
 Tecnómica	Política de Certificación para Canales de comunicación por VPN	Cód.		
		Rev.	01	
		Total de Pág.	24	

**ENTIDAD PRESTADORA DE SERVICIOS
CRIPTOGRÁFICOS DE CERTIFICACIÓN
(PSCC)
ACTECNOMATICA**



**POLÍTICA DE CERTIFICADOS
PARA
CANALES DE COMUNICACIÓN
(VPN)**

(Versión 1.0)

ENERO 2022



“AÑO 64 DE LA REVOLUCIÓN”



 Tecnomática	Política de Certificación para Canales de comunicación por VPN	Cód.		 Cupet UNIÓN CubaPetróleo
		Rev.	01	
		Total de Pág.	24	



RELACIÓN DE REVISIONES

Rev. 01	Nombres y Apellidos	Cargo	Firma	Fecha
Elaborado por:	Soraya del C. López Galban.	Esp Princ. B Seguridad Informática		30/01/2022
	Yesneiler Matos Quintero	EP Tecn Com, Elect, Autom y S.Tecn		30/01/2022
	Zenia Ivis Meneses Santiesteban	Esp. B Ciencias Inf.		30/01/2022
Revisado por:	Idanelys Tirado Rubio	Dir. UEB Infocomunicaciones		30/01/2022
	Betty Iznaga Alarcón	Esp. Gestión de la Calidad		30/01/2022
	Lourdes Ramos López	Esp. Princ. Gestión de la Calidad		30/01/2022
Aprobado por:	Armando Estévez Alonso	Director General		30/01/2022



 Tecnomática	Política de Certificación para Canales de comunicación por VPN	Cód.		 Cupet UNIÓN CubaPetróleo
		Rev.	01	
		Total de Pág.	24	

1 Contenido



1	INTRODUCCIÓN.....	7
1.1	GENERALIDADES.....	7
1.2	NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO.....	8
1.3	PARTICIPANTES DE LA INFRAESTRUCTURA DE LLAVE PÚBLICA	9
1.3.1	Estructura general de la Infraestructura de LLave Pública (PKI) .	9
1.3.2	Autoridad de Certificación (ACTECNOMATICA)	9
1.3.3	Autoridades de Registro (RA)	9
1.3.4	Autoridad de Validación (VA)	9
1.3.5	Autoridad de Sellado de Tiempo	10
1.3.6	Repositorio de Certificados:	10
1.3.7	Solicitante.....	10
1.3.8	Titulares o Suscriptor.....	10
1.3.9	Terceros de buena fe.....	10
1.4	USO DE LOS CERTIFICADOS.....	10
1.4.1	Uso prohibido de los certificados	11
1.5	Administración de las políticas	11
1.6	DEFINICIONES Y ACRÓNIMOS	11
1.6.1	Definiciones.....	11
2	RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIOS.....	11
3	IDENTIFICACIÓN Y AUTENTICACIÓN.....	12
3.1	Registro de Nombres.	12

 Tecnomática	Política de Certificación para Canales de comunicación por VPN	Cód.		 Cupet UNIÓN CubaPetróleo
		Rev.	01	
		Total de Pág.	24	



3.2	Validación inicial de identidad.	12
3.2.1	Métodos de prueba de la posesión de la llave privada Generación y construcción de un PKCS#12 descargable.	12
3.2.2	Autenticación de identidad de Autoridades de Registro.....	12
3.2.3	Autenticación de la identidad de una entidad.	12
3.2.4	Autenticación de la identidad de una persona.	13
3.2.5	Información no verificada del suscriptor.	13
3.2.6	Validación de Autoridad.	13
3.3	Identificación y Autenticación de solicitudes de renovación de llaves.	13
3.4	Identificación y Autenticación de solicitudes de revocación.	13
4	REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DE LOS CERTIFICADOS.	14
4.1	Solicitud de certificados.....	14
4.1.1	Habilitados para solicitar certificados.....	14
4.1.2	Proceso de solicitud y responsabilidades.....	14
4.2	Procesamiento de la solicitud del certificado.	14
4.3	Emisión del certificado.....	15
4.4	Aceptación del certificado por el solicitante.....	15
4.5	Uso del certificado y el par de llaves.	15
4.5.1	Uso de la llave privada por parte del suscriptor.....	15
4.6	Renovación de certificado.....	15
4.7	Cambio de llave del certificado.....	15
4.8	Modificación del certificado.....	16
4.9	Revocación de certificados.	16

