecha de firma del presente Convenio y hasta doce (12) meses posteriores a la fecha de su terminación cualquiera que fuera la causa, a no ofrecer propuestas de trabajo o contratar de manera directa al personal de la otra sin que medie autorización escrita para ello.

En caso de incumplimiento a la obligación objeto de este apartado, la parte que incumpla pagará a la parte afectada, una pena convencional equivalente al cien por ciento (100%) de los salarios o contraprestación pagada a la persona de que se trate durante los doce (12) meses anteriores a la fecha de terminación de su relación con la parte afectada.

9.4. La no utilización de algún derecho por alguna de las Partes no implicará la renuncia al ejercicio de dicho derecho.

9.5. El presente Convenio y sus Anexos si los hubiera, constituyen la totalidad del acuerdo al que han llegado las Partes, cancelando cualquier aviso o comunicación que al efecto hayan celebrado con anterioridad y sólo podrá ser modificado mediante la celebración de un Convenio o Contrato diverso entre las Partes, debidamente firmado por sus representantes legales.

9.6 En relación con las estipulaciones del presente Convenio, cuando éstos se deban por causas de caso fortuito o fuerza mayor, en tanto que dicha causa sea subsanable en un periodo razonable de tiempo.

9.7. Todos los avisos o notificaciones legales que se dirijan las Partes deberán efectuarse por mensajero con acuse de recibo o mediante correo certificado a los domicilios señalados por cada una de ellas.

9.8. Todos los impuestos que se generen con motivo del cumplimiento del presente Convenio y/o del Contrato de Prestación de Servicios y sus Anexos, si los hubiera, serán pagados por la Parte a quien le correspondan, de conformidad con las disposiciones legales aplicables.

9.9. Ambas Partes tendrán derecho a convocar reuniones especiales, cuando así lo consideren conveniente, con el objeto de discutir cuestiones relativas al objeto del presente Convenio.

10. DISPUTAS.

10.1. Las Partes están de acuerdo en:

- a) Resolución Administrativa de Disputas. Las Partes acuerdan reunirse y debatir de buena fe cualesquiera asuntos controvertidos, reclamados o disputados que surjan en relación con este Convenio. Si dichos asuntos no pudieran resolverse entre los contactos técnicos y/o contractuales de las Partes, cada una de ellas podrá someter dichos asuntos a sus respectivos Representantes Legales, durante un plazo de 10 (diez) días, mediante notificación por escrito que explique la Disputa con razonable detalle, a fin de darle solución a la misma.
- b) Resolución Judicial. En caso de que las Partes no puedan resolver de manera Administrativa cualquier asunto controvertido, reclamado o disputado, se resolverá de manera definitiva en base a la legislación y tribunales competentes de la Ciudad de México.

11. SITUACIONES NO PREVISTAS.

11.1. LAS PARTES convienen en que intentarán resolver de común acuerdo aquellas situaciones no previstas en el presente Convenio, quedando entendido que las resoluciones que se adopten deberán constar por escrito y serán firmadas por ambas PARTES.

12. DOMICILIOS PARA NOTIFICACIONES.

12.1. Cualquier aviso o notificación que se dirijan LAS PARTES deberán efectuarse por mensajero o correo certificado a los domicilios señalados por cada una de ellas:

**A “NOMBRE DE _____
DIGITALIZADOR”
en:**

A “SEGURIDATA” en: Insurgentes Sur, No. 2375, 3er piso, Colonia Tizapán San Ángel,
C.P. 01000, Ciudad de México.

Por lo que cualquier notificación, documentación o aviso enviado por LAS PARTES al domicilio señalado, surtirá todos los efectos legales a que haya lugar, en tanto no sea notificado por escrito con acuse de recibo cualquier cambio de domicilio, con por lo menos 5 (cinco) días de anticipación.

13. DISPOSICIONES LEGALES.

13.1. Cualquier término o disposición del presente Convenio que contravenga a las leyes o disposiciones de los Estados Unidos Mexicanos, se considerará reformada de tal manera que se observe el cumplimiento de dichas leyes o disposiciones, sin perjuicio de que los términos y condiciones acordes con dicha legislación no sufrirán modificación alguna y continuarán vigentes para todos los efectos legales derivados del presente instrumento.

14. TÍTULOS.

14.1. Los títulos de las Cláusulas son meramente indicativos, sin que afecten directa o indirectamente a la interpretación que deba otorgarse a las Cláusulas que los encabezan.

15. JURISDICCIÓN.

15.1. Para la interpretación y cumplimiento del presente Convenio, las Partes se someten a la jurisdicción y competencia de los tribunales de la Ciudad de México, renunciando a cualquier otro fuero que por razón de su domicilio presente o futuro o que por cualquier otra causa pudiese corresponderles.

ENTERADAS LAS PARTES DEL CONTENIDO Y ALCANCE LEGAL DE ESTE CONVENIO, PROCEDEN A FIRMARLO POR DUPLICADO EN LA CIUDAD DE MEXICO, CON FECHA

“NOMBRE DE DIGITALIZADOR”	“SEGURIDATA”
“NOMBRE DE DIGITALIZADOR” S.A. DE C.V.	SEGURIDATA PRIVADA, S.A. DE C.V.
	LIC. JAVIER ALARCON IRIGOYEN. REPRESENTANTE LEGAL

LA PRESENTE PÁGINA DE FIRMAS CORRESPONDE AL CONVENIO DE ALIANZA ESTRATEGICA CELEBRADO ENTRE “NOMBRE DE DIGITALIZADOR”, S.A DE C.V., (“NOMBRE DE DIGITALIZADOR”) Y “SEGURIDATA PRIVADA, S.A. DE C.V.”, (“SEGURIDATA”). EL RESTO DE LA PÁGINA PERMANECE SIN TEXTO. -----

CONTRATO DE PRESTACION DE SERVICIOS QUE CELEBRAN POR UNA PARTE NOMBRE DE DIGITALIZADOR, A QUIEN EN LO SUCESIVO SE LE DENOMINARA COMO _____, REPRESENTADA EN ESTE ACTO POR EL SR. _____, EN SU CARÁCTER DE REPRESENTANTE LEGAL, Y POR LA OTRA PARTE, **SEGURIDATA PRIVADA, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE**, REPRESENTADA EN ESTE ACTO POR EL SEÑOR JAVIER ALARCON IRIGOYEN, EN SU CARÁCTER DE REPRESENTANTE LEGAL, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ COMO “**SEGURIDATA**”, Y QUE CONJUNTAMENTE CON “**NOMBRE DE DIGITALIZADOR**” SE LES DENOMINARÁ COMO “**LAS PARTES**”, DE CONFORMIDAD CON LAS SIGUIENTES:

DECLARACIONES

I.- Declara “nombre de digitalizador”, por conducto de su representante que:

I.1. Es una sociedad mercantil constituida de conformidad con la legislación mexicana, lo que acredita en términos de la Escritura Pública número _____ de fecha _____, otorgada ante la fe del _____ Notario Público No. _____ del _____, e inscrita ante el Registro Público de la Propiedad y de Comercio de esta Ciudad, en el Folio Mercantil No. _____.

I.2. Cuentan con las facultades suficientes y necesarias para obligar a su representada en los términos del presente instrumento, como lo acreditan con la Escritura Pública Número _____ de fecha _____, otorgada ante la fe del Notario Público Número _____ del _____, Licenciado _____, e inscrita en el Registro Público de Comercio de esta Ciudad, bajo el folio mercantil número _____, manifestando que dichas facultades no les han sido revocadas ni modificadas en forma alguna a esta fecha.

I.3. Tiene su domicilio en _____.

I.4. Su Registro Federal de Contribuyentes es: _____.

I.5. Con motivo del Convenio de Alianza Estratégica que tiene celebrado con “**SEGURIDATA**”, es su deseo celebrar el presente Contrato de Prestación de Servicios

II.- Declara “SEGURIDATA”, por conducto de su representante que:

II.1. Su representada es una persona moral de nacionalidad mexicana, constituida bajo las leyes de los Estados Unidos Mexicanos, como consta en Escritura Pública número 29,170 de fecha 17 de diciembre de 1996, otorgada ante la fe del Notario Público Número 107 del Distrito Federal, Licenciado Maximiliano Pérez Salinas, e inscrita en el Registro Público de Comercio del Distrito Federal, bajo el folio mercantil número 218826.

II.2. Cuenta con facultades para celebrar el presente Convenio, como lo acredita en términos de la Escritura Pública número 35,187 de fecha 15 de noviembre de 2011, otorgada ante la fe del Notario Público Número 218 del Distrito Federal, Licenciado José Luis Villavicencio

Rúbricas	NOMBRE DE DIGITALIZADOR	SEGURIDATA
----------	-------------------------	------------

Castañeda. Manifestando bajo protesta de decir verdad, que dichas facultades no le han sido revocadas, limitadas, ni modificadas en forma alguna a esta fecha.

II.3. Tiene su domicilio en Insurgentes Sur, 2375, 3er piso, Colonia Tizapán San Ángel, C.P. 01000, Ciudad de México.

II.4. Con motivo del Convenio de Alianza Estratégica que tiene celebrado con NOMBRE DE DIGITALIZADOR, en lo sucesivo “El Convenio” es su deseo celebrar asimismo el presente Contrato de Prestación de Servicios.

II.5 Su Registro Federal de Contribuyentes es: SPR961217 NK9

II.6 Que es un Prestador de Servicios de Certificación debidamente acreditado por la Secretaría de Economía para fungir como Tercero Legalmente Autorizado (TLA), acreditación que fue publicada en Diario Oficial de Federación el día 03 de diciembre de 2019

III.- Declaran las Partes por conducto cada uno de sus respectivos representantes que:

III.1. Es interés de las Partes promover la suscripción del presente Contrato de Prestación de Servicios en cumplimiento a lo señalado en la Regla 173 de las “Reglas a las que deberán sujetarse los Prestadores de Servicios de Certificación publicada en el Diario Oficial de la Federación, el 14 de mayo de 2018, a efecto de establecer las obligaciones y responsabilidades que tendrán cada una de las Partes en el proceso de digitalización documental en favor de (llenar con el nombre de El Cliente) (a quien para efectos del presente Convenio podrá denominársele como “El Cliente”)

III.2. Cada una de las Partes asume las obligaciones y responsabilidades inherentes a las actividades que a cada uno compete y que son descritas en el presente contrato y en el Convenio, lo anterior, de conformidad con la normatividad y ordenamientos jurídicos que le son aplicables, enunciativa mas no limitativamente: el Código De Comercio, las Reglas a las que deberán sujetarse los Prestadores de Servicios de Certificación, la Norma Oficial Mexicana “Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos” que para tal efecto ha emitido la Secretaría de Economía (en lo sucesivo NOM 151- SCFI 2016) publicada en el Diario Oficial de la Federación el 30 de marzo de 2017, o la que en su momento la sustituya.

Expuesto lo anterior, ambas Partes de conformidad, acuerdan en celebrar el presente Convenio sujetándolo a las siguientes:

CLÁUSULAS

1. CONTRATANTES INDEPENDIENTES.

Rúbricas	NOMBRE DE DIGITALIZADOR	SEGURIDATA
----------	----------------------------	------------

1.1. Las Partes convienen, que son dos (2) sociedades independientes y que nada de lo contenido en el presente Convenio les otorgará derecho a: (i) Tener cualquiera de las Partes, poder y control directo en las operaciones diarias de la otra Parte; (ii) Constituirse las Partes como accionistas y/o copropietarios de la otra Parte; (iii) Asumir alguna obligación en nombre de la otra Parte bajo ningún propósito; (iv) Todas las obligaciones financieras, laborales, de seguridad social o cualesquiera otras asociadas con los negocios de **NOMBRE DE DIGITALIZADOR y SeguriData** son de la exclusiva responsabilidad de cada una de las Partes, según sea el caso.

2. OBJETO DEL CONTRATO

2.1. Las Partes mediante la firma del presente Contrato se obligan a prestar los servicios que a cada una corresponda en el Proceso de digitalización que se llevará a cabo a solicitud de El Cliente, de conformidad con la normatividad y ordenamientos jurídicos que le son aplicables, enunciativa mas no limitativamente: (a) el Código de Comercio, (b) las Reglas a las que deberán sujetarse los Prestadores de Servicios de Certificación, (en lo sucesivo "Las Reglas") (c) la Norma Oficial Mexicana NOM 151- SCFI 2016 "Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos" que para tal efecto ha emitido la Secretaría de Economía (en lo sucesivo NOM 151- SCFI 2016) publicada en el Diario Oficial de la Federación el 30 de marzo de 2017, o la que en su momento la sustituya.

2.2 Para efectos del presente Contrato se entenderá por digitalización lo señalado en el Código de Comercio:

"Digitalización: Migración de documentos impresos a mensaje de datos, de acuerdo con lo dispuesto en la Norma Oficial Mexicana sobre Digitalización y Conservación de mensajes de datos que para tal efecto emita la Secretaría".

Así como lo dispuesto en el numeral 4.3 de la NOM-151-SCFI-2016:

"Digitalización: Proceso que permite la migración de documentos impresos a mensajes de datos, conforme a lo establecido en el Apéndice Normativo B de la presente Norma Oficial Mexicana"

3. OBLIGACIONES Y RESPONSABILIDADES

3.1. Las Partes mediante la firma del presente Contrato se obligan a prestar los servicios que a continuación se relacionan con motivo de los servicios de Digitalización que se prestarán en favor de El Cliente:

Por parte de El Cliente:

El Cliente debe definir los documentos que desea digitalizar y solicitar los servicios de digitalización, a SeguriData.

El Cliente junto con el TLA SeguriData y el Digitalizador, definen el tipo de muestreo que se usará para la verificación de la Digitalización, así como el tamaño de la muestra.

El Cliente debe resguardar sus claves de acceso a usar en el servicio de Digitalización de documentos en soporte físico.

El Cliente deberá verificar que el certificado no esté revocado

Rúbricas	NOMBRE DE DIGITALIZADOR	SEGURIDATA
----------	----------------------------	------------

El Cliente podrá participar de manera opcional en la validación de la muestra que permitan realizar un proceso de cotejo de los mensajes de datos resultantes de la digitalización contra los documentos en soporte físico

Por parte de NOMBRE DE DIGITALIZADOR:

NOMBRE DE DIGITALIZADOR, llevará a cabo la digitalización de documentos impresos de El Cliente, en los términos que se establezca en la NOM 151-SCFI-2016 o la que en su momento la sustituya, incluida la preparación de los documentos objeto de la digitalización.

