

ANEXO II

**PERFIL DEL CERTIFICADO DEL PRESTADOR NO CUALIFICADO
DE SERVICIOS DE CONFIANZA**

DOC-ICPP-20

Versión 1.0



**POR LA CUAL SE REGLAMENTA EL PROCESO DE
COMUNICACIÓN DE INICIO Y MODIFICACIÓN DE LA
PRESTACIÓN DE SERVICIOS DE CONFIANZA NO
CUALIFICADOS**

Anexo de la
Resolución
N° 1384/2022

CONTROL DOCUMENTAL

Documento	
Título: Perfil del certificado del Prestador no cualificado de Servicios de Confianza	Nombre Archivo: DOC-ICPP-20 Vers 1.0
Código: DOC-ICPP-20	Soporte Lógico: https://www.acraiz.gov.py/
Fecha: 06 / 10 /2022	Versión: 1.0

Registro de cambios		
Versión	Fecha	Motivo de cambio
1.0	06 / 10 /2022	Versión inicial

Distribución del documento
Ministerio de Industria y Comercio (MIC)
Prestadores de Servicios de Confianza (PSC)
Documento Público

Control del documento	
Elaborado por: JENNY RUÍZ DÍAZ	
Verificado y aprobado por: LUCAS SOTOMAYOR	

 <p>TETĀ MBA'E'APOPY HA ÑEMU Motenondecha Ministerio de INDUSTRIA Y COMERCIO</p>	<p align="center">MINISTERIO DE INDUSTRIA Y COMERCIO</p> <p align="center">POR LA CUAL SE REGLAMENTA EL PROCESO DE COMUNICACIÓN DE INICIO Y MODIFICACIÓN DE LA PRESTACIÓN DE SERVICIOS DE CONFIANZA NO CUALIFICADOS</p>	<p align="center">Página 3</p> <p align="center">Anexo de la Resolución N° 1384/2022</p>
--	---	--

Contenido

1.	Introducción	4
2.	Perfil de certificado del Prestador No Cualificado de Servicios de Confianza	5
3.	Perfiles de certificado de entidades finales	7
3.1.	Certificado NO cualificado de Firma Electrónica	7
3.2.	Certificado NO cualificado de Sello electrónico	10

 <p>TETĀ MBA'E'APOPY HA ÑEMU Moronondecha Ministerio de INDUSTRIA Y COMERCIO</p>	<p align="center">MINISTERIO DE INDUSTRIA Y COMERCIO</p> <p align="center">POR LA CUAL SE REGLAMENTA EL PROCESO DE COMUNICACIÓN DE INICIO Y MODIFICACIÓN DE LA PRESTACIÓN DE SERVICIOS DE CONFIANZA NO CUALIFICADOS</p>	<p align="center">Página 4</p> <p align="center">Anexo de la Resolución N° 1384/2022</p>
--	---	--

1. INTRODUCCIÓN

El presente documento constituye una guía que tiene por objetivo definir los perfiles de los certificados de Prestadores no cualificados de Servicios de Confianza relativos a los servicios de firma electrónica y sello electrónico.

Los perfiles contemplados corresponden específicamente a:

- 1) Prestador no cualificado de Servicios de Confianza
- 2) Entidades finales:
 - a) Certificado no cualificado de firma electrónica
 - b) Certificado no cualificado de sello electrónico



**POR LA CUAL SE REGLAMENTA EL PROCESO DE
COMUNICACIÓN DE INICIO Y MODIFICACIÓN DE LA
PRESTACIÓN DE SERVICIOS DE CONFIANZA NO
CUALIFICADOS**

Anexo de la
Resolución
N° 1384/2022

2. PERFIL DE CERTIFICADO DEL PRESTADOR NO CUALIFICADO DE SERVICIO DE CONFIANZA

Campo	Contenido	Obligatoriedad	
1. Versión	3	Sí	
2. Serial Number	Número identificativo único del certificado.	Sí	
3. Signature Algorithm	Sha256withRsaEncryption	Sí	
4. Issuer Distinguished Name	Entidad emisora del certificado (AC Raíz)	Sí	
	4.1. Country	C="Siglas del País de la AC Raíz"	Sí
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O="Nombre AC Raíz"	Sí
5. Validity	10 años	Sí	
6. Subject	Entidad emisora del certificado (AC Subordinada)	Sí	
	6.1. Country	C=PY	Sí
	6.2. Organization	O= Prestador NO Cualificado de Servicio de Confianza	Sí
	6.3. Organizational Unit	Denominación (nombre "oficial" de la organización) del prestador no cualificado de servicios de confianza (emisor del certificado). OU="Nombre PSC"	Sí
	6.4. Serial Number	Número único de identificación de la entidad, aplicable de acuerdo con el país. En Paraguay, RUC de la entidad suscriptora.	Sí



