




POLÍTICA CERTIFICADO FIRMA ELECTRÓNICA SIMPLE

e-certchile
CAMARA DE COMERCIO DE SANTIAGO


El presente documento es propiedad de e-certchile y está prohibida su descarga o distribución sin previa autorización

La impresión o descarga de este documento constituye una COPIA NO CONTROLADA

 CAMARA DE COMERCIO DE SANTIAGO	POLÍTICA CERTIFICADO FIRMA ELECTRÓNICA SIMPLE				Código	SGI-PO-07
					Versión	0
Confidencialidad	Público	Nivel de Criticidad	Alta	Página	2 de 18	

ÍNDICE

- 1. Introducción..... 3**
- 2. Titular del certificado..... 3**
- 3. Obligaciones..... 4**
- 4. Responsabilidades..... 8**
- 5. Ciclo de vida del certificado. 9**
- 6. Identificación y autenticación. 9**
- 7. Usos del certificado. 9**
- 8. Aplicación de firma..... 15**
- 9. Usuario..... 15**
- 10. Verificación de firma. 16**
- 11. Instalaciones, gestión y controles operacionales..... 17**
- 12. Controles técnicos de seguridad. 17**

 CAMARA DE COMERCIO DE SANTIAGO	POLÍTICA CERTIFICADO FIRMA ELECTRÓNICA SIMPLE				Código	SGI-PO-07
					Versión	0
Confidencialidad	Público	Nivel de Criticidad	Alta	Página	3 de 18	

1. Introducción.

Este documento presenta la Política de Certificación (CP) para los certificados de firma electrónica simple, la que ha sido generada siguiendo las especificaciones del documento RFC 3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” propuesto por Network Working Group para este tipo de documentos.

En ella se describe la forma en que el suscriptor de un certificado de firma electrónica simple podrá utilizarlo para autenticarse y/o suscribir electrónicamente un documento. Asimismo, describe la aplicación utilizada para generar dicha firma y el tipo de dispositivo o servicio que utilizará para custodiarla y activarla. Asimismo, la forma en que deberán ser almacenados los datos generados por la misma. Finalmente, señala la forma en que cualquier usuario que recibe una autenticación o documento firmado electrónicamente debe determinar si confiar o no en ésta.


El modelo de confianza que ha implementado e-certchile para promover el comercio y gobierno electrónico seguro se sustenta en la regulación establecida por la Ley 19.799, el Decreto Supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo, las normas técnicas dictadas conforme a éstas y la Resolución Exenta N° 9, de 15 de Febrero del 2001, del Servicio de Impuestos Internos.

2. Titular del certificado.

Es la persona natural mayor de 18 años que es suscriptor de un certificado de firma electrónica simple.

El certificado permite al suscriptor demostrar su nombre completo, RUT y correo electrónico, posibilitando, así mismo, su uso para suscribir documentos electrónicos o recibir documentación cifrada para él con su clave público.

El régimen de responsabilidades de éste se encuentran detalladamente establecidas en la Práctica de Certificación e-certchile (CPS e-certchile), siendo especialmente importante

 CAMARA DE COMERCIO DE SANTIAGO	POLÍTICA CERTIFICADO FIRMA ELECTRÓNICA SIMPLE				Código	SGI-PO-07
					Versión	0
Confidencialidad	Público	Nivel de Criticidad	Alta	Página	4 de 18	


relevar que el certificado es personal e intransferible, que todo acto generado por el mismo será considerado como propio aunque el mismo haya sido realizado por otra persona a la cual le ha entregado una copia o acceso al los datos de creación de firma y que si bajo cualquier circunstancia considera que los datos de creación de firma han sido vulnerados debe solicitar sin dilación la revocación del certificado.

3. Obligaciones.

3.1. e-certchile.