 Tecnomática	Política de Certificación para Canales de comunicación por VPN	Cód.		 Cupet UNIÓN CubaPetróleo
		Rev.	01	
		Total de Pág.	24	

4.10	Servicios de comprobación del estado de los certificados.	16
4.11	Finalización de la suscripción.	16
4.12	Custodia y recuperación de llaves.	16
5	CONTROLES DE SEGURIDAD FÍSICOS Y OPERACIONALES.	17
6	CONTROLES DE SEGURIDAD TÉCNICA	17
6.1	Generación e instalación del par de llaves	17
6.1.1	Entrega de la llave privada al titular	17
6.1.2	Entrega de la llave pública al emisor del certificado.	17
6.1.3	Entrega de la llave pública de la ACTECNOMATICA a los usuarios	18
6.1.4	Algoritmo y Tamaño de llaves	18
6.2	Protección de la llave privada.	18
6.2.1	Control multipersona de la llave privada	18
6.2.2	Custodia de la llave privada	19
6.2.3	Copia de seguridad de la llave privada.....	19
6.2.4	Archivo de la llave privada.....	19
6.3	Controles de seguridad informática	19
6.4	Fines del uso de la llave	19
6.5	Protección de la llave privada	19
6.6	Otros aspectos de la gestión de llaves	19
6.6.1	Períodos operacionales del certificado y períodos de uso de las llaves	19
6.7	Datos de activación	20
6.8	Controles de seguridad computacional.	20

 Tecnomática	Política de Certificación para Canales de comunicación por VPN	Cód.		 Cupet <small>UNIÓN</small> CubaPetróleo
		Rev.	01	
		Total de Pág.	24	

7	PERFILES DE CERTIFICADOS, LISTAS DE REVOCACIÓN (CRL)	20
7.1	Perfil del certificado.....	20
7.1.1	Número de versión.....	22
7.1.2	Extensiones del certificado	23
7.1.3	Identificador de objeto del algoritmo	24
7.1.4	Formato de Nombre	24
7.2	Perfil de la CRL.....	24
7.3	Lista de revocación de Certificados (CRL).....	25
8	AUDITORÍA DE CONFORMIDAD	25
9	REQUISITOS LEGALES Y COMERCIALES	25

 Tecnómica	Política de Certificación para Canales de comunicación por VPN	Cód.		
		Rev.	01	
		Total de Pág.	24	

1 INTRODUCCIÓN



Este documento recoge la Política de Certificación (PC) de los Certificados para canales de comunicación por VPN, emitidos por la Infraestructura de Clave Pública (en adelante PKI) de la Autoridad de Certificación ACTECNOMATICA acreditada, mediante la Instrucción No.7 del Jefe de la Dirección de Criptografía del Ministerio del Interior (RS: 0001215), como PRESTADOR CORPORATIVO DE SERVICIOS DE CONFIANZA subordinada a la Autoridad Raíz de la República de Cuba.

Esta Política de Certificación asume que el lector conoce los conceptos básicos y Reglamento de la Infraestructura de Llave Pública de la República de Cuba vigente por la Resolución 2/2016 del Ministro del Interior, la Declaración de Prácticas de Certificación (DPC) nuestra y de la Autoridad de Certificación del Servicio Central Cifrado (en lo adelante ACSCC), documentos oficiales que establecen las reglas y normas aplicables para la solicitud, validación, aceptación, emisión, entrega, uso, suspensión, renovación y revocación de los Certificados Digitales de Llave Pública emitidos por la ACTECNOMATICA, así como las restricciones, aplicaciones, deberes y derechos de las partes participantes, en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento.

Todos los certificados que emite la PKI de la Autoridad de Certificación ACTECNOMATICA son conformes con la versión 3 del estándar X.509, permitiendo la inclusión de extensiones para certificación de atributos.

