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

## OID: 2.16.484.101.10.316.100.5.1.6.1.1

**Versión 1.4**
**Octubre 2019**

# Tabla de Contenidos

# 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 | NOVIEMBRE 2018 | DOCUMENTO INICIAL |
| 1,.1 | MAYO 2019 | ACTUALIZACION POR RECOMENDACIÓN ISO/TR13028 Y ACT DE COMENTARIOS REVISION PRELIMINAR |
| 1.2 | JULIO 2019 | ACTUALIZACIÓN POR COMENTARIOS DE SECRETARIA DE ECONOMÍA |
| 1.3 | AGOSTO 2019 | ACTUALIZACIÓN DE DOCUMENTO |
| 1.4 | 22 OCT 2019 | ACTUALIZACIÓN DE OID |

# 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 |
|---|---|---|---|
| CDMEX. | INSURGENTES SUR 2375 | OLGA GARCIA | MAGNETICO Y PAPEL |
| CDMEX. | 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 del tercero legalmente autorizado, lo que no implica una actualización del mismo.

| FECHAS PROGRAMADAS |
|---|

| DE FUTURAS REVISIONES |
|---|
| 01/02/2019 |
| 01/02/2020 |
| 02/10/2021 |
| 02/10/2022 |
| 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, Emisión de Sellos digitales de Tiempo y Emisión de Constancias de Conservación de Mensajes de datos NOM 151-SCFI 2016, y como Tercero Legalmente Autorizado, en la Digitalización de Documentos en Soporte Físico de conformidad con la NOM-151-SCFI-2016, ante la Secretaria de Economía.

La presente Política contiene las políticas 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.

La presente Política tiene por objeto el permitir a personas físicas o morales (por medio del representante legal), acreditar ante cualquier tercero o autoridad que la representación en medios electrónicos de la digitalización de documentos en soporte físico se han conservados íntegros y sin cambios desde el momento de su digitalización.

Esta política está en concordancia con la Declaración de Prácticas de digitalización, la Política está presentando el Que se va a realizar y la Declaración, él Como se va a realizar.

# 3. Alcance

El ámbito de aplicación es para cualquier documento físico de carácter mercantil que requiera digitalizarse, de las empresas y comerciantes, 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 digitalizado, en concordancia con las mejores prácticas definidas en el ISO/TR 1328.

# 4. Referencias

La estructura de esta Política 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: **DOF: 30/03/2017**.
- Código de Comercio, CAPITULO I Bis denominado “De la Digitalización”, con los artículos 95 bis1, 95 bis 2, 95 bis 3, 95 bis 4, 95 bis 5, y 95 bis 6: **DOF: 07/04/2016**
- Reforma a las Reglas generales a las que deberán sujetarse los prestadores de servicios de certificación. (publicado(a) en el Diario Oficial de la Federación el 14/mayo/2018).
- ISO/TR 132

# 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 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 Sintax 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 |

| TÉRMINO | DEFINICIÓN |
|---|---|
| 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 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 Política de la Autoridad de Digitalización que funge como Tercero Legalmente autorizado

| | |
|---|---|
| **Nombre del documento** | Política 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** | 14 |
| **Autor** | SeguriData Privada S.A. de C.V. |
| **Estado del documento** | AUTORIZADO |
| **Fecha de emisión** | Agosto 2019 |

| | |
|---|---|
| **Fecha de inicio de uso** | Sin determinar |
| **Fecha de expiración** | No es aplicable |
| **Identificador Digital de Objetos – OID (Object Identifier Digital)** | 2.16.484.101.10.316.100.5.1.6.1.1 |
| **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 |
| **Política de Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico Asociada a:** | 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 |

### 6.1 Concordancia de la Política de Digitalización de documentos en soporte físico, con la Declaración de prácticas de Digitalización de documentos en Soporte Físico conforme la NOM 151-SCFI-2016

Se asegura la concordancia de la Política de Digitalización de documentos en soporte físico, con la Declaración de prácticas de Digitalización de documentos en Soporte Físico y con los procedimientos operacionales definidos, en dicha Declaración.

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

Esta política está en concordancia con la Declaración de Prácticas de digitalización, la Política está presentando el Que se va a realizar y la Declaración, él Como se va a realizar.

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

| **Responsable de la Administración de la Política 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 Política de Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico y su Publicación.