Se obliga a:

- a. Ofrecer y mantener instalaciones, sistemas, programas informáticos y los recursos humanos necesarios para otorgar los certificados en los términos establecidos en la Ley 19.799, el Decreto supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo y la Resolución Exenta N° 9, de 15 de Febrero del 2001, del Servicio de Impuestos Internos.
- b. Cumplir y respetar los procedimientos establecidos en esta Práctica de Certificación e-certchile (CPS e-certchile) y en esta Práctica de Certificados (CP) para la emisión de certificados.
- c. Cumplir con todas las otras obligaciones establecidas en la Ley 19.799, el Decreto Supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo y las normas técnicas dictadas conforme a éste.
- d. Aprobar o rechazar las solicitudes de certificados, directamente o a través de las autoridades de registro, de conformidad con la Práctica de Certificación e-certchile (CPS e-certchile).
- e. Emitir los certificados en conformidad al procedimiento establecido en la Práctica de Certificación e-certchile (CPS e-certchile).
- f. Comunicar al suscriptor de la emisión de su certificado.


 CAMARA DE COMERCIO DE SANTIAGO	POLÍTICA CERTIFICADO FIRMA ELECTRÓNICA SIMPLE				Código	SGI-PO-07
					Versión	0
Confidencialidad	Público	Nivel de Criticidad	Alta	Página	5 de 18	

- g. Proveer las técnicas y medios electrónicos que permitan al suscriptor generar y descargar el certificado en el dispositivo de almacenamiento por él elegido.
- h. Configurar y mantener un Registro de Acceso Público de Certificados, con expresa indicación del estado de éstos (vigente, suspendido o revocado).
- i. Revocar o suspender los certificados, notificando de ello al suscriptor.
- j. Realizar razonables esfuerzos para comunicar a los suscriptores cualquier hecho conocido por e-certchile que pudiera afectar la validez del certificado.
- k. Delegar la función de autoridad de registro en entidades de su confianza, asumiendo la responsabilidad por su cometido en el desarrollo de dicha función.
- l. Mantener www.e-certchile.cl con información para el público sobre los servicios de e-certchile.

3.2. Autoridad de Registro.

Se obliga a:

- a. Comprobar la identidad del solicitante de un certificado de conformidad al procedimiento establecido en la Práctica de Certificación e-certchile (CPS e-certchile) y en la forma señalada en esta Prácticas de Certificado (CP).
- b. Registrar y custodiar por 6 años los antecedentes, requeridos a los solicitantes, que sirvieron de base para la emisión de los certificados.
- c. Aprobar o rechazar las solicitudes de emisión de certificados.
- d. Recibir las solicitudes de revocación o suspensión de certificados e informarlas a e-certchile.
- e. Obtener la aceptación en forma inequívoca de los términos y condiciones del servicio por parte del solicitante.
- f. Permitir operar solamente certificados que hayan sido aceptados por el solicitante.

 CAMARA DE COMERCIO DE SANTIAGO	POLÍTICA CERTIFICADO FIRMA ELECTRÓNICA SIMPLE				Código	SGI-PO-07
					Versión	0
Confidencialidad	Público	Nivel de Criticidad	Alta	Página	6 de 18	

g. Prestar cualquier otro servicio que e-certchile le solicite.

Todas las actuaciones indicadas en las letras anteriores, las realiza la Autoridad de Registro por cuenta y riesgo de e-certchile.


3.3. Suscriptor.

Antes de la emisión del certificado se obliga a:


- a. Ser persona natural mayor de 18 años.
- b. Solicitar la emisión del certificado aceptando los términos y condiciones descritos en la Práctica de Certificación e-certchile (CPS e-certchile) y esta Política de Certificados (CP).
- c. Proveer a e-certchile y/o la autoridad de registro toda la información que de acuerdo con esta Política de Certificados (CP) es requerida para verificar su identidad.
- d. Crear y descargar el certificado en un dispositivo de almacenamiento al que se tenga acceso y control.
- e. No revelar el PIN del dispositivo que contiene los datos de creación de firma asociados al certificado y/o no relevar el mecanismo de activación de la firma.
- f. Pagar las tarifas convenidas por concepto de los servicios de certificación, aun cuando no se acepten o no se ocupen los certificados emitidos.

Una vez emitido el certificado se obliga a:

- a. Aceptar el certificado. Se entiende que un certificado es aceptado por el suscriptor cuando:
 - i) Haya sido emitido por e-certchile, aun cuando el certificado no haya entrado en vigor por contener una fecha de inicio de operación posterior a su fecha de emisión.