1.1 GENERALIDADES

La Empresa Tecnomática constituida como Prestador de Servicios de Certificación Criptográficos en virtud del Decreto de Ley 199/99 y la Resolución No. 2/2016 emitida por el Ministro del Interior, y a tenor de las atribuciones otorgadas como Autoridad Registradora y Certificadora subordinada a la Autoridad Raíz en virtud de lo cual norma la siguiente Política de Certificación para canales de comunicación por VPN.

 Tecnomática	Política de Certificación para Canales de comunicación por VPN	Cód.		
		Rev.	01	
		Total de Pág.	24	

La presente Política de Certificación está redactada siguiendo las especificaciones del Ministerio del Interior contenidas en la Resolución No. 2 del 2016 y se ha estructurado teniendo en cuenta las recomendaciones de la (Request for comments) RFC 3647 “Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework”, de IETF. propuesto por *Network Working Group* y completada con aspectos exigidos en:

- ETSI TS 101 456: “Policy Requirements for certification authorities issuing qualified certificates”.
- ETSI TS 101 862: “Profile for Qualified Certificate”.
- ETSI TS 102 042: “Policy Requirements for certification authorities issuing public key certificates”.



Igualmente, se ha considerado como normativa básica aplicable a la materia:

- El Decreto Ley 199/99.
- La Resolución 2 del 2002 del MININT.
- La Resolución 2 del 2016 del MININT
- Los Decretos de ley y resoluciones de la gaceta oficial número 45 de julio del 2019.

Para brindar el conocimiento a los titulares de Certificados Digitales de Llave Pública de las prácticas y reglas específicas que se aplican en el sistema de certificación de la ACTECNOMATICA, se ponen a su disposición esta PC, la DPC y demás documentos afines disponibles en el sitio web oficial <https://actecnomatica.cupet.cu>

1.2 NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

Este documento se titula “Política de Certificación para canales de comunicación por VPN.” (versión 1.0) de la Autoridad de Certificación (ACTECNOMATICA), emitido el 30 enero del 2022, disponible en sitio web de la entidad <https://actecnomatica.cupet.cu>, relacionado con la Declaración de Prácticas de Certificación versión 1.

 Tecnomática	Política de Certificación para Canales de comunicación por VPN	Cód.		 Cupet UNIÓN CubaPetróleo
		Rev.	01	
		Total de Pág.	24	

1.3 PARTICIPANTES DE LA INFRAESTRUCTURA DE LLAVE PÚBLICA

1.3.1 Estructura general de la Infraestructura de Llave Pública (PKI)

Esta Política de Certificados regula una comunidad de usuarios, que obtienen certificados sólo para diversas relaciones administrativas, de acuerdo con la Resolución No. 2/2016 del Ministro del Interior.

1.3.2 Autoridad de Certificación (ACTECNOMATICA)

La Autoridad de Certificación de la Empresa de Informática Automática y Comunicaciones de la Unión Cuba Petróleo - Cupet está destinada para emitir, renovar, suspender, revocar y firmar Certificados Digitales de Llave Pública en interés de los OACE, OSDE cuya función es la emisión entre otros de certificados para canales de comunicación por VPN en la protección de la información de sus suscriptores, asumiendo la responsabilidad de emitir y mantener actualizadas sus PC y la DPC; así como emitir y mantener actualizada la información del estado de los Certificados Digitales de Llave Pública que emite, a través de la publicación de las Listas de Revocación de Certificados (en lo adelante CRL, por sus siglas en inglés) y del servicio de validación en línea OCSP.

El Certificado Digital de Llave Pública de la ACTECNOMATICA, con el cual legaliza y mantiene un entorno certificado, seguro y confiable a todos los servicios que brinda, es generado por la ACSCC.



Los certificados de la entidad emisora son válidos por un periodo de uno o dos 2 años según se contratena partir de su puesta en funcionamiento.