**POR LA CUAL SE REGLAMENTA EL PROCESO DE
COMUNICACIÓN DE INICIO Y MODIFICACIÓN DE LA
PRESTACIÓN DE SERVICIOS DE CONFIANZA NO
CUALIFICADOS**

Anexo de la
Resolución
N° 1384/2022

		serialNumber="Siglas RUC seguido del número de RUC del PSC"	
	6.5. Common Name	CN=PSC-"Nombre PSC"	Sí
7. Authority Key Identifier		Identificador de la clave pública de la entidad raíz. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la AC para firmar el certificado de esta AC Subordinada	Sí
8. Subject Public Key Info		Clave pública de la AC Subordinada, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí
9. Subject Key Identifier		Identificador de la clave pública de la AC Subordinada. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí
10. Key Usage		Uso permitido de las claves.	Sí
	10.1. Digital Signature	0	Sí
	10.2. Content Commitment	0	Sí
	10.3. Key Encipherment	0	Sí
	10.4. Data Encipherment	0	Sí
	10.5. Key Agreement	0	Sí
	10.6. Key Certificate Signature	1	Sí
	10.7. CRL Signature	1	Sí
11. Certificate Policies		Política de certificación	Sí
	11.1. Policy Identifier	"Debe contener los OIDs de las PCs implementadas por el PSC titular del certificado, para la emisión de certificados de personas físicas o jurídicas"	Sí



**POR LA CUAL SE REGLAMENTA EL PROCESO DE
COMUNICACIÓN DE INICIO Y MODIFICACIÓN DE LA
PRESTACIÓN DE SERVICIOS DE CONFIANZA NO
CUALIFICADOS**

Anexo de la
Resolución
N° 1384/2022

	11.2. Policy Qualifier Id		
	11.2.1 CPS Pointer	“Debe contener la dirección web de la DPC que emite el certificado”	Sí
	11.2.2 User Notice	Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de [nombre dela Entidad Emisora del Certificado]”	Sí
12. CRL Distribution Point		Punto de distribución (localizador) de la LCR	Sí
	12.1. Distribution Point 1	Punto de distribución 1 de la LCR Dirección URL=”debe contener la dirección web donde se obtiene la LCR correspondiente al certificado”	Sí
13. Authority Info Access			
	1.1. Access Method 1	Identificador de método de acceso a la información de revocación: “debe contener el identificador de método de acceso a la información de revocación (OCSP)”	Sí
	1.2. Acces Location 1	“debe contener la dirección Web del servicio del OCSP”	Sí
14. Basic Constraints		Esta extensión sirve para identificar si el sujeto de certificación es una AC así como el máximo nivel de “profundidad” permitido para las cadenas de certificación”.	
	14.1. Subject Type	AC	
	14.2. Path Length	0	

3. PERFILES DE CERTIFICADO DE ENTIDADES FINALES

3.1. CERTIFICADO NO CUALIFICADO DE FIRMA ELECTRÓNICA:

Campo	Contenido	Obligatoriedad
1. Version	3	Sí



**POR LA CUAL SE REGLAMENTA EL PROCESO DE
COMUNICACIÓN DE INICIO Y MODIFICACIÓN DE LA
PRESTACIÓN DE SERVICIOS DE CONFIANZA NO
CUALIFICADOS**

Anexo de la
Resolución
N° 1384/2022

2. Serial Number		Número identificativo único del certificado. Este número se asigna de forma aleatoria.	Si
3. Signature Algorithm		Sha256withRsaEncryption	Si
4. Issuer Distinguish Name		Entidad emisora del certificado	Si
	4.1. Country	C=PY	Si
	4.2. Organization	O=Prestador NO Cualificado de Servicio de Confianza	Si
	4.3. Organizational Unit	Denominación (nombre “oficial” de la organización) del prestador no cualificado de servicios de confianza (emisor del certificado). OU=“Nombre PSC”	Si
	4.4. Serial Number	Número único de identificación de la entidad, aplicable de acuerdo con el país. En Paraguay, RUC de la entidad suscriptora. serialNumber=“Siglas RUC seguido del número de RUC del PSC”	Si
	4.5. Common Name	CN=PSC-“Nombre PSC”	Si
5. Validity		Hasta 4 años	Si
6. Subject		Identificación/descripción del custodio/responsable de las claves certificadas	Si
	6.1. Country	C=PY	Si
	6.2. Organization	O= CERTIFICADO NO CUALIFICADO DE FIRMA ELECTRÓNICA	Si
	6.3. Organizational Unit	Descripción del tipo de certificado. En este caso: OU=FIRMA ELECTRÓNICA	Si