Por parte de SEGURIDATA

SeguriData por medio del presente Contrato se compromete a llevar a cabo los siguientes servicios:

- Servicios relacionados con firmas electrónicas
- Expedición de certificados digitales de firma electrónica,
- Prestar servicios relacionados con la firma electrónica como la conservación de mensajes de datos y sellos digitales de tiempo
- Fungir en calidad de tercero legalmente autorizado (TLA)

3.2. El servicio para el Cliente final estará conformado por 2 (dos) componentes que se complementan perfectamente entre sí, uno aportado por “**NOMBRE DE DIGITALIZADOR**” y otro aportado por “**SEGURIDATA**”:

3.2.1. “**SEGURIDATA**” es responsable de:

1.- Proporcionar a NOMBRE DE DIGITALIZADOR en su carácter de Digitalizador los elementos técnicos necesarios para integrar las funcionalidades de Firma Electrónica Avanzada en los documentos digitalizados, como TLA en función de la NOM 151-SCFI-2016

2.- Atender la solicitud de NOMBRE DE DIGITALIZADOR para la generación de constancias de conservación de mensaje de datos y sellos digitales de tiempo en su carácter de Prestador de Servicios de certificación, Servicio de Sellos Digitales de tiempo y Constancias de Conservación de mensajes de Datos; a partir de los archivos electrónicos resultantes del proceso de digitalización.

3.- La responsabilidad está limitada exclusivamente a proveer los servicios que le corresponden en términos del presente Contrato, de acuerdo con lo establecido en sus propias Declaraciones y Políticas, acordes a la normatividad aplicable.

4.- SeguriData deberá mantener y administrar los reportes de cotejo y las actas circunstanciadas de la digitalización de documentos en soporte físico realizadas

Rúbricas	NOMBRE DE DIGITALIZADOR	SEGURIDATA
----------	----------------------------	------------

5.- SeguriData Privada S.A. de C.V. estará exenta de toda responsabilidad en los casos que enunciativa, pero no limitativamente se señalan a continuación:

- a) Por cualquier actividad no prestada directamente por SeguriData y que correspondan a NOMBRE DE DIGITALIZADOR o a El Cliente
- b) Por los daños y/o perjuicios que se causen, si El Cliente entrega datos y/o documentos falsos o alterados, para la obtención de los servicios objeto del presente Contrato.
- c) Por cualquier tipo de daños y/o perjuicios que sufran sus clientes, siempre que éstos deriven de la indebida utilización de los servicios por parte de dichos clientes.
- d) Por los daños y/o perjuicios que se causen al Cliente por la errónea interpretación, análisis, síntesis o conclusión respecto de los Servicios por parte de NOMBRE DE DIGITALIZADOR o del propio Cliente, sin que estas hayan sido confirmadas expresamente por SeguriData.
- e) Por la interrupción o alteración temporal del servicio por causas ajenas a SeguriData que afecte sus instalaciones o limiten la libertad en las comunicaciones.

3.2.2. "NOMBRE DE DIGITALIZADOR" aportará y desarrollará todas las tareas operativas asociadas a los servicios siguientes:

a) Preparación para digitalización:

- NOMBRE DE DIGITALIZADOR recibirá o trasladará a sus instalaciones, los documentos físicos de El Cliente a ser digitalizados, generando un acta de recepción con el detalle de dichos documentos la cual deberá ser firmada por el cliente.
- Una vez con los documentos a digitalizar en sus instalaciones y de acuerdo con el alcance del servicio con el Cliente, se podrán clasificar, reordenar, validar contra una lista de comprobación, para su acomodo previo a su digitalización.
- De igual forma se debe validar que los documentos no contengan grapas, clips u otro tipo de objetos que impidan su adecuada digitalización.
- Los documentos ya ordenados, indexados o clasificados quedaran listos para su digitalización por parte de NOMBRE DE DIGITALIZADOR.
- Define en conjunto con El Cliente el Método de Control como ID.

b) Digitalización de documentos:

- Los documentos se digitalizarán en el scanner definido por NOMBRE DE DIGITALIZADOR para el proceso en el área correspondiente.
- Durante su digitalización no deberán alterarse, ni desordenarse, para que al terminar el proceso vuelva a quedar integrado de acuerdo con lo convenido en el servicio.
- Los documentos físicos se deberán resguardar para su devolución al Cliente o destrucción según el alcance del servicio convenido.
- En caso de devolución al Cliente se deberá generar un acta de entrega con el detalle de los documentos entregados la cual deberá ser firmada por El Cliente.
- En caso de destrucción se deberá generar un acta de destrucción.

c) Archivos de imágenes certificadas:

Rúbricas	NOMBRE DE DIGITALIZADOR	SEGURIDATA
----------	-------------------------	------------

- Durante el proceso de digitalización, NOMBRE DE DIGITALIZADOR solicitará vía web services a SEGURIDATA la Firma Electrónica Avanzada como Tercero Legalmente Autorizado de la muestra y posteriormente de la totalidad de documentos digitalizados, y al Cliente le solicitara la aceptación de la muestra , y posteriormente del total de documentos digitalizados, plasmando su firma electrónica, para embeberlos en el archivo digital resultante de la digitalización certificada de cada documento , agregando un sello y una constancia de conservación.
- SEGURIDATA en su carácter de PSC acreditado ante Secretaria de Economía, deberá tener habilitados sus servicios de certificados digitales, estampillas de tiempo y constancias de la NOM-151 para el servicio, así como el de TLA.
- Como resultado del proceso de digitalización certificada se obtendrán los archivos digitales en el formato definido para el Cliente, ya sea para su entrega o resguardo según el alcance del servicio contratado por El Cliente.

d) Resguardo de imágenes certificadas:

- Si el Cliente requiere del resguardo de sus archivos digitales, NOMBRE DE DIGITALIZADOR se encargará de ofrecer el espacio de almacenamiento y los esquemas de consulta de estos.
- Se definirá el lapso del servicio y el esquema de entrega de información al terminar la vigencia del contrato del servicio.
- De igual forma se podría definir que al término del ciclo de vida de la información, los archivos digitales puedan ser eliminados tomando en cuenta la legislación aplicable para cada tipo de documento.

e) Niveles de calidad

- El mensaje de datos resultante de la digitalización debe ser fiel al contenido original y garantizar su integridad por medio de la firma electrónica de SeguriData como TLA, NOMBRE DE DIGITALIZADOR como Digitalizador y el Cliente; y de manera opcional de así solicitarlo el cliente, la firma del fedatario.
- El nivel de calidad mínimo para los mensajes de datos resultantes será de 200 píxeles por pulgada o superior para representaciones en blanco y negro, color o escala de grises
- Se generará un mensaje de datos que permita asegurar la fidelidad e integridad conforme a los documentos amparados en soportes físicos; el mensaje de datos generado debe ser de alta calidad y se tratará con un intenso control de calidad, de manera que, si existe algún error en el proceso de captura, ésta deberá efectuarse una vez más.
- El mensaje de datos será fiel al documento en soporte físico, para lo cual:
 - a) Respetará la geometría o aspecto del origen en tamaños y proporciones;
 - b) No contendrá caracteres o gráficos que no figurasen en el soporte físico, y
 - c) El mensaje de datos generado a partir del proceso de digitalización, deberá permanecer no disponible para su modificación o consulta por parte del solicitante del servicio, mientras se genere la constancia de conservación de mensajes de datos.

Rúbricas	NOMBRE DE DIGITALIZADOR	SEGURIDATA
----------	-------------------------	------------

d) Su generación atenderá en todo momento a lo establecido en la NOM-151-SCFI-2016, al igual que los parámetros definidos, para la compulsa con el algoritmo aplicado para la obtención de la muestra a revisar

e) Atención de revisiones que SeguriData requiera realizar a NOMBRE DE DIGITALIZADOR , en función a lo referido En la NOM 151-SCFI-2016, en cuanto a Hardware, Software y documentación relacionada al servicio de Digitalización en soporte físico de documentos.

Asimismo, “**NOMBRE DE DIGITALIZADOR**” definirá a su sola discreción el precio final que ésta última cobrará a sus Clientes.

3.2.3. NOMBRE DE DIGITALIZADOR deberá cumplir con el Plan de Gestión de Calidad definido por el TLA.

De igual manera deberá mantener las medidas de seguridad definidas en la Política de Seguridad del TLA.

3.2.4. Responsabilidades de NOMBRE DE DIGITALIZADOR:

NOMBRE DE DIGITALIZADOR será responsable directamente por cualquier error, falla u omisión en el proceso de digitalización o preparación para la digitalización, debiendo sacar y mantener en paz a SeguriData de cualquier reclamación por parte del Cliente, siendo SeguriData el responsable en todo momento frente al Cliente.

3.2.5. Cada una de las Partes actuará bajo su propio nombre ante sus respectivos Clientes, por lo que convienen y aceptan que cada una de ellas asume de manera independiente cualquier responsabilidad, reclamación o demanda que pudieran instaurar una en contra de la otra; o incluso los Clientes en contra de una u otra, en virtud de la prestación de los servicios que cada una realice, en términos de la Cláusula Novena.

4. CONTRAPRESTACIÓN

4.1. Para efectos del presente contrato, Las Partes recibirán los pagos o comisiones en la forma que se determina en el Anexo 1, el cual debidamente firmado por las Partes forma parte integrante del mismo.

5. FECHA DE ENTREGA DE LOS SERVICIOS

5.1. Las Partes en este acto se obligan a llevar a cabo Los Servicios de acuerdo al Cronograma que para tales efectos se agrega al Anexo 1.

6. CONFIDENCIALIDAD

6.1. Las Partes en este acto se obligan a guardar y mantener la confidencialidad de cualquier información que sea recibida, proporcionada o dada a conocer por la otra Parte y/o cualquiera de sus subsidiarias o filiales, incluyendo de manera enunciativa más no limitativa, toda aquella información relativa a sus operaciones, ruta crítica, negocios, productos, servicios, métodos, procesos, procedimientos, información de sistemas, contratos, convenios, descubrimientos, ideas, diseños, dibujos, programas, “know-how”, información financiera,

Rúbricas	NOMBRE DE DIGITALIZADOR	SEGURIDATA
----------	-------------------------	------------

información técnica, listas de clientes actuales o potenciales, bases de datos, planes, proyectos y políticas de negocio, métodos de mercadeo, estrategias, costos, o cualquier otra información aun cuando dicha información conste en cualquier clase de documento, archivo, material, medio magnético y/o electrónico, así como las conversaciones y pláticas que sean grabadas o conservadas en cualquier medio magnético y/o electrónico, documento, archivo y/o material en donde se haga constar la citada información (en lo sucesivo la “Información Confidencial”).

7. PROTECCION DE DATOS PERSONALES

7.1. En caso de que con motivo de la Prestación de los Servicios objeto del presente contrato, se integre información que permita la posibilidad de identificar al titular de la misma, o las Partes tengan acceso a datos personales de personas físicas de aquella documentación que sea digitalizada, le son aplicables las disposiciones relacionadas con la protección de datos siempre que como se ha indicado sea posible identificar al titular de la misma, es decir los “Datos Personales”. Por lo anterior, las Partes en este acto se notifican respectivamente su responsabilidad respecto de tratamiento de los Datos Personales y de las medidas de seguridad física, administrativa y tecnológica para conservar la seguridad de los datos. Los Datos Personales serán utilizados por las Partes únicamente para el cumplimiento de lo contratado en el presente instrumento y en concordancia a los términos de sus respectivos Avisos de Privacidad, mismos que se obligan en este acto a respetar, sin perjuicio de la obligación de confidencialidad asumida en términos del presente Contrato.

7.2 Las Partes aceptan que es de su conocimiento que los Datos Personales únicamente podrán ser remitidos previo consentimiento de sus titulares y siempre garantizando la confidencialidad de los mismos conforme a las finalidades contenidas del Aviso de Privacidad correspondiente, así como de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y demás normatividad aplicable

7.3 La obligación de confidencialidad será vitalicia; sin embargo, a la terminación del presente Contrato y/o sus Anexos, las Partes inmediatamente procederán cuando fuere posible, a la destrucción de los Datos Personales de acuerdo a sus propias políticas y conforme a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares o de las leyes que los rijan dependiendo de la naturaleza de los datos obtenidos.

8. PROPIEDAD INDUSTRIAL Y/O INTELECTUAL.

8.1 Las Partes deberán garantizar a El Cliente haber obtenido de los titulares respectivos, los derechos de propiedad industrial e intelectual, que resulten necesarios para la aportación de los Bienes, Software y/o Servicios requeridos por El Cliente y, por lo tanto, garantizan que no se vulnera disposición legal, convenio, derecho o propiedad intelectual de terceros, ni de ningún modo constituye competencia desleal.

8.1 Las Partes se comprometen y garantizan que los Bienes, Software y/o Servicios aportados por cada una ellas y que forman parte del presente instrumento, no violan disposición gubernamental, ley o reglamento vigente alguno, ni tampoco derechos de propiedad industrial o intelectual de terceros, por lo que, en caso de que cualquier tercero

Rúbricas	NOMBRE DE DIGITALIZADOR	SEGURIDATA
----------	----------------------------	------------

iniciara en contra de alguna de ellas o de El Cliente alguna denuncia, querella, demanda, requerimiento extrajudicial, juicio o procedimiento judicial o administrativo relacionado de manera directa o indirecta con derechos de propiedad industrial o intelectual de terceros, Las Partes se compromete a su cargo y costa a poner en paz y a salvo los intereses de la otra Parte o de El Cliente dejando a El Cliente, libre de cualquier responsabilidad.

9. VIGENCIA Y TERMINACION.

9.1. El presente Contrato tendrá una vigencia indefinida, sin embargo cada proceso de digitalización tendrá la vigencia que se señale particularmente en el Anexo 1.

9.2. Las Partes convienen que podrán dar por terminado el presente Contrato, y sus Anexos respectivos, en forma anticipada, por cause justificada, debiendo en tal caso notificar a la otra parte, de su voluntad en tal sentido por escrito y con 24 horas de anticipación a la fecha deseada de terminación anticipada, sin embargo quedan obligadas a concluir cualquier contrato ya entablado con El Cliente.

10. PENAS CONVENCIONALES

10.1 Las Partes reconocen que el cumplimiento en tiempo de sus obligaciones es un factor muy importante para El Cliente, y que cualquier error o retraso en la prestación de los Servicios podría causar daños o perjuicios a El Cliente cuya cuantificación resulta imposible en este momento. Por lo anterior, en caso de que, por causas imputables o circunstancias atribuibles a alguna de las Partes “los Servicios” no sean prestados dentro de los tiempos establecidos para ello en el Anexo 2 o no se presten conforme lo dispone la NOM 151-SCFI-2016 y el presente Contrato, la Parte que incumpla, será responsable de pagar a El Cliente la cantidad que este reclame por concepto de pena convencional, misma que deberá ser únicamente sobre el valor de los servicios prestados con retraso o sin reunir las especificaciones de la mencionada Norma Mexicana.