1.3.3 Autoridades de Registro (RA)

De acuerdo con lo especificado en la DPC de la ACTECNOMATICA (1.3.3)

1.3.4 Autoridad de Validación (VA)

De acuerdo con lo especificado en la DPC de la ACTECNOMATICA (1.3.4)

 Tecnómica	Política de Certificación para Canales de comunicación por VPN	Cód.		
		Rev.	01	
		Total de Pág.	24	

1.3.5 Autoridad de Sellado de Tiempo

De acuerdo con lo especificado en la DPC de la ACTECNOMATICA (1.3.5)

1.3.6 Repositorio de Certificados:

De acuerdo con lo especificado en la DPC de la ACTECNOMATICA (1.3.6)

1.3.7 Solicitante

De acuerdo con lo especificado en la DPC de la ACTECNOMATICA (1.3.7)

Y a los efectos de la presente PC se entenderá como solicitante a toda persona jurídica que a través de un Representante acreditado realice una solicitud de Certificado Digital, previa relación contractual con la empresa Tecnomática.

Así mismo, se entenderá como titular a toda persona jurídica, que requiera en su ámbito de acción intercambiar información por canales de comunicación protegidos empleando el protocolo IPSEC, cuya identidad del certificado está vinculada a los datos de creación y verificación de firma.

1.3.8 Titulares o Suscriptor



De acuerdo con lo especificado en la DPC de la ACTECNOMATICA (1.3.8)

1.3.9 Terceros de buena fe

De acuerdo con lo especificado en la DPC de la ACTECNOMATICA (1.3.9)

1.4 USO DE LOS CERTIFICADOS

En la Infraestructura de Llave Pública de Tecnomática, los certificados digitales emitidos bajo esta PC pueden utilizarse solamente en los propósitos permitidos y durante su período de vigencia para dar cumplimiento a las funciones que le son propias y legítimas, de acuerdo a la Políticas de Certificación (PC).

 Tecnomática	Política de Certificación para Canales de comunicación por VPN	Cód.		
		Rev.	01	
		Total de Pág.	24	

Certificado Digital de	Uso apropiado del Certificado
Certificado de Firma Digital para canales de comunicación por VPN	Establecer una comunicación a través de túneles VPN dotando a los Servidores y clientes de una autenticación segura y capacidades de cifrado que proteja la confidencialidad e integridad de los datos que circulan por una Red Privada Virtual.
Certificado de autenticación de cliente por VPN	Para autenticarse a través de túneles VPN garantizando una comunicación segura.

1.4.1 Uso prohibido de los certificados

De acuerdo con lo especificado en la DPC de la ACTECNOMATICA (1.4.2)

1.5 Administración de las políticas

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA (1.5) responsable de la elaboración, modificación, actualización y presentación de la presente PC.

La DC del Minint es la entidad facultada para la aprobación de la presente PC.



1.6 DEFINICIONES Y ACRÓNIMOS

1.6.1 Definiciones

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA (1.6)

2 RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIOS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA.

 Tecnomática	Política de Certificación para Canales de comunicación por VPN	Cód.		 Cupet UNIÓN CubaPetróleo
		Rev.	01	
		Total de Pág.	24	

3 IDENTIFICACIÓN Y AUTENTICACIÓN.

A los efectos de esta PC y como regla general, según lo especificado en la Resolución 2/2016 del Minint, el par de llaves criptográficas, pública y privada, será gestionado y descargado por el solicitante del Certificado Digital.

En casos excepcionales, de acuerdo con lo especificado en la propia Resolución, la persona natural o jurídica puede solicitar oficialmente, siendo refrendado además en el Contrato, que la ACTECNOMATICA asuma la responsabilidad de la generación del par de llaves criptográficas, pública y privada, del solicitante.

3.1 Registro de Nombres.

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA.

3.2 Validación inicial de identidad.

3.2.1 Métodos de prueba de la posesión de la llave privada Generación y construcción de un PKCS#12 descargable.



Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA.

3.2.2 Autenticación de identidad de Autoridades de Registro

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA.

3.2.3 Autenticación de la identidad de una entidad.

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA.

 Tecnomática	Política de Certificación para Canales de comunicación por VPN	Cód.		
		Rev.	01	
		Total de Pág.	24	

3.2.4 Autenticación de la identidad de una persona.

Las solicitudes de certificados para las personas jurídicas se realizan por parte del Representante del suscriptor, quien avala la identidad y veracidad de los datos de las solicitudes realizadas.