 CAMARA DE COMERCIO DE SANTIAGO	POLÍTICA CERTIFICADO FIRMA ELECTRÓNICA SIMPLE				Código	SGI-PO-07
					Versión	0
Confidencialidad	Público	Nivel de Criticidad	Alta	Página	7 de 18	

- ii) No se haya formulado un reclamo por error o inexactitud en la emisión al momento de su recepción.
 - iii) Se haya utilizado la clave de confirmación comunicada por e-certchile para retirar el certificado, se haya instalado éste en el dispositivo de generación y almacenamiento de firma o haya sido utilizado por el suscriptor.
- b. Comunicar a e-certchile cualquier error o inexactitud en el certificado que reciba. Si no lo hace al momento de su recepción todas las declaraciones se tendrán por verdaderas.
 - c. Usar los datos de creación de firma asociados al certificado para fines legales y autorizados, de conformidad con lo previsto en la Ley 19.799, la Práctica de Certificación e-certchile (CPS e-certchile) y en esta Prácticas de Certificado (CP).
 - d. Utilizar correctamente el certificado.
 - e. Ser un usuario final, y no usar el certificado para actuar como certificador de firma electrónica.
 - f. Comunicar inmediatamente a e-certchile y/o a una autoridad de registro el compromiso, pérdida, hurto, robo, acceso no autorizado o extravío, falsificación de sus datos de creación de firma o certificado o cualquier circunstancia que pudiera ser causal de suspensión o revocación de un Certificado.
 - g. Custodiar los datos de creación de firma, tomando precauciones razonables para evitar su pérdida, modificación y uso no autorizado.
 - h. Solicitar la suspensión o revocación del certificado cuando se presente alguna de las causales indicadas para este efecto.
 - i. No usar los datos de creación de firma una vez que el certificado haya expirado o haya sido solicitada la suspensión o revocación.

 CAMARA DE COMERCIO DE SANTIAGO	POLÍTICA CERTIFICADO FIRMA ELECTRÓNICA SIMPLE				Código	SGI-PO-07
					Versión	0
Confidencialidad	Público	Nivel de Criticidad	Alta	Página	8 de 18	

- j. Destruir los datos de creación de firma en caso que e-certchile así se lo solicite y haya sido revocado previamente el certificado.

3.4. Usuarios.

Se obliga a:

- Verificar la validez del certificado mediante una consulta al registro de acceso público de certificados.
- Verificar la firma del suscriptor.
- Comprobar cualquier limitación funcional que incorpore el certificado.
- Validar el uso de certificado para propósitos autorizados de conformidad con la legislación vigente.

4. Responsabilidades.

4.1. e-certchile.

De acuerdo con lo especificado en la Práctica de Certificación e-certchile (CPS e-certchile).

4.2. Limitación de responsabilidad.


De acuerdo con lo especificado en la Práctica de Certificación e-certchile (CPS e-certchile).

4.3. Autoridad de Registro.

De acuerdo con lo especificado en la Práctica de Certificación e-certchile (CPS e-certchile).

4.4. Suscriptor.

De acuerdo con lo especificado en la Práctica de Certificación e-certchile (CPS e-certchile).

 CAMARA DE COMERCIO DE SANTIAGO	POLÍTICA CERTIFICADO FIRMA ELECTRÓNICA SIMPLE				Código	SGI-PO-07
					Versión	0
Confidencialidad	Público	Nivel de Criticidad	Alta	Página	9 de 18	

4.5. Usuario.

De acuerdo con lo especificado en la Práctica de Certificación e-certchile (CPS e-certchile).

5. Ciclo de vida del certificado.

De acuerdo con lo especificado en la Práctica de Certificación e-certchile (CPS e-certchile).

6. Identificación y autenticación.

De acuerdo con lo especificado en la Práctica de Certificación e-certchile (CPS e-certchile), relevándose el hecho de que el solicitante puede hacer el trámite por completo en forma electrónica sin que se haga necesario su comparecencia personal ante e-certchile o una de sus autoridades de registro.

7. Usos del certificado.

7.1. Composición del certificado.


e-certchile tiene en operación dos CA Root que cumple con los requisitos exigidos por la Ley 19.799 y el Decreto Supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo, así como, por las normas técnicas dictadas conforme a éste, una CA Root para los certificados en SHA1 y otra para los emitidos en SHA2.

Certificado tipo firma electrónica simple de e-certchile SHA 1.