10.2 El pago de dichas cantidades no liberará a las Partes de su obligación de entregar los Servicios de acuerdo al presente contrato.

10.3 El pago de las penas convencionales mencionadas podrá ser por medio de una deducción del pago respectivo que tenga que hacer SeguriData a NOMBRE DE DIGITALIZADOR, o NOMBRE DE DIGITALIZADOR a SeguriData, según corresponda, o bien en efectivo o transferencia electrónica dentro de los 5 (cinco) días hábiles siguientes al requerimiento de pago por parte de la parte que no incumplió.

10.4 En caso de que alguna de las partes incumpla alguna de las estipulaciones del objeto del contrato, la parte ofendida podrá exigir el cumplimiento forzoso de conformidad con los términos señalados en la presente Cláusula o dar por rescindido el presente contrato, sin necesidad de declaración judicial y podrá exigirle a la otra parte el pago de las penas convencionales objeto de este contrato, o bien, reclamar el pago de daños y perjuicios. La elección de exigir el cumplimiento forzoso o la rescisión del presente contrato así como la reclamación del pago de daños y perjuicios, en ambos casos quedará a cargo de la parte que no incumplió.

Rúbricas	NOMBRE DE DIGITALIZADOR	SEGURIDATA
----------	----------------------------	------------

10.5 Las Partes convienen que en el cumplimiento o incumplimiento de cualquier obligación y/o, respecto de cualquier ejecución, omisión o acto por el cual, se les finque cualquier tipo de responsabilidad, se les exija el pago de daños y perjuicios o cualquier otro tipo de penalización relacionado con el presente Contrato y sus Anexos, a cualquiera de ellas, la responsabilidad frente a la otra Parte o frente a cualquier otra persona o Entidad, en ningún caso, individualmente considerada y/o en su conjunto, excederá del cien por ciento del monto de la contraprestación total que deba ser pagada al Proveedor por los Servicios objeto del presente contrato, quedando excluidas, cualquier responsabilidad por pérdidas de negocios, paros laborales, pérdida de datos, daños indirectos o incidentales.

No obstante lo anterior, la limitación a la responsabilidad, no será aplicable en el supuesto de que los daños o perjuicios hayan sido ocasionados por negligencia, culpa, dolo o mala fe de la parte en incumplimiento.

11. GENERALES.

11.1. Ninguna de las estipulaciones del presente Contrato podrá ser cedida o transferida por las Partes a terceros sin el consentimiento previo y por escrito de cada una de ellas.

11.2. En virtud de lo estipulado en el párrafo anterior, cada una de las Partes se obliga a mantener, indemnizar y a sacar en paz y a salvo a la otra, en contra de cualquier demanda o reclamación que se le hiciere por parte de alguno de sus trabajadores o prestadores de servicios, así como en contra de cualquier reclamación de parte de alguna autoridad derivada del cumplimiento o incumplimiento de obligaciones patronales o de seguridad social a cargo de la parte de que se trate.

11.3. Las Partes se comprometen a partir de la fecha de firma del presente Contrato y hasta doce (12) meses posteriores a la fecha de su terminación cualquiera que fuera la causa, a no ofrecer propuestas de trabajo o contratar de manera directa al personal de la otra sin que medie autorización escrita para ello.

En caso de incumplimiento a la obligación objeto de este apartado, la parte que incumpla pagará a la parte afectada, una pena convencional equivalente al cien por ciento (100%) de los salarios o contraprestación pagada a la persona de que se trate durante los doce (12) meses anteriores a la fecha de terminación de su relación con la parte afectada.

11.4. La no utilización de algún derecho por alguna de las Partes no implicará la renuncia al ejercicio de dicho derecho.

11.5. El presente Contrato y sus Anexos si los hubiera, constituyen la totalidad del acuerdo al que han llegado las Partes, cancelando cualquier aviso o comunicación que al efecto hayan celebrado con anterioridad y sólo podrá ser modificado mediante la celebración de un Contrato entre las Partes, debidamente firmado por sus representantes legales.

Rúbricas	NOMBRE DE DIGITALIZADOR	SEGURIDATA
----------	----------------------------	------------

11.6. Ninguna de las Partes será responsable frente a la otra por incumplimiento o demora en relación con las estipulaciones del presente Contrato, cuando éstos se deban por causas de caso fortuito o fuerza mayor, en tanto que dicha causa sea subsanable en un periodo razonable de tiempo.

11.7. Todos los avisos o notificaciones legales que se dirijan las Partes deberán efectuarse por mensajero con acuse de recibo o mediante correo certificado a los domicilios señalados por cada una de ellas.

11.8. Todos los impuestos que se generen con motivo del cumplimiento del presente Contrato y/o del Contrato de Prestación de Servicios y sus Anexos, si los hubiera, serán pagados por la Parte a quien le correspondan, de conformidad con las disposiciones legales aplicables.

11.9. Ambas Partes tendrán derecho a convocar reuniones especiales, cuando así lo consideren conveniente, con el objeto de discutir cuestiones relativas al objeto del presente Contrato.

12. DISPUTAS.

12.1. Las Partes están de acuerdo en:

- a) Resolución Administrativa de Disputas. Las Partes acuerdan reunirse y debatir de buena fe cualesquiera asuntos controvertidos, reclamados o disputados que surjan en relación con este Contrato. Si dichos asuntos no pudieran resolverse entre los contactos técnicos y/o contractuales de las Partes, cada una de ellas podrá someter dichos asuntos a sus respectivos Representantes Legales, durante un plazo de 10 (diez) días, mediante notificación por escrito que explique la Disputa con razonable detalle, a fin de darle solución a la misma.
- b) Resolución Judicial. En caso de que las Partes no puedan resolver de manera Administrativa cualquier asunto controvertido, reclamado o disputado, se resolverá de manera definitiva en base a la legislación y tribunales competentes de la Ciudad de México.

13. SITUACIONES NO PREVISTAS.

13.1. Las Partes convienen en que intentarán resolver de común acuerdo aquellas situaciones no previstas en el presente Contrato, quedando entendido que las resoluciones que se adopten deberán constar por escrito y serán firmadas por ambas Partes.

14. DOMICILIOS PARA NOTIFICACIONES.

Rúbricas	NOMBRE DE DIGITALIZADOR	SEGURIDATA
----------	----------------------------	------------

14.1. Cualquier aviso o notificación que se dirijan LAS PARTES deberán efectuarse por mensajero o correo certificado a los domicilios señalados por cada una de ellas en el Capítulo de Declaraciones. Por lo que cualquier notificación, documentación o aviso enviado por Las Partes al domicilio señalado, surtirá todos los efectos legales a que haya lugar, en tanto no sea notificado por escrito con acuse de recibo cualquier cambio de domicilio, con por lo menos 5 (cinco) días de anticipación.

15. DISPOSICIONES LEGALES.

15.1. Cualquier término o disposición del presente Contrato que contravenga a las leyes o disposiciones de los Estados Unidos Mexicanos, se considerará reformada de tal manera que se observe el cumplimiento de dichas leyes o disposiciones, sin perjuicio de que los términos y condiciones acordes con dicha legislación no sufrirán modificación alguna y continuarán vigentes para todos los efectos legales derivados del presente instrumento.

16. JURISDICCIÓN.

16.1. Para la interpretación y cumplimiento del presente Contrato, las Partes se someten a la jurisdicción y competencia de los tribunales de la Ciudad de México, renunciando a cualquier otro fuero que por razón de su domicilio presente o futuro o que por cualquier otra causa pudiere corresponderles.

ENTERADAS LAS PARTES DEL CONTENIDO Y ALCANCE LEGAL DE ESTE CONTRATO, PROCEDEN A FIRMARLO POR DUPLICADO EN LA CIUDAD DE MEXICO, CON FECHA _____ DEL 20_____

"NOMBRE DE DIGITALIZADOR "	"SEGURIDATA"
	SEGURIDATA PRIVADA, S.A. DE C.V.
	LIC. JAVIER ALARCON IRIGOYEN. REPRESENTANTE LEGAL

Rúbricas	NOMBRE DE DIGITALIZADOR	SEGURIDATA
-----------------	------------------------------------	-------------------

22.5 Anexo 5 Procedimiento para la generación de claves

**Procedimiento para la Generación de claves
Criptográficas de la Autoridad Certificadora de
TLA (Tercero legalmente autorizado)
Digitalización de documentos en soporte Físico**

Tabla de Contenido

1 Pre-Requisitos.....	3
2 Crear Security World.....	3
3.- Creación del conjunto de Operadores.....	7
3.1 Creación de Operadores OCS	7
4. Creación de la llave privada y pública de la AC en el módulo criptográfico.....	11
5.- Configuración del servicio de Autoridad Certificadora.	16
6.- Configuración de datos de conexión a la Base de Datos.	18
7.- Creación de Certificado de AC y llaves del Administrador.....	22
8.- Instalación del Servicio de la Autoridad Certificadora.....	30
9.- Configuración del Administrador de la AC.....	31

Versión	Fecha	Descripción
1.0	Febrero 2019	Creación del documento

1 Pre-Requisitos

- Tener configurado el dispositivo HSM
- Tener creada la Base de Datos con un usuario y password definido
- Tener el software de SeguriServer instalado
- Tener la definición de las ACS y OCS

- ACS 2/4 (Administrador)
- OCS 1/4 (Operador)

Los cuales se asignan de acuerdo a la siguiente tabla

- Administradores

Administrador principal	Administrador de sistemas
Administrador alterno	Profesional Jurídico
Administrador respaldo 1	Director general
Administrador respaldo 2	Auxiliar de apoyo informático de seguridad
Administrador respaldo 3	Operador de sistemas
Administrador respaldo 4	Administrador de base de datos

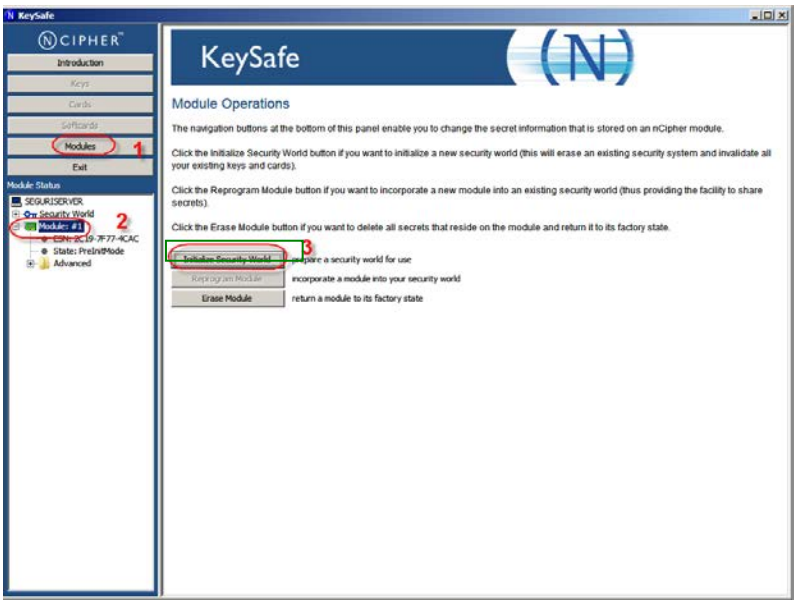
- Operadores

Operador requerido – Site interlomas	Operador de sistemas
Operador segundo modulo HSM – Site interlomas	Operador de sistemas
Operador tercer modulo HSM – Tultitlan	Administrador de redes
Operador respaldo 1	Profesional jurídico

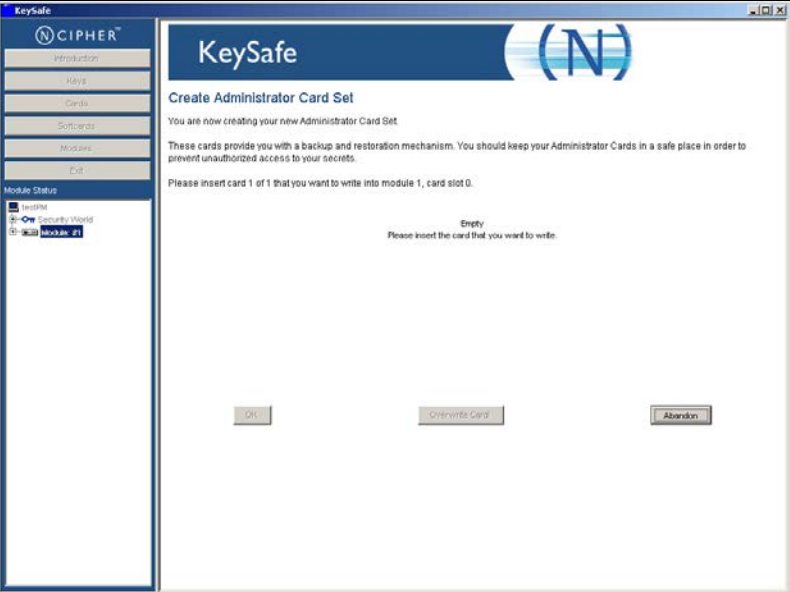
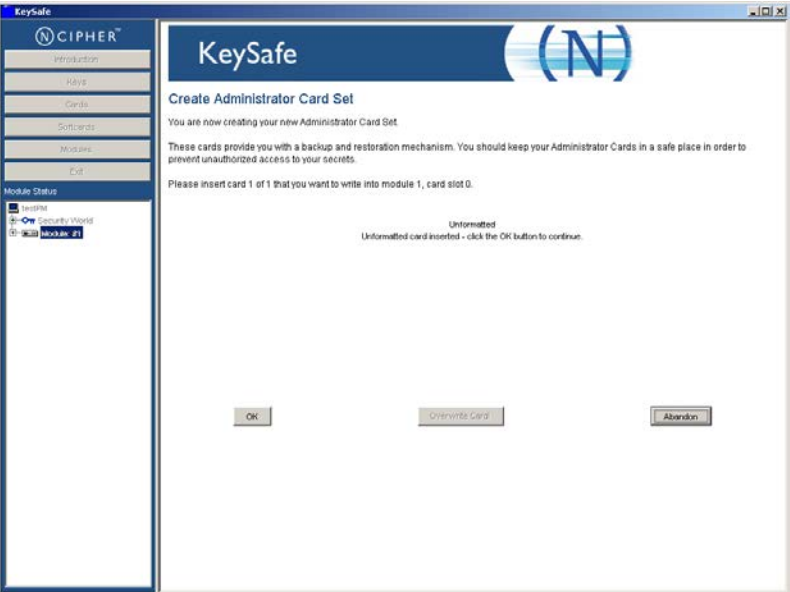
2 Crear Security World

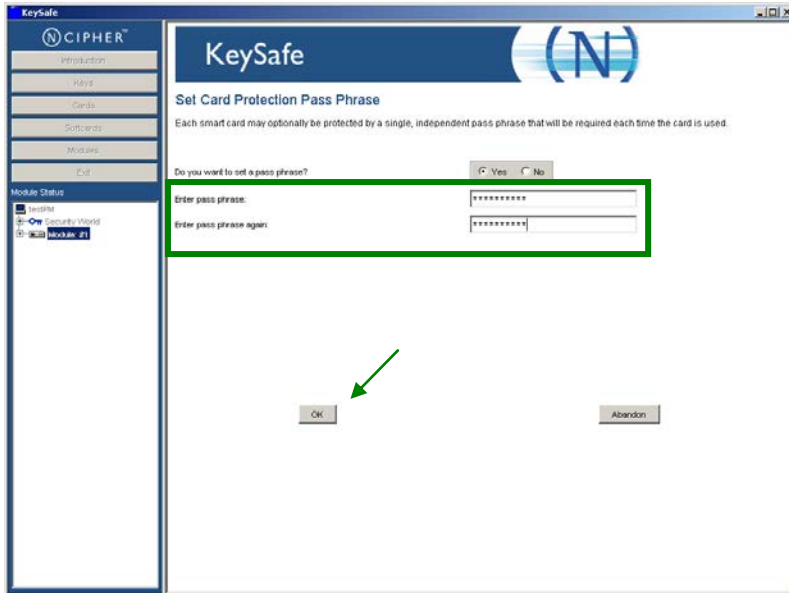
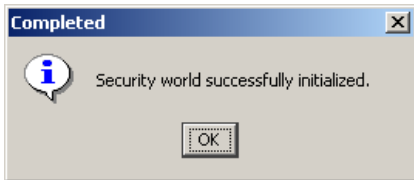
Dentro de la configuración del módulo criptográfico se creará la “Security World” por medio del ambiente gráfico del KeySafe.

Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
1	Administrador del Módulo Criptográfico	Detener el servicio “nfast Server” desde la consola de administración de Windows “mmc”	
2	Administrador del Módulo Criptográfico	Levantar el servicio “nFast Server” desde la consola de administración de servicios de Windows “mmc”	

Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
3	Administrador del Módulo Criptográfico	Abrir la aplicación KeySafe que se ubica en la ruta: Start > All Program > nCipher > KeySafe 	
4	Administrador del Módulo Criptográfico	Elegimos la opción de “Modules” Posteriormente elegimos el módulo : #1 Finalmente escogemos la opción “Initialize security world” como se muestra a continuación: 	

Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
5	Administrador del Módulo Criptográfico	En la siguiente ventana se ingresará: El número total de custodios administradores del sistema El número de administradores requeridos para realizar tareas administrativas. Una vez que se ingresaron el número total de custodios y los requeridos, Presionar el boton: "Initialize Security World" 	
6	Administrador del Módulo Criptográfico	En este momento se inicia la interacción con los primeros custodios (administradores) ingresando las tarjetas de los custodios en blanco.	

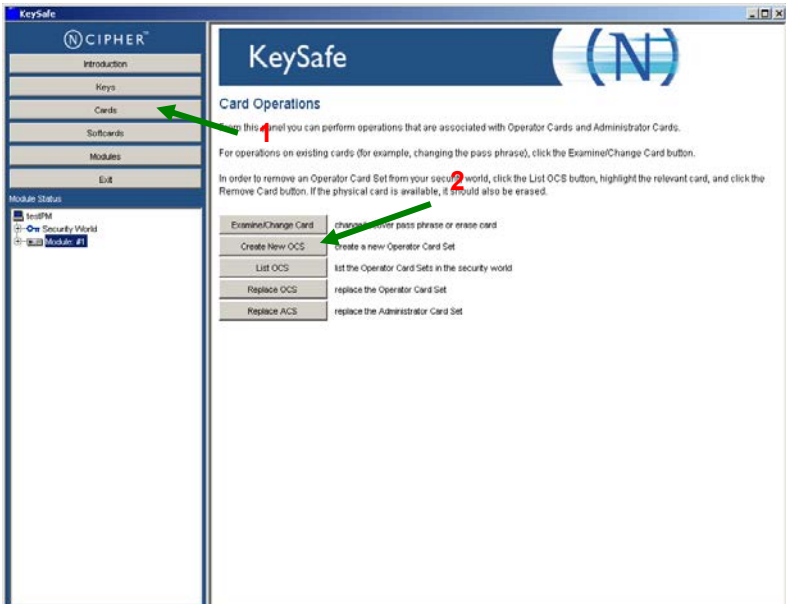
Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
			
7	Administrador del Módulo Criptográfico	Se inserta la tarjeta en el modulo criptográfico y damos clic en el botón "OK" 	

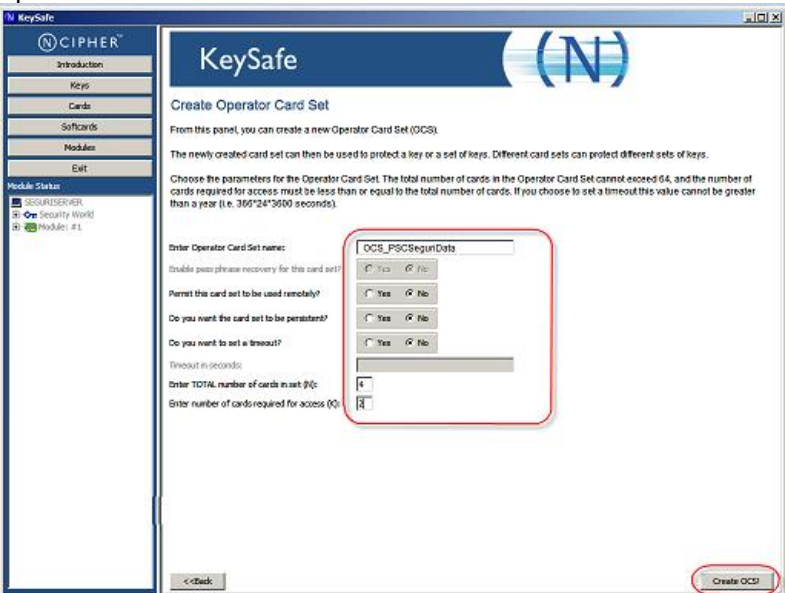
Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
8	Administrador del Módulo Criptográfico	Enseguida se deberá ingresar el PWD de esa tarjeta:  Finalmente dar clic en el botón “OK”. Repetir pasos de 6 al 8 dependiendo del número de tarjetas de administrador a configurar.	
9	Administrador del Módulo Criptográfico	Al finalizar esta actividad y si se siguieron exactamente los pasos anteriores, nos desplegará la siguiente ventana:  Donde nos indica que la Security World se ha inicializado satisfactoriamente.	

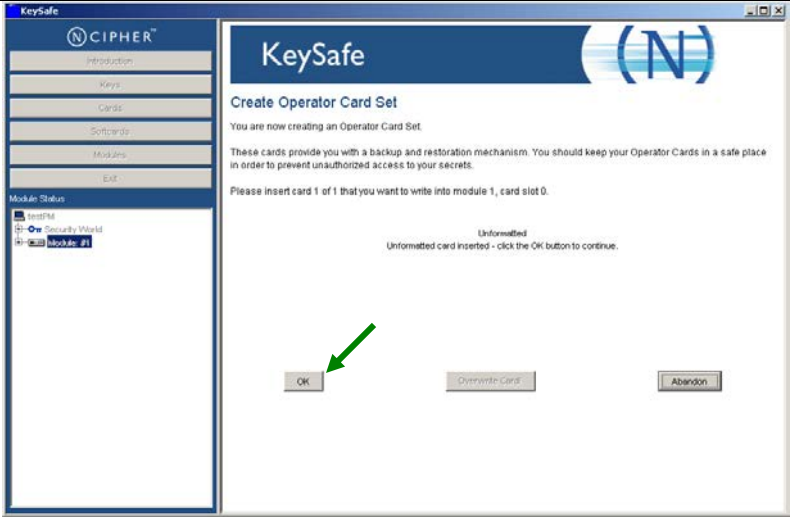
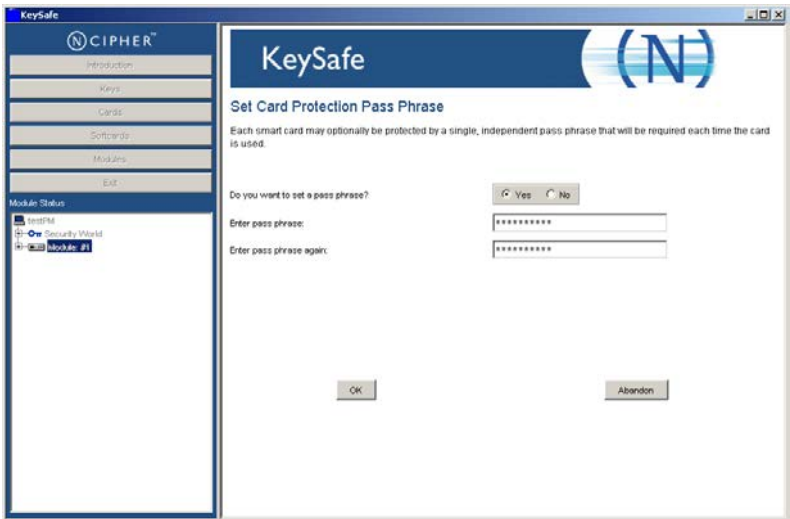
3.- Creación del conjunto de Operadores.

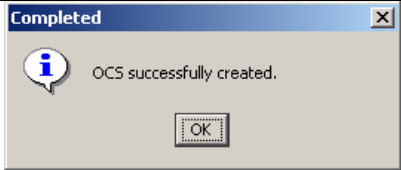
3.1 Creación de Operadores OCS

Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
10	Administrador del Módulo Criptográfico	Detener el servicio “Nfast Server” desde el panel de administración de servicios.	

Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
11	Administrador del Modulo Criptográfico	Levantar el servicio "Nfast Server" desde el panel de administración de servicios "mmc"	
12	Administrador del Modulo Criptográfico	Abrir el KeySafe que se ubica en la ruta: Start > All Program > nCipher > KeySafe 	
13	Administrador del Modulo Criptográfico	Aplicar la opción: 1.- "Cards" como se muestra. 2.- elegir la opción "Create New OCS" 	

Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
14	Administrador del Modulo Criptográfico	Una vez que damos clic en “Create New OCS” nos mostrará la siguiente ventana: En donde debemos ingresar: El nombre del set de tarjetas de Operadores = “OCS_PSCSeguriData” Enable pass phrase recovery for this card set = N/A Permit this card set to used remotely = NO Do you want the card set to be persistent = NO Do you want to set a timeout = NO Timeout in seconds = N/A El número total de Operadores = 6 El número de operadores requerido para acceder = 2 Aplicar el botón “Create OCS” 	
15	Administrador del Modulo Criptográfico	En este momento se deberá interactuar con los custodios Operadores ingresando las tarjetas de los custodios en blanco.	

Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
		 Una vez insertada la tarjeta en el Modulo criptográfico se debe aplicar el botón "OK"	
16	Administrador del Modulo Criptográfico	Enseguida se deberá ingresar la contraseña asociada a cada usuario de cada tarjeta:  Presionar botón OK.	
17	Administrador del Modulo Criptográfico	Se debe repetir los pasos 15 y 16 dependiendo del número de tarjetas a configurar. Al finalizar esta actividad y si se siguieron exactamente los pasos anteriores, nos desplegará la siguiente ventana:	

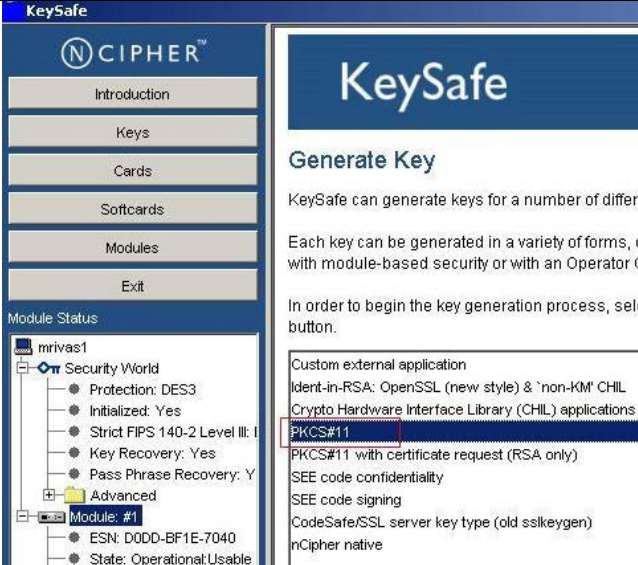
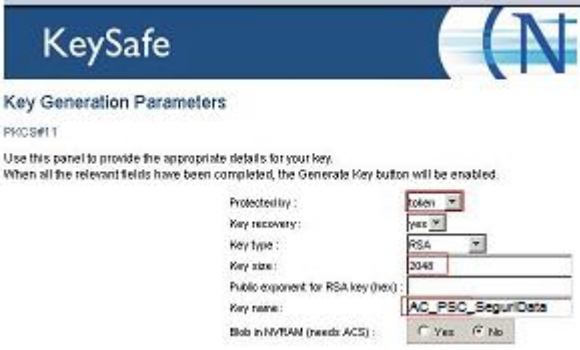
Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
		 Donde nos indica que la OCS se ha creado satisfactoriamente. Cerrar la aplicación de administración del módulo “Keysafe”	

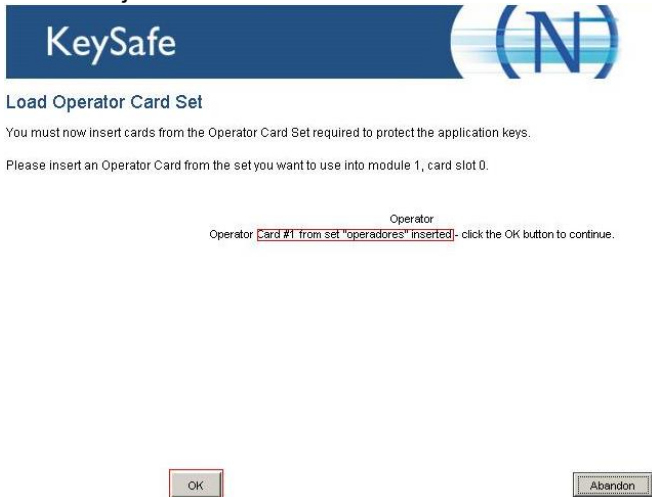
4. Creación de la llave privada y pública de la AC en el módulo criptográfico

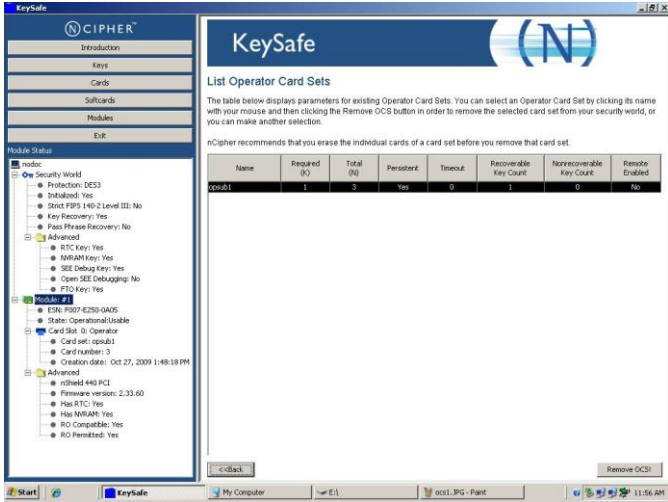
Ahora procederemos con la Creación de la llave privada de la Autoridad Certificadora.

Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
18	Administrador del Modulo Criptográfico	Abrir el KeySafe que se ubica en la ruta: Start > All Program > nCipher > KeySafe 	
19	Administrador del Modulo Criptográfico	Una vez que se abre el KeySafe, lo primero que se deberá verificar es: el estado del modulo como se muestra en la imagen: “State: OperationalUsable”	

Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
			
20	Administrador del Modulo Criptográfico	Para crear la llave privada. Elegir en la barra de Menú Opción KEYS >>>> Generate Key. 	
21	Administrador del Modulo Criptográfico	Una vez que aplicamos en "Generate key" nos mostrará una pantalla donde nos preguntará el tipo de llave que queremos crear.	

Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
		 Seleccionamos la PKCS11 y damos clic en el botón NEXT	
22	Administrador del Modulo Criptográfico	Enseguida nos preguntará los parámetros para la generación de la llave. Protected by = Token Key Recovery = Yes Key Type = RSA Key Size = 4096 Public Exponent for RSA Key (hex) = N/A Key Name = AC_PSC_TLA_SeguriData 	
23	Administrador del Modulo Criptográfico	Si los datos son correctos, entonces nos aparecerá la siguiente ventana:	

Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
		 Donde nos indica que tenemos que Insertar el número de tarjetas necesarias de acuerdo al Operador OCS.	
24	Administrador del Modulo Criptográfico	Una vez insertada la tarjeta, nos pedirá la confirmación del uso de esa tarjeta. 	
25	Administrador del Modulo Criptográfico	Una vez que confirmamos el uso de esa tarjeta nos pedirá que ingresemos la contraseña asociada a dicha tarjeta.  Damos clic en OK	

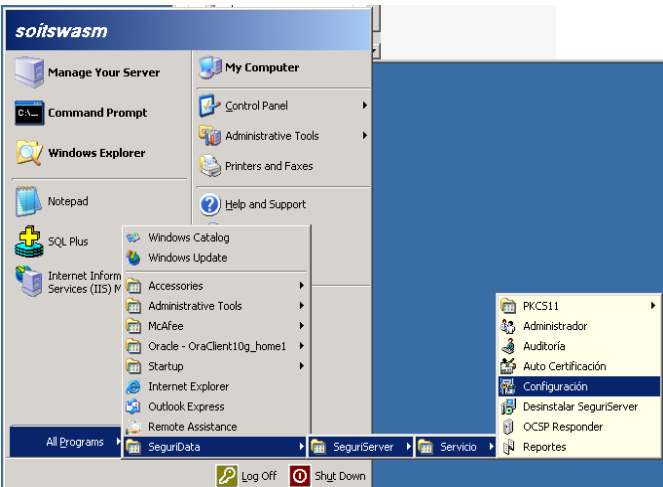
Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
26	Administrador del Modulo Criptográfico	Una vez introducida el password de la tarjeta, nos aparecerá la siguiente ventana:  Hemos creado la llave correctamente.	
27	Administrador del Modulo Criptográfico	Para confirmar que tenemos la llave, regresamos al menú de "KEY" y damos clic en "LIST KEYS"  Key Operations The buttons on this panel enable you to create new keys for a wic application key. You can discard an existing key by clicking the List Keys button b Before you can use a module to generate keys, you must have ei - initialized a security world using the module - reprogrammed the module with an existing security world. Use the options in the Module Operations panel to either initialize sidebar in order to go to the Module Operations panel. Generate Key create a new application key List Keys list all keys in the current security world Import Key import an application key from an outside source	
32	Administrador del Módulo Criptográfico	Y nos aparecerán las llaves que tenemos creadas hasta el momento.  Key name: AC_PSC_TLA_SeguriData	

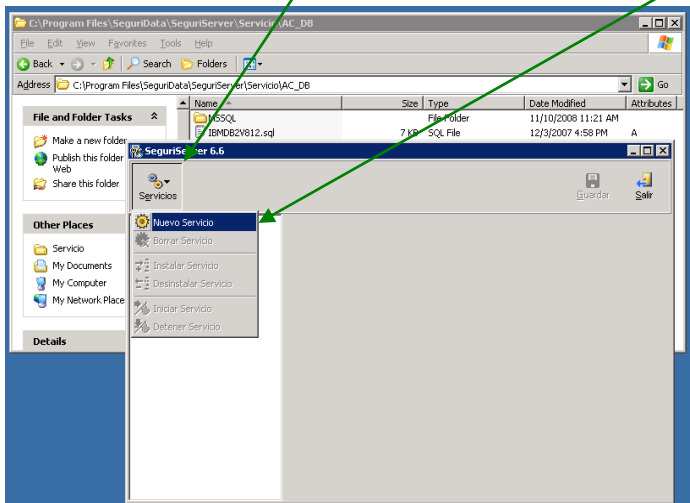
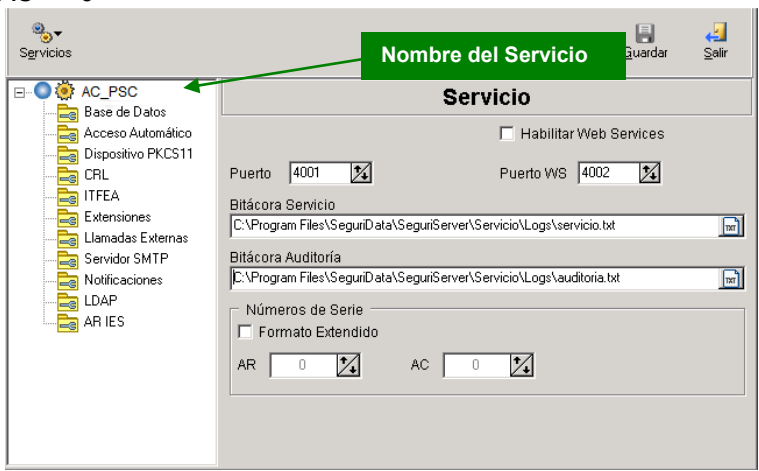
Cerramos la aplicación “KeySafe” con lo cual concluimos la generación de las llaves de la Autoridad Certificadora en el módulo criptográfico y que están asociadas a un conjunto de operadores (OCS_PSCSeguriData).

5.- Configuración del servicio de Autoridad Certificadora.

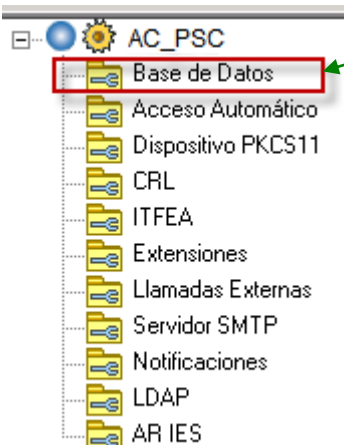
Una vez que ya contamos con las tablas y los objetos, procedemos a configurar el servicio para crear, borrar, dar de alta, de baja cualquier servicio.

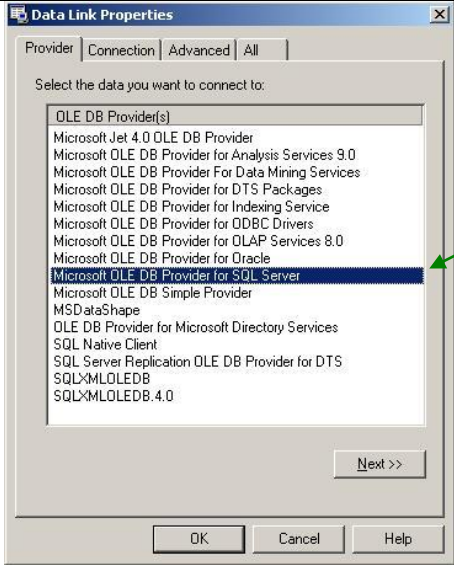
Para esto, necesitamos hacer lo siguiente:

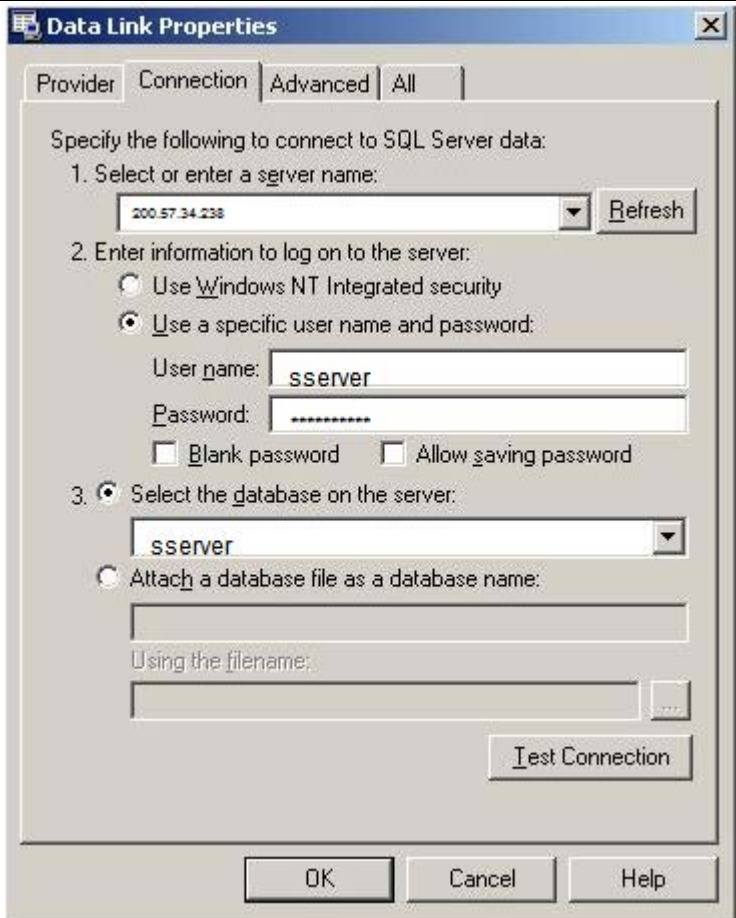
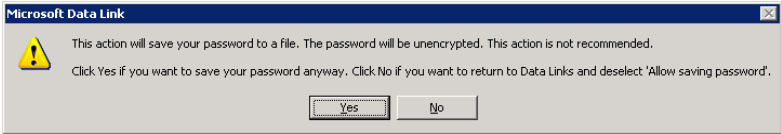
Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
33	Administrador del Sistema	Ubicarse en la ruta: Start > All programs> Seguridata> Servicio> Seguriserver> Configuración 	

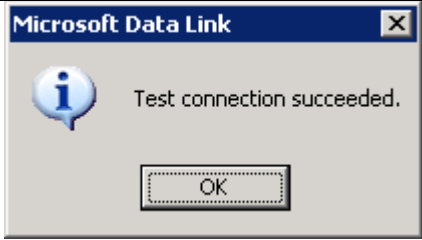
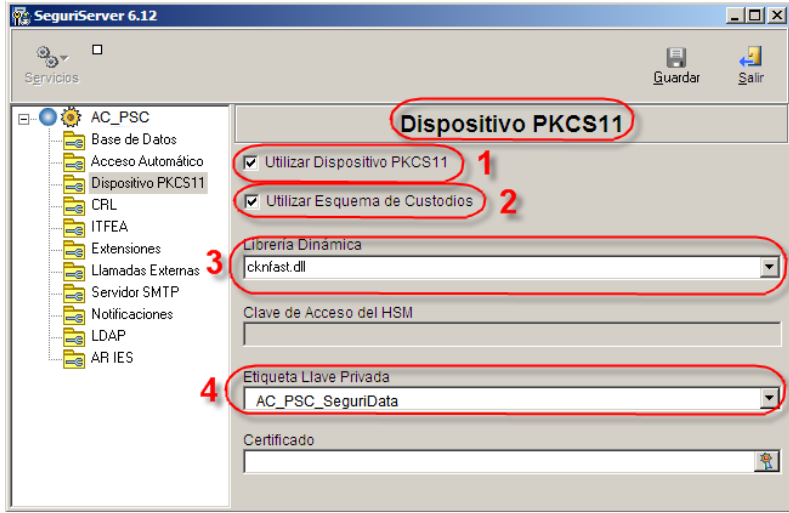
Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
34	Administrador del Sistema	Una vez realizado el paso anterior nos aparecerá una ventana de Bienvenida y enseguida aparece otra ventana donde debemos elegir en el recuadro de “Servicios”, la opción “Nuevo Servicio”. 	
35	Administrador del Sistema	Una vez que se le da la opción de “Nuevo Servicio” , debemos ingresar: El nombre del servicio = AC_PSC Los puertos = 4001 La ruta y el nombre de: Bitácoras de servicio = C:\Program Files\SeguriData\SeguriServer\Servicio\Logs\servicio.txt Bitácora de la auditoria = C:\Program Files\SeguriData\SeguriServer\Servicio\Logs\auditoria.txt Números de serie: Formato Extendido = Habilitado AR = 0 AC = 0 	

6.- Configuración de datos de conexión a la Base de Datos.

Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
36	Administrador del Sistema	En la ventana del lado izquierdo, elegir la opción “Base de Datos”. 	
37		Posteriormente crearemos el archivo con el nombre udl.udl y lo ejecutaremos para crear la cadena de conexión a la base de datos, como se observa en los siguientes pasos:	
38	Administrador del Sistema	Una vez que nos ha abierto esa nueva ventana procedemos a ubicarnos en la pestaña de “Provider” y seleccionamos el proveedor de la Base de Datos, que en este caso es: MS SQL Server Ventana Data Link Properties	

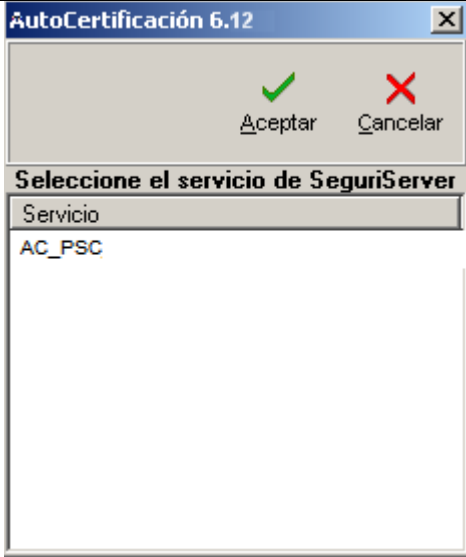
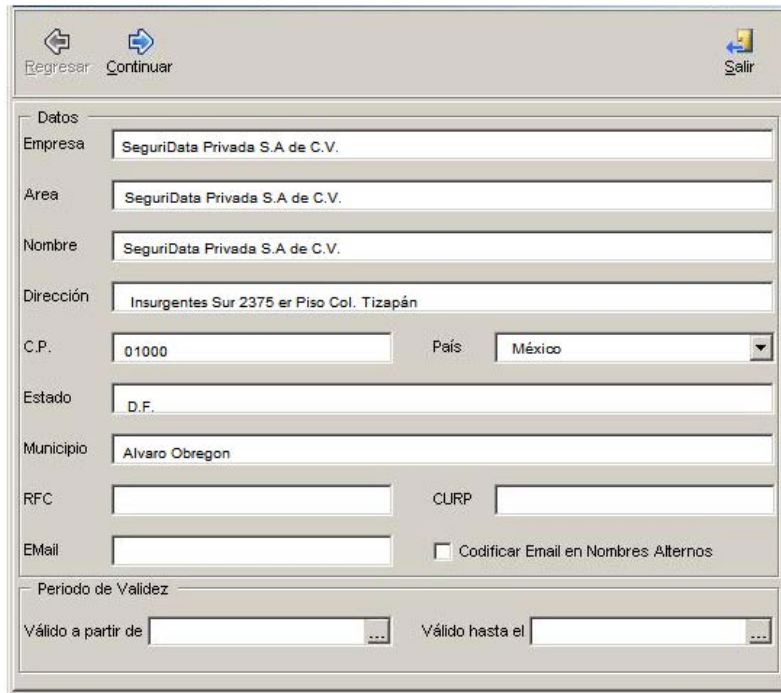
Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
		 Proveedor de BD MICROSOFT OLE DB PROVIDER for SQL SERVER	
39	Administrador del Sistema	En esa misma ventana pero en la pestaña de “Connection” proporcionamos los datos como se nos pide a continuación: Server name: = 200.57.34.238 User name: = sserver Password: = xxxxxxxxxx Allow saving Password = Habilitar Select the database on the server: = sserver	

Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
		 Al habilitar la casilla "Allow Saving Password" nos aparecerá la siguiente advertencia para no volver a teclear la contraseña. 	
40	Administrador del Sistema	En la misma ventana, en la parte inferior derecha, dar clic en Test Connection para probar la conexión. Si la conexión es correcta nos mostrará la siguiente ventana:	

Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
			
41		Elegimos la opción Dispositivo PKCS11, dentro este menú aplicamos las opciones como se observan en la imagen: Incluir imagen 	
42	Administrador del Sistema	Una vez que ya se han configurado todos los parámetros necesarios aplicamos el botón 	

7.- Creación de Certificado de AC y llaves del Administrador.

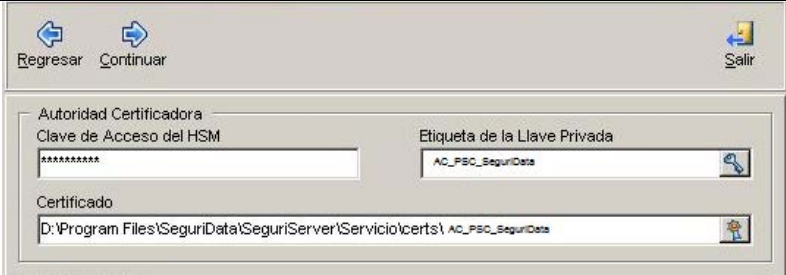
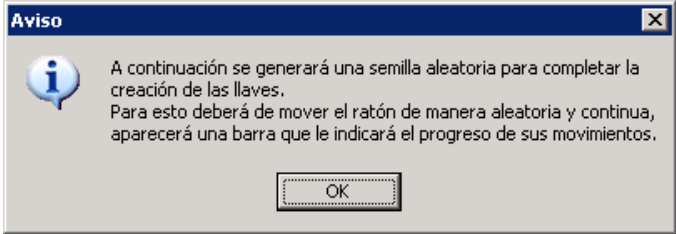
Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
43	Administrador del Sistema	Abrir el programa Start > All Programs> Seguridata> Seguriserver> Servicio>PKCS11 > Autocertificación 	
44	Administrador del Sistema	Una vez que aplicamos en Auto Certificación, nos abrirá una ventana donde observaremos el servicio que queremos autocertificar y relacionar con la llave privada previamente creada y lo debemos de seleccionar. Una vez que lo seleccionamos aplicamos el botón “Aceptar”	

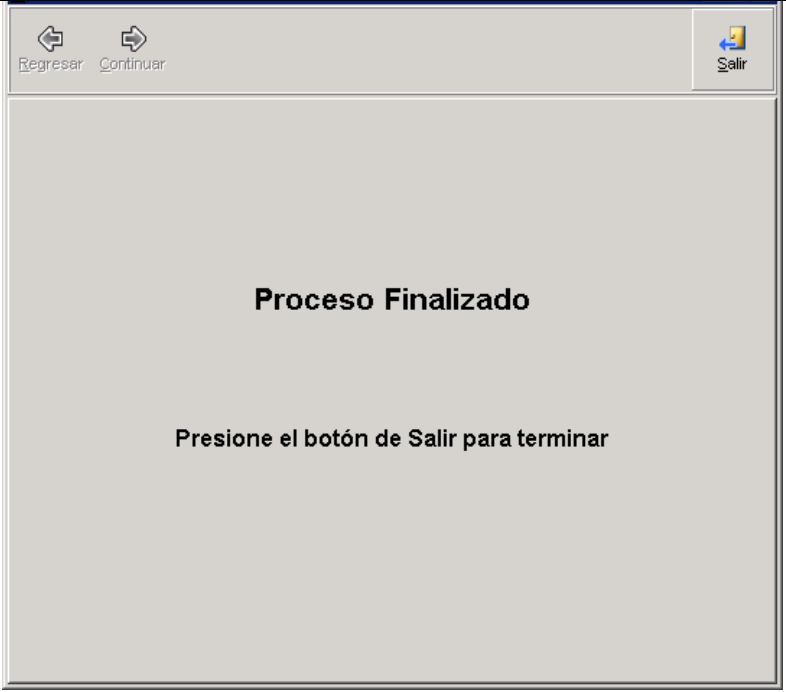
Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
			
45	Administrador del Sistema	Enseguida se abrirá una ventana donde te pedirá los datos para certificar. 	

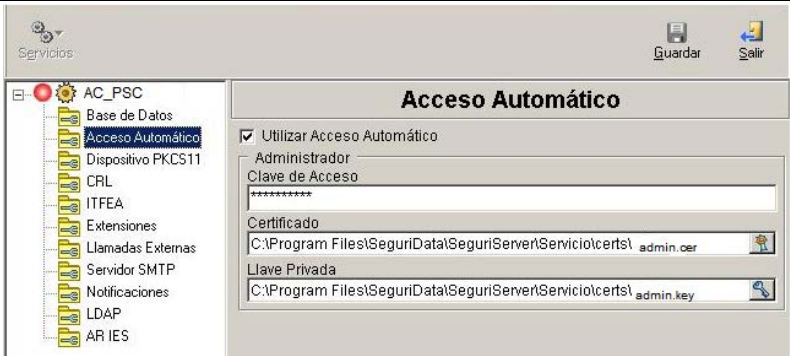
Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
46	Administrador del Sistema	Estos datos serán proporcionados por parte del Usuario, en este caso el “Administrador de PSC de SeguriData”. Una vez que se llenan los datos se da clic en el botón 	
47	Administrador del Sistema	Enseguida aparecerá otra ventana con las siguientes pestañas: 	
48	Administrador del Sistema	Pestaña “Uso de Llave” = NO MODIFICAR	
49	Administrador del Sistema	Pestaña “Nombres Alternos/Identificadores” = NO MODIFICAR	
50	Administrador del Sistema	Pestaña “Políticas” En esta pestaña se deberá habilitar la casilla de “Incluir CPS” y llenar los datos como se muestra a continuación:	

Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
		 Extensión crítica = habilitar OID = 2.16.484.101.10.316.2.5 URL (1) = http://seguridata.psc.com/ Texto (1) = No aplica URL (2) = No aplica Texto (2) = No aplica	
51	Administrador del Sistema	Pestaña “CRL/OCSP” En esta pestaña se habilitará la casilla “Incluir AIA (Authority Info Access)” y la casilla “Extensión Crítica” y proporcionar los datos (si es necesario) como se muestra a continuación:	

Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
		 CRL Distribution Point (CDP) = No aplica Authority Info Access (AIA) Incluir AIA = Habilitar URL de OCSP = http://200.57.34.238:8082 Extensión crítica = habilitar	
52	Administrador del Sistema	Pestaña "Otras Extensiones". = No Aplica.	
53	Administrador del Sistema	Una vez que se llenan los datos para las Extensiones, se da clic en el botón 	
54	Administrador del Sistema	Y enseguida te pedirá la etiqueta de la llave privada generada en el módulo criptográfico AC_PSC_TLA_SeguriData Debe definir la ruta donde se depositará el certificado una vez que el proceso haya terminado	

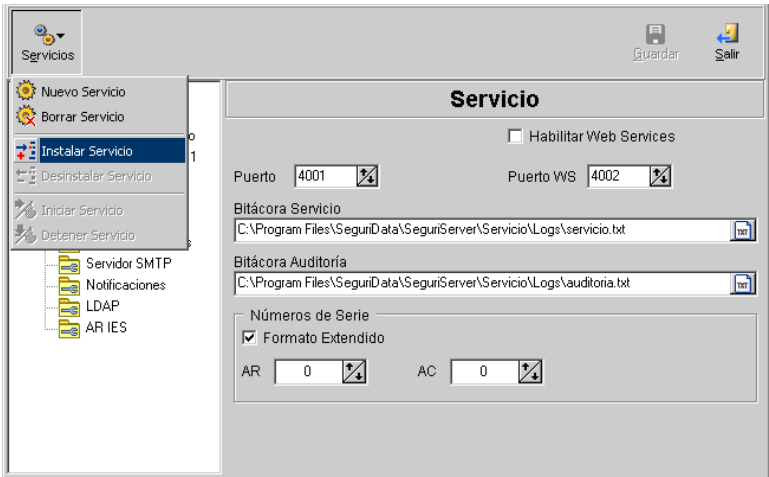
Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
			
55		En la misma ventana pero en la parte inferior, se deberá introducir la clave de acceso del administrador del servicio, el tamaño de la llave que es 4096 y la ruta y nombre donde se guardará la llave privada y el certificado. Debe introducir la Clave de Acceso para las Llaves del administrador de la Autoridad Certificadora la cual solo permite Letras y números y debe de construirse con un mínimo de 8 caracteres y no más de 255 caracteres. 	
56	Administrador del Sistema	Dar clic en el botón 	
57	Administrador del Sistema	Una vez que se da clic en “Siguiente”, saldrá una ventana de aviso en donde dice que se procederá a crear las llaves y se deberá mover el ratón de manera aleatoria y continua, como lo indica. 	
58	Administrador del Sistema	Por último ya que se han creado las llaves, saldrá la siguiente pantalla:	

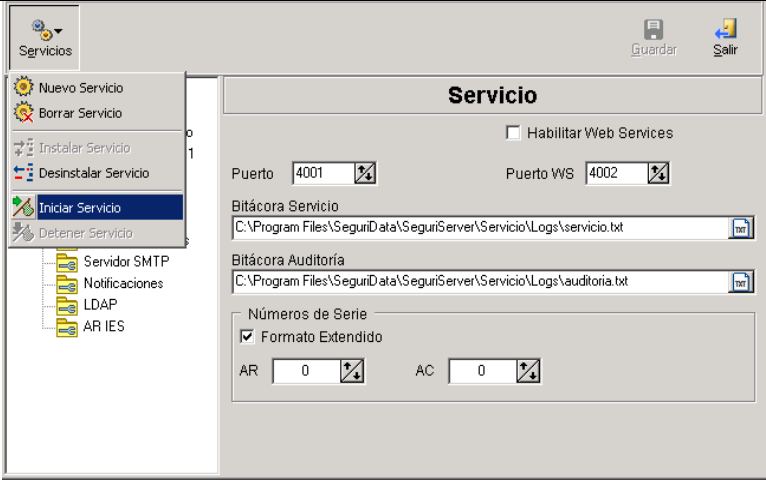
Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
			
59	Administrador del Sistema	Una vez que ya creamos las llaves tanto del Administrador, como las llaves de la Autoridad Certificadora, regresamos a la ventana de “SeguriServer 6.12”, dando clic en la parte de “Dispositivo PKCS11”, llenando los datos que se piden a continuación: 	
60	Administrador del Sistema	Una vez que ya creamos las llaves tanto del Administrador, como las llaves de la Autoridad Certificadora, regresamos a la ventana de “SeguriServer”, dando clic en la parte de “Acceso Automático” y llenamos los datos como aparece:	

Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
			
61	Administrador del Sistema	Una vez que ya hemos proporcionado las claves y las llaves, damos clic en el botón 	
62	Administrador del Sistema	En la parte de “Extensiones”, aparecen dos pestañas, la primera, “Políticas” en donde se debe habilitar la casilla “Incluir CPS” y la casilla “Extensión Crítica”, también se debe llenar los datos como se muestra a continuación: 	
63	Administrador del Sistema	En la pestaña CRL/OCSP se habilita la casilla Incluir AIA y la casilla Extensión Crítica. Los datos que se piden se deben de llenar con lo mismo que se puso en el Certificado de la AC durante el proceso de AutoCertificación Nota: La URL de OCSP es http://200.57.34.238:8082	

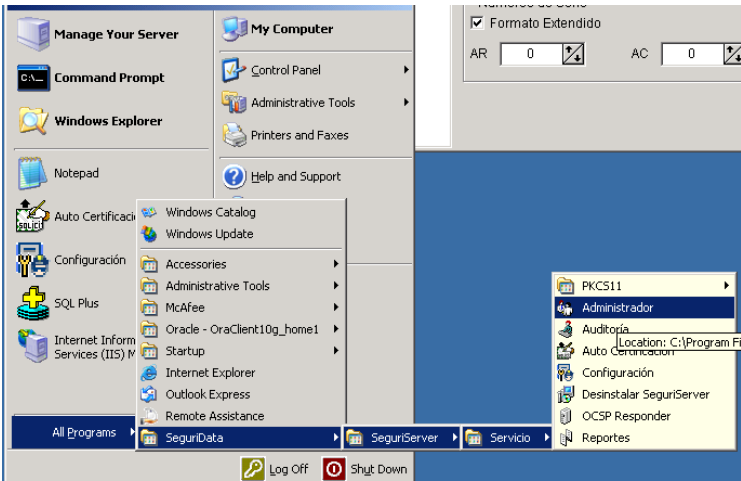
Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
64	Administrador del Sistema	Por ultimo nuevamente damos clic en el botón  y se finaliza con la configuración del Servicio.	