Ante la solicitud, de manera presencial y por primera vez, de varios Certificados Digitales por una persona jurídica a través de un Representante acreditado, la AR le orienta como solicitar y gestionar por el mecanismo establecido la emisión del Certificado Digital de manera que, como parte del proceso de solicitud, el Representante pueda enviar, vía correo electrónico, firmado digitalmente el Modelo de Solicitud que corresponda, empleando su Certificado Digital, emitido por la ACTECNOMATICA.

3.2.5 Información no verificada del suscriptor.

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA.

3.2.6 Validación de Autoridad.



Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA.

3.3 Identificación y Autenticación de solicitudes de renovación de llaves.

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA.

3.4 Identificación y Autenticación de solicitudes de revocación.

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA.

 Tecnómica	Política de Certificación para Canales de comunicación por VPN	Cód.		
		Rev.	01	
		Total de Pág.	24	

4 REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DE LOS CERTIFICADOS.

El ciclo de vida de los certificados emitidos bajo esta política de certificación es de uno y hasta 2 años.

4.1 Solicitud de certificados.

4.1.1 Habilitados para solicitar certificados

Los Representantes nombrados por los Directores Generales de las organizaciones superiores, quienes certifican la veracidad de los datos registrados en las solicitudes de los modelos previstos en el ANEXO 6 del contrato para la Solicitud Certificado VPN (Datos identificativos del responsable de su custodia y del representante, Direcciones IP, Dominio, Nombre común, y la relación de los datos identificativos de los usuarios que se autenticarán por estos canales de comunicación con los servidores definidos, la tarifa de estos certificados viene dada por la cantidad de usuarios a autenticarse a esos servidores)



Anexo que es recepcionado y validado por el funcionario de la AR una vez que se realicen las solicitudes que corresponda por la plataforma facilitada al efecto, siguiendo los pasos definidos en instructivo Generación de una solicitud de Certificado Digital.

4.1.2 Proceso de solicitud y responsabilidades.

El proceso de solicitud de certificados de canales de comunicación por VPN se lleva a cabo según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA y referenciado en el instructivo publicado en el sitio.

4.2 Procesamiento de la solicitud del certificado.

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA.

 Tecnomática	Política de Certificación para Canales de comunicación por VPN	Cód.		 Cupet UNIÓN CubaPetróleo
		Rev.	01	
		Total de Pág.	24	

4.3 Emisión del certificado.

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA.

4.4 Aceptación del certificado por el solicitante.

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA.

4.5 Uso del certificado y el par de llaves.

4.5.1 Uso de la llave privada por parte del suscriptor.

El suscriptor solo podrá utilizar los Certificados de canales de comunicación por VPN tras aceptar las condiciones establecidas en la DPC en los documentos oficiales de la empresa, para los propósitos descritos en el acápite 1.4 USO DE LOS CERTIFICADOS



4.6 Renovación de certificado.

Se entiende por renovación de un certificado, el proceso de emisión de un nuevo par de llaves y su certificado correspondiente, para sustituir a uno que haya expirado, para lo cual debe realizarse el mismo proceso de contratación, esclareciendo que se trata de una renovación.

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA.

4.7 Cambio de llave del certificado.

En la ACTECNOMATICA no se permite el cambio de llave de un certificado. Cuando se requiera realizar un cambio de llaves, es necesario revocar y realizar la solicitud de un nuevo certificado.

 Tecnomática	Política de Certificación para Canales de comunicación por VPN	Cód.		
		Rev.	01	
		Total de Pág.	24	

4.8 Modificación del certificado.

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA.

4.9 Revocación de certificados.

La revocación del certificado ocasiona el cese de la operatividad e impide su uso legítimo. Esto implica su publicación en la Lista de Certificados Revocados (CRL) de acceso público.

Los certificados revocados no podrán bajo ningún criterio volver al estado activo. La ACTECNOMATICA mantiene publicada las CRL permanentemente en la URL <http://ocsp.cupet.cu>.

El proceso de revocación de los certificados de canales de comunicación por VPN se lleva a cabo como se muestra en los sub acápite (4.9.1. Circunstancias para la revocación y 4.9.2 Procedimiento de solicitud de la revocación) descriptos en la DPC.

4.10 Servicios de comprobación del estado de los certificados.



Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA

4.11 Finalización de la suscripción.

Toda la documentación generada durante los procesos anteriormente descritos, debe ser archivada por un período de 15 años. Todo lo demás se mantiene Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA.