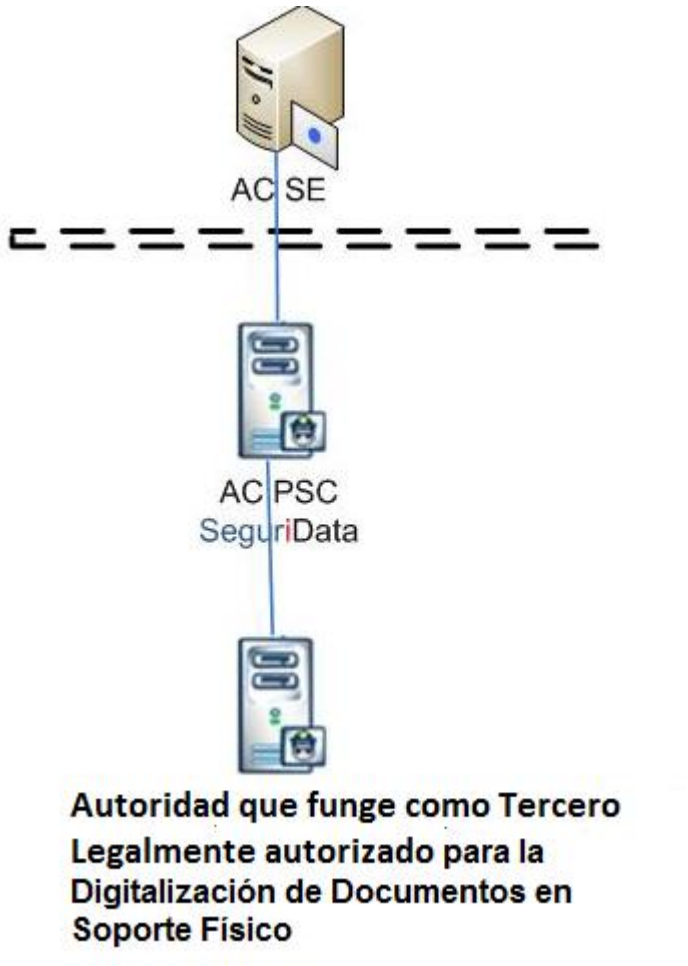
Las modificaciones propuestas o las nuevas aportaciones a incluir en esta Política, deberán, previa a su aprobación, ser contrastadas con la Declaración definida, a fin de asegurar que sean soportados estos cambios.

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 Política de Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico, es publica, y su consulta se realiza en el sitio WEB del PSC SeguriData, cumpliendo con lo establecido en las reglas generales a las que están sujetos los PSC en su título octavo

# 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

### 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 Secretaria 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 para la Digitalización de Documentos en Soporte Físico

Autoridad acreditada por la Secretaría de Economía para fungir como Tercero Legalmente autorizado para la Digitalización de documentos en soporte físico

### 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 a los que están sujetos los PSC

### 8.1.9 Fedatario

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

## 9 Objetivos y alcances de la Digitalización de documentos en soporte físico.

La digitalización es el proceso de convertir documentos impresos o de otro soporte no digital a un formato digital. Puede suponer tomar fotografías digitales de los documentos originales o escanearlos (crear imágenes digitales).

Una vez que los documentos se han convertido en mensajes de datos digitales, pueden:

a) capturarse como imágenes estáticas (imágenes de barrido) representadas por píxeles;

b) procesarse con tecnología de reconocimiento óptico de caracteres que convierte los píxeles en representaciones digitales que se pueden buscar, editar y manipular; o capturarse en ambos formatos.
En líneas generales existen dos tipos de digitalización:

-digitalización durante el proceso de trabajo: digitalización rutinaria continua como parte de los procesos de negocio diarios; y

-proyectos de digitalización: digitalización de grandes volúmenes de documentos previamente existentes.

Por lo que, de acuerdo a la definición y los tipos de digitalización, SeguriData como TLA y el digitalizador, tienen el objetivo de manejar documentos en soporte físico para ser digitalizados cumpliendo con las mejores prácticas definidas en el ISO /TR 13028

## 9.1 Alcance

El alcance de la digitalización de documentos en soporte físico, es de cualquier documento sea original, copia, o copia certificada, de carácter mercantil, pasando por el proceso de digitalización con un escaneado para la generación de imágenes tipo TIF, y después convertirlas a PDF para su firma y emisión de NOM 151-SCFI 2016. La digitalización de documentos en soporte físico se realizará en las instalaciones del digitalizador, teniendo los documentos en custodia, y serán trasladados de las oficinas del cliente a las instalaciones del digitalizador, con las medidas de seguridad establecidas.