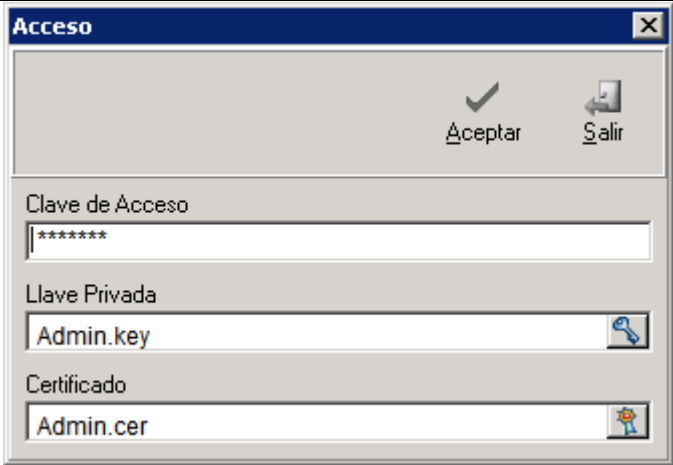
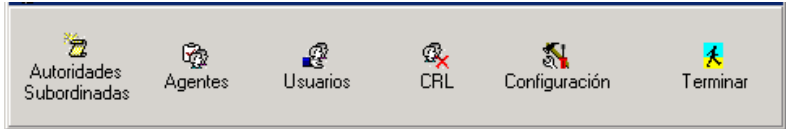
8.- Instalación del Servicio de la Autoridad Certificadora.

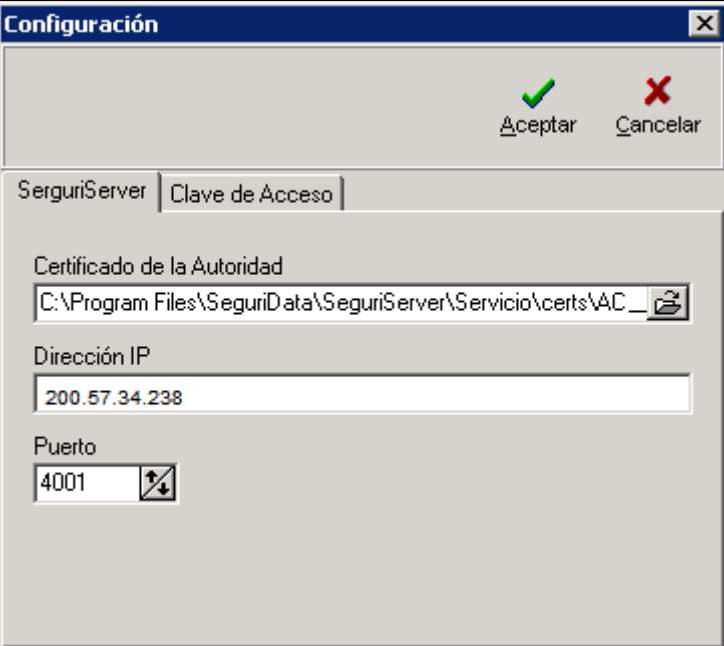
Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
65	Administrador del Sistema	Una vez que ya hemos creado las llaves, configurado el Servicio, procedemos a instalar el Servicio de la Autoridad Certificadora. Esto lo hacemos de la siguiente manera: Dar clic en el botón “Servicios” y desplegar una lista y ubicamos la opción “Instalar Servicio” 	
66	Administrador del Sistema	Una vez que se ha instalado el servicio procederemos a iniciarlo. Dar clic en el botón “Servicios” y desplegar una lista y ubicamos la opción “Iniciar Servicio”	

Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
			

9.- Configuración del Administrador de la AC

Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
67	Administrador del Sistema	Para configurar el Administrador, nos ubicamos en la ruta: Menú > All Programs> Seguridata> Seguriserver> Servicio> Administrador 	
68	Administrador del Sistema	Enseguida aparece una ventana donde te pide capturar las claves de acceso y la ruta de las llaves del Administrador (.key y .cer)	

Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
			
69	Administrador del Sistema	Una vez que capturamos las claves de acceso y damos clic en el botón “Aceptar” se abrirá una ventana con un menú que nos servirá para configurar el Administrador. 	
70	Administrador del Sistema	Para configurar el servicio del administrador, le proporcionamos los datos de Certificado (.cer) y la IP del Host del servicio, en la opción de “Configuración”	

Descripción de Actividades			
Paso	Responsable	Actividad	Iniciales Revisor
			
71	Administrador del Sistema	Ha concluido la instalación y configuración del SeguriServer.	

Reponsabilidades :

Las actividades se llevan a cabo por el administrador de sistemas en conjunto con el operador de sistemas; participan los propietarios de las tarjetas definidas para el arranque y administración del HSM

Las medidas de seguridad para los accesos deben ser autorizadas y vigiladas por el profesional informático y el auxiliar de apoyo informático de seguridad

22.6 Anexo 6 Reporte de muestra

Fecha: 20/06/2019 11:51:14 am

MUESTRA LOTE NÚMERO 1906201151

Operado por TESTER USER 3 (TEST USER 3)

NOMBRE DEL CLIENTE DEMO SAFE		REPRESENTANTE LEGAL	
DOMICILIO ,, , CP 00000			
NOMBRE DEL COMERCIANTE			
NOMBRE DE LA DIGITALIZADORA		TERCERO LEGALMENTE AUTORIZADO Seguridata	
PROFESIONAL JURÍDICO JOE DOE		PROFESIONAL DEL INFORMÁTICO JUAN PEREZ	
NÚMERO DE LOTE 20190620114935	DOCUMENTOS DIGITALIZADOS 2	FOLIO INICIAL 0000000000000126	FOLIO FINAL 0000000000000127
TAMAÑO DE LA MUESTRA 1	NIVEL DE CONFIANZA 1.6500	LÍMITE DE ERROR 5%	DESVIACIÓN ESTÁNDAR 0.5000
FECHA DE DIGITALIZACIÓN 20/06/2019 11:51:14 a.m			

NÚMEROS ALEATORIOS GENERADOS

233737881; 987854034

SEMILLA ALEATORIA 1441723200	FECHA / HORA 2019-06-20 11:51:14	TÉCNICA DE MUESTREO Aleatorio Sistemático
---------------------------------	-------------------------------------	--

RAZONES POR LAS QUE SE ELIGIÓ LA TÉCNICA DE MUESTREO

MEJOROPCION

FOLIOS SELECCIONADOS QUE FORMAN LA MUESTRA

0000000000000127

22.7 Anexo 7 Reporte de Cotejo

Fecha: 20/06/2019 11:51:14 am

COTEJO DE LA MUESTRA LOTE NÚMERO 1906201151

Operado por TESTER USER 3 (TEST USER 3)

NOMBRE DEL CLIENTE DEMO SAFE		REPRESENTANTE LEGAL	
DOMICILIO , , , CP 00000			
NOMBRE DEL COMERCIANTE			
NOMBRE DE LA DIGITALIZADORA		TERCERO LEGALMENTE AUTORIZADO Seguridata	
PROFESIONAL JURÍDICO JOE DOE		PROFESIONAL DEL INFORMÁTICO JUAN PEREZ	
NÚMERO DE LOTE 20190620114935	DOCUMENTOS DIGITALIZADOS 2	FOLIO INICIAL 0000000000000126	FOLIO FINAL 0000000000000127
TAMAÑO DE LA MUESTRA 1	NIVEL DE CONFIANZA 1.6500	LÍMITE DE ERROR 5%	DESVIACIÓN ESTÁNDAR 0.5000
FECHA DE COTEJO 20/06/2019 11:51:14 a.m			

NÚMEROS ALEATORIOS GENERADOS

233737881; 987854034

SEMILLA ALEATORIA	FECHA / HORA	TÉCNICA DE MUESTREO
1441723200	2019-06-20 11:51:14	Aleatorio Sistemático

RAZONES POR LAS QUE SE ELIGIÓ LA TÉCNICA DE MUESTREO

MEJOR OPCION

FOLIOS SELECCIONADOS QUE FORMAN LA MUESTRA

0000000000000127

RESULTADO DEL COTEJO DE LA MUESTRA

NO HUBO DIFERENCIAS EN LA MUESTRA

ESTAMPA DE TIEMPO

NÚMERO SECUENCIA ESTAMPA DE TIEMPO 41557	EMITIDO POR TSP722	FECHA 2019-06-20 11:51:14
NOMBRE CERTIFICADO AUTORIDAD CERTIFICADORA AUTORIDAD CERTIFICADORA	DIGESTIÓN ESTAMPA DE TIEMPO 786205B8420F3ADB9F4E9C7D74DFE295D2B3D4E28A0953D05F08C2709773CA0C	POLÍTICA 1.3.6.1.4.1.9203.2.1

FIRMA DEL TLA

FIRMADO POR: PRUEBA 1
AC: Autoridad Certificadora Windows 2012 Oracle 12c
ID: 5199
HASH:
418BFA8A14C9A96989096AA5E9182B7FE9DDEE1
2285586E5D25A5C81998CD6BF

22.8 Anexo 8 Acta circunstanciada

- Sin diferencias
- Aceptada con anomalías justificables
- No aceptada con animalias justificables
- Con animalias no justificables

ACTA CIRCUNSTANCIADA

En la Ciudad de México, siendo las ____ horas con ____ minutos, del día ____ de ____ del dos mil 20____, reunidos en las oficinas que ocupa ____ ubicadas en ____, estando presentes la Lic. Cynthia Peña Bravo en su carácter de Profesional Jurídico y el Ing. Moisés Bautista Osorno en su carácter de Profesional Informático de SEGURIDATA PRIVADA S.A. DE C.V. (SeguriData) en su calidad de **Tercero Legalmente Autorizado (TLA)**, ____, en su calidad de **Digitalizador** representado en este acto por ____ y ____ en lo sucesivo **EL Cliente**, representado por su apoderado ____ , quienes firman para debida constancia y a quienes se les exhorta para que se conduzcan con verdad en el levantamiento de la presente acta; con fundamento en los artículos 95 bis 4 del Código de Comercio, la Norma Oficial Mexicana SCFI-151-2016 "Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos" en lo sucesivo "NOM 151" y las reglas 181 y 228 de las Reglas a las que deberán sujetarse los Prestadores de Servicios de Certificación , en lo sucesivo "Las Reglas"; se procede a instrumentar la presente acta circunstanciada para dejar constancia de las actividades de cotejo de la documentación en soporte físico y mensajes de datos que se realizaron a solicitud de El Cliente.

HECHOS

Se otorga el uso de la palabra a la C. Cynthia Peña Bravo, Profesional Jurídico de SeguriData Privada S.A. de C.V. quien en este acto manifiesta:

Que de acuerdo al Contrato de Prestación de Servicios de Digitalización de fecha ____, celebrado entre SeguriData Privada S.A. de C.V. en su carácter de Tercero Legalmente Autorizado y El Cliente; SeguriData procedió por conducto del Digitalizador a la migración de documentos en soporte físico a formato digital, de los documentos señalados en dicho contrato, y del cual obra un tanto en poder de cada una de las Partes contratantes y se tiene aquí por reproducido como si a la letra se insertase.-----

Una vez digitalizados los documentos, se procedió al cotejo de los mismos bajo la supervisión del Profesional Informático y Jurídico de SeguriData, y con la presencia de los demás comparecientes, realizando el cotejo sobre el muestreo determinado previamente por ambas partes, bajo las características del Anexo 1 del mencionado contrato de servicios entre SeguriData y El Cliente en términos de la normatividad mencionada y de la Política de Digitalización de SeguriData, **SIN QUE SE HUBIERAN ENCONTRADO DIFERENCIAS** entre los documentos en soporte físico y los datos de mensajes de datos resultantes de la digitalización.-----

El representante legal del Digitalizador en uso de la palabra señala hace constar que la migración de los documentos físicos proporcionados por El Cliente para tales efectos se realizó de manera íntegra e inalterablemente por lo que garantiza la fidelidad e integridad de los mensajes de datos resultantes de la digitalización de documentos en soporte físico.-----

El Cliente en uso de la palabra señala su entera satisfacción con el cotejo realizado y con el servicio prestado por lo que expresa su conformidad para recibir los mensajes de datos resultantes del proceso de digitalización de documentos en soporte físico en la forma que se ha determinado en el contrato, sin tener comentario adicional u objeción alguna que efectuar.-----

(CUANDO APLIQUE) De igual manera se hace constar que a solicitud de El Cliente, el Lic. _____(Notario o Corredor) Público número _____ de la Ciudad de México, participó en la Ceremonia de Cotejo para dar fe de la misma.-----

POR LO ANTERIOR Y EN VIRTUD DE QUE EL COTEJO NO ARROJA DIFERENCIAS se procedió a la firma electrónica de los mensajes de datos obtenidos como resultado de la digitalización de documentos en soporte físico, por SeguriData como Tercero Legalmente Autorizado, por _____ como Digitalizador así como por El Cliente. De igual manera se procedió a la incorporación de los sellos digitales de tiempo y la constancia de conservación de mensaje de datos NOM 151 correspondientes.-----

En razón de lo anterior y toda vez que no existe algún otro asunto que tratar, las Partes están de acuerdo en que se declare por concluida la presente acta circunstanciada, siendo las _____ horas con _____ minutos del día, mes y año de su inicio, firmando al calce quienes en ella intervinieron para debida constancia legal. -----

FIRMAS

EL CLIENTE

DIGITALIZADOR

**TERCERO LEGALMENTE
AUTORIZADO
SeguriData Privada S.A. de
C.V.**

Representante Legal

Representante Legal

Representante Legal

ACTA CIRCUNSTANCIADA

En la Ciudad de México, siendo las ____ horas con ____ minutos, del día ____ de ____ del dos mil 20____, reunidos en las oficinas que ocupa _____ ubicadas en _____, estando presentes la Lic. Cynthia Peña Bravo en su carácter de Profesional Jurídico y el Ing. Moisés Bautista Osorno en su carácter de Profesional Informático de SEGURIDATA PRIVADA S.A. DE C.V. (SeguriData) en su calidad de **Tercero Legalmente Autorizado (TLA)**, _____, en su calidad de **Digitalizador** representado en este acto por _____ y _____ en lo sucesivo **EL Cliente**, representado por su apoderado _____, quienes firman para debida constancia y a quienes se les exhorta para que se conduzcan con verdad en el levantamiento de la presente acta; con fundamento en los artículos 95 bis 4 del Código de Comercio, la Norma Oficial Mexicana SCFI-151-2016 "Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos" en lo sucesivo "NOM 151" y las reglas 181 y 228 de las Reglas a las que deberán sujetarse los Prestadores de Servicios de Certificación, en lo sucesivo "Las Reglas"; se procede a instrumentar la presente acta circunstanciada para dejar constancia de las actividades de cotejo de la documentación en soporte físico y mensajes de datos que se realizaron a solicitud de El Cliente.