4.12 Custodia y recuperación de llaves.

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA.

 Tecnomática	Política de Certificación para Canales de comunicación por VPN	Cód.		 Cupet UNIÓN CubaPetróleo
		Rev.	01	
		Total de Pág.	24	

5 CONTROLES DE SEGURIDAD FÍSICOS Y OPERACIONALES.

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA.

6 CONTROLES DE SEGURIDAD TÉCNICA

6.1 Generación e instalación del par de llaves

El par de llaves de un titular es generado de acuerdo a lo establecido en el instructivo Generación de una solicitud de Certificado Digital disponible en el sitio web de la PKI, previo contrato firmado por ambas partes.



6.1.1 Entrega de la llave privada al titular

Las llaves privadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación se encuentran en los contenedores con formato PKCS#12 que genera cada una de la solicitud realizada. Estos ficheros contienen además los certificados de usuario y cadena de certificación y son auto gestionados y descargados por sus titulares.

Al ser auto gestionado por el propio usuario la solicitud de un certificado digital, la contraseña de protección de la llave privada, sólo es de conocimiento del titular. Siendo responsabilidad de los responsables de su custodia de implementar los certificados en los servidores y asesorar a los usuarios en la autenticación y uso de estos canales.

6.1.2 Entrega de la llave pública al emisor del certificado.

La llave pública incluida dentro del criptomaterial del contenedor en formato PKCS#12 es generada por la Autoridad de Certificación, tras la recepción de una solicitud validada y aceptada por el operador de la Autoridad de Registro, Bajo ninguna circunstancia se certificarán llaves generadas por los usuarios.

 Tecnomática	Política de Certificación para Canales de comunicación por VPN	Cód.		 Cupet UNIÓN CubaPetróleo
		Rev.	01	
		Total de Pág.	24	

6.1.3 Entrega de la llave pública de la ACTECNOMATICA a los usuarios

Las llaves públicas de todas las AC pertenecientes a la jerarquía de confianza de la ACTECNOMATICA se pueden descargar en su sitio oficial.

6.1.4 Algoritmo y Tamaño de llaves

Bajo el ámbito de la presente Política de Certificación para canales de comunicación por VPN a solicitud del cliente se pueden generar dos tipos de algoritmos con sus respectivos tamaños de las llaves para los siguientes certificados.



- **Certificado de canales VPN Servidor (ECDSA):** Ambos con la norma ECDSA (Elliptic Curve Digital Signature Algorithm) de 384 bits
- **Certificado de canales VPN Servidor (RSA) y Certificado de Firma de Código (RSA):** Ambos con la norma RSA (Rivest Shenir Adlenos) de 4096 bits
- **Certificado autenticación Cliente VPN (ECDSA):** con la norma ECDSA (Elliptic Curve Digital Signature Algorithm) de 384 bits
- **Certificado autenticación Cliente VPN (RSA)** con la norma RSA (Rivest Shenir Adlenos) de 4096 bits

Todos con el mismo nivel de Seguridad, con la ventaja que la norma ECDSA nos facilita firmar documentos elaborados con tecnología Blockchain. El tipo de algoritmo a utilizar para la generación del criptomaterial que le recomendamos es RSA, a no ser que por intereses específicos requiera del uso de la norma ECDSA.

6.2 Protección de la llave privada.

6.2.1 Control multipersona de la llave privada

Las llaves privadas para los certificados de firma emitidos bajo el ámbito de la presente Política de Certificación se encuentran bajo el control exclusivo de sus suscriptores. Ya que una vez entregadas a los usuarios son borrados con modo seguro los contenedores generados.

 Tecnomática	Política de Certificación para Canales de comunicación por VPN	Cód.		 Cupet UNIÓN CubaPetróleo
		Rev.	01	
		Total de Pág.	24	

6.2.2 Custodia de la llave privada

La ACTECNOMATICA no admite la realización de copia, almacenamiento o custodia de las llaves privadas de los suscriptores de los certificados definidos por la presente política.

6.2.3 Copia de seguridad de la llave privada

La ACTECNOMATICA no realiza copia de seguridad de dichas llaves.

6.2.4 Archivo de la llave privada

El archivo de llave privada se encuentra dentro del contenedor pkcs12 que se auto gestiona y descarga el suscriptor.