Nombre	Descripción	Tipo Dato	Valor
Versión	Versión del certificado que deberá ser versión 3.	Fijo	V3
Nº de Serie	Número que identifica unívocamente al certificado dentro de los certificados de firma electrónica	Variable	10 bytes en formato hexadecimal

Nombre	Descripción	Tipo Dato	Valor
	simple emitidos por e-certchile.		
Algoritmo de firma	Algoritmo usado por e-certchile para firmar el certificado	Fijo	sha1RSA
Algoritmo hash de firma	Algoritmo hash usado por e-certchile	Fijo	sha1
Nombre del Emisor	Nombre distintivo (DN) del emisor, en el formato del estándar X.500. Deben incluirse los siguientes tipos: CN =Tipo de certificado E = email del Prestador de Servicios de Certificación emisora Número de serie = Número identificador del Emisor	Variable	E = sclientes@e-certchile.cl CN = E-CERTCHILE CA FIRMA ELECTRONICA SIMPLE OU = Autoridad Certificadora O = E-CERTCHILE L = Santiago S = Region Metropolitana C = CL
Periodo desde	Fecha de inicio en que es válido el certificado.	Variable	[Día de la semana], [dia] de [mes] de [año] hh:mm:ss
Período hasta	Fecha de termino en que es válido el certificado.	Variable	[Día de la semana], [dia] de [mes] de [año] hh:mm:ss
Nombre del Titular	Nombre distintivo (DN) del titular del certificado, en el formato del estándar X.500.	Variable	E = [correo titular] CN = [nombre titular] OU = * O = [nombre titular] L = [ciudad] S = [región] C = CL
Clave pública	Clave pública del titular del certificado	Variable	RSA de 1024 bits

Nombre	Descripción	Tipo Dato	Valor
KeyUsage	Esta extensión define el propósito para el cual deben ser usadas las claves correspondientes al certificado. El certificado debe ser utilizado sólo para los propósitos definidos por esta extensión.	Fijo	Firma digital, Sin repudio, Cifrado de clave, Cifrado de datos (f0)
AuthorityKeyIdentifier	Medio para identificar la llave pública de e-certchile El campo KeyId es idéntico al valor de la extensión SubjectKeyIdentifier .	Fijo	Id. de clave=78e13e9fd212b37a3c8dcd300e53b3432907b355
CertificatePolicy	Ver Política de Certificados	Fijo	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.8658.5 [1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: http://www.e-certchile.cl/CPS.htm [1,2]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=El responder este formulario es un requisito indispensable para dar inicio al proceso de certificación. Posteriormente,
IssuerAltName	Identificador alternativo del emisor, corresponde al RUT.	Fijo	Otro nombre: 1.3.6.1.4.1.8321.2=16 0a 39 36 39 32 38 31 38 30 2d 35

 CAMARA DE COMERCIO DE SANTIAGO	POLÍTICA CERTIFICADO FIRMA ELECTRÓNICA SIMPLE				Código	SGI-PO-07
					Versión	0
Confidencialidad	Público	Nivel de Criticidad	Alta	Página	12 de 18	


Nombre	Descripción	Tipo Dato	Valor
SubjectAltName	Permite definir términos que identifican al sujeto o titular del certificado, adicionalmente a lo establecido en el campo estándar Subject.	Variable	Otro nombre: 1.3.6.1.4.1.8321.1=16 0a 31 33 39 31 34 31 31 31 2d 33
CrlDistributionPoint	En este campo se establece la localización del CRL correspondiente para consultar sobre revocaciones. Contiene la siguiente estructura: DistribuitonPoint: Un URI para identificar el CRL.	Fijo	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://crl.e-certchile.cl/ecertchilecaFES.crl
Huella digital		Variable	76b4d2d4895b1ad03ad7d280bb2eee02c7f9f253

Certificado tipo firma electrónica simple de e-certchile SHA 2.

Nombre	Descripción	Tipo Dato	Valor
Versión	Versión del certificado que deberá ser versión 3.	Fijo	V3
Nº de Serie	Número que identifica unívocamente al certificado dentro de los certificados de firma electrónica simple emitidos por e-certchile.	Variable	10 bytes en hexadecimal
Algoritmo de firma	Algoritmo usado por e-certchile para firmar el certificado	Fijo	sha256RSA

Nombre	Descripción	Tipo Dato	Valor
Algoritmo hash de firma	Algoritmo hash usado por e-certchile	Fijo	sha1
Nombre del Emisor	Nombre distintivo (DN) del emisor, en el formato del estándar X.500. Deben incluirse los siguientes tipos: CN =Tipo de certificado E = email del Prestador de Servicios de Certificación emisora Número de serie = Número identificador del Emisor	Variable	E = scliente@e-certchile.cl CN = E-CERTCHILE CA FES 02 OU = Autoridad Certificadora O = E-CERTCHILE L = Santiago S = Region Metropolitana C = CL
Periodo desde	Fecha de inicio en que es válido el certificado.	Variable	[Día de la semana], [dia] de [mes] de [año] hh:mm:ss
Período hasta	Fecha de termino en que es válido el certificado.	Variable	[Día de la semana], [dia] de [mes] de [año] hh:mm:ss
Nombre del Titular	Nombre distintivo (DN) del titular del certificado, en el formato del estándar X.500.	Variable	E = [correo titular] CN = [nombre titular] OU = * O = [nombre titular] L = [ciudad] S = [región] C = CL
Clave pública	Clave pública del titular del certificado	Variable	RSA de 2048 bits
KeyUsage	Esta extensión define el propósito para el cual deben ser usadas las claves correspondientes al certificado. El certificado debe ser utilizado sólo para los propósitos	Fijo	Firma digital, Sin repudio, Cifrado de clave, Cifrado de datos (f0)

Nombre	Descripción	Tipo Dato	Valor
	definidos por esta extensión.		
AuthorityKeyIdentifier	Medio para identificar la llave pública de e-certchile El campo KeyId es idéntico al valor de la extensión SubjectKeyIdentifier .	Fijo	Id. de clave=74d621b3f45ae82d7cbb59066343ef69b43a9304
CertificatePolicy	Ver Política de Certificados	Fijo	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.8658.5 [1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: https://www.e-certchile.cl/ [1,2]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=El responder este formulario es un requisito indispensable para dar inicio al proceso de certificación. Posteriormente,
IssuerAltName	Identificador alternativo del emisor, corresponde al RUT.	Fijo	Otro nombre: 1.3.6.1.4.1.8321.2=16 0a 39 36 39 32 38 31 38 30 2d 35
SubjectAltName	Permite definir términos que identifican al sujeto o titular del certificado, adicionalmente a lo establecido en el campo estándar Subject.	Variable	Otro nombre: 1.3.6.1.4.1.8321.1=16 0a 31 36 30 37 32 36 34 39 2d 30
CrlDistributionPoint	En este campo se establece la localización del CRL correspondiente para consultar sobre revocaciones. Contiene la siguiente.	Fijo	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL= http://crl.ecertchile.cl/E-CERTCHILECAFES02.crl

 CAMARA DE COMERCIO DE SANTIAGO	POLÍTICA CERTIFICADO FIRMA ELECTRÓNICA SIMPLE				Código	SGI-PO-07
					Versión	0
Confidencialidad	Público	Nivel de Criticidad	Alta	Página	15 de 18	

Nombre	Descripción	Tipo Dato	Valor
	estructura: DistribuitonPoint: Un URI para identificar el CRL.		
Huella digital		Variable	257a9f0aead18e233d58033eacfcf2cda4f8c65e

8. Aplicación de firma.

La aplicación que el suscriptor utilice para firmar electrónicamente un documento es de su responsabilidad, sin embargo, le sugerimos que tenga especial preocupación que aquella que elija garantice que los datos de creación de firma nunca queden expuestos a terceros usuarios o aplicaciones.

8.1. Efectos.


De conformidad con lo dispuesto en la Ley 19.799 los actos y contratos suscritos por medio de firma electrónica serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel.

Dichos actos y contratos se reputarán como escritos, en los casos en que la ley exija que los mismos consten de ese modo, y en todos aquellos casos en que la ley prevea consecuencias jurídicas cuando constan igualmente por escrito.

Finalmente, es importante que el suscriptor y el usuario tengan presente que los instrumentos públicos no se pueden suscribir con certificados de firma electrónica simple.

9. Usuario.

El usuario es aquella persona que voluntaria y libremente decide hacer uso y/o confiar en un certificado de firma electrónica simple emitido por e-certchile.