HECHOS

Se otorga el uso de la palabra a la C. Cynthia Peña Bravo, Profesional Jurídico de SeguriData Privada S.A. de C.V. quien en este acto manifiesta: -----

Que de acuerdo al Contrato de Prestación de Servicios de Digitalización de fecha _____, celebrado entre SeguriData Privada S.A. de C.V. en su carácter de Tercero Legalmente Autorizado y El Cliente; SeguriData procedió por conducto del Digitalizador a la migración de documentos en soporte físico a formato digital, de los documentos señalados en dicho contrato, y del cual obra un tanto en poder de cada una de las Partes contratantes y se tiene aquí por reproducido como si a la letra se insertase.-----

Una vez digitalizados los documentos, se procedió al cotejo de los mismos bajo la supervisión del Profesional Informático y Jurídico de SeguriData, y la presencia de los demás comparecientes, en términos de la normatividad mencionada y de la Política de Digitalización de SeguriData, realizando el cotejo sobre el muestreo determinado previamente por ambas partes, bajo las Características del Anexo 1 del mencionado contrato de servicios entre SeguriData y El Cliente, ENCONTRANDOSE ANOMALÍAS NO JUSTIFICABLES EN LA VALIDACION DE LA MUESTRA.-----

La “Anomalía No Justificable”, se define como la alteración de un documento digitalizado contra el original: puede ser que falte texto o que tenga un texto que no coincida por el documento original, donde existe presunción de actuación con dolo.-----

Por lo anterior y en términos de la Política de Digitalización de SeguriData Privada S.A. de C.V. y de la normatividad aplicable, el Profesional Jurídico del Tercero Legalmente Autorizado deja constancia de lo anterior, por lo que no se procede a la firma de los mensajes de datos resultantes de la digitalización y se procederá a dar aviso por medios electrónicos a la Secretaría de Economía.-----

El Cliente en uso de la palabra señala que con motivo de lo que ha quedado explicado por el TLA, rechaza los servicios y por tanto no recibe de conformidad los mensajes de datos resultantes del proceso de digitalización-----

(CUANDO APLIQUE) De igual manera se hace constar que a solicitud de El Cliente, el Lic. _____(Notario o Corredor) Público número _____ de la Ciudad de México, participó en la Ceremonia de Cotejo para dar fe de la misma.-----

En razón de lo anterior y toda vez que no existe algún otro asunto que tratar, las Partes están de acuerdo en que se declare concluida la presente acta circunstanciada, siendo las ____ horas con _____ minutos del día, mes y año de su inicio, firmando al calce y margen quienes en ella intervinieron para debida constancia legal. -----

FIRMAS

EL CLIENTE

DIGITALIZADOR

**TERCERO LEGALMENTE
AUTORIZADO
SeguriData Privada S.A. de
C.V.**

Representante Legal

Representante Legal

Representante Legal

ACTA CIRCUNSTANCIADA

En la Ciudad de México, siendo las ____ horas con ____ minutos, del día ____ de ____ del dos mil 20____, reunidos en las oficinas que ocupa ____ ubicadas en ____, estando presentes la Lic. Cynthia Peña Bravo en su carácter de Profesional Jurídico y el Ing. Moisés Bautista Osorno en su carácter de Profesional Informático de SEGURIDATA PRIVADA S.A. DE C.V. (SeguriData) en su calidad de **Tercero Legalmente Autorizado (TLA)**, ____, en su calidad de **Digitalizador** representado en este acto por ____ y ____ en lo sucesivo **EL Cliente**, representado por su apoderado ____ quienes firman para debida constancia y a quienes se les exhorta para que se conduzcan con verdad en el levantamiento de la presente acta; con fundamento en los artículos 95 bis 4 del Código de Comercio, la Norma Oficial Mexicana SCFI-151-2016 "Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos" en lo sucesivo "NOM 151" y las reglas 181 y 228 de las Reglas a las que deberán sujetarse los Prestadores de Servicios de Certificación, en lo sucesivo "Las Reglas"; se procede a instrumentar la presente acta circunstanciada para dejar constancia de las actividades de cotejo de la documentación en soporte físico y mensajes de datos que se realizaron a solicitud de El Cliente

HECHOS

Se otorga el uso de la palabra a la C. Cynthia Peña Bravo, Profesional Jurídico de SeguriData Privada S.A. de C.V. quien en este acto manifiesta:

Que de acuerdo al Contrato de Prestación de Servicios de Digitalización de fecha ____, celebrado entre SeguriData Privada S.A. de C.V. en su carácter de Tercero Legalmente Autorizado y El Cliente; SeguriData procedió por conducto del Digitalizador a la migración de documentos en soporte físico a formato digital, de los documentos señalados en dicho contrato, y del cual obra un tanto en poder de cada una de las Partes contratantes y se tiene aquí por reproducido como si a la letra se insertase.-----

Una vez digitalizados los documentos, se procedió al cotejo de los mismos bajo la supervisión del Profesional Informático y Jurídico de SeguriData, y la presencia de los demás comparecientes, realizando el cotejo sobre el muestreo determinado previamente por ambas partes, bajo las Características del Anexo 1 del mencionado contrato de servicios entre SeguriData y El Cliente, en

términos de la normatividad mencionada y de la Política de Digitalización de SeguriData, ENCONTRANDOSE ANOMALÍAS JUSTIFICABLES EN LA VALIDACION DE LA MUESTRA.-----

Una “**Anomalía Justificable**” se define como la falta de nitidez de la imagen que se revisa, de manera que exista un criterio de aceptación de la nitidez y calidad de la imagen, o en su caso de rechazo y se solicite de nuevo la digitalización.-----

El Cliente en uso de la palabra manifiesta entender lo que ha señalado el TLA y señala que decide aceptar el cotejo y continuar con el proceso de firma electrónica de los mensajes de datos y expresa asimismo su conformidad para recibir los mensajes de datos resultantes del proceso de digitalización en la forma en que lo ha acordado previamente con el TLA.-----

Por lo anterior se procedió a la firma electrónica del mensaje de datos obtenido como resultado de la digitalización de documentos en soporte físico, por SeguriData como Tercero Legalmente Autorizado, por _____ como Digitalizador así como por El Cliente y a la incorporación del sello digital de tiempo y constancia de conservación de mensaje de datos correspondientes.-----

(CUANDO APLIQUE) De igual manera se hace constar que a solicitud de El Cliente, participó en la Ceremonia de Cotejo, el Lic. _____(Notario o Corredor) Público número _____de la Ciudad de México, para dar fe de la misma.-----

En razón de lo anterior y toda vez que no existe algún otro asunto que tratar, las Partes están de acuerdo en que se declare concluida la presente acta circunstanciada, siendo las ____ horas con ____ minutos del día, mes y año de su inicio, firmando al calce y margen quienes en ella intervinieron para debida constancia legal. -----

EL CLIENTE

DIGITALIZADOR

**TERCERO LEGALMENTE
AUTORIZADO
SeguriData Privada S.A. de
C.V.**

Representante Legal

Representante Legal

Representante Legal

ACTA CIRCUNSTANCIADA

En la Ciudad de México, siendo las ____ horas con ____ minutos, del día ____ de ____ del dos mil 20____, reunidos en las oficinas que ocupa ____ ubicadas en _____, estando presentes la Lic. Cynthia Peña Bravo en su carácter de Profesional Jurídico y el Ing. Moisés Bautista Osorno en su carácter de Profesional Informático de SEGURIDATA PRIVADA S.A. DE C.V. (SeguriData) en su calidad de **Tercero Legalmente Autorizado (TLA)**, _____, en su calidad de **Digitalizador** representado en este acto por _____ y _____ en lo sucesivo **El Cliente**, representado por _____ en su carácter de representante legal, quienes firman para debida constancia y a quienes se les exhorta para que se conduzcan con verdad en el levantamiento de la presente acta; con fundamento en los artículos 95 bis 4 del Código de Comercio, la Norma Oficial Mexicana SCFI-151-2016 "Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos" en lo sucesivo "NOM 151" y las reglas 181 y 228 de las Reglas a las que deberán sujetarse los Prestadores de Servicios de Certificación, en lo sucesivo "Las Reglas"; se procede a instrumentar la presente acta circunstanciada para dejar constancia de las actividades de cotejo de la documentación en soporte físico y mensajes de datos que se realizaron a solicitud de El Cliente.-----

HECHOS

Se otorga el uso de la palabra a la C. Cynthia Peña Bravo, Profesional Jurídico de SeguriData Privada S.A. de C.V. quien en este acto manifiesta: -----

Que de acuerdo al Contrato de Prestación de Servicios de Digitalización de fecha _____, celebrado entre SeguriData Privada S.A. de C.V. en su carácter de Tercero Legalmente Autorizado y El Cliente; SeguriData procedió por conducto del Digitalizador a la migración de documentos en soporte físico a formato digital, de los documentos señalados en dicho contrato, y del cual obra un tanto en poder de cada una de las Partes contratantes y se tiene aquí por reproducido como si a la letra se insertase.-----

Una vez digitalizados los documentos, se procedió al cotejo de los mismos bajo la supervisión del Profesional Informático y Jurídico de SeguriData, y con la presencia de los demás comparecientes, realizando el cotejo sobre el muestreo determinado previamente por ambas partes, bajo las características del Anexo 1 del mencionado contrato de servicios entre SeguriData y El Cliente, en términos de la normatividad mencionada y de la Política de Digitalización de SeguriData, **ENCONTRANDOSE ANOMALÍAS JUSTIFICABLES EN LA VALIDACION DE LA MUESTRA.**-----

Una "**Anomalia Justificable**" se define como la falta de nitidez de la imagen que se revisa, de manera que exista un criterio de aceptación de la nitidez y calidad de la imagen, o en su caso de rechazo y se solicite de nuevo la digitalización.-----

El Cliente en uso de la palabra manifiesta que no acepta el Cotejo y solicita reiniciar la digitalización de los documentos mejorando la calidad de la misma.-----

Una vez repetida la digitalización, se procede de nuevo a su cotejo bajo la supervisión del Profesional Informático y Jurídico de SeguriData, y con la presencia de los demás comparecientes, comprobando que ya no arroja diferencias entre los documentos en soporte físico y los datos de mensajes de datos resultantes de la digitalización.-----

El Cliente en uso de la palabra señala su satisfacción con el cotejo realizado y con el servicio prestado por lo que manifiesta su conformidad para recibir los mensajes de datos resultantes del proceso de digitalización de documentos en soporte físico en los términos acordados en el contrato, sin tener comentario adicional u objeción alguna que efectuar.-----

El representante legal del Digitalizador en uso de la palabra señala hace constar que la digitalización de los documentos físicos proporcionados por El Cliente para tales efectos se realizó de manera íntegra e inalterablemente por lo que garantiza la fidelidad e integridad de los mensajes de datos resultantes de la digitalización de documentos en soporte físico. -----

Por lo anterior se procedió a la firma electrónica de los mensajes de datos obtenidos como resultado de la digitalización de documentos en soporte físico, por SeguriData como Tercero Legalmente Autorizado, por _____ como Digitalizador así como por El Cliente. De igual manera se procedió a la incorporación de los sellos digitales de tiempo y la constancia de conservación de mensaje de datos NOM 151 correspondientes.-----

(CUANDO APLIQUE) De igual manera se hace constar que a solicitud de El Cliente, el Lic. _____ (Notario o Corredor) Público número _____ de la Ciudad de México, participó en la Ceremonia de Cotejo para dar fe de la misma.-----

En razón de lo anterior y toda vez que no existe algún otro asunto que tratar, las Partes están de acuerdo en que se declare por concluida la presente acta circunstanciada, siendo las _____ horas con _____ minutos del día, mes y año de su inicio, firmando al calce quienes en ella intervinieron para debida constancia legal. -----

FIRMAS

EL CLIENTE

DIGITALIZADOR

**TERCERO LEGALMENTE
AUTORIZADO
SeguriData Privada S.A. de C.V.**

Representante Legal

Representante Legal

Representante Legal

22.9 Anexo 9 Formato de recepción – entrega de documentos en soporte físico

Cliente (Comerciante)	
Fecha de Recepción:	
Folio :	
Tipo de Envase:	Bolsa con sello _____ Valija con cintillo _____ Ambos _____

Cantidad de Documentos	Tipo de Documento		
	Original	Copia	Copia certificada

OBSERVACIONES ESPECIALES

--

Domicilio para Recepción:			
Domicilio para Entrega:			
Persona que recoge/entrega:	Nombre	Fecha	Firma
Comerciante que recoge/entrega:	Nombre	Fecha	Firma
Comerciante que recoge/entrega:	Nombre	Fecha	Firma

22.10 Anexo 10 Formato de Devolución de documentos en soporte físico



FORMATO DEVOLUCIÓN DE DOCUMENTOS EN FÍSICO DESPUÉS DE DIGITALIZACIÓN

Cliente (Comerciante)	
Fecha de Devolución:	
Folio :	
Tipo de Envase:	Bolsa con sello _____ Valija con cintillo _____ Ambos _____

Cantidad de Documentos	Tipo de Documento		
	Original	Copia	Copia certificada

OBSERVACIONES ESPECIALES

--

Domicilio para Devolución:			
Persona que hace devolución:	Nombre	Fecha	Firma
Comerciante que recibe:	Nombre	Fecha	Firma