6.3 Controles de seguridad informática

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA.

6.4 Fines del uso de la llave

Los fines del uso de las llaves emitidas bajo esta política es solamente para la realización con garantías de las comunicaciones por VPN y el no repudio de la información contenida en ella, mediante una autenticación inequívoca de la misma.



6.5 Protección de la llave privada

Todo lo referente a la protección de la llave privada de las aplicaciones es responsabilidad de cada uno de los responsables de su custodia.

6.6 Otros aspectos de la gestión de llaves

6.6.1 Períodos operacionales del certificado y períodos de uso de las llaves

Los períodos de uso de las llaves de los certificados de canales de comunicación por VPN y los Certificados de Autenticación de Clientes regidos bajo esta Política de certificación son de hasta dos (2) años como máximo.

 Tecnómica	Política de Certificación para Canales de comunicación por VPN	Cód.		
		Rev.	01	
		Total de Pág.	24	

La caducidad producirá automáticamente la invalidación de los Certificados, originando el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de asociados.

6.7 Datos de activación

No procede

6.8 Controles de seguridad computacional.

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA (6.5.1).

7 PERFILES DE CERTIFICADOS, LISTAS DE REVOCACIÓN (CRL)

7.1 Perfil del certificado

Los certificados emitidos por el sistema de la ACTECNOMATICA serán conformes con las siguientes normas:



- Resolución 2/2016 del MININT.
- **ITU-T Recommendation X.509:** Information Technology –Open Systems Interconnection - The Directory: Authentication Framework.
- **RFC 5280:** Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile.

Uso apropiado del certificado Canales de comunicación VPN

Establecer una comunicación a través de túneles VPN dotando a los Servidores y clientes de una autenticación segura y capacidades de cifrado que proteja la confidencialidad e integridad de los datos que circulan por una Red Privada Virtual.



Uso apropiado del certificado Autenticación cliente por VPN

Para autenticarse a través de túneles VPN garantizando una comunicación segura.

 Tecnomática	Política de Certificación para Canales de comunicación por VPN	Cód.		
		Rev.	01	
		Total de Pág.	24	

Campo	Valor (Certificados Digitales de canales de comunicación por VPN)
Versión	V3
Número de Serie	Valor único (en formato hexadecimal) generado por ACTECNOMATICA
Algoritmo de firma	SHA512WithRSAEncryption
Algoritmo hash	SHA512
Emisor	CN=ACTECNOMATICA OU=TECNOMATICA O=CUPET-MINEM L=Centro Habana ST=La Habana C=CU E=pkitym@tm.cupet.cu
Válido desde	Especifica la fecha y hora a partir de la cual el certificado es válido.
Válido hasta	Especifica la fecha y hora a partir de la cual el certificado deja de ser válido.
Sujeto	CN=Nombre común de la entidad. (Servicio) NIF = IP (No obligatorio) OU=Unidad Organizacional O=Organización (siglas) ST=Provincia C=CU E=usuario@servidor.dominio (Responsable del Certificado)
Llave pública	Se codifica de acuerdo con la RFC 5280 la longitud de llave de 4096 bits de algoritmo RSA.



A los efectos de esta Política de Certificación, los Certificados Digitales de canales de comunicación por VPN, y los de Autenticación de los clientes incluyen los siguientes campos:

 Tecnomática	Política de Certificación para Canales de comunicación por VPN	Cód.		
		Rev.	01	
		Total de Pág.	24	

Campo	Valor (Certificado autenticación cliente VPN)
Versión	V3
Número de Serie	Valor único (en formato hexadecimal) generado por ACTECNOMATICA
Algoritmo de firma	SHA512WithRSAEncryption
Algoritmo hash	SHA512
Emisor	CN=ACTECNOMATICA OU=TECNOMATICA O=CUPET-MINEM L=Centro Habana ST=La Habana C=CU E=pkitym@tm.cupet.cu
Válido desde	Especifica la fecha y hora a partir de la cual el certificado es válido.
Válido hasta	Especifica la fecha y hora a partir de la cual el certificado deja de ser válido.
Sujeto	CN=Nombre común de la entidad.(Persona) OU=Unidad Organizacional (siglas) O=Organización (siglas) L=Municipio ST=Provincia NIF = Carnet de Identidad C=CU E=usuario@servidor.dominio
Llave pública	Se codifica de acuerdo con la RFC 5280 la longitud de llave de 2028 bits de algoritmo RSA.