## 9.2 Limitaciones

1) La digitalización será centralizada. el establecimiento de una sola ubicación para digitalizar en la que se acumulan todos los documentos que van a procesarse antes de su digitalización.

2) Para la destrucción de documentos originales no digitales deberían identificarse primero cualquier legislación pertinente, la necesidad de autorizaciones u otros requisitos de la organización para su conservación como evidencias, siempre que cumpla los requisitos de veracidad y fiabilidad estipulados en el capítulo 8.2 de la Norma ISO 15489-1:2016, y entonces podría, teniendo en cuenta las consideraciones legislativas mencionadas anteriormente, plantearse conservar únicamente los documentos digitalizados. La limitante se refiere a la responsabilidad del cliente de la decisión de destruir los documentos en soporte físico.

# 10 Obligaciones y Responsabilidades

## 10.1 Obligaciones 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 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.

- Proporcionar a los clientes la información necesaria sobre los términos y condiciones respecto al uso del Servicio de Digitalización de documentos en soporte físico fungiendo como Tercero Legalmente autorizado, mediante un contrato entre el digitalizador y el cliente (comerciante)

- 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 Titulo 8 de las reglas generales a las que están sujetos los PSC en materia de Digitalización de documentos en soporte Físico.

- Mantener y administrar los reportes de cotejo y las actas circunstanciadas, de las digitalizaciones de documentos en soporte físico de conformidad con la NOM 151- SCFI 2016.

- 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

## 10.2 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 PSC, que se emite para uso exclusivo de este servicio, 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.

## 10.3 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.

## 10.4 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 medidas de seguridad definidas en la Política de seguridad
- Conocer y cumplir el Modelo operacional

## 10.5 Responsabilidad 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

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 Secretaria 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 Publico.

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 Secretaria de Economía o de levantar un acta ante el Ministerio Publico.

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 titulo 8 Digitalización de documentos en soporte físico como TLA de las reglas generales que deben cumplir los PSC.

## 10.6 Responsabilidad del Cliente - Comerciante

- Conservar los documentos digitalizados
- Usar el certificado PSC únicamente para firma de documentos digitalizados
- Validar la muestra y aprobarla, esto de manera opcional su participación
- Entrega de documentos en soporte físico al digitalizador
- Recepción de documentos en soporte físico por parte del digitalizador, formando parte de la cadena de custodia de los documentos

## 10.7 Responsabilidad del Administrador

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

### 10.8 Responsabilidad del Fedatario

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

## 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. 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

# 13 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:<br>-Transformación de documentos en soporte físico a Metadatos<br>- Muestra de escaneo<br>- Firma de documento digitalizado<br>- Constancia NOM 151 de documento digitalizado | | | Digitalizador<br>Base de datos |
| 7.-Generación de acta | | | TLA |

| | | | |
|---|---|---|---|
| circunstanciada | | | |
| 8.- Devolución de documentos en soporte físico | | | Digitalizador<br><br>Formato de entrega |

# 14 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 Titulo 8 de las reglas generales a las que están sujetos loa PSC en materia de Digitalización de documentos en soporte físico:

Cumpliendo con los elementos Humanos, Elementos económicos, Elementos Materiales y Elementos tecnológicos, incluidos los de seguridad, entre los que destacan:

1) Al menos un equipo digitalizador que será del tipo de producción, con al menos las siguientes características: 130 hojas por minuto, alimentador de 500 hojas, digitalizar 60,000 hojas por día, de preferencia con conexión SCSI
2) Canales seguros de comunicación entre equipo digitalizador, servidor de misión crítica del software y/o sistema de digitalización de documentos en soporte físico, equipo HSM, el equipo de almacenamiento, y cualquier enlace que se requiera por cuestiones de seguridad.
3) Antes de iniciar un proceso de migración, se deberá contar con un esquema autónomo de verificación del software y/o sistema de Digitalización de Documentos en Soporte Físico, el cual deberá incluir un análisis de seguridad del código fuente y del código en ejecución, cuyo resultado será entregado a la Secretaría para su revisión. Esto se realizara como parte de auditoria del TLA al Digitalizador.
4) Cumplir con lo especificado en el documento de Plan de Gestión de Calidad para el Servicio 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:

5) 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.
6) Contar con las medidas de seguridad adoptadas para proteger los Datos de Creación de Firma Electrónica del Certificado del Tercero Legalmente Autorizado
7) Contar con un procedimiento en caso de robo de los Datos de Creación de Firma Electrónica del Certificado del Tercero Legalmente Autorizado.
8) 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.

9) 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.

# 15 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 Publico.
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* 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 para los sellos de tiempo emitidos por cada firma de documentos digitalizado

5.- La seguridad que se tiene al emitir una constancia de conservación por cada documento digitalizado

### 16.1 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.

# 17 Administración de la Autoridad que funge como tercero Legalmente Autorizado para la Digitalización de Documentos en Soporte Físico de SeguriData Privada

### 17.1 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.

### 17.2 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

### 17.2.1 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 alterno 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 políticas de seguridad física, 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.

## 17.3 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.

Los roles cumplen con lo definido en las reglas generales a las que están sujetos los PSC Título octavo Capítulo III de los Elementos humanos, a continuación se detallan los requisitos , y las funciones y responsabilidades asociadas a cada uno de los elementos humanos.

**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 generales a los que están sujetos los 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

### 17.3.1 Número de Personas Requeridas por Tarea

El número de personas requeridas por tarea se da de acuerdo ha:

| Tarea | Personas requeridas |
|---|---|
| Contratación del servicio | Administrador |
| Digitalización de los documentos | Digitalizador |
| Revisión de muestra | Profesional jurídico, Profesional informático, comerciante de manera opcional , digitalizador, y fedatario de manera opcional |
| Elaboración y firma de acta circunstanciada | Profesional informático<br>Profesional jurídico<br>Fedatario en caso de haber participado<br>Digitalizador |
| Administración de la base de datos | Administrador de base de datos |
| Administrar las comunicaciones | Auxiliar informático de redes de redes |
| Revisar procesos de auditoria 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. Para asegurar mejor la integridad de los equipos donde opera la Infraestructura de TLA se aplicarán esfuerzos para identificar a un individuo distinto para cada rol de confianza, de acuerdo a la tabla siguiente:

| Rol original | Reemplazo temporal de rol |
|---|---|
| Auxiliar informático de seguridad | Profesional Jurídico |

| | |
|---|---|
| Auxiliar informático de redes | Auxiliar informático de seguridad |
| Administrador de base de datos | Auxiliar informático de redes |
| Administrador de sistemas | Operador de Sistemas |
| Operador de sistemas | Administrador de Sistemas |

### 17.3.2 Identificación y Autenticación para cada Función

Las personas que realizan las funciones relevantes están sometidas a una seguridad apropiada. Cada individuo que realiza cualquiera de las funciones relevantes.

### 17.3.3 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 punto 17.7

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.

## 17.4 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.

### 17.4.1 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.

### 17.4.2 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.

### 17.4.3 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.

### 17.4.4 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.

# 18 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

## 18.1 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 auditoria
- Todos los documentos digitalizados tienen asociada una NOM 151 si 2016 para posteriores validaciones de auditoria de así requerirse y son resguardadas en base de datos.

## 18.2 Frecuencia de Registro

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

### 18.2.1 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.

### 18.2.2 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.

### 18.2.3 Notificación al Individuo que Genera un Suceso

Cuando se registra un suceso, al emitir el reporte de auditoria 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.

### 18.2.4 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.

### 18.2.5 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

### 18.2.6 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 Medidas de privacidad y protección de datos en materia de firma electrónica avanzada.

La protección de datos en materia de firma electrónica avanzada se da a través del uso de algoritmos SHA 256 y tamaño de llave de 4096, supeditado a la actualización de dichos algoritmos y tamaño de llave en función de la publicación del NIST

## 19.1 Protección de confidencialidad de la información. Medidas de privacidad

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 clausulas 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.

### 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 de documentos en soporte físico de conformidad con la NOM 151 SCFI 2016, 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 pueden tener que ser conservados para cumplir con las exigencias legales, o para asegurar actividades de negocio esenciales.

#### 19.1.1 Información No Confidencial

La Información incluida en el servicio de digitalización 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.

#### 19.1.2 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.

#### 19.1.3 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.

## 19.2 Derechos de Propiedad Intelectual

Esta Política 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.

### 19.2.1 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., y del Digitalizador tal y como se especifica en esta Política y en la declaración de prácticas de la autoridad de Tercero Legalmente Autorizado.

## 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.

## Limitación de Responsabilidad

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

### 19.2.2 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.

## 19.3 Responsabilidades Económicas

### Indemnización por Parte del TLA

Estipulado en la Declaración de Prácticas de la Autoridad de TLA

### 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.