ENTIDAD PRESTADORA DE SERVICIOS CRIPTOGRÁFICOS DE CERTIFICACIÓN (PSCC) ACTECNOMATICA

POLÍTICA DE CERTIFICADOS PARA APLICACIONES WEB (SSL-TLS)

(Versión 1.1) ENERO 2023

"AÑO 65 DE LA REVOLUCIÓN"

RELACIÓN DE REVISIONES

Rev. 01	**Nombres y Apellidos**	**Cargo**	**Firma**
Elaborado por:	Soraya del C. López Galban	EP B Seguridad Informática	
	Yesneiler Matos Quintero	Dir. UEB Infocomunicaciones	
	Zenia Ivis Meneses Santiesteban	Esp. B Ciencias informáticas	
Revisado por:	Betty Iznaga Alarcón	Esp. Gestión de la Calidad	
	Lourdes Ramos López	EP Gestión de la Calidad	
Aprobado por:	Armando Estévez Alonso	Director General	

1 Contenido

1 INTRODUCCIÓN

Este documento recoge la Política de Certificación (PC) de los Certificados para Aplicaciones Web y servidores (SSL-TLS) 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 Raiz 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 Certificacion (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 Aplicaciones Web (SSL-TLS).

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 de Aplicaciones Web (SSL-TLS)." (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.

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, acorde con esta política tiene como función la emisión de certificados de Aplicaciones Web (SSL/TLS), entre otros, para la protección de Sitios y Aplicaciones web que garanticen una comunicación segura para 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 contraten a 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)

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 propietario de un Certificado Digital para intercambiar información por sitios y aplicaciones web protegidos, cuya identidad del certificado está vinculada a los datos de creación y verificación.

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).

Certificado Digital de Aplicaciones Web	**Uso apropiado del Certificado**
Certificado Digital para Aplicaciones WEB (SSL/TLS)	Para proteger servicios y aplicaciones WEB dotando a los servidores del protocolo SSL/TLS con el objetivo de garantizar la seguridad en el intercambio de información cifrada entre clientes y servidores.

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.

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 generado por el solicitante del Certificado Digital.

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.

3.2.4 Autenticación de la identidad de una persona.

Las solicitudes de certificados para las personas jurídicas son realizadas por el 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 por el mecanismo establecido la emisión de su Certificado Digital de Firma 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.

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 5 del contrato para la Solicitud Certificado SSL (Datos identificativos del responsable de su custodia y del representante, Direcciones IP, Dominio, Nombre común).

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

4.1.2 Proceso de solicitud y responsabilidades.

El proceso de solicitud de certificados de Aplicaciones Web (SSL-TLS) se lleva a cabo según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA.

4.2 Procesamiento de la solicitud del certificado.

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de la ACTECNOMATICA y descrito en el instructivo “Generación de una solicitud de Certificado Digital en ACTECNOMATICA”, disponible en el sitio web de la PKI.

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 Aplicaciones Web tras aceptar las condiciones establecidas en la DPC en los documentos oficiales de la empresa, para los propósitos descriptos 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.

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://crl.cupet.cu.

El proceso de revocación de certificados de Aplicaciones Web (SSL-TLS) 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.

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 solicitud de Certificado digital en ACTECNOMATICA" 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 contenedores con formato PKCS#12. Estos ficheros contienen además los certificados de usuario y cadena de certificación que son auto gestionados y descargados por sus titulares.

Al ser auto gestionada por el propio usuario la solicitud de un certificado digital, la contraseña de protección del fichero que contiene la llave privada sólo es de conocimiento del titular.

6.1.2 Entrega de la llave pública al emisor del certificado.

La llave pública estará incluida dentro del criptomaterial del contenedor en formato PKCS#12 generada por la Autoridad de Certificación, tras la recepción de una solicitud validada y aceptada por el operador de la Autoridad de Registro y descargado por el emisor.

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 el sitio oficial https://actecnomatica.cupet.cu.

6.1.4 Algoritmo y Tamaño de llaves

Bajo el ámbito de la presente Política de Certificación para Aplicaciones Web (SSL-TLS) se pueden generar dos tipos de algoritmos con sus respectivos tamaños de las llaves para los siguientes certificados de Aplicaciones Web.

- **Certificado de Aplicaciones Web (SSL-TLS) ECDSA):** con la norma ECDSA (Elliptic Curve Digital Signature Algorithm) de 384 bits

- **Certificado de Aplicaciones Web (SSL-TLS) (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 Custodia de la llave privada

La protección de la llave privada de los certificados para las aplicaciones web es asignada, por el Representante a través de ANEXO 5 del contrato para la Solicitud Certificado SSL ante la AR, a un responsable de su custodia.

6.2.2 Copia de seguridad 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 Archivo de la llave privada

El archivo de llave privada se encuentra dentro del contenedor pkcs12 que auto gestiona y descarga el suscriptor con credenciales creadas por él.

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

Las llaves emitidas bajo esta política se usarán para dotar a los Servidores y Aplicaciones Web de protocolos SSL/TLS con la finalidad de establecer comunicaciones seguras a través de Internet, de acuerdo con lo especificado en los campos KeyUsage y ExtendedKeyUsage del Certificado Digital.

6.5 Otros aspectos de la gestión de llaves

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

Los períodos de uso de las llaves de los certificados de Aplicaciones Web (SSL-TLS) regidos bajo esta Política de certificación son de hasta dos (2) años como máximo.

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.

6.6 Datos de activación

No procede

6.7 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

Para proteger servicios y aplicaciones WEB dotando a los servidores del protocolo SSL/TLS con el objetivo de garantizar la seguridad en el intercambio de datos entre clientes y servidores.

A los efectos de esta Política de Certificación, los Certificados Digitales de Aplicaciones Web, incluyen los siguientes campos:

Campo	Valor
Versión	V3
Número de Serie	Valor único (en formato hexadecimal) generado por ACTECNOMATICA
Algoritmo de firma	SHA512WithRSAEncryption o ECDSAWithSHA512
Algoritmo hash	SHA512
Emisor	CN=ACTECNOMATICA OU=TECNOMATICA O=CUPET-MINEM L=Centro Habana ST=La Habana C=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. (Aplicación) NIF = IP (No obligatorio) OU=Unidad Organizacional O=Organización (siglas) ST=Provincia C=CU
Llave pública	Se codifica de acuerdo con la RFC 5280 la longitud de llave de 4096 bits para el algoritmo RSA y con RFC 5480 la longitud de llave de 384 bits para algoritmo ECDSA.

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.

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 Aplicaciones web**

Campo	Descripción	Crítico
Uso de Llave (Key Usage)	Firma Digital (Digital signature)	Si
	Cifrado de llave (Key encipherment)	
Uso extendido de Llave (ExtendedKeyUsage)	Autenticación Servidor (Server 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)	https://actecnomatica.cupet.cu/ficherospki/categoriapki2/PC_Aplicaciones_WEB_ACTECNOMATICA.pdf	No
Acceso información de la Autoridad (AuthorityInformationAccess)	Especifica la URL de publicación de la DPC de la ACTECNOMATICA: https://actecnomatica.cupet.cu/ y el estado de los certificados en línea http://ocsp.cupet.cu	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.

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.