 CAMARA DE COMERCIO DE SANTIAGO	POLÍTICA CERTIFICADO FIRMA ELECTRÓNICA SIMPLE				Código	SGI-PO-07
					Versión	0
Confidencialidad	Público	Nivel de Criticidad	Alta	Página	16 de 18	

Por lo tanto, el usuario es responsable de validar el contenido del documento, la firma y el certificado asociado a dicha firma con anterioridad a tomar la decisión de confiar en él.

e-certchile a través de tecnologías y procedimientos que dispone, permite asegurar la identidad del suscriptor de un certificado para firma electrónica y las acciones que efectúe con él.

10. Verificación de firma.

La verificación de la firma electrónica simple de un documento electrónico se realiza para determinar que:

- La firma electrónica fue creada por los datos de creación de firma correspondiente a la clave pública contenida en el certificado del suscriptor que firma.
- El mensaje no ha sido modificado con posterioridad a su suscripción.


10.1. Efecto de validar al suscriptor.

La firma electrónica simple genera efectos jurídicos para el que la incorpora a través de sus datos de creación de firma en un documento electrónico, siempre y cuando:

- Haya sido creada durante el período de vigencia del certificado.
- La firma electrónica simple pueda ser verificada por medio de la cadena de verificación.
- El usuario no tiene conocimiento del incumplimiento de la Práctica de Certificación e-certchile (CPS e-certchile) por parte del suscriptor
- El usuario ha cumplido con todos los requisitos de la Práctica de Certificación e-certchile (CPS e-certchile).

10.2. Responsabilidad por no validar una firma.

Un usuario que confía en una firma electrónica que no ha sido verificada en forma total, por cualquier razón, asume todos los riesgos y no puede hacer ninguna presunción de

 CAMARA DE COMERCIO DE SANTIAGO	POLÍTICA CERTIFICADO FIRMA ELECTRÓNICA SIMPLE				Código	SGI-PO-07
					Versión	0
Confidencialidad	Público	Nivel de Criticidad	Alta	Página	17 de 18	

que la firma es válida bajo los términos de la Práctica de Certificación e-certchile (CPS e-certchile).

10.3. Confianza en la firma electrónica.

Un usuario sólo puede confiar en la firma electrónica simple con que se ha suscrito un documento electrónico en la medida que:

- La firma electrónica haya sido creada durante el período de vigencia del certificado.
- La confianza es razonable de acuerdo con las circunstancias.

La decisión de confiar o no en una determinada firma electrónica simple la toma en forma libre y exclusiva el usuario que realiza la verificación.

10.4. Almacenamiento de antecedentes.

Para efectos de disponer de los adecuados antecedentes para una verificación posterior de la firma electrónica, el usuario debe mantener los siguientes antecedentes:


- Documento que se firmó electrónicamente.
- Firma Electrónica.
- Certificado del suscriptor o en su defecto alguna identificación que permita buscar posteriormente el certificado en el registro de acceso público de e-certchile.

11. Instalaciones, gestión y controles operacionales.

De acuerdo con lo especificado en la Práctica de Certificación e-certchile (CPS e-certchile).

12. Controles técnicos de seguridad.

De acuerdo con lo especificado en la Práctica de Certificación e-certchile (CPS e-certchile).

 CAMARA DE COMERCIO DE SANTIAGO	POLÍTICA CERTIFICADO FIRMA ELECTRÓNICA SIMPLE				Código	SGI-PO-07
					Versión	0
	Confidencialidad	Público	Nivel de Criticidad	Alta	Página	18 de 18

NORMA(S) QUE APLICA(N)	
Norma	Referencia Normativa
ISO 9001:2015	5.2 Política 8.2.2 Determinación de los requisitos relacionados con los productos y servicios (SGI-PO-05)
ISO 27001:2013	5.2 Política
Guía de Acreditación (Minecon) FEA	PO01
Guía de Acreditación (Minecon) BIO	N/A
Guía de Acreditación (Minecon) TSA	N/A

CONTROL DE CAMBIOS		
Nº DE VERSIÓN	FECHA	DESCRIPCIÓN DE CAMBIOS
0	2020/07	Creación del documento, se recomienda lectura completa del documento.