**POR LA CUAL SE REGLAMENTA EL PROCESO DE
COMUNICACIÓN DE INICIO Y MODIFICACIÓN DE LA
PRESTACIÓN DE SERVICIOS DE CONFIANZA NO
CUALIFICADOS**

Anexo de la
Resolución
N° 1384/2022

Campo		Contenido	Obligatoriedad
6.4. Serial Number	6.4. Serial Number	serialNumber="Siglas CI o PAS seguido del número de Cédula de Identidad o Pasaporte según corresponda"	Sí
	6.5. Surname	Apellido del titular de certificado, de acuerdo con documento de identificación	Sí
	6.6. Given Name	Nombre del titular de certificado, de acuerdo con documento de identidad (CI/Pasaporte)	Sí
	6.7. Common Name	Nombre y apellido de acuerdo con documento de identidad (CI/Pasaporte)	Sí
7. Authority Key Identifier		Identificador de la clave pública de la AC Emisora. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la AC para firmar un certificado.	Sí
8. Subject Public Key Info		Clave pública asociada a la persona física, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí
9. Subject Key Identifier		Identificador de la clave pública del suscriptor o poseedor de claves. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí
10. Key Usage		Uso permitido de las claves	Sí
10.1. Digital Signature	10.1. Digital Signature	1	
	10.2. Content Commitment	1	
	10.3. Key Encipherment	1	
	10.4. Data Encipherment	0	
	10.5. Key Agreement	0	



**POR LA CUAL SE REGLAMENTA EL PROCESO DE
COMUNICACIÓN DE INICIO Y MODIFICACIÓN DE LA
PRESTACIÓN DE SERVICIOS DE CONFIANZA NO
CUALIFICADOS**

Anexo de la
Resolución
N° 1384/2022

	10.6. Key Certificate Signature	0	
	10.7. CRL Signature	0	
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí
	11.1. Email protection	1.3.6.1.5.5.7.3.4	Sí
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2	Sí
12. Certificate Policies		Política de certificación	Sí
	12.1. Policy Identifier	“debe contener los OIDs de las PCs implementadas por el PSC titular del certificado, para la emisión de certificados de personas físicas o jurídicas”	Sí
	12.1.1. Policy Qualifier Id		
	12.1.1.1 CPS Pointer	“debe contener la dirección web de la DPC del PSC”	Sí
	12.1.1.2 User Notice	Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación del [nombre del PSC]”	Sí
13. Subject Alternative Names		Identificación	Sí
	13.1. rfc822 Name	Correo electrónico del titular de certificado	Opcional
14. CRL Distribution Point		Punto de distribución (localizador) de la CRL	Sí



**POR LA CUAL SE REGLAMENTA EL PROCESO DE
COMUNICACIÓN DE INICIO Y MODIFICACIÓN DE LA
PRESTACIÓN DE SERVICIOS DE CONFIANZA NO
CUALIFICADOS**

Anexo de la
Resolución
N° 1384/2022

	14.1. Distribution Point 1	Punto de distribución 1 de la LCR Dirección URL="debe contener la dirección web donde se obtiene la LCR correspondiente al certificado"	Sí
15. Authority Info Access			Sí
	15.1. Access Method 1	Identificador de método de acceso a la información de revocación: "debe contener el identificador de método de acceso a la información de revocación (OCSP)"	Sí
	15.2. Acces Location 1	"debe contener la dirección Web del servicio del OCSP"	Sí
16 Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación". También sirve para distinguir una CA de las entidades finales	
	16.1. Subject Type	Entidad final (valor FALSE)	Sí

3.2. CERTIFICADO NO CUALIFICADO DE SELLO ELECTRÓNICO:

Campo	Contenido	Obligatoriedad	
1. Versión	3	Sí	
2. Serial Number	Número identificativo único del certificado. Este número se asigna de forma aleatoria.	Sí	
3. Signature Algorithm	Sha256withRsaEncryption	Sí	
4. Issuer Distinguish Name	Entidad emisora del certificado	Sí	
	4.1. Country	C=PY	Sí
	4.2. Organization	O=Prestador NO Cualificado de Servicio de Confianza	Sí



**POR LA CUAL SE REGLAMENTA EL PROCESO DE
COMUNICACIÓN DE INICIO Y MODIFICACIÓN DE LA
PRESTACIÓN DE SERVICIOS DE CONFIANZA NO
CUALIFICADOS**

Anexo de la
Resolución
N° 1384/2022

	4.3. Organizational Unit	Denominación (nombre “oficial” de la organización) del prestador no cualificado de servicios de confianza (emisor del certificado). OU=“Nombre PSC”	Sí
	4.4. Serial Number	Número único de identificación de la entidad, aplicable de acuerdo con el país. En Paraguay, RUC de la entidad suscriptora. serialNumber=“Siglas RUC seguido del número de RUC del PSC”	Sí
	4.5. Common Name	CN=PSC-“Nombre PSC”	Sí
5. Validity		Hasta 4 años	Sí
6. Subject		Identificación/descripción del custodio/responsable de las claves	Sí
	6.1. Country	C=PY	Sí
	6.2. Organization	O= CERTIFICADO NO CUALIFICADO DE SELLO ELECTRÓNICO	Sí
	6.3. Organizational Unit	Descripción del tipo de certificado. En este caso: OU=SELLO ELECTRÓNICO	Sí



**POR LA CUAL SE REGLAMENTA EL PROCESO DE
COMUNICACIÓN DE INICIO Y MODIFICACIÓN DE LA
PRESTACIÓN DE SERVICIOS DE CONFIANZA NO
CUALIFICADOS**

Anexo de la
Resolución
N° 1384/2022

Campo		Contenido	Obligatoriedad
6.4. Serial Number	6.4. Serial Number	serialNumber="Siglas RUC seguido del número de Cédula TRIBUTARIA"	Sí
	6.5. Common Name	Nombre de la Persona Juridica	Sí
7. Authority Key Identifier		Identificador de la clave pública de la AC Emisora. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la AC para firmar un certificado.	Sí
8. Subject Public Key Info		Clave pública asociada a la persona física, codificada de acuerdo con el algoritmo criptográfico. En este caso RSA Encryption.	Sí
9. Subject Key Identifier		Identificador de la clave pública del suscriptor o poseedor de claves. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí
10. Key Usage		Uso permitido de las claves	Sí
10.1. Digital Signature	10.1. Digital Signature	1	
	10.2. Content Commitment	1	
	10.3. Key Encipherment	1	
	10.4. Data Encipherment	0	
	10.5. Key Agreement	0	
	10.6. Key Certificate Signature	0	
	10.7. CRL Signature	0	
11. Extended Key Usage		Uso mejorado o extendido de las claves	Sí
11.1. Email protection	11.1. Email protection	1.3.6.1.5.5.7.3.4	Sí
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2	Sí
	11.3. Microsoft Smart Card Logon	1.3.6.1.4.1.311.20.2.2	Sí



**POR LA CUAL SE REGLAMENTA EL PROCESO DE
COMUNICACIÓN DE INICIO Y MODIFICACIÓN DE LA
PRESTACIÓN DE SERVICIOS DE CONFIANZA NO
CUALIFICADOS**

Anexo de la
Resolución
N° 1384/2022

Campo		Contenido	Obligatoriedad	
12. Certificate Policies		Política de certificación	Sí	
	12.1. Policy Identifier	“debe contener los OIDs de las PCs implementadas por el PSC titular del certificado, para la emisión de certificados de personas físicas o jurídicas”	Sí	
	12.1.1 Policy Qualifier Id			
		12.1.1.1 CPS Pointer	“debe contener la dirección web de la DPC del PSC”	Sí
		12.1.1.2 User Notice	Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación del [nombre del PSC]”	Sí
13. Subject Alternative Names		Identificación	Sí	
	13.1. rfc822 Name	Correo electrónico del responsable del certificado	Opcional	
	13.1. DirectoryName	OID= 2.5.4.5= “nombre y apellido del responsable del certificado”	Sí	
	13.3. DirectoryName	OID= 2.5.4.5= [siglas CI seguido del número de cédula de identidad civil o las siglas PAS seguido del número de pasaporte según sea el caso	Sí	
14. CRL Distribution Point		Punto de distribución (localizador) de la CRL	Sí	
	14.1. Distribution Point 1	Punto de distribución 1 de la LCR Dirección URL=“debe contener la dirección web donde se obtiene la LCR correspondiente al certificado”	Sí	
15. Authority Info Access			Sí	



**TETĀ MBA'E'APOPY
HA ÑEMU**
Motenondcha
Ministerio de
**INDUSTRIA
Y COMERCIO**

MINISTERIO DE INDUSTRIA Y COMERCIO

Página | 15

**POR LA CUAL SE REGLAMENTA EL PROCESO DE
COMUNICACIÓN DE INICIO Y MODIFICACIÓN DE LA
PRESTACIÓN DE SERVICIOS DE CONFIANZA NO
CUALIFICADOS**

Anexo de la
Resolución
N° 1384/2022

	15.1. Access Method 1	Identificador de método de acceso a la información de revocación: “debe contener el identificador de método de acceso a la información de revocación (OCSP)”	Sí
	15.2. Access Location 1	“debe contener la dirección Web del servicio del OCSP”	Sí
16 Basic Constraints		Esta extensión sirve para identificar si el sujeto de certificación es una AC así como el máximo nivel de “profundidad” permitido para las cadenas de certificación”. También sirve para distinguir una AC de las entidades finales	Sí
	16.1. Subject Type	Entidad final (valor FALSE)	