7.1.1 Número de versión

ACTECNOMATICA opera mediante el empleo de certificados digitales X.509 en su versión 3; estándar desarrollado por la Unión Internacional de Telecomunicaciones.



 Tecnomática	Política de Certificación para Canales de comunicación por VPN	Cód.		 Cupet UNIÓN CubaPetróleo
		Rev.	01	
		Total de Pág.	24	

7.1.2 Extensiones del certificado

En los certificados contemplados en esta PC, se utilizarán como mínimo los siguientes campos de las extensiones estándar X.509.

- Extensiones del Certificado de canales de comunicación por VPN**

Campo	Descripción	Crítico
Uso de Llave (Key Usage)	Firma Digital (Digital signature)	Si
	No repudio (Non Repudiation)	
	Cifrado de llave (Key encipherment)	
	Acuerdo de llave (Key agreement)	
Uso extendido de Llave (ExtendedKeyUsage)	Autenticación Servidor (Server Authentication)	No
	Internet Key Exchange for IPSec	
Nombre alternativo de Sujeto (SubjectAlternativeName)	Especifica otros nombres asociados al certificado	No
Punto de distribución de Listado de Certificados Revocados (CRLDistributionsPoints)	Especifica las URL de descarga de las CRL http://crl.cupet.cu	No
Identificador llave pública de la Autoridad (AuthorityKeyIdentifier)	Identificador de la llave pública de la ACTECNOMATICA	
Políticas de Certificados (CertificatePolicies)	Especifica la URL de publicación de la presente PC	No
Acceso información de la Autoridad (AuthorityInformationAccess)	Especifica la URL de publicación de la DPC de la ACTECNOMATICA: https://pki.cupet.cu/ca y el servicio OCSP en http://ocsp.cupet.cu (Configurados en el perfil de la CA)	No

 Tecnomática	Política de Certificación para Canales de comunicación por VPN	Cód.		
		Rev.	01	
		Total de Pág.	24	

- **Extensiones del Certificado de Autenticación de cliente por VPN**

Campo	Descripción	Crítico
Uso de Llave (Key Usage)	Firma Digital (Digital signature)	Si
	No repudio (Non Repudiation)	
	Cifrado de llave (Key encipherment)	
	Acuerdo de llave (Key agreement)	
Uso extendido de Llave (ExtendedKeyUsage)	Autenticación Cliente (Client Authentication)	No
Nombre alternativo de Sujeto (SubjectAlternativeName)	Especifica otros nombres asociados al certificado	No
Punto de distribución de Listado de Certificados Revocados (CRLDistributionsPoints)	Especifica las URL de descarga de las CRL http://crl.cupet.cu	No
Identificador llave pública de la Autoridad (AuthorityKeyIdentifier)	Identificador de la llave pública de la ACTECNOMATICA	
Políticas de Certificados (CertificatePolicies)	Especifica la URL de publicación de la presente PC	No
Acceso información de la Autoridad (AuthorityInformationAccess)	Especifica la URL de publicación de la DPC de la ACTECNOMATICA: https://pki.cupet.cu/ca y el servicio OCSP en http://ocsp.cupet.cu (Configurados en el perfil de la CA)	No

7.1.3 Identificador de objeto del algoritmo



De acuerdo a lo especificado en la DPC de la ACTECNOMATICA.

7.1.4 Formato de Nombre

Es el definido en el numeral 3.1 de la DPC.

7.2 Perfil de la CRL.

De acuerdo a lo especificado en la DPC de la ACTECNOMATICA.

 Tecnomática	Política de Certificación para Canales de comunicación por VPN	Cód.		
		Rev.	01	
		Total de Pág.	24	

7.3 Lista de revocación de Certificados (CRL).

De acuerdo a lo especificado en la DPC de la ACTECNOMATICA.

8 AUDITORÍA DE CONFORMIDAD

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA.

9 REQUISITOS LEGALES Y COMERCIALES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA.