CORREO URUGUAYO

Administración Nacional de Correos del Uruguay

Servicios de Certificación

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

OID: 1.3.6.1.4.1.31439.1.1

Versión: 3.5

21 de Abril de 2015

1 INTRODUCCIÓN

1.1 RESUMEN

El presente documento busca describir las políticas, prácticas y procedimientos utilizados por la Administración Nacional de Correos (en adelante ANC) para brindar Servicios de Certificación. De esta manera, se da transparencia a los métodos utilizados para proveer dichos servicios, y se asegura la calidad de los mismos.

El presente documento se encuentra publicado en formato electrónico en http://www.correo.com.uy/correocert/CPS.pdf o puede ser solicitado en la Casa Central de la ANC.

La estructura de este documento se basa en la propuesta de estándar para la documentación de prácticas de certificación del grupo de trabajo IETF PKIX. Esta propuesta, catalogada como RFC 3647 (Request For Comments) y en su versión de noviembre 2003, se titula "Certificate Policy and Certification Practices Framework". Este documento sucede al RFC 2527 sobre el cual se basó la versión 1.0 de este documento.

1.2 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

Este documento se titula "Declaración de Prácticas de Certificación, versión 3.3" de los Servicios de Certificación de la ANC. También se le puede hacer referencia bajo las denominaciones "Declaración de Prácticas de Certificación", "CPS", "CPS 3.3", "DPC" o "DPC 3.3". El acrónimo "CPS" proviene del inglés "Certifictate Practice Statement".

La fecha de entrada en vigencia de este documento es el 12 de Abril de 2011 y permanece vigente hasta la salida de una nueva versión que se notifique.

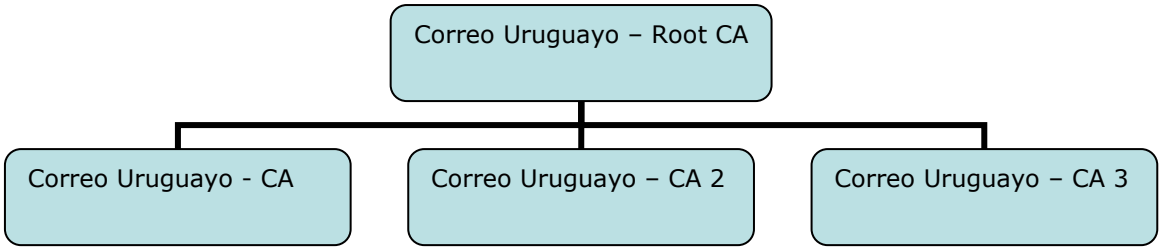
La Autoridad en materia de Políticas de la CA notificará de los cambios que se producirán, a través del sitio Web de la CA.

1.3 ENTIDADES Y PERSONAS INTERVINIENTES

1.3.1 Autoridades de Certificación

La Autoridad de Certificación (Correo Uruguayo - CA) de la División Servicios Electrónicos de la ANC es la entidad encargada de la firma electrónica de los certificados emitidos y de las listas de revocación de certificados.

El certificado de la autoridad de certificación "Correo Uruguayo - Root CA" es el certificado de nivel más alto en la jerarquía general de la PKI de la ANC la cual se diagrama a continuación.



- Un primer nivel en el que se ubica la CA raíz que representa el punto de confianza de todo el sistema.
- Un segundo nivel, constituido por las CA subordinadas de la CA Raíz que emitirán los certificados de entidad final.
- La ANC consta en la actualidad con una única CA subordinada.

A continuación se detalla la información de los certificados de "Correo Uruguayo – Root CA" y "Correo Uruguayo – CA"

1.3.1.1 Correo Uruguayo – Root CA

Certificado.
El certificado de los Servicios de Certificación de la ANC es un certificado X.509 versión 3. Este certificado está disponible en http://www.correo.com.uy/correocert/.

Nombre Distintivo.
CN = Correo Uruguayo - Root CA
OU = SERVICIOS ELECTRONICOS
O = ADMINISTRACION NACIONAL DE CORREOS
C = UY

Número de Serie.
00 ca 22 79 08 23 2a f0 f5 82 b8 85 d3 63 dd f1

Clave.
La clave privada y pública de los Servicios de Certificación de la ANC son claves RSA de largo de 4096 bits.

Firma.
El certificado de los Servicios de Certificación de la ANC está auto-firmado.

Algoritmo.
El algoritmo de firma utilizado es SHA-1 con RSA

Validez.
El certificado es válido hasta el Martes, 31 de Diciembre de 2030.

Clave pública en formato Base 64.


```
-----BEGIN CERTIFICATE-----
MIIGGjCCBAKgAwIBAgIQAMoieQgjKvD1griF02Pd8TANBgkqhkiG9w0BAQUFADB/
MQswCQYDVQQGEwJVWTErMCkGA1UECgwiQURNSU5JU1RSQUNJT04gTkFDSU9OQUwg
REUgQ09SUkVPUzEfMB0GA1UECwwWU0VSVklDSU9TIEVMRUNUUk9OSUNPUzEiMCAG
A1UEAwwZQ29ycmVvIFVydWd1YXlvIC0gUm9vdCBDQTAeFw0wODA3MTQxNjUyMTVa
Fw0zMDEyMzEwMjU5NTlaMH8xCzAJBgNVBAYTAlVZMSswKQYDVQQKDCJBRE1JTklT
VFJBQ0lPTiBOQUNJT05BTCBERSBDT1JSRU9TMR8wHQYDVQQLDBZTRVJWSUNJT1Mg
RUxFQ1RST05JQ09TMSIwIAYDVQQDDBlDb3JyZW8gVXJ1Z3VheW8gLSBSb290IENB
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAsT3SpyVwl4N4DtcyyWYO
eCPkKhvsw+9ThYO7ys9+6lOZbSdVyNE4IUBuSU3DPfYJKwYZQ6mYyQFO9KqAMAdV
8/W3fZm3c4XVHGVWbA0ymwgONGEqQAmEN8Nm7Q1MnAx4QDrs7avMpITydTGVQKiq
u5O1d5hs8sjgIVoj5EKnk8ioHTjOpBpAQL88k5CbX9aUwSJbRtfFABXVj8b33guv
bosFj1uAlQ6jvZPMkPJ940h+ss0HPRvtFJB08900H3zkA1nxLc3go6A7IS5crqwI
BlAVMTXuX/kfDTSlgG5ick/jIbo4QF1f22gqXDTGCDv2fC6ojcS3pq3Zm78ZQQ5I
OQlmbg00AcW7BxEjpNr+YJYoR9yPZ5sTr315DnjNwIwvuyEs/HQWHt7AMp36eDqG
uj7JeAoA0eTgyRLiW9zru4CaMjWr8DDDDkiEL40ICvYsjE0ygEVVCNvNDai/CHq4
52hdmpSJlbz8mo64fzrYbNX0GKxp4qTBC7Mfo4Kf84o8hUA4CfrCBT7hnIn6wwVs
CI9dUfR/u8TzbAG9PU/EGYs52crM6XmIBFWrbbjaFkVlORUFGPsLLHMB7ZRS5X0M
ATsJoE3xPQiBZjQ2F0TwZ/Nb8gW2IZhY2fShN9lv5u9WxPu/VmICrDAwtgLW0hb8
TuqHQ5poXYijkUYoK785FRUCAwEAAaOBkTCBjjAPBgNVHRMBAf8EBTADAQH/MA4G
A1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUfbtp64hh4UDPRyNkAIaiZmvchJUwTAYD
VR0gBEUwQzBBBgRVHSAAMDkwNwYIKwYBBQUHAgEWK2h0dHA6Ly93d3cuY29ycmVv
LmNvbS51eS9jb3JyZW9jZXJ0L2Nwcy5wZGYwDQYJKoZIhvcNAQEFBQADggIBAFbf
E4m+YrcOgSFzpNQ3yu23L5V014n4S0eB7mftuCnfIaD8VGdnyFcsW6EKdXghIcqg
qN9rnNk2Ao24AcFvjntsyaSyxUapykwCgfqje509SObKQGbSRJ124FW5ppyn0UPY
9aC0nfj35aamQvMCMllGcisU7F5l1VGBeM6qL42WiXlq+w/IW8+0rpC2X+N8Ymy3
pv+QgbWYkXMSMK/H6IECaHMpu1h1PbfWQ9WuTfJCufDf2jEAE9rhs7YGi1v9yZi4
ohPRuo/BihqeD/+CvgSC5SuTPh61ogwbxhqwc4l2g7yOO7sXbRTDi759FSa1qZwX
elB6LevpmZSumBC97ipdXdaONFusHodga5jHh4/TnLJoBUkH+akxZpz+v6dZ6Czw
NtTyqBmCwJ6nOfmxmDSjH/rNyRkteN63/WLwk6P+AFvWCuTzfnyXKOEF7AU0RRP/
KRNhiidP27jSkiEntYh3Z6h+zyQ8hwgEM3OPC7aG+M/vsqYkHguRkQBQFjIS2Akl
2mNO3dst1+cEa+NjH6n+qQFjxMpMFGiDvAWsWRb7bqEHb7tLvm2YSHYle0oRllQI
rKnzN6uDw9HNgZjA5UA1uJ+R52/mSyAWilN7rDrRmDVU0NS/rn6aSx7pdaMlsDvn
Zb9PlfQdvcS6yU2BUcI/WtkS9CEb1pXqPZD+qZPi
-----END CERTIFICATE-----
```


1.3.1.2 Correo Uruguayo – CA

Certificado.
El certificado de los Servicios de Certificación de la ANC es un certificado X.509 versión 3. Este certificado está disponible en http://www.correo.com.uy/correocert/.

Nombre Distintivo.
CN = Correo Uruguayo - CA
OU = SERVICIOS ELECTRONICOS
O = ADMINISTRACION NACIONAL DE CORREOS
C = UY

Número de Serie.
76 be 4e a7 00 0f 7f 81 48 7c ce bd 35 a0 f9 a1

Clave.
La clave privada y pública de los Servicios de Certificación de la ANC son claves RSA de largo de 4096 bits.

Firma.
El certificado de los Servicios de Certificación de la ANC firmado por:
CN = Correo Uruguayo - Root CA
OU = SERVICIOS ELECTRONICOS
O = ADMINISTRACION NACIONAL DE CORREOS
C = UY

Algoritmo.
El algoritmo de firma utilizado es SHA-1 con RSA.

Validez.
El certificado es válido hasta el Martes, 31 de Diciembre de 2030.

Clave pública en formato Base 64.


```
-----BEGIN CERTIFICATE-----
MIIGfDCCBGSgAwIBAgIQdr5OpwAPf4FIfM69NaD5oTANBgkqhkiG9w0BAQUFADB/
MQswCQYDVQQGEwJVWTErMCkGA1UECgwiQURNSU5JU1RSQUNJT04gTkFDSU9OQUwg
REUgQ09SUkVPUzEfMB0GA1UECwwWU0VSVklDSU9TIEVMRUNUUk9OSUNPUzEiMCAG
A1UEAwwZQ29ycmVvIFVydWd1YXlvIC0gUm9vdCBDQTAeFw0wODA3MTUxNjE1NDBa
Fw0zMDEyMzEwMjUwMDBaMHoxCzAJBgNVBAYTAlVZMSswKQYDVQQKDCJBRE1JTklT
VFJBQ0lPTiBOQUNJT05BTCBERSBDT1JSRU9TMR8wHQYDVQQLDBZTRVJWSUNJT1Mg
RUxFQ1RST05JQ09TMR0wGwYDVQQDDBRDb3JyZW8gVXJ1Z3VheW8gLSBDQTCCAiIw
DQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAN1dc8SYuZBgmqy7JbY42n42u7oV
wUUVY8tdz1Bafr3mvXEziRq8ZMGDziTfmsTW9jtUYM8NTQjcBoaoCSurwdyvz+G9
f1OmEvfVPbv84BoP4Nj2HtSQ/WiKWgOg/jBz9F+W7/YJXoGA10Lz/JFkDPGEEIot
NW3o22BtU+57XTtM9tL9J+nDzAtatyzs+x8fUmm0mfdthjwCq4jwTX6+OQJNG8h9
o2Bjvn35t2bW7WmLnKIvJiwr5Cx1thQEx4W1fzNarm9OMU6uHb1MY4MX4mQOADPe
3dw8k/Bh/fWL7Mnsh3fCHpvLziqbtztVsRu9+ZhpVk/Zw/HzhVgF0I/C/ARJyduX
dMCigLp88YWhpHkzYdvpNH4St1lNjsQ9z+3fhUWS/citkAGZ2H26n6xvxSZzRAfF
LmENq6aHfShPl58uuIFzmP9S8vlBx+VCDVwOceRiBRA5JO1tTZhErGDabMTHMvZg
bhBD5zWCAYUN2MmlCbThHIcHirGb9LfukzPtOyzd34pCztdxo23Dd0UY6GAohNYi
+58LosfSzArEAb3mooaSBrerb3JVgigRT4y1GlfxoRThZrJdxbtgMy108cyO5fCC
uyAX2KyiGKHK1bbdF5ark1oZbNfxnpuj+IEN8ZXHaJBVEqlqm1vvAPcoBXzO0c8+
lyfk8/mTHSB8suCJAgMBAAGjgfgwgfUwEgYDVR0TAQH/BAgwBgEB/wIBADAOBgNV
HQ8BAf8EBAMCAQYwHQYDVR0OBBYEFCWP30Mvjmq6C75GXFdQk7dRvvzZMB8GA1Ud
IwQYMBaAFH27aeuIYeFAz0cjZACGomZr3ISVMEwGA1UdIARFMEMwQQYEVR0gADA5
MDcGCCsGAQUFBwIBFitodHRwOi8vd3d3LmNvcnJlby5jb20udXkvY29ycmVvY2Vy
dC9jcHMucGRmMEEGA1UdHwQ6MDgwNqA0oDKGMGh0dHA6Ly93d3cuY29ycmVvLmNv
bS51eS9Db3JyZW9DZXJ0L2FuY19yb290LmNybDANBgkqhkiG9w0BAQUFAAOCAgEA
WaTxZ3s8Dxndzw9LVXRxgJawxwybLHJ0/qDP9pk3wGDhvRZe+WyumLMgKLDLpZ+T
RFf3DsA41Nf6aX2/FO5cRZB83B++x6En30oDQ6vpQhuIfFFTmKHZCZnq1giTM8tt
ou6aUdxzLvDxOkDlbl17PKIGP0L+6q+aNyjZaojrWddx3ZzwFAKR8UmxLN9ErNOK
9SMVGrwr/jJbyHa9m2sV8UBDGR6vSrEHCbtDHpQIBJxicKvBXTvBjyGfbrCV4sTj
3TUtCt/ZG9Tqp2SDbSJCo2Po1T6xy/2ra9Sl3z9AjHJ2MF/6CcmRjR0e309a1RN5
iXfrPnOAi0zLQY34TiIs5uDYjbi5pqDLqO3wZrvfuLFQxnM6kIXKZwjREzlzyAqF
hmAfcocqO9mgu+spCaXDbkwFM4o64Z7BBB1JlCbhRktRH6OXyGGMDtdUB2areJbW
ddiIUoWOd2OblD7FliFJVbia3/kGByDnCWAQKtSzxX74M1w8jg8yR/WMOno8r61z
dFbe0DAkZ1IrwW73aCQjXMbV3PDWdZqTJuQPVmvb+Zf243c0DWTzYa4hNmiFZTft
76RKbktC+WhkuMwJqu1CbtkYFwUS+9VUK8KfEMadjQp7ZfAWXIvJmR8cPIT3GF3/
zp9PwwehQhf+eLRpwcEG0qlVXakwPqYkXw6yihkL854=
-----END CERTIFICATE-----
```


1.3.2 Autoridades de Registro

Las Autoridades de Registro (RA) son parte integrante de los Servicios de Certificación de la ANC. Funcionan en los denominados "Puntos de Emisión" de certificados y tienen como misión realizar las funciones de identificación, registro y autenticación.

Podrán ser puntos de emisión todos los locales de la ANC automatizados con personal entrenado para dicho fin. La lista actualizada de locales puede accederse en:

http://www.correo.com.uy/index.asp?codPag=codPost&switchMapa=locales

1.3.3 Usuario suscriptor

Se entiende como usuario en la presente CPS a cualquier persona o sistema que voluntariamente confíe y haga uso de un certificado emitido por los Servicios de Certificación de la ANC, o que sea el elemento final de una cadena de certificación que incluya a los Servicios de Certificación de la ANC. El término "uso de un certificado" se refiere tanto a la presentación de un certificado (como lo haría el "titular" o "propietario" de éste).

Es obligación de todo usuario el conocimiento de las condiciones y limitaciones expresadas en esta CPS.

1.3.4 Terceros aceptantes

Los Terceros Aceptantes son todas las personas o entidades diferentes del titular que deciden aceptar y confiar en un certificado emitido por los Servicios de Certificación de la ANC.

1.4 USO DE LOS CERTIFICADOS

1.4.1 Usos apropiados de los certificados

Dependiendo de los tipos de certificados difieren los usos apropiados de los mismos. A continuación se describen los usos apropiados, pero su uso no se limita exclusivamente a los mismos:

Tipo de Certificado Firma Digital – Persona
Firma y cifrado de correo electrónico con validez legal.
Firma y cifrado de documentos o archivos con validez legal.
Autenticación ante una aplicación, página o servicio web.

Tipo de Certificado Firma Digital – Email
Firma y cifrado de correo electrónico.

Tipo de Certificado Firma Digital – Sitio
Autenticación ante un tercero de una aplicación, página o servicio web.
Cifrado de datos.

Tipo de Certificado Firma Digital – Empresa
Firma y cifrado de correo electrónico con validez legal.
Firma y cifrado de documentos o archivos con validez legal.
Autenticación ante una aplicación, página o servicio web.

1.4.2 Limitaciones y restricciones en el uso de los certificados

Los certificados deben emplearse únicamente de acuerdo con la legislación que le sea aplicable.

Los certificados no pueden utilizarse para actuar ni como Autoridad de Registro ni como Autoridad de Certificación, firmando certificados de clave pública de ningún tipo ni Listas de Certificados Revocados (CRL).

Los servicios de certificación que ofrece ANC, no han sido diseñados ni autorizados para ser utilizados en actividades de alto riesgo o que requieran una actividad a prueba de fallos, como las relativas al funcionamiento de instalaciones hospitalarias, nucleares, de control de tráfico aéreo o ferroviario, o cualquier otra donde un fallo pudiera conllevar la muerte, lesiones personales o daños graves al medioambiente.

1.5 ADMINISTRACIÓN DE LAS POLÍTICAS

1.5.1 Correo Uruguayo como responsable de la CPS

La versión 1.0 de esta CPS fue redactada y revisada por un grupo de trabajo multidisciplinario compuesto por personal de la Administración Nacional de Correos y docentes de la Universidad de la República Oriental del Uruguay. La dirección de este grupo estuvo a cargo del Ing. Marcelo Bagnulo (ANC) y del Ing. Juan Pechiar (Universidad de la República).

La versión 1.0 de este documento ha sido revisado y aprobado por:

- Administración Nacional de Correos:
Ing. Álvaro Fernández - Gerente de Sistemas de Información
Giannella Viñoly - Gerente de Asesoría Jurídica

- Facultad de Ingeniería (Universidad de la República):
Prof. María Simon - Decana
Dr. José Vieitez - Director de Instituto de Matemáticas y Estadística
Ing. Omar Barreneche
Ing. Gabriel Gómez - Jefe del Departamento de Telecomunicaciones

La ANC tiene un grupo encargado de la CA con autoridad y responsabilidad para especificar y aprobar las modificaciones y nuevas versiones de la CPS, en el marco de su competencia, recabando la anuencia del Jerarca. El grupo encargado del manejo de políticas ha evaluado los riesgos del negocio y determinado los requerimientos de seguridad y la forma de operar que deben ser incluidas en las CP y/o CPS.

Grupo encargado de la CA:

Lic. Javier Lago – Gerente de Servicios Electrónicos
A/s Gabriel Casas – Administrador de Servicios Electrónicos

1.5.2 Persona de contacto

Todo comentario o sugerencia relativa a esta CPS puede ser dirigido a:

Lic. Javier Lago
Administración Nacional de Correos
Buenos Aires 451
Montevideo, CP 11000
Uruguay

Teléfono: 598-29160200 332
FAX: 598-29160200 331
Correo electrónico: sel@correo.com.uy

1.5.3 Determinación de la adecuación de la CPS a las políticas.

En caso que se tuviese que evaluar la posibilidad de que una CA externa interactúe con la PKI de ANC estableciendo relaciones de confianza, el grupo encargado de la CA es responsable de determinar la adecuación de la CPS de la CA externa a la Política de Certificación afectada.

1.5.4 Procedimientos de aprobación de esta CPS

El grupo encargado de la CA es encargado de la aprobación de la presente CPS y de las Políticas de Certificación asociadas. A este grupo también le compete aprobar las modificaciones de dichos documentos, en el marco de su competencia, recabando la anuencia del Jerarca.

1.6 DEFINICIONES Y ACRÓNIMOS

1.6.1 Definiciones

En el ámbito de esta CPS se utilizan las siguientes denominaciones:

Autenticación: procedimiento de comprobación de la identidad de una persona o entidad.

Certificado reconocido: Certificado expedido por un Prestador de Servicios de Certificación que cumple los requisitos establecidos en la Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.

Clave de Sesión: clave que establece para cifrar una comunicación entre dos entidades. La clave se establece de forma específica para cada comunicación, sesión, terminando su utilidad una vez finalizada ésta.

Clave Personal de Acceso (PIN): Secuencia de caracteres conocidos únicamente por el titular que permiten el acceso a los certificados.

Clave Pública y Clave Privada: la criptografía asimétrica en la que se basa la PKI emplea un par de claves en la que lo que se cifra con una de ellas sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y se la incluye en el certificado, mientras que a la otra se la denomina privada y únicamente es conocida por el titular del certificado.

Directorio: Repositorio de información que sigue el estándar X.500 de ITU-T.

Dispositivo criptográfico: instrumento que sirve para generar y almacenar los certificados tal que la generación y utilización del mismo se produzcan dentro del dispositivo y bajo la protección de un PIN.

Firma digital: es aquella firma electrónica que permite establecer la identidad personal del suscriptor respecto de los datos firmados y comprobar la integridad de los mismos, por estar vinculada de manera exclusiva tanto al suscriptor, como a los datos a que se refiere, y por haber sido creada por medios que mantiene bajo su exclusivo control. También puede ser utilizado en este documento como nombre comercial de los tipos de certificados que maneja la CA. En este caso siempre estarán acompañados de un guión y una descripción.

Firma electrónica: es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación personal.

Función hash: es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible deducir otros mensajes distintos que generen el mismo resultado al aplicar la Función hash.

Hash o Huella digital: resultado de tamaño fijo que se obtiene tras aplicar una función hash a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.

Identificación: procedimiento de reconocimiento de la identidad de un solicitante o titular de certificados.

Identificador: conjunto de caracteres que se utilizan para la identificación unívoca de un usuario en un sistema.

Jerarquía de confianza: Conjunto de autoridades de certificación que mantienen relaciones de confianza por las cuales una AC de nivel superior garantiza la confiabilidad de una o varias de nivel inferior. En el caso de ANC, la jerarquía tiene dos niveles, la AC Raíz en el nivel superior garantiza la confianza de sus AC subordinadas.

Listas de Revocación de Certificados: lista donde figuran exclusivamente las relaciones de certificados revocados o suspendidos (no los caducados).

Módulo Criptográfico: módulo de hardware utilizado para realizar funciones criptográficas y almacenar claves en modo seguro.

Prestador de Servicios de Certificación: persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

Solicitante: persona que solicita un certificado para sí mismo o para una entidad que le pertenece

Tercero Aceptante: persona o entidad diferente del titular que decide aceptar y confiar en un certificado de un tercero.

Titular: persona o entidad para el que se expide un certificado

1.6.2 Acrónimos

AGESIC: Agencia para el desarrollo del Gobierno de gestión Electrónica y la Sociedad de la Información y del Conocimiento.
ANC: Administración Nacional de Correos del Uruguay
ARL: Authority Revocation List (Lista de Autoridades Revocadas)
C: Country (País). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
CA: Autoridad de Certificación
CEN: Comité Européen de Normalisation (Comité Européo de Normalización)
CI: Cédula de Identidad
CN: Common Name (Nombre Común). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
CP: Políticas de Certificación
CPS: Certificate Practice Statement (Declaración de Prácticas de Certificación)
CRL: Certificate Revocation List (Lista de Certificados Revocados)
CWA: CEN Workshop Agreement
DN: Distinguished Name (Nombre Distintivo). Identificación unívoca de una entrada dentro de la estructura de directorio X.500.
E: Email (Correo electrónico). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
FIPS: Federal Information Processing Standard (Estándares del Gobierno Norteamericano para el procesamiento de la información)
HSM: Hardware Security Module. Módulo de seguridad criptográfico empleado para almacenar claves y realizar operaciones criptográficas de modo seguro.
IETF: Internet Engineering Task Force (Organismo de estandarización de Internet)
O: Organization. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
OCSP: Online Certificate Status Protocol. Este protocolo permite comprobar en línea la vigencia de un certificado electrónico.
OID: Object identifier (Identificador de objeto único)
OU: Organizational Unit. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
PDC: Primary Domain Controller (Controlador de Dominio Primario)
PKCS: Public Key Cryptography Standards. Estándares de PKI desarrollados por RSA Laboratories y aceptados internacionalmente.
PKI: Public Key Infrastructure (Infraestructura de Clave Pública)
PKIX: Grupo de trabajo del IETF (Public Key Infrastructure X509 IEFT WorkingGroup) constituido con el objeto de desarrollar las especificación relacionadas con las PKI e Internet.
RA: Autoridad de Registro
RFC: Request For Comments (Estándar emitido por la IETF)
S: State (Estado). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

2 REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

2.1 REPOSITORIOS

Se puede navegar en el sitio web de ANC por toda la documentación de información relacionada a la CA e instructivos para clientes. La información contenida en los repositorios de información no es de carácter confidencial. Los enlaces directos a la información relacionada con la PKI se adjuntan a continuación.

Certificados de la CA Raíz y la CA Subordinada

http://www.correo.com.uy/correocert/caroot.crt
http://www.correo.com.uy/correocert/ca.crt

Lista de Autoridades revocadas (ARL)

http://www.correo.com.uy/correocert/arl.crl

Lista de Certificados revocados (CRL)

http://www.correo.com.uy/correocert/anc.crl

Ubicación de la CPS

http://www.correo.com.uy/correocert/cps.pdf

Ubicación de la CPs

http://www.correo.com.uy/correocert/cppersona.pdf
http://www.correo.com.uy/correocert/cpemail.pdf
http://www.correo.com.uy/correocert/cpsitio.pdf
http://www.correo.com.uy/correocert/cpempresa.pdf

2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

El contenido de esta CPS, junto con cualquier otra información que se publique estará ubicada a título informativo en la dirección de Internet http://www.correo.com.uy/CorreoCert.

Cualquier persona que lo solicite podrá obtener una impresión de la CPS firmada por cualquiera de las autoridades responsables de la misma solicitándola por cualquier vía de contacto disponible en esta CPS.

La autoridad en materia de Políticas de la CA puede estimar que algunas de las revisiones de esta CPS tienen un efecto mínimo, o no tienen efecto, sobre los suscriptores y partes que hacen confianza que utilizan certificados y CRL emitidos por la CA. Esas revisiones pueden hacerse sin que se notifique de ello a los usuarios de la CPS. Las revisiones a las políticas de Certificación apoyadas por la presente CPS, así como las revisiones a la CPS que la Autoridad en materia de Políticas de la CA estime tengan un efecto importante sobre los usuarios de esta CPS, se harán notificando a los suscriptores y partes que hacen confianza.

La Autoridad en materia de Políticas de la CA notificará de los cambios que se producirán, a través del sitio Web de la CA.

La información del estado de revocación de las autoridades subordinadas será publicado periódicamente en la ARL ubicada en:
http://www.correo.com.uy/correocert/arl.crl

La información del estado de revocación de los certificados digitales será publicado periódicamente en la CRL ubicada en:
http://www.correo.com.uy/correocert/anc.crl

2.3 TIEMPO O FRECUENCIA DE PUBLICACIÓN

Para los certificados de la CA Raíz y CA Subordinada

La publicación de los certificados de la jerarquía de la ANC se llevará a cabo con anterioridad al comienzo de la prestación del servicio a través de la página oficial de ANC.

La incorporación de una nueva CA al dominio de certificación se notificará también a través del mismo medio.

Para la lista de autoridades revocadas (ARL)

La CA publicará las autoridades revocadas a la CRL pertinente dentro del periodo de tiempo estipulado en el punto *4.9.7 Frecuencia de emisión de CRLs*.

Para la lista de certificados revocados (CRL)

La CA publicará los certificados revocados a la CRL pertinente dentro del periodo de tiempo estipulado en el punto *4.9.7 Frecuencia de emisión de CRLs*.

Para la CPS

La publicación de la CPS se llevará a cabo con anterioridad al comienzo de la prestación del servicio y se mantendrá en vigencia hasta la publicación de una nueva CPS.

2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS

El acceso para la lectura a los repositorios antes mencionados (certificados de CA, ARLs, CRLs CPS y Políticas) es abierto y público, pero sólo personal autorizado podrá modificar, sustituir o eliminar información de su repositorio y sitio web. Para ello ANC establecerá controles que impidan a personas no autorizadas manipular la información contenida en los repositorios.

3 IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE CERTIFICADOS

3.1 NOMBRES

3.1.1 Tipos de nombres

Los certificados emitidos por ANC contienen el nombre distintivo (*distinguished name* o DN) X.500 del emisor y el destinatario del certificado en los campos *issuer name* y *subject name* respectivamente.

El DN del emisor tiene los siguientes campos y valores fijos:

CN = Correo Uruguayo - CA
OU = SERVICIOS ELECTRONICOS
O = ADMINISTRACION NACIONAL DE CORREOS
C = UY

En el DN de la entidad solicitante se incluyen los siguientes campos dependiendo del tipo de certificado:

Tipo de certificado Firma Digital – Persona

CN = Nombre1 Nombre2 Apellido1 Apellido2
NÚMERO DE SERIE = XXXNúmero de documento
C = Código de país
E = Correo electrónico

XXX podrá tomar el valor IDE para cédulas de identidad de Uruguay o PAS para pasaportes y únicamente esos valores.

Tipo de certificado Firma Digital – Email

E = Correo electrónico

Tipo de certificado Firma Digital – Sitio

CN = URL
OU = División dentro de la organización u organización que administra el servidor web
O = Organización
C = País

Tipo de certificado Firma Digital – Empresa

CN = Nombre de fantasía
O = Nombre de registro
OU = División o área dentro de la organización
OU = Podrá contener subdivisiones
NÚMERO DE SERIE = XXXNúmero de registro
C = Código de país
S = Departamento
E = Correo electrónico

XXX podrá tomar el valor RUC para números de registro ante DGI o BPS para números de registro de BPS y únicamente esos valores.

3.1.2 Necesidad de que los nombres sean significativos

Las reglas definidas en el apartado anterior, garantizan que los nombres distintivos (DN) de los certificados son suficientemente significativos para vincular la clave pública con una identidad o entidad.

3.1.3 Anonimato de los solicitantes

Se emiten certificados anónimamente solo en el caso de los certificados de Firma Digital – Email los cuales no tienen validez legal de firma.

3.1.4 Reglas para interpretar varios formatos de nombres

La regla utilizada por ANC para interpretar los nombres distintivos de los titulares de certificados que emite es ISO/IEC 9595 (X.500) Distinguished Name (DN). La RFC 3280 ("*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*") establece que todos los certificados emitidos a partir del 31 de diciembre de 2003 deben utilizar la codificación *UTF8String* para todos los atributos *DirectoryString* de los campos *issuer* y *subject*.

En los certificados emitidos por la PKI de ANC, los atributos de dichos campos están codificados en *UTF8String*, a excepción de los campos *country* y *serialnumber*, que están codificados en *PrintableString* de acuerdo a su definición.

3.1.5 Unicidad de los nombres

En el caso de que el certificado corresponda a una persona el campo Distinguished Name contendrá entre sus datos el número de cédula de identidad o número de pasaporte adjunto a las 3 letras que identifican el tipo de documento. Esta información implica la unicidad del nombre.

En el caso de que el certificado corresponda a un correo electrónico es requerimiento que el correo electrónico este funcional y pueda recibir correos, con lo cual no pueden existir duplicados.

En el caso de que el certificado corresponda a un servidor es requerimiento que el nombre de dominio haya sido correctamente registrado, con lo cual no pueden existir duplicados.

En el caso de que el certificado corresponda a una persona jurídica el campo Distinguished Name contendrá entre sus datos el número de registro adjunto a las 3 letras que identifican el tipo de registro. Esta información implica la unicidad del nombre

3.1.6 Reconocimiento, autenticación y papel de las marcas registradas

La documentación a presentar en el momento de solicitud de un certificado asegura la utilización legítima y el permiso explícito para la utilización de toda denominación registrada.

3.2 VALIDACIÓN DE LA IDENTIDAD INICIAL

3.2.1 Medio de prueba de posesión de la clave privada

Cuando el certificado corresponde a una persona física o jurídica, se solicita el certificado a través de la web oficial de la ANC utilizando un canal SSL. En esta solicitud genera su par de claves en uno de los medios homologados por la CA o ingresando una solicitud PKCS10. En este proceso de solicitud recibe un identificador único el cual debe presentar en las oficinas del correo ante un funcionario de la ANC que verifica su identidad.

Cuando el certificado se emite para un correo electrónico se verifica que el solicitante tenga acceso al mismo enviándole un correo con un vínculo. Se le envía el certificado a ese mismo correo electrónico.

Cuando el certificado corresponde a un servidor web o servicio, la generación del par de claves en dicho servidor se hará en presencia de un funcionario autorizado de la CA de ANC el cual auditará el proceso de generación y quedará en posesión de la clave pública que se certificará.

3.2.2 Autenticación de la identidad de una persona jurídica

No aplica para certificados de persona o de correo electrónico.

En el caso de los certificados de sitios web la identidad de la organización propietaria de un certificado es verificada por el funcionario que asiste a la generación de claves en el servidor, como se especifica en la Política de Certificación correspondiente.

En el caso de los certificados para personas jurídicas la identidad de la organización, número de registro y división es verificada a través de certificado notarial que lo acredita.

3.2.3 Autenticación de la identidad de una persona física

No aplica únicamente para certificados de correo electrónico.

En cualquier otro caso el solicitante debe presentar documento vigente y en buenas condiciones. Este documento de identidad puede ser la cédula de identidad para ciudadanos uruguayos o el pasaporte para extranjeros.

3.2.4 Información no verificada sobre el solicitante

Para todos los casos se verifica toda la información contenida en el certificado de acuerdo a los mecanismos expuestos en la Política de Certificación (CP) correspondiente a cada tipo.

3.2.5 Comprobación de las facultades de representación

Para los certificados de persona jurídica el representante deberá presentar un poder que lo habilita a realizar la solicitud así como un certificado notarial que acredita a la persona jurídica y al solicitante.

Para los demás tipos de certificado no aplica, siempre debe realizar la solicitud el titular.

3.2.6 Criterios para operar con CAs externas

No se opera con CAs externas.

3.3 IDENTIFICACIÓN Y AUTENTICACIÓN EN LAS PETICIONES DE RENOVACIÓN DE CLAVES Y CERTIFICADOS

3.3.1 Identificación y autenticación por una renovación de claves de rutina

El procedimiento de renovación en todos los casos es exactamente el mismo que el procedimiento de emisión por primera vez, por lo tanto no hay consideraciones especiales.

3.3.2 Identificación y autenticación para una renovación de claves tras una revocación

El procedimiento de renovación en este caso es exactamente el mismo que el procedimiento de emisión por primera vez, por lo tanto no hay consideraciones especiales.

4 REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS

4.1 SOLICITUD DE CERTIFICADOS

4.1.1 Quién puede efectuar una solicitud

Puede solicitar certificados cualquier persona, con cédula de identidad vigente para el caso de los ciudadanos uruguayos o con pasaporte vigente para el caso de extranjeros.

4.1.2 Registro de las solicitudes de certificados

Para todos los casos, la solicitud de certificados se hace a través de la web http://www.correo.com.uy seleccionando el tipo de certificado que se desea.

Para el caso de los certificados del tipo **Firma Digital – Persona** el titular deberá concurrir a cualquiera de las oficinas de ANC autorizadas como punto de emisión luego de haber realizado la solicitud a través de la página.

Para el caso de los certificados del tipo **Firma Digital – Email** el titular deberá concurrir a cualquiera de las oficinas de ANC autorizadas como punto de emisión luego de haber realizado la solicitud a través de la página.

Para el caso de los certificados del tipo **Firma Digital – Sitio** el titular deberá llamar por teléfono al número que se le presenta en pantalla con el fin de coordinar la visita de personal de la CA para auditar la generación de claves.

Para el caso de los certificados del tipo **Firma Digital – Empresa** el titular deberá concurrir a cualquiera de las oficinas de ANC autorizadas como punto de emisión luego de haber realizado la solicitud a través de la página.

4.2 TRAMITACIÓN DE LAS SOLICITUDES DE CERTIFICADOS

4.2.1 Realización de las funciones de identificación y autenticación

Las funciones de identificación y autenticación son realizadas en todos los casos por funcionarios de ANC los cuales validan la información en presencia del titular y su documento de identidad. Estos funcionarios están debidamente capacitados para el correcto desempeño de esta tarea.

4.2.2 Aprobación o denegación de las solicitudes de certificados

El personal de la CA aprobará y emitirá los certificados digitales solo en el caso que se hayan seguido los procedimientos de emisión descritos en las Políticas de Certificación correspondientes a cada tipo de certificado.

Si por algún motivo el funcionario que realiza la identificación y autenticación o bien el personal de la CA que aprueba los certificados detecta una anomalía en la información presentada o una falta a los procedimientos definidos, no se emitirá el certificado.

4.2.3 Plazo para la tramitación de las solicitudes de certificados

El plazo de tramitación de certificados varía dependiendo de cada tipo de certificado y el lugar donde se realiza. Para todos los casos el plazo comienza a correr a partir de finalizada la solicitud a través de la página web y la realización del contacto con la ANC para iniciar el trámite.

Para el caso de los certificados de **Firma Digital – Persona** tramitados en la Casa Central de la ANC la entrega del certificado será inmediata. En caso de ser solicitado en otro local de Montevideo o del Interior del país tardará un plazo mínimo de 1 día y un plazo máximo de 3 días hábiles.

Para el caso de los certificados de **Firma Digital – Email** tardará un plazo mínimo de 1 día y un plazo máximo de 3 días hábiles.

Para el caso de los certificados de **Firma Digital – Sitio** deberá coordinarse una visita de personal de la CA a las oficinas del cliente. Luego de realizada la visita la entrega del certificado será en un plazo no superior a 4 horas.

Para el caso de los certificados de **Firma Digital – Empresa** tramitados en la Casa Central de la ANC la entrega del certificado será inmediata. En caso de ser solicitado en otro local de Montevideo o del Interior del país tardará un plazo mínimo de 1 día y un plazo máximo de 3 días hábiles.

4.3 EMISIÓN DE CERTIFICADOS

4.3.1 Actuaciones de la CA durante la emisión de los certificados

El personal de la CA luego de corroborar que todos los procedimientos de la Política de Certificación correspondiente fueron realizados correctamente admite la realización del certificado. Este certificado se genera utilizando un procedimiento que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.

En todo momento se protege la confidencialidad e integridad de los datos de registro cifrando a través de SSL toda información que viaja entre la RA y la CA. La CA genera y publica el certificado en la base de datos de la RA para su posterior notificación al solicitante de la emisión de su certificado.

Todas las actuaciones de la CA quedan registradas en una bitácora disponible para aquellos auditores del sistema de la CA designados para dicho fin.

4.3.2 Notificación al solicitante de la emisión por la CA del certificado

La CA notifica al solicitante de la emisión de su certificado a través del correo electrónico seleccionado para dicho fin por el solicitante. Éste puede descargarse el certificado de la página web de la ANC.

4.4 ACEPTACIÓN DEL CERTIFICADO

4.4.1 Forma en la que se acepta el certificado

La solicitud de certificados es de carácter voluntario y cualquier persona puede solicitar la revocación de su certificado de forma gratuita.

Si el usuario no manifiesta la intención de revocar dichos certificados tras la expedición, se dará por confirmada la aceptación de los mismos, así como de sus condiciones de uso.

El usuario tendrá hasta 1 mes corrido a partir de su emisión para realizar cualquier reclamación sobre su certificado o sobre cualquier condición que no considere adecuada y podrá solicitar una reemisión de su certificado sin costo. Luego de transcurrido un mes, el certificado se dará como aceptado completamente y no podrá ser reclamado.

4.4.2 Publicación del certificado por la CA

No aplica ya que los certificados emitidos no se publicarán en ningún repositorio de acceso libre.

4.4.3 Notificación de la emisión del certificado por la CA a otras Entidades

Solo cuando el titular así lo indique en su solicitud y a su expreso consentimiento la CA podrá notificar de la emisión de un certificado a otra entidad para facilitar su uso.

4.5 PAR DE CLAVES Y USO DEL CERTIFICADO

4.5.1 Uso de la clave privada y del certificado por el titular

El titular sólo puede utilizar la clave privada y el certificado para los usos autorizados en esta CPS y de acuerdo con lo establecido en los campos 'Key Usage' (Uso de la Clave) de los certificados. Del mismo modo, el titular solo podrá utilizar el par de claves y el certificado tras aceptar las condiciones de uso establecidas en esta CPS y acorde a la normativa vigente.

Tras la extinción de la vigencia o la revocación del certificado el titular deberá dejar de usar la clave privada asociada para todo uso. Pese a que es recomendable que se acceda a todos los datos cifrados antes del vencimiento para re-cifrarlo con un nuevo certificado vigente se permite el uso de estas claves para el acceso a datos que pudieran estar cifrados para re-cifrarlos con un nuevo certificado.

4.5.2 Uso de la clave pública y del certificado por los terceros aceptantes

Los Terceros Aceptantes sólo pueden depositar su confianza en los certificados para aquello que establece esta CPS y de acuerdo con lo establecido en el campo 'Key Usage' del certificado.

Los Terceros Aceptantes han de realizar las operaciones de clave pública de manera satisfactoria para confiar en el certificado, así como asumir la responsabilidad de verificar el estado del certificado utilizando los medios que se establecen en esta CPS. Asimismo, se obligan a las condiciones de uso establecidas en estos documentos y en la normativa vigente.

4.6 RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVES

4.6.1 Circunstancias para la renovación de certificados sin cambio de claves

No aplica ya que todas las renovaciones de certificados realizadas en el ámbito de esta CPS se realizarán con cambio de claves.

4.7 RENOVACIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES

4.7.1 Circunstancias para una renovación con cambio claves de un certificado

El procedimiento de renovación es exactamente el mismo que el procedimiento de emisión por primera vez pudiéndose utilizar el mismo dispositivo para el certificado siempre y cuando este dispositivo siga estando homologado por la CA.

El procedimiento de renovación puede llevar un descuento en el precio.

4.7.2 Quién puede pedir la renovación de un certificado

El proceso de renovación de los certificados deberá ser solicitado de forma voluntaria y por iniciativa del solicitante. Éste deberá realizar la solicitud a través de la página web de la ANC seleccionando el tipo de certificado a renovar.

4.7.3 Tramitación de las peticiones de renovación con cambio de claves

El procedimiento de tramitación es exactamente el mismo que el procedimiento de tramitación por primera vez.

4.7.4 Notificación de la emisión de nuevos certificado al titular

El procedimiento de notificación es exactamente el mismo que el procedimiento de notificación por primera vez.

4.7.5 Forma de aceptación del certificado con nuevas claves

Las consideraciones de la forma de aceptación son exactamente las mismas que las de la primera vez.

4.7.6 Publicación del certificado con las nuevas claves por la CA

No aplica ya que los certificados emitidos no se publicarán en ningún repositorio de acceso libre.

4.7.7 Notificación de la emisión del certificado por la CA a otras Autoridades

Solo cuando el titular así lo indique en su solicitud y a su expreso consentimiento la CA podrá notificar de la renovación de un certificado a otra entidad para facilitar su uso.

4.8 MODIFICACIÓN DE CERTIFICADOS

4.8.1 Causas para la modificación de un certificado

No se realizan modificaciones a un certificado por ninguna causa. El solicitante podrá solicitar una revocación de su certificado y la tramitación de un nuevo certificado siguiendo los procedimientos antes mencionados.

Si esta revocación y su nueva solicitud se realizan en el plazo menor a un mes corrido a partir de su emisión original el certificado nuevo será sin costo.

4.9 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

La revocación y suspensión de los certificados son mecanismos a utilizar en el supuesto de que por alguna causa se deje de confiar en dichos certificados antes de la finalización del período de validez originalmente previsto.

La revocación de un certificado es el acto por el cual se deja sin efecto la validez de un certificado antes de su fecha de caducidad. El efecto de la revocación de un certificado es la pérdida de validez del mismo, originando el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia la revocación de un certificado inhabilita el uso legítimo del mismo por parte del titular.

4.9.1 Causas para la revocación

Los certificados pueden ser revocados por:

- Simple voluntad del titular.
- Sustracción, extravío o destrucción del dispositivo soporte del certificado.
- Información del certificado errónea.
- Fallecimiento del titular.
- Compromiso de las claves privadas del titular.
- Compromiso de la clave privada de la Autoridad de Certificación de la ANC.
- Por resolución judicial que lo ordene.
- Por incumplimiento por parte de la Autoridad de Certificación, de los funcionarios responsables de la expedición o del solicitante de las obligaciones establecidas en esta CPS.

4.9.2 Quién puede solicitar la revocación

Estará legitimado para solicitar la revocación de un certificado:

- El titular.
- Una autoridad judicial competente.
- Cualquier persona con la versión original del certificado de defunción del titular.
- La propia ANC como Autoridad de Certificación cuando tenga constancia de cualquier falta a esta CPS.

4.9.3 Procedimiento de solicitud de revocación

Para solicitar la revocación de un certificado se admiten indistintamente dos procedimientos. El primer método en el que la solicitud se realiza telefónicamente y el segundo método requiere presentarse en una dependencia de la autoridad.

4.9.3.1 Solicitud por Vía Telefónica

Para realizar una solicitud de revocación telefónica se requiere conocer:

• Número del documento de identidad.
• El nombre del titular del certificado tal como aparece en el mismo.
• El identificador único recibido por el solicitante al realizar la solicitud.

Este procedimiento no intenta verificar la identidad de quien solicita la revocación, más allá del conocimiento de la identidad del titular y su identificador único.

Procedimiento:

1- El interesado llama al servicio de atención en línea e indica su intención de revocar el certificado.

2- El Operario pregunta al interesado cuál es la razón para la revocación. Una vez aclarado el motivo y el alcance de la revocación, y si el interesado está de acuerdo en proseguir con la misma, el Operario continuará con el proceso.

3- El Operario informa al interesado que el proceso de revocación es irreversible, y que implica la pérdida definitiva del certificado. Asimismo se le informa que la nueva lista de certificados revocados será emitida en un plazo máximo de 24 horas.

4- El Operario solicita el nombre del titular del certificado, el número de documento de identidad, y el identificador único recibido por el solicitante al realizar la solicitud.

5- El Operario realiza la solicitud de revocación.

4.9.3.2 Solicitud Directa

En este caso, se requiere la presencia física del interesado en uno de los puntos de revocación. La documentación a presentar depende de quién sea el interesado:

Si el interesado es el titular, deberá presentar su documento de identidad vigente.
En caso de defunción del titular, la solicitud de revocación la puede efectuar cualquier persona mayor de edad que presente un acta de defunción.

En caso de revocación por orden judicial, se deberá presentar un funcionario apoderado con la orden correspondiente.

Procedimiento:

1- El interesado se presenta en uno de los puntos de revocación

2- El Operario pregunta al interesado cuál es la razón para la revocación.

3- El Operario verifica que la documentación presentada por el interesado sea correcta.

4- El Operario informa al interesado que el proceso de revocación es irreversible, y que implica la pérdida definitiva del certificado. Asimismo se le informa que la nueva lista de certificados revocados será emitida en un plazo máximo de 24 horas.

5- El Operario realiza la solicitud de revocación.

4.9.4 Período de gracia de la solicitud de revocación

La revocación se llevará a cabo de forma inmediata a la tramitación de cada solicitud verificada como válida. Por tanto, no existe ningún periodo de gracia asociado a este proceso durante el que se pueda anular la solicitud de revocación.

4.9.5 Plazo en el que la CA debe resolver la solicitud de revocación

La CA generará una nueva CRL diariamente por lo tanto el plazo máximo hasta la publicación de una nueva CRL es de 24 horas.

4.9.6 Requisitos de verificación de las revocaciones por los terceros aceptantes

La verificación de las revocaciones es obligatoria para todo uso de los certificados de cualquier tipo. El procedimiento ordinario de comprobación de la validez de un certificado será la verificación contra la CRL publicada. Un tercero aceptante puede descargar esta CRL y mantenerla de forma local durante toda la vigencia de la misma pudiendo realizar esta verificación contra la CRL local por motivos de eficiencia.

4.9.7 Frecuencia de emisión de CRLs

La CA emitirá una nueva CRL cada 24 horas. La validez de esta CRL será de 48 horas siendo esas 24 horas un tiempo adicional para que terceros aceptantes puedan actualizar sus CRLs.

Para el caso de las ARLs la frecuencia de publicación será de 1 año y la validez de 2 años.

4.9.8 Tiempo máximo entre la generación y la publicación de las CRL

La CA genera y publica la CRL en un mismo proceso, por lo tanto no existe un tiempo entre generación y publicación.

4.9.9 Disponibilidad de un sistema en línea de verificación del estado de los certificados

Por el momento la CA de la Administración Nacional de Correos no cuenta con un sistema en línea de verificación de estado de los certificados.

4.9.10 Requisitos de comprobación en línea de revocación

No aplica ya que no se cuenta con un sistema de comprobación en línea

4.9.11 Otras formas de divulgación de información de revocación disponibles

No existen otras formas de divulgación.

4.9.12 Requisitos especiales de renovación de claves comprometidas

No existe renovación de claves comprometidas.

4.9.13 Circunstancias para la suspensión

No se suspenden certificados.

4.9.14 Quién puede solicitar la suspensión

No aplica.

4.9.15 Procedimiento para la solicitud de suspensión

No aplica.

4.9.16 Límites del periodo de suspensión

No aplica.

4.10 SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS

4.10.1 Características operativas

La CRL se encuentra accesible, en formato X.509 v2, en la siguiente URL: http://www.correo.com.uy/correocert/anc.crl. Esta dirección también puede estar presente en la extensión "cRLDistributionPoints" en cada certificado emitido.

La Autoridad no publica información sobre los certificados, más allá de la CRL.

4.10.2 Disponibilidad del servicio

La CRL está disponible de forma ininterrumpida todos los días del año.

4.10.3 Características adicionales

No aplica.

4.11 FINALIZACIÓN DE LA SUSCRIPCION

4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1 Prácticas y políticas de custodia y recuperación de claves

No se realiza custodia de claves ni tampoco recuperación de claves. Para todos los casos de clave comprometida se deberá revocar el certificado y emitir un nuevo certificado.

4.12.2 Prácticas y políticas de protección y recuperación de la clave de sesión

No aplica.

5 CONTROLES DE SEGURIDAD FÍSICA, DE INSTALACIONES, DE GESTIÓN Y OPERACIONALES

En la presente sección se describirá el entorno de seguridad física en el que se encuentran enmarcados los servicios de certificación de la ANC. En particular y entre otros, se detallaran los controles de los servicios de certificación, la seguridad física de la oficina central y los controles sobre el personal.

5.1 CONTROLES FÍSICOS

5.1.1 Ubicación física y construcción

La Casa Central de la Administración Nacional de Correos está ubicada en la Ciudad Vieja de Montevideo. En esta zona se ubica el centro financiero y económico del país. El edificio cuenta con vigilancia especializada las 24 horas del día 365 días al año. El acceso a la Casa Central es controlado por dicha vigilancia y es necesaria la presentación de documentación de identificación para acceder al edificio.

Para circular dentro del edificio es necesario exhibir tarjetas magnéticas que dan cuenta del alcance de la visita dentro del edificio.

5.1.2 Acceso físico

Todas las operaciones sensibles se realizan dentro de un recinto físicamente seguro con diversos niveles de seguridad para acceder a las máquinas y aplicaciones críticas.

Para el acceso las instalaciones de la CA de la ANC se mantienen los siguientes criterios:

- Se obtiene la protección física definiendo un claro perímetro de seguridad englobando el lugar físico de la CA.
- Este perímetro está sellado, no tiene ventanas ni puertas traseras.
- Se mantienen barreras de seguridad para prevenir accesos no autorizados.
- Las puertas de acceso al lugar físico de la CA tienen alarmas y están cerradas.

- El lugar físico de la CA queda protegido con alarma cuando nadie lo ocupa.
- El lugar físico de la CA queda trancado.
- El trabajo de personal externo a la CA no supervisado no está permitido.
- El acceso al lugar físico de la CA se debe hacer mediante un proceso de identificación.
- Los visitantes permitidos dentro de la CA deben ser supervisados y se debe registrar su entrada.

5.1.3 Alimentación eléctrica y aire acondicionado

Las salas donde se ubican los equipos de la infraestructura de ANC disponen de suministro de electricidad y aire acondicionado adecuado a los requisitos de los equipos en ellas instalados. La infraestructura está protegida contra caídas de tensión o cualquier anomalía en el suministro eléctrico.

Las instalaciones disponen de sistemas de alimentación ininterrumpida con una potencia suficiente para mantener autónomamente la red eléctrica durante los períodos de apagado controlado del sistema y para proteger a los equipos frente a fluctuaciones eléctricas que los pudieran dañar. El apagado de los equipos sólo se producirá en caso de períodos prolongados de falta de suministro de energía eléctrica.

5.1.4 Exposición al agua

Se han tomado las medidas adecuadas para prevenir la exposición al agua de los equipos y el cableado. La sala se encuentra en un tercer piso en una zona donde nunca a habido inundación y no tiene ventanas hacia el exterior.

5.1.5 Protección y prevención de incendios

La sala donde se ubican los equipos de la infraestructura de ANC dispone de los medios adecuados de prevención, detección y extinción de incendios.

El cableado se encuentra en falso suelo de materiales ignífugos y la sala está equipada con un sistema de control de temperatura y un sistema de detección de humo.

5.1.6 Sistema de almacenamiento

La CA de ANC ha establecido los procedimientos necesarios para asegurar el almacenamiento de información seguro y con el respaldo adecuado.

Se cuenta con redundancia de discos en un mismo equipo y con redundancia de equipos. Se utilizan mecanismos seguros de réplica de información. Se realizan diariamente respaldos a dispositivos extraíbles que se guardan en cajas fuertes fuera de las instalaciones.

El acceso a estos soportes está restringido a personal autorizado.

5.1.7 Eliminación de los soportes de información

La eliminación de soportes, tanto papel como magnéticos, se realiza mediante mecanismos que garanticen la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se procede al formateo, borrado permanente, o destrucción física del soporte.

En el caso de documentación en papel, éste se somete a un tratamiento físico de destrucción.

5.1.8 Copias de seguridad fuera de las instalaciones

Se realizan diariamente respaldos de toda la información crítica a dispositivos extraíbles que se guardan en cajas fuertes fuera de las instalaciones con una separación física adecuada.

5.2 CONTROLES DE PROCEDIMIENTO

5.2.1 Roles responsables del control y gestión de la PKI

Se distinguen los siguientes roles para la operación y gestión del sistema:

• **Administradores HSM (Modulo Seguridad Hardware)**: Encargados de la definición de claves de administración del HSM, de su custodia, de su configuración y puesta en marcha.

• **Administradores PKI**: Encargados de la configuración del software de PKI. Este rol es responsable de la configuración general del software de PKI, que incluye, entre otros, las configuraciones de acceso a las bases de datos, la configuración de los dispositivos criptográficos a utilizar para la autenticación ante el sistema y los directorios de trabajo del sistema.

• **Auditores de Sistema**: Autorizados a consultar archivos, trazas y logs de auditoría de las entidades de la PKI.

• **Oficiales de Registro**: Son los responsables de solicitar en nombre de las entidades finales la generación/revocación de los certificados. Los funcionarios y personal contratado responsable de un puesto de expedición desempeñarán el rol de oficial de registro.

• **Oficiales de Seguridad:** Los usuarios pertenecientes a este grupo tienen la responsabilidad global de administrar la implementación de las políticas y prácticas de seguridad. Entre otras tareas definen los permisos de los roles dentro del sistema de PKI y son responsables de ejecutar tareas de backup y recuperación a este nivel.

• **Soporte Técnico**: Conjunto de usuarios autorizados a realizar ciertas tareas relacionadas con la instalación, configuración y mantenimiento de las aplicaciones base a los sistemas PKI. Responsable del funcionamiento de los sistemas de hardware y del software base. La responsabilidad de este perfil incluye, entre otros, la administración del sistema de base de batos, del repositorio de información y de los

sistemas operativos. Encargados también de ejecutar los procedimientos de backup y recuperación a este nivel.

5.2.2 Número de personas requeridas por tarea

Se requiere un mínimo de dos personas para realizar las tareas correspondientes al **Oficial de Seguridad de la CA Root** y **Administradores del HSM de la CA Root.**

5.2.3 Identificación y autenticación para cada usuario

Los Administradores HSM se identifican y autentican en los HSM mediante tarjetas criptográficas específicas de los HSM.
El resto de roles autorizados a ingresar al sistema de PKI se identifican mediante certificados electrónicos emitidos por la propia infraestructura de ANC y se autentican por medio de dispositivos criptográficos USB.

5.2.4 Roles que requieren segregación de funciones

Entre los roles se establecen las siguientes incompatibilidades, de forma que un usuario no pueda tener dos roles incompatibles:

- Incompatibilidad entre el rol Auditor del sistema y cualquier otro rol.
- Incompatibilidad entre el rol Soporte Técnico y Administradores HSM Administradores PKI y Oficiales de Seguridad.

5.3 CONTROLES DE PERSONAL

5.3.1 Requisitos relativos a la contratación, conocimiento y experiencia

Los Servicios de Certificación mantienen controles para asegurar que las prácticas de contratación de personal soportan y mejoran la confianza de las operaciones sobre la CA.

En la descripción del trabajo se establecen las responsabilidades tal como se especifican en las políticas de seguridad. Se realizan chequeos de verificación de personal a la hora de tomar nuevo personal permanente y estos firman un acuerdo de confidencialidad como parte de las condiciones iniciales de empleo. Todo personal de los Servicios de Certificación son funcionarios públicos.

El personal contratado pasa por un período no menor a 3 meses de capacitación y entrenamiento en las áreas referentes a la PKI antes pertenecer a los roles de administradores o de oficiales de seguridad de la PKI.

5.3.2 Procedimientos de comprobación de antecedentes

Conforme a la normativa general de la Administración del Estado

5.3.3 Requerimientos de formación

El personal relacionado con la administración de la PKI, recibirá la formación necesaria para asegurar la correcta realización de sus funciones.

Se incluyen en la formación los siguientes aspectos:

- Lectura completa de la Declaración de Prácticas y Políticas de Certificación.
- Concienciación sobre la seguridad física, lógica y técnica.
- Operación del software y hardware para cada papel específico.
- Procedimientos de seguridad para cada rol específico.
- Procedimientos de operación y administración para cada rol específico.
- Procedimientos para la recuperación de la operación en caso de desastres.

5.3.4 Requerimientos y frecuencia de actualización de la formación

El proceso de actualización de formación es un proceso permanente donde el personal de la PKI se mantendrá al día con cursos o seminarios relacionados con los aspectos de la PKI.

No obstante si hubiera una actualización o cambio en el software o un cambio de hardware que amerite un curso especializado, la ANC contratará en sus propias oficinas un curso especializado para el personal de la PKI.

5.3.5 Frecuencia y secuencia de rotación de tareas

No se realiza rotación de tareas.

5.3.6 Sanciones por actuaciones no autorizadas

Un proceso disciplinario existe y se utiliza para empleados que hayan incumplido las políticas o procedimientos de seguridad. Estas políticas y procedimientos tienen asociadas sanciones contra acciones no autorizadas del personal. Se toman las acciones apropiadas para que un empleado que cese en su cargo no afecte la seguridad.

Estas irregularidades serán analizadas por las áreas competentes, acorde a la reglamentación del Estado y sancionadas, en su caso, por el Directorio de la ANC.

5.3.7 Requisitos de contratación de terceros

No se realiza contratación de terceros. De realizarse se aplicaría la normativa general de la ANC acorde a la reglamentación del Estado para la contratación de terceros.

5.3.8 Documentación proporcionada al personal

Se proporcionarán la documentación de la normativa general de la ANC así como también esta CPS y las Políticas de Certificación asociadas.

5.4 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

5.4.1 Tipos de eventos registrados

Se registrarán todos los eventos relacionados con la operación y gestión del sistema, así como los relacionados con la seguridad del mismo, entre otros:

- Arranque y parada de aplicaciones.
- Intentos exitosos o fracasados de inicio y fin de sesión.
- Intentos exitosos o fracasados de crear, modificar o borrar usuarios del sistema autorizados.
- Los relacionados con la gestión del ciclo de vida de los certificados y CRLs.
- Acceso a dispositivos de respaldo.
- Cambios en la configuración del sistema.
- Mantenimiento del sistema.
- Cambios en las claves de la Autoridad de certificado.
- Cambios en las políticas de emisión de certificados y en la presente CPS.
- Registros de acceso físico de personal no perteneciente a la PKI.

Estos eventos se agrupan por categorías facilitando el acceso a los tipos de eventos a auditar.

5.4.2 Frecuencia de procesado de registros de auditoría

Los registros se analizan dependiendo de la criticidad de los eventos y pueden procesarse inmediatamente mediante alertas o manualmente con una frecuencia mensual o anual.

5.4.3 Periodo de conservación de los registros de auditoría

La información generada por los registros de auditoría se mantiene en línea y es accesible a través del sistema de PKI. Estos registros se mantendrán accesibles hasta el vencimiento de la CA Root y permanecerán accesibles al menos 5 años con posterioridad a su caducidad.

5.4.4 Protección de los registros de auditoría

Los registros de auditoría están protegidos mediante técnicas criptográficas, de forma que nadie, salvo las propias aplicaciones de visualización de eventos, con su debido control de accesos, pueda acceder a ellos.

5.4.5 Procedimientos de respaldo de los registros de auditoría

Estos registros están almacenados en las bases de datos y por lo tanto cuentan con todos los mecanismos de respaldo asociados a las mismas.

Se realizan diariamente respaldos de toda la información crítica (que incluye los registros de auditoría) a dispositivos extraíbles que se guardan en cajas fuertes fuera de las instalaciones con una separación física adecuada.

5.4.6 Sistema de recolección de información de auditoría

El sistema de recolección de auditoría está totalmente integrado con la aplicación de PKI, tanto CA como RA por lo tanto la segregación de roles y la incompatibilidad entre el rol de auditor y los demás roles.

Dentro de las características del sistema de registro de auditorías se destaca:

• Permite verificar la integridad de la base de datos, es decir, detecta una posible manipulación fraudulenta de los datos.
• Asegura el no repudio por parte de los autores de las operaciones realizadas sobre los datos. Esto se consigue mediante las firmas electrónicas de los registros.
• Guarda un registro histórico de actualización de datos, es decir, almacena versiones sucesivas de cada registro resultante de diferentes operaciones realizadas sobre él.
• Procedimiento especial de bloqueo de la aplicación. Ante una imposibilidad de acceder a la base de datos de registro de auditoría, se guarda un registro especial en el disco local y se prohíbe toda acción en el sistema. Esto asegura la integridad de los registros y que no podrá haber acciones que no se registren por error.

5.4.7 Notificación al sujeto causa del evento

El sistema maneja varios informes de error que se muestran al usuario los cuales generan registros de auditoría, pero no se prevé la notificación automática de la acción de los ficheros de registro de auditoría al causante del evento. Será decisión de los auditores la notificación al operador o a las autoridades cuando ésta sea relevante.

5.4.8 Análisis de vulnerabilidades

Tanto el hardware como el software adquirido para el desarrollo de la PKI de ANC cumplen con los más altos estándares de seguridad del mundo. Estos estándares y criterios analizan profundamente los sistemas y el hardware contra vulnerabilidades.

La ANC en su proceso de auditoría anual realiza pruebas de vulnerabilidad de toda la cadena de emisión de la PKI, desde procedimientos, solicitud, emisión y entrega.

5.5 ARCHIVO DE REGISTROS

5.5.1 Tipo de registros archivados

La CA conserva toda la información concerniente a las operaciones realizadas con los certificados en línea hasta 5 años posteriores al vencimiento de la CA Root.

No existe un proceso de archivo de eventos y terminado este período toda la información se destruye siguiendo las reglas establecidas en el punto 5.1.7.

5.5.2 Periodo de conservación del archivo

Los registros se mantienen en línea y es accesible a través del sistema de PKI. Estos registros se mantendrán accesibles hasta el vencimiento de la CA Root y permanecerán accesibles al menos 5 años con posterioridad a su caducidad.

5.5.3 Protección del archivo

No aplica.

5.5.4 Procedimientos de respaldo del archivo

No aplica.

5.5.5 Requerimientos para el sellado de tiempo de los registros

Los sistemas de PKI empleados por ANC garantizan el registro del tiempo en los que se realizan. El instante de tiempo de los sistemas se sincroniza con el servidor PDC (Controlador de Dominio Primario) de la ANC.

5.5.6 Sistema de administración del archivo

No aplica ya que la información de auditoría está siempre en línea.

5.5.7 Procedimientos para obtener y verificar información archivada

No aplica.

5.6 CAMBIO DE CLAVES DE UNA CA

Los procedimientos para proporcionar, en caso de cambio de claves de una CA, la nueva clave pública de esa CA a los titulares y terceros aceptantes son los mismos que para proporcionar la clave pública en vigor. En consecuencia, la nueva clave se publicará en el sitio web http://www.correo.com.uy.

5.7 RECUPERACIÓN EN CASOS DE COMPROMISO O CATÁSTROFE

5.7.1 Procedimientos de gestión de incidentes y vulnerabilidades

La ANC tiene establecidos mecanismos de respaldos y contingencia ante un posible acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación para recuperar las operaciones de la CA en un tiempo razonable.

Estos mecanismos, entre otros aspectos, cuentan con los siguientes componentes:

• La redundancia de los componentes más críticos.
• Equipos de respaldo alternativos.
• Procedimientos de respaldo diarios de todos los datos críticos.
• Separación de roles de administración y respaldo.
• Mínimo de 2 personas para realizar las tareas más críticas
• Custodia con único acceso del Directorio de la ANC de las tarjetas de recuperación del HSM.

5.7.2 Alteración de los recursos hardware, software y/o datos

La ANC tiene establecidos mecanismos de respaldos para recuperar las operaciones de la CA en un tiempo razonable, en caso de interrupción o falla de procesos críticos.

Para todos los casos excepto el compromiso de claves se procede a levantar los servicios de la CA en una máquina dispuesta para ese fin, recuperando la información de los respaldos más reciente. Este proceso lleva a lo sumo 48 horas.

5.7.3 Procedimiento de actuación ante el compromiso de la clave privada de la Autoridad

En el caso de que se viera afectada la seguridad de la clave privada de una Autoridad se procederá a su revocación inmediata. Seguidamente, se generará y publicará la correspondiente ARL, cesando el funcionamiento de actividad de la Autoridad.

Si la clave de la CA Root estuviera comprometida, se procedería inmediatamente a la revocación de toda la jerarquía de certificados y a la publicación en la página http://www.correo.com.uy/correocert/ de las ARLs y CRLs actualizadas.

Los certificados firmados por cualquiera de las CA dependientes de la CA afectada en el periodo comprendido entre el compromiso de la clave y la revocación del certificado correspondiente, dejarán de ser validos por lo que sus titulares podrán solicitar el reintegro de la suma abonada por el certificado revocado o solicitar la emisión de nuevos certificados bajo otra jerarquía.

5.7.4 Instalación después de un desastre natural u otro tipo de catástrofe

El sistema de los Servicios de Certificación de la ANC puede ser reconstruido en caso de desastre (destrucción completa de la sala de servidores).

Para llevar a cabo esta reconstrucción es necesario contar con:
• Un sistema con hardware, software y dispositivo HSM similar al existente.
• Los dispositivos criptográficos USB de administrador y oficial de seguridad de todas las Autoridades de Certificación de ANC.
• Las tarjetas de administrador y operador del HSM y backup del material criptográfico.
• Una copia de respaldo de la base de datos anterior al desastre.

Con estos elementos es posible reconstruir el sistema tal y como estaba en el momento de la copia de respaldo realizada y, por lo tanto, recuperar la AC, incluidas sus claves privadas.

El almacenamiento de todos los elementos se lleva a cabo en un lugar diferente, lo suficientemente alejado y protegido como para dificultar al máximo la concurrencia de catástrofes simultáneas en los sistemas en producción y en los elementos de recuperación.

5.8 CESE DE UNA CA O RA

5.8.1 Autoridad de Certificación

Solamente el Directorio de la ANC podrá poner fin a la actividad de la CA. En la circunstancia de que la CA ponga un término a sus actividades, la CA dejará de emitir nuevos certificados pero se mantendrán todos los servicios de verificación de validez de los certificados emitidos hasta la fecha de vencimiento del último certificado de entidad final. La CA dará aviso de su finalización de actividad, con una anterioridad mínima de tres meses, a todas las unidades empresariales que utilizan sus servicios.

Al concretarse la terminación de sus actividades la custodia de las claves, quedará a cargo de personal de confianza de la ANC, durante el año en que se mantiene el servicio de publicación, para ser destruidas después.

5.8.2 Autoridad de Registro

No se cesará la actividad de una RA sin cese de actividades de la CA.

6 CONTROLES DE SEGURIDAD TÉCNICA

En la presente sección se describirá el entorno de seguridad técnica en el que se encuentran enmarcados los servicios de certificación de la ANC. En particular y entre otros, se detallaran los controles de los servicios de certificación, la protección de las claves de la autoridad, seguridad informática y redes.

6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1 Generación del par de claves

Los pares de claves para los componentes internos de la PKI de ANC, concretamente CA Root y CA Subordinada, se generan en módulos de hardware criptográficos que cumplen los requisitos establecidos en un perfil de protección de dispositivo seguro de firma electrónica de autoridad de certificación de acuerdo con ITSEC, Common Criteria o FIPS 140-1 Nivel 3. Los sistemas de hardware y software que se emplean son conformes a las normas CWA 14167-1 y CWA 14167-2.

El largo de clave de las claves de los Servicios de Certificación de la ANC es de 4096 bits y su clave pública se encuentra publicada en esta CPS en formato Base64 o a disposición de quien la quiera consultar en la página web de ANC.

6.1.2 Entrega de la clave privada al titular

Para todos los casos las claves son generadas por la entidad final y la forma de generación puede variar de acuerdo al tipo de certificado.

Para los certificados de **Firma Digital - Persona** y **Firma Digital – Email y Firma Digital - Empresa** las claves son generadas por el titular ya sea en el almacén de seguridad de su navegador o en un dispositivo criptográfico homologado para dicho fin.

En el caso de los certificados de **Firma Digital – Sitio** las claves son generadas en el servidor web del solicitante donde será luego instalado el certificado.

En todos los casos las claves privadas de entidades finales están bajo su única posesión.

6.1.3 Entrega de la clave publica al emisor del certificado

Para los tipos de certificados de **Firma Digital – Persona**, **Firma Digital – Email y Firma Digital - Empresa** el propio proceso de generación de claves a través de la página web de ANC devuelve la clave pública. Al solicitante se le entrega un número de identificador único el cual tendrá que presentar en las oficinas de ANC junto a su documento de identidad para su identificación y autenticación.

Para el tipo de certificado de **Firma Digital – Sitio** la generación de claves se realiza en presencia de un funcionario de la ANC el cual guarda esta clave pública a un dispositivo magnético.

6.1.4 Entrega de la clave pública de la CA a los terceros aceptantes

Las claves públicas de las CA Root y CA Subordinadas están publicadas en el sitio web de la ANC (http://www.correo.com.uy) en formato PEM y Base64. También están publicadas en esta CPS en formato Base64.

Puede solicitarse la clave pública de la CA Root y CA Subordinada personalmente en las oficinas de ANC.

ANC es parte del "Windows Root Certificate Program" y la CA Root podrá ser distribuida en los productos Microsoft.

6.1.5 Tamaño de las claves

El tamaño de las claves de la AC Raíz es de 4096 bits.

El tamaño de las claves de las AC Subordinadas será de 4096 bits.

El tamaño de las claves de los certificados de Firma Digital - Persona es de 1024 bits.

El tamaño de las claves de los certificados de Firma Digital - Email es de 1024 bits.

El tamaño de las claves de los certificados de Firma Digital - Sitio podrá ser de 1024 o 2048 bits.

El tamaño de las claves de los certificados de Firma Digital - Empresa es de 1024 bits.

6.1.6 Parámetros de generación de la clave pública y verificación de la calidad

La clave pública de la CA Raíz y de la CA Subordinada está codificada de acuerdo con RFC 3280 y PKCS#1. El algoritmo de generación de claves es el RSA de 4096 bits.

El Hardware utilizado para la generación de las claves cumple con el estándar FIPS 140-1 Nivel 3 y cumple con todos los requerimientos de generación de claves de alta calidad.

6.1.7 Usos admitidos de la clave (campo KeyUsage de X.509 v3)

Los usos admitidos de la clave para cada tipo de certificado emitido por ANC están definidos por la Política de Certificación que le sea aplicable.

Todos los certificados emitidos por ANC contienen la extensión 'Key Usage' definida por el estándar X.509 v3, la cual se califica como crítica.

6.2 PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS

6.2.1 Estándares para los módulos criptográficos

Los HSM donde se encuentran las claves privadas de la CA Root y CA Subordinada, son módulos de hardware criptográficos que cumplen los requisitos establecidos en un perfil de protección de dispositivo seguro de firma electrónica de autoridad de certificación de acuerdo con ITSEC, Common Criteria o FIPS 140-1 Nivel 3. Los sistemas de hardware y software que se emplean son conformes a las normas CWA 14167-1 y CWA 14167-2.

6.2.2 Control multipersona (m de n) de la clave privada

El acceso a la clave privada de la CA Root está bajo un control multipersona de 2 de 3 (con tarjetas de respaldo de 2 de 3) para un total de 2 de 6 tarjetas. Las tarjetas de respaldo están bajo custodia del Directorio de la ANC según acta elaborada el doce de agosto de 2008.

El acceso a la clave privada de la CA Subordinada está bajo protección 1 de 3 (con tarjetas de respaldo 1 de 3) para un total de 1 de 6.

Todos los mecanismos de acceso se realizan por autenticación doble (dispositivo o tarjeta y clave)

6.2.3 Custodia de la clave privada

La ANC no contrata a terceros para custodia de sus claves ni custodia claves de entidades finales.

6.2.4 Copia de seguridad de la clave privada

Las claves privadas de las CAs de la ANC están guardadas bajo la protección de los HSM que cada una de ellas posee. La clonación del material criptográfico de un HSM sólo es viable a través de un mínimo de dos personas.

Las tarjetas de respaldo están en cajas fuertes ignífugas bajo custodia del Directorio de la ANC según acta elaborada el doce de agosto de 2008. En esta acta el Directorio de la ANC se compromete a no dar acceso a ninguna persona, incluidos los titulares de las mismas salvo en situaciones debidamente probadas en que se produzca un siniestro informático y/o en que uno de los titulares se desvincule de la organización.

6.2.5 Archivo de la clave privada

Las claves privadas de la CAs del ANC quedan respaldadas en ficheros cifrados con claves fragmentadas en las tarjetas antes mencionadas custodiadas por el Directorio de la ANC.

Estas tarjetas pueden ser utilizadas para recuperar la clave privada en caso de fallo del HSM. Las tarjetas se custodian en cajas fuertes ignífugas.

6.2.6 Transferencia de la clave privada a o desde el módulo criptográfico

La transferencia de la clave privada de las CAs de los servicios de certificación de la ANC sólo se puede hacer entre módulos criptográficos (HSM) y requiere de la intervención de de un mínimo de dos personas autorizadas.

6.2.7 Almacenamiento de la clave privada en un módulo criptográfico

Las claves privadas se generan directamente en el módulo criptográfico en el momento de la creación de cada una de las Autoridades de ANC que hacen uso de dichos módulos.

6.2.8 Método de activación de la clave privada

La clave privada tanto de la CA Root como de la CA Subordinada, se activa mediante la inicialización del software de CA por medio de la combinación mínima de personas de la AC correspondiente y el ingreso de su clave (PIN). Posterior a la activación la persona autorizada deberá autenticarse ante el sistema con su dispositivo criptográfico USB con su respectiva clave (PIN). Éste es el único método de activación de dicha clave privada.

6.2.9 Método de desactivación de la clave privada

Un administrador puede proceder a la desactivación de la clave de las Autoridades de

Certificación de ANC mediante la detención del software de CA. Para su reactivación es necesario seguir el método expresando anteriormente.

6.2.10 Método de destrucción de la clave privada

En términos generales la destrucción siempre debe ser precedida por una revocación del certificado asociado a la clave, si éste estuviese todavía vigente.

En el caso de las CAs de la jerarquía de la ANC la destrucción consistiría en el borrado seguro de las claves de los HSM que las albergase, así como de las copias de seguridad la misma. Para ello el HSM cuenta con herramientas diseñadas para dicho fin.

6.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

6.3.1 Archivo de la clave pública

Los servicios de certificación de ANC mantendrán publicadas sus claves públicas hasta el vencimiento del último certificado de entidad final emitido por la correspondiente CA.

6.3.2 Periodos operativos de los certificados y periodo de uso para el par de claves

Los periodos de utilización de las claves son los determinados por la duración del certificado, y una vez transcurrido no se pueden continuar utilizando.

El certificado y el par de claves de la CA Root de ANC se mantiene válido hasta el Martes 31 de Diciembre de 2030 a las 12:59:59 a.m.

El certificado y el par de claves de la CA Subordinada de ANC se mantiene válido hasta el Martes 31 de Diciembre de 2030 12:50:00 a.m.

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 certificación.

Los certificados de entidad final tienen una validez de 1 o 2 años a partir de su emisión. La caducidad de un certificado de entidad final inhabilita el uso legítimo por parte de dicha entidad.

6.4 DATOS DE ACTIVACIÓN

6.4.1 Generación e instalación de los datos de activación

Para la generación de la Autoridad de Certificación de la ANC se crearon credenciales en dispositivos criptográficos, que servirán para actividades de administración, funcionamiento y recuperación. La CA opera con varios tipos de roles, cada uno con

sus correspondientes dispositivos criptográficos donde se almacenan los datos de activación.

Para la activación del sistema de la CAs es necesaria la intervención de los administradores del HSM que tienen el conocimiento del PIN o clave de acceso al dispositivo que permite activar las claves privadas. A su vez los usuarios autorizados del sistema tendrán sus dispositivos criptográficos el conocimiento del PIN de acceso al sistema.

En el caso de las claves asociadas a los certificados de entidad final, el dato de activación consiste en el PIN o clave personal de acceso del dispositivo o almacén que las contiene.

6.4.2 Protección de los datos de activación

Sólo el personal autorizado de la PKI de la ANC correspondientes a cada AC, posee los dispositivos criptográficos y conoce las claves de acceso para acceder a los datos de activación.

En el caso de las claves asociadas a los certificados de entidad final, sólo el titular conoce la clave de acceso o PIN, siendo por tanto el único responsable de la protección de los datos de activación de sus claves privadas. Esta responsabilidad está a su vez plasmada en un contrato en soporte papel que se firma entre la ANC y la entidad final donde el titular se compromete a su correcto resguardo.

6.4.3 Otros aspectos de los datos de activación

En todos los casos las claves de acceso son de carácter confidencial, personal e intransferible y es el parámetro que protege las claves privadas permitiendo la utilización de los certificados en los distintos sistemas; por lo tanto, debe seleccionarse a conciencia y tratarse con especial cuidado.

6.5 CONTROLES DE SEGURIDAD INFORMÁTICA

6.5.1 Requerimientos técnicos de seguridad específicos

El acceso a los sistemas de la CA está restringido a personal autorizado mediante controles de acceso de usuarios a los sistemas operativos y a las aplicaciones de PKI.

Existen políticas de control de acceso a los sistemas que incluyen:

- Roles con sus correspondientes permisos
- Identificación y autenticación por usuario
- Autenticación doble (dispositivo criptográfico y clave)
- Segregación de tareas
- Control multipersona para la realización de tareas críticas.

Se sigue un proceso de registro y borrado de usuarios para permitir el acceso a los sistemas y la modificación de privilegios y el manejo de las claves de acceso de los mismos está restringida y controlada.

Se requiere a todos los usuarios del sistema que sigan procedimientos seguros en la elección y modificación de claves de acceso.

6.5.2 Evaluación de la seguridad informática

Los subsistemas que constituyen la PKI de la ANC son fiables, de acuerdo con la especificación técnica CWA 14167-1. Al momento de selección del software de PKI a utilizar se realizó un exhaustivo análisis de los sistemas existentes evaluando especialmente las normas de seguridad que cumplían. El sistema de PKI de los Servicios de Certificación de la ANC cumple con los más altos estándares de seguridad.

6.6 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

6.6.1 Controles de desarrollo de sistemas

Al momento de selección del software de PKI a utilizar la ANC realizó un exhaustivo análisis de los sistemas existentes. El sistema de PKI adquirido de los servicios de certificación de la ANC cumple con el Common Criteria EAL 4+ "Methodically Designed, Tested and Reviewed".

6.6.2 Controles de gestión de seguridad

El correcto funcionamiento de los sistemas se chequea por personal calificado de forma periódica y se realizan pruebas de funcionamiento y un seguimiento de las necesidades de crecimiento.

6.6.3 Controles de seguridad del ciclo de vida

Existen controles de seguridad a lo largo de todo el ciclo de vida de los sistemas que tengan impacto en la seguridad de ANC por ejemplo el análisis de intentos fallidos de ingresos no autorizados al sistema.

6.7 CONTROLES DE SEGURIDAD DE LA RED

La infraestructura de la red utilizada por el sistema de la ANC cuenta con todos los mecanismos de seguridad necesarios para garantizar un servicio fiable e íntegro donde se destacan los siguientes:

- Se le provee acceso a los usuarios solo a los servicios que les fueron autorizados.
- Se controla, filtra y cifra el acceso desde los clientes hasta los servidores.
- Todo acceso está restringido por defecto y solo se accede con permiso específicamente configurado.
- Los componentes más críticos están totalmente desconectados de la red.
- Para proteger la red interna de accesos desde redes externas se utiliza un firewall y se utiliza otro firewall para separar los sistemas de PKI de los demás sistemas de la ANC.

6.8 SELLADOS DE TIEMPO

Todos los sistemas que constituyen la infraestructura de clave pública de la ANC guardan registros de tiempo de todas las actividades. Estos sistemas estarán sincronizados en fecha y hora utilizando como fuente el servidor PDC (Controlador de Dominio Primario) de la ANC.

7 PERFILES DE LOS CERTIFICADOS, CRL Y OCSP

7.1 PERFIL DE CERTIFICADO

7.1.1 Número de versión

Los certificados de entidades finales emitidos por la CA utilizan el estándar X.509 versión 3. (X.509 v3)

7.1.2 Extensiones del certificado

Las extensiones de los certificados genéricas dependen de su tipo. Para todos sus certificados, la ANC tiene definida una política de asignación de OIDs dentro de su rango privado de numeración por la cual el OID de todas las extensiones propietarias de Certificados de ANC comienza con el prefijo 1.3.6.1.4.1.31439.1.

Extensiones para cada tipo de certificado:

Firma Digital - PERSONA	
Campos X509v1	**Contenido**
1. Version	V3
2. Serial Number	No secuencial
3. Signature	sha1RSA o sha256RSA
4. Issuer	CN = Correo Uruguayo - CA OU = SERVICIOS ELECTRONICOS O = ADMINISTRACION NACIONAL DE CORREOS C = UY
5. Validity	1 año
6. Subject	CN = NOMBRE1 NOMBRE2 APELLIDO1 APELLIDO2 SERIALNUMBER = [IDE o PAS][Numero de documento] C = Código de país
	E = Correo Electrónico
7. Subject Public Key	RSA (1024 bits)
Campos X509v3	
1. Authority Key Identifier	Hash sobre la clave de la CA
2. Subject Key Identifier	Hash sobre la clave del sujeto
3. Key Usage	Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement
4. Private Key Usage Period	No se usará
5. Certificate Policies	OID = 1.3.6.1.4.1.31439.1.1.1.1 Valor = http://www.correo.com.uy/correocert/cps.pdf
6. Policy Mappings	No se usará
7. Subject Alternative Name	RFC822 = Correo Electrónico
8. Issuer Alternative Name	No se usará
9. Subject Directory Attributes	No se usará
10. Basic Constraints	Entidad final
11. Name Constraints	No se usará
12. Policy Constraints	No se usará
13. Extended key usage field	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)
14. CRL Distribution Points	http://www.correo.com.uy/CorreoCert/anc.crl
15. 1.3.6.1.4.1.31439.1.1.1.1.1	Especifica el medio (Disco / Dispositivo)

Firma Digital - EMAIL	
Campos X509v1	**Contenido**
1. Version	V3
2. Serial Number	No secuencial
3. Signature	sha1RSA o sha256RSA
4. Issuer	CN = Correo Uruguayo - CA OU = SERVICIOS ELECTRONICOS O = ADMINISTRACION NACIONAL DE CORREOS C = UY
5. Validity	1 año
6. Subject	E = Correo electrónico
7. Subject Public Key	RSA (1024 bits)
Campos X509v3	
1. Authority Key Identifier	Hash sobre la clave de la CA
2. Subject Key Identifier	Hash sobre la clave del sujeto
3. Key Usage	Digital Signature, Data Encipherment
4. Private Key Usage Period	No se usará
5. Certificate Policies	OID = 1.3.6.1.4.1.31439.1.1.1.2 Valor = http://www.correo.com.uy/correocert/cps.pdf
6. Policy Mappings	No se usará
7. Subject Alternative Name	RFC822 = Correo Electrónico
8. Issuer Alternative Name	No se usará
9. Subject Directory Attributes	No se usará
10. Basic Constraints	Entidad final
11. Name Constraints	No se usará
12. Policy Constraints	No se usará
13. Extended key usage field	Correo seguro (1.3.6.1.5.5.7.3.4)
14. CRL Distribution Points	http://www.correo.com.uy/CorreoCert/anc.crl

Firma Digital - SITIO	
Campos X509v1	**Contenido**
1. Version	V3
2. Serial Number	No secuencial
3. Signature	sha1RSA o sha256RSA
4. Issuer	CN = Correo Uruguayo - CA OU = SERVICIOS ELECTRONICOS O = ADMINISTRACION NACIONAL DE CORREOS C = UY
5. Validity	1 año o 2 años
6. Subject	CN = URL O = Organización OU = Unidad Organizativa C = País E = Correo Electrónico
7. Subject Public Key	RSA (1024 bits) o RSA (2048 bits)
Campos X509v3	
1. Authority Key Identifier	Hash sobre la clave de la CA
2. Subject Key Identifier	Hash sobre la clave del sujeto
3. Key Usage	Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement
4. Private Key Usage Period	No se usará
5. Certificate Policies	OID = 1.3.6.1.4.1.31439.1.1.1.3
	Valor = http://www.correo.com.uy/correocert/cps.pdf
6. Policy Mappings	No se usará
7. Subject Alternative Name	DNSname = Podrá contener URLs alternativas.
8. Issuer Alternative Name	No se usará
9. Subject Directory Attributes	No se usará
10. Basic Constraints	Entidad final
11. Name Constraints	No se usará
12. Policy Constraints	No se usará
13. Extended key usage field	Autenticación de servidor (1.3.6.1.5.5.7.3.1) Autenticación del cliente (1.3.6.1.5.5.7.3.2)
14. CRL Distribution Points	http://www.correo.com.uy/CorreoCert/anc.crl

Firma Digital – EMPRESA	
Campos X509v1	**Contenido**
1. Version	V3
2. Serial Number	No secuencial
3. Signature	sha1RSA o sha256RSA
4. Issuer	CN = Correo Uruguayo - CA OU = SERVICIOS ELECTRONICOS O = ADMINISTRACION NACIONAL DE CORREOS C = UY
5. Validity	1 año
6. Subject	CN = Nombre de fantasía de la persona jurídica O = Nombre de registro de la persona jurídica OU = División o Unidad dentro de la persona jurídica OU = Subsecuentes OU podrán contener subdivisiones C = Código de país S = Departamento E = Correo electrónico SerialNumber = [RUC o BPS][Numero de registro]
7. Subject Public Key	RSA (1024 bits)
Campos X509v3	
1. Authority Key Identifier	Hash sobre la clave de la CA
2. Subject Key Identifier	Hash sobre la clave del sujeto
3. Key Usage	Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement
4. Private Key Usage Period	No se usará
5. Certificate Policies	OID = 1.3.6.1.4.1.31439.1.1.1.4 Valor = http://www.correo.com.uy/correocert/cps.pdf
6. Policy Mappings	No se usará
7. Subject Alternative Name	RFC822 = Correo electrónico otherName = Podrá contener la identificación de la persona física solicitante en el formato: [IDE o PAS][Numero de documento]/[NOMBRE COMPLETO]
8. Issuer Alternative Name	No se usará
9. Subject Directory Attributes	No se usará
10. Basic Constraints	Entidad final
11. Name Constraints	No se usará
12. Policy Constraints	No se usará
13. Extended key usage field	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)
14. CRL Distribution Points	http://www.correo.com.uy/CorreoCert/anc.crl

7.1.3 Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos:

SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)

7.1.4 Formatos de nombres

Los certificados emitidos por ANC contienen el *distinguished name* X.500 del emisor y del titular del certificado en los campos *"Issuer" y "Subject"* respectivamente.

El *Subject* para los certificados de **Firma Digital – PERSONA** estará compuesto de los siguientes elementos: CN, SerialNumber, C, E.

El atributo "CN" (commonName) contendrá el nombre completo en mayúsculas manteniendo el formato de uno o dos nombres y luego apellidos.

El atributo "SerialNumber" contendrá el tipo y número de documento de identidad. Este atributo concatenará un tipo de documento que será exclusivamente "IDE" para cédulas de identidad de Uruguay o "PAS" para pasaportes, con el número de documento de identidad.

El atributo "C" (*countryName*) tendrá el código de país y se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements",* en *PrintableString*.

El atributo "E" (e*mailAddress*) tendrá el correo electrónico y se codificará*,* en *IA5String*.

El *Subject* para los certificados de **Firma Digital – EMAIL** estará compuesto del siguiente elemento: E.

El atributo "E" (e*mailAddress*) tendrá el correo electrónico y se codificará*,* en *IA5String*.

El *Subject* para los certificados de **Firma Digital – SITIO** estará compuesto de los siguientes elementos: CN, O, OU, C, S, E.

El atributo "CN" (commonName) contendrá la URL a certificar.

El atributo "O" (organizationName) contendrá el nombre de registro o fantasía de la empresa.

El atributo "OU" (organizationalUnitNames) contendrá el nombre de la unidad (división, área, sector, departamento, etc.) dentro de la empresa.

El atributo "C" (*countryName*) tendrá el código de país y se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements",* en *PrintableString*.

El atributo "S" (*stateName*) tendrá el nombre del departamento, estado o provincia de registro de la organización.

El atributo "E" (e*mailAddress*) tendrá el correo electrónico y se codificará, en *IA5String*.

El *Subject* para los certificados de **Firma Digital – EMPRESA** estará compuesto de los siguientes elementos: CN, O, OU, OU, C, S, E, serialNumber.

El atributo "CN" (commonName) contendrá el nombre de fantasía de la persona jurídica completo en mayúsculas.

El atributo "O" (organizationName) contendrá el nombre de registro de la persona jurídica completo en mayúsculas.

El atributo "OU" (organizationalUnitNames) contendrá el nombre de la unidad (división, área, sector, departamento, etc.) dentro de la organización.

Subsecuentes atributos "OU" (organizationalUnitNames) podrán existir y contener subdivisiones dentro de la unidad (división, área, sector, departamento, etc.).

El atributo "C" (*countryName*) tendrá el código de país y se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements",* en *PrintableString*.

El atributo "S" (*stateName*) tendrá el nombre del departamento, estado o provincia de registro de la organización.

El atributo "E" (e*mailAddress*) tendrá el correo electrónico y se codificará, en *IA5String*.

El atributo "SerialNumber" contendrá el tipo y número de registro de la persona jurídica. Este atributo concatenará un tipo de registro que será exclusivamente "RUC" para números de registro ante la Dirección General Impositiva o "BPS" para números de registro ante el Banco de Previsión Social, con el número de registro o documento.

7.1.5 Restricciones de los nombres

Los nombres contenidos en los certificados están restringidos a *"Distinguished Names"* X.500, que son únicos y no ambiguos.

7.1.6 Identificador de objeto (OID) de la Política de Certificación

El OID de la presente CPS es 1.3.6.1.4.1.31439.1.1.

Se le añade una extensión para cada autoridad emisora de certificados y otra extensión para cada tipo de certificado que ésta emite.

Correo Uruguayo - CA	1.3.6.1.4.1.31439.1.1.1
• Firma Digital – PERSONA	1.3.6.1.4.1.31439.1.1.1.1
• Firma Digital – EMAIL	1.3.6.1.4.1.31439.1.1.1.2
• Firma Digital – SITIO	1.3.6.1.4.1.31439.1.1.1.3
• Firma Digital – EMPRESA	1.3.6.1.4.1.31439.1.1.1.4

7.1.7 Uso de la extensión "PolicyConstraints"

No aplica.

7.1.8 Sintaxis y semántica de los "PolicyQualifier"

La extensión 'Certificate Policies' contiene los siguientes 'Policy Qualifiers':

Identificador de directiva=1.3.6.1.4.1.31439.1.1.1.x
[1,1]Información de calificador de directiva:
Id. de calificador de directiva=CPS
Calificador: http://www.correo.com.uy/correocert/cps.pdf

7.1.9 Tratamiento semántico para la extensión "Certificate Policy"

La extensión 'Certificate Policies' contiene para cada tipo de certificado el identificador de directiva asociado al mismo.

7.2 PERFIL DE CRL

7.2.1 Número de versión

La infraestructura del ANC utiliza CRLs X.509 versión 2 (v2).

7.2.2 CRL y extensiones

Las CRLs emitidas por la PKI de ANC serán conformes con la norma RFC 3280 (Internet X.509 Public Key Infrastructure - Certificate and CRL Profile).

7.3 PERFIL DE OCSP

No se utiliza un servidor de validación en línea OCSP.

7.3.1 Número de versión

No aplica.

7.3.2 Extensiones OCSP

No aplica.

8 AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

8.1 FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES PARA CADA AUTORIDAD

Acorde a las atribuciones delegadas en AGESIC por el gobierno de de la República Oriental del Uruguay, esta agencia realizará auditorías de cumplimiento con las normativas vigentes y a la adecuación del funcionamiento y operativa con las estipulaciones incluidas en esta CPS.

Establecer la frecuencia de estos controles estará en manos de la AGESIC.

Sin perjuicio de lo anterior, personal de la ANC realizará auditorías internas bajo su propio criterio o en cualquier momento, ya sea para asegurar el cumplimiento o a causa de una sospecha de incumplimiento de alguna medida de seguridad por parte de alguno de sus operadores.

8.2 IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR

Todo equipo o persona designada para realizar una auditoría de seguridad sobre el sistema de PKI deberá cumplir los siguientes requisitos:

- Adecuada capacitación y experiencia en PKI, seguridad, tecnologías criptográficas y procesos de auditoría.
- Independencia a nivel organizativo de la ANC.

8.3 RELACIÓN ENTRE EL AUDITOR Y LA AUTORIDAD AUDITADA

Al margen de la función de auditoría, el auditor externo y la ANC no deberán tener relación alguna que pueda derivar en un conflicto de intereses. En el caso de los auditores internos, estos no podrán tener relación funcional con el área objeto de la auditoría.

8.4 ASPECTOS CUBIERTOS POR LOS CONTROLES

La auditoría determinará la adecuación de los servicios de PKI de ANC con esta CPS. También determinará los riesgos del incumplimiento de alguna de las políticas definidas por este documento.

8.5 ACCIONES A EMPRENDER COMO RESULTADO DE LA DETECCIÓN DE DEFICIENCIAS

La identificación de deficiencias detectadas como resultado de la auditoría dará lugar a la adopción de medidas correctivas. El grupo encargado de la CA en colaboración con el auditor, será la responsable de la determinación de las mismas.

En el caso de observarse deficiencias graves el grupo encargado de la CA podrá adoptar, entre otras, las siguientes decisiones: suspensión temporal de las

operaciones hasta que las deficiencias se corrijan, revocación del certificado de la Autoridad, cambios en el personal implicado y auditorías y controles más frecuentes.

8.6 COMUNICACIÓN DE RESULTADOS

El equipo auditor comunicará los resultados de la auditoría al grupo encargado de la CA, a las autoridades de responsables de la PKI y al Directorio de la ANC.

9 OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

9.1 TARIFAS

9.1.1 Tarifas de emisión de certificado o renovación

La ANC cobra únicamente por la emisión y renovación de los certificados digitales que emite. El titular no adquiere ninguna otra deuda por solicitud, acceso, solicitud de revocación o soporte sobre de ningún tipo.

Las tarifas asociadas a cada tipo de certificado podrán variar acorde a las decisiones comerciales de la ANC y no estarán publicadas en esta CPS.

9.1.2 Tarifas de acceso a los certificados

No aplica.

9.1.3 Tarifas de acceso a la información de estado o revocación

No aplica.

9.1.4 Tarifas de otros servicios tales como información de políticas

No aplica.

9.1.5 Política de reembolso

El solicitante tendrá hasta 30 días a partir de la fecha de emisión para solicitar cualquier reclamo. Pasado ese tiempo se entenderá total aceptación al pago y a la información contenida en el certificado.

En el caso de haberse producido una falla en la emisión y previo a los 30 días el titular podrá solicitar un reembolso de la totalidad del importe abonado o la reemisión de su certificado sin costo alguno.

Pasados los 30 días no habrá reembolsos ni devoluciones de ningún tipo.

9.2 RESPONSABILIDADES ECONÓMICAS

La ANC se hará cargo de la responsabilidad económica de su PKI por incumplimiento de toda garantía expresa comprometida según los términos de esta CPS y/o CP aplicable, limitándose a los daños directos hasta un monto máximo del costo del certificado en el momento de la compra. En la contratación quedan claros los límites en cuanto al posible uso del Certificado y las transacciones válidas que pueden realizarse empleándolo; notificándose expresamente la limitación cuantitativa de responsabilidad de la que da cuenta la presente cláusula.

9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN

9.3.1 Ámbito de la información confidencial

Toda información que no sea declarada expresamente como pública en esta CPS será el carácter de confidencial.

Se declara expresamente como información confidencial:

• Confidencialidad de la clave privada de la Autoridad de Certificación:

La Autoridad de Certificación garantiza la confidencialidad frente a terceros de su clave privada, la cual, al ser el punto de máxima confianza será generada y custodiada conforme a lo que se especifique en esta CPS.

• Confidencialidad de la clave privada de entidades finales:

Para garantizar la confidencialidad de las claves privadas de entidades finales la Autoridad de Registro de la ANC, proporcionará los medios para que la generación de dichas claves sólo se realice de modo seguro por el titular o en su presencia.

La Autoridad de Registro como de Certificación no tendrán la posibilidad de almacenar, copiar o conservar cualquier tipo de información que sea suficiente para reconstruir estas claves.

• Confidencialidad en la prestación de servicios de certificación:

La ANC publicará exclusivamente aquellos datos imprescindibles para la validación de los certificados digitales que emite.

• Protección de datos

Existe un repositorio de datos personales de los solicitantes con la finalidad de servir a los usos previstos en esta CPS o cualquier otro relacionado con los servicios de PKI.

La ANC no podrá compartir o divulgar estos datos a ninguna otra organización sin el previo consentimiento del titular de la información.

• Registros de auditoría

Los resultados de auditorías tanto internas como externas son de carácter confidencial.

• Cualquier otra información

Toda información, clasificada o no como confidencial, a excepción de la expresamente declarada como pública en esta CPS será de carácter confidencial.

9.3.2 Información no confidencial

Se considera información pública y por lo tanto accesible por terceros:

• La contenida en la presente Declaración de Prácticas de Certificación y Políticas de Certificación.

• La información sobre el estado de los certificados.

• Toda otra información marcada por ANC como "Pública".

9.3.3 Responsabilidad de protección de la información confidencial

Los funcionarios de la ANC que participen en cualquier tarea propia o derivada de la PKI están obligados al deber de secreto profesional y por lo tanto sujetos a la normativa reguladora que les es aplicable.

9.4 PROTECCIÓN DE LA INFORMACIÓN PERSONAL

9.4.1 Política de protección de datos de carácter personal

Existe un repositorio de datos personales de los solicitantes con la finalidad de servir a los usos previstos en esta CPS o cualquier otro relacionado con los servicios de PKI.

Se permitirá al interesado el ejercicio de los derechos de oposición, acceso, rectificación y cancelación de sus datos de carácter personal, en los términos y plazos legales.

9.4.2 Información tratada como privada

Toda información personal no incluida en el certificado o en el proceso de validación del mismo es considerada como privada.

9.4.3 Información no calificada como privada

Es considerada no confidencial la siguiente información:

- Los certificados
- Los usos y límites expresados en el certificado.
- La fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha de cada uno de ellos.

9.4.4 Responsabilidad de la protección de los datos de carácter personal

Los funcionarios de la ANC que participen en cualquier tarea propia o derivada de la PKI están obligados al deber de secreto profesional y por lo tanto sujetos a la normativa reguladora que les es aplicable.

9.4.5 Comunicación y consentimiento para usar datos de carácter personal

El proceso de solicitud de un certificado digital será consentimiento del uso de la información de carácter personal para dicho fin.

9.4.6 Revelación en el marco de un proceso judicial

Los datos de carácter personal solo podrán ser comunicados a terceros, sin consentimiento del afectado, en el marco de un probado proceso judicial.

9.4.7 Otras circunstancias de publicación de información

La ANC podrá enviar la información de la clave pública de un certificado sólo con expreso consentimiento del titular y sólo a pedido del mismo, para simplificar el procedimiento de uso ante algún otro organismo.

9.5 DERECHOS DE PROPIEDAD INTELECTUAL

La ANC es titular en exclusiva de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que regula esta CPS.

Esta CPS así como cualquiera de sus versiones anteriores y las políticas en materias de certificados son propiedad de la ANC. Se prohíbe por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos sin la autorización expresa por su parte.

9.6 OBLIGACIONES

9.6.1 Obligaciones de la CA

Es la obligación fundamental de la CA el garantizar la validez y la correspondencia entre los datos contenidos en los certificados que emite, durante todo el período de validez de los mismos.

Por lo tanto debe estar siempre disponible para atender solicitudes de revocación de certificados, según se detalla en esta CPS.

Otras obligaciones particulares se detallan a continuación:

- Realizar sus operaciones en conformidad con esta CPS.
- Publicar esta CPS y comunicar los cambios.
- Emitir certificados conformes con la información conocida en el momento de su emisión, y libres de errores de entrada de datos.
- Revocar los certificados en los términos expresados en esta CPS y publicar los certificados revocados en la CRL
- Publicar los certificados correspondientes a las Autoridades de Certificación de de la ANC.
- Proteger la clave privada de las Autoridades de Certificación de la ANC.
- Conservar registrada toda la información y documentación relativa a los certificados que se emiten.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.
- No almacenar en ningún caso los datos de creación de firma, clave privada ni claves (PIN ni PUK) de los titulares de certificados.
- Colaborar con los procesos de auditoría.
- Operar de acuerdo con la legislación aplicable.

9.6.2 Obligaciones de la RA

La RA está obligada a verificar, contra presentación de documentación, la identidad del solicitante y toda la información a incluir en un certificado.

La RA se compromete a no hacer público ninguno de los datos aportados por el solicitante en el momento de emisión del certificado. Asimismo, se compromete a no guardar copia alguna de las claves privadas generadas en el momento de emisión de un certificado.

Otras obligaciones particulares se detallan a continuación:

- Realizar sus operaciones en conformidad con esta CPS.
- Comprobar exhaustivamente la identidad de las personas así como toda la información incluida o incorporada por referencia en el certificado.
- Informar a entidades finales de las responsabilidades y cuidados que debe tener para su correcto uso.
- Tramitar las peticiones de revocación con celeridad.
- Aprobar la emisión de los certificados luego de asegurar su veracidad no almacenando ni copiando los datos de creación de firma.
- No hacer público ninguno de los datos aportados por el solicitante en los términos definidos por esta CPS.

9.6.3 Obligaciones de los titulares de los certificados

Se entiende por titular de un certificado, a la persona que tiene acceso o posee la clave privada correspondiente al certificado y es su obligación mantener bajo su custodia dicha clave.

Otras obligaciones particulares se detallan a continuación:

- Suministrar a las Autoridades de Registro información correcta y completa y presentar documentación legítima en el momento de solicitud de un certificado.
- Conocer y aceptar las condiciones de utilización de los certificados, en particular las contenidas en esta CPS que le sean de aplicación, así como las modificaciones que se realicen sobre las mismas.
- Mantener bajo su custodia y no revelar ni facilitar de manera alguna el acceso a su clave privada para evitar su pérdida, revelación, alteración o uso no autorizado.
- Cumplir y aceptar las restricciones de uso que pudiera haber impuestas a sus claves y certificados emitidos por la ANC.
- Solicitar inmediatamente la revocación de un certificado en caso de tener conocimiento o sospecha del compromiso de la clave privada, entre otras causas por pérdida, robo, compromiso potencial, conocimiento por terceros de la clave personal de acceso y detección de inexactitudes en la información.
- Asegurarse de que toda la información contenida en su certificado es correcta. De lo contrario notificarlo inmediatamente.

9.6.4 Obligaciones de los terceros aceptantes

Es tercero aceptante de un certificado toda persona u organismo que, directamente o a través de algún sistema, solicita a terceros la presentación de un certificado, e interpreta su contenido.

Las obligaciones particulares se detallan a continuación:

- Limitar el uso de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados y en esta CPS.
- Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos mediante la comprobación de que el certificado es válido y no está caducado o ha sido o revocado.
- Asumir su responsabilidad en la correcta verificación de las firmas electrónicas.
- Asumir su responsabilidad en la comprobación de la validez, revocación y estado de los certificados en que confía.
- Conocer las garantías y responsabilidades derivadas de la aceptación de los certificados en los que confía y asumir sus obligaciones.
- Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo.

9.6.5 Obligaciones de otros participantes

No aplica.

9.7 LIMITACIONES DE GARANTÍAS

A excepción de lo expresamente previsto en contrario en esta CPS, y CP aplicable o por estatutos o reglamento, la total responsabilidad de la CA por incumplimiento de toda garantía expresa comprometida según los términos de esta CPS y/o CP aplicable, se limitará a los daños directos hasta un monto máximo del costo del certificado en el momento de la compra. En la contratación quedan claros los límites en cuanto al posible uso del Certificado y las transacciones válidas que pueden realizarse empleándolo; notificándose expresamente la limitación cuantitativa de responsabilidad de la que da cuenta la presente cláusula.

9.8 LIMITACIONES DE RESPONSABILIDAD

El límite máximo de responsabilidad propuesto en esta CPS será el mismo, independientemente de la cantidad de firmas digitales, transacciones, o reclamaciones relativas al certificado en cuestión. Por otra parte, en la circunstancia de que se sobrepase ese tope, el tope disponible será distribuido de la siguiente forma: primero, a las reclamaciones, según el orden en que fueron presentadas, para alcanzar la solución final del diferendo, a menos que un tribunal competente disponga en contrario.

A excepción de lo establecido por las disposiciones de la presente CPS, la ANC no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados o terceros aceptantes.

9.9 INDEMNIZACIONES

En ningún caso, la CA estará obligada a pagar más que la indemnización total correspondiente a cada certificado, independientemente del método de distribución entre los reclamantes que se aplique al monto total de la indemnización. En la contratación quedan claros los límites en cuanto al posible uso del Certificado y las transacciones válidas que pueden realizarse empleándolo; notificándose expresamente la limitación cuantitativa de responsabilidad de la que da cuenta la presente cláusula.

9.10 PERIODO DE VALIDEZ

9.10.1 Plazo

Esta CPS entra en vigor desde el momento de su publicación en el repositorio de ANC.

Esta CPS estará en vigor mientras no se derogue expresamente por la emisión de una nueva versión o por la renovación de las claves de la CA Raíz, momento en que obligatoriamente se dictará una nueva versión.

9.10.2 Sustitución y derogación de la CPS

Esta CPS será sustituida por una nueva versión con independencia de la trascendencia de los cambios efectuados en la misma, de forma que siempre será de aplicación en su totalidad.

Cuando la CPS quede derogada se retirará del repositorio público ANC, si bien se conservará como mínimo hasta el vencimiento del último certificado emitido bajo su vigencia.

9.10.3 Efectos de la finalización

Las obligaciones y restricciones que establece esta CPS, en referencia a auditorías, información confidencial, obligaciones y responsabilidades, u otras definiciones nacidas bajo su vigencia, vencerán tras su sustitución o derogación por una nueva versión a excepción de los derechos de propiedad intelectual.

9.11 NOTIFICACIONES INDIVIDUALES Y COMUNICACIONES CON LOS PARTICIPANTES

Las entidades finales podrán comunicarse con la ANC por todas las vías disponibles y públicas en esta CPS.

La ANC podrá comunicarse tanto a través del correo electrónico expresado como contacto así como por correo postal a la dirección registrada.

9.12 CAMBIOS EN LAS ESPECIFICACIONES

9.12.1 Procedimiento para los cambios

La Autoridad con atribuciones para realizar y aprobar cambios sobre esta CPS es el grupo encargado de la CA. Este grupo encargado de la CA podrá hacer modificaciones menores a esta CPS y publicarlas en el repositorio con todos los cambios especificados en el último apartado de *"Últimos Cambios"*.

9.12.2 Periodo y procedimiento de notificación

En el caso de que el grupo encargado de la CA juzgue que los cambios a la especificación pueden afectar a la aceptabilidad de los certificados para propósitos específicos se comunicará a los usuarios de los certificados correspondientes que se ha efectuado un cambio y que deben consultar la nueva CPS en el repositorio establecido. El mecanismo de comunicación será la dirección de Internet http://www.correo.com.uy/CorreoCert y publicación en el Diario Oficial.

9.12.3 Circunstancias en las que el OID debe ser cambiado

En los casos en que, a juicio del Grupo encargado de la CA, los cambios de las especificaciones no afecten a la aceptabilidad de los certificados se procederá al incremento del número menor de versión del documento y no se variará el número de Identificador de Objeto (OID) que lo representa. No se considera necesario comunicar este tipo de modificaciones a los usuarios de los certificados.

En el caso de que el Grupo encargado de la CA juzgue que los cambios a la especificación pueden afectar a la aceptabilidad de los certificados para propósitos específicos se procederá al incremento del número mayor de versión del documento y la puesta a cero del número menor de la misma. En este caso se modificará número del Identificador de Objeto (OID) que lo representa. Este tipo de modificaciones se comunicará a los usuarios de los certificados según lo establecido en esta CPS.

9.13 RECLAMACIONES Y DISPUTAS

En la eventualidad de cualquier disputa que implique a los servicios o prestaciones que incluye la presente CPS (u otra divulgación de las políticas comerciales de la CA), la parte ofendida notificará primero a la CA y a todas las partes interesadas con relación a la disputa. La CA asignará al personal adecuado para resolver el litigio.

9.14 NORMATIVA APLICABLE

La ley aplicable a este documento será la vigente sobre esta materia en el territorio de la República Oriental del Uruguay, así como los acuerdos internacionales que suscriba el país sobre la misma temática.

9.15 CUMPLIMIENTO DE LA NORMATIVA APLICABLE

Las normas vigentes en esta materia regularán la obligatoriedad e interpretación de esta CPS (u otra divulgación de políticas comerciales de la CA) para garantizar procedimientos e interpretaciones uniformes para todos los usuarios.

La CA de ANC obedece los estándares definidos en las normativas MERCOSUR.

9.16 ESTIPULACIONES DIVERSAS

9.16.1 Cláusula de aceptación completa

Todas las entidades finales y terceros aceptantes asumen la aceptación en su totalidad el contenido de la última versión de esta CPS y CP que les sean aplicables.

9.16.2 Delegación

No estipulado.

9.16.3 Divisibilidad

En el caso de que una o más estipulaciones de esta CPS sean o llegasen a ser inválidas, nulas, o inexigibles legalmente, se entenderán por no puestas, salvo que dichas estipulaciones fueran esenciales de manera que al excluirlas de la CPS careciera ésta de toda eficacia jurídica.

9.16.4 Ejecución

Cada caso será tratado por las áreas competentes de la ANC en forma independiente.

9.16.5 Fuerza Mayor

Las áreas competentes de la ANC analizarán particularmente los casos de fuerza mayor que pudieren presentarse, no siendo tratados en esta CPS.

9.17 OTRAS ESTIPULACIONES

No se contemplan.

10 ÚLTIMOS CAMBIOS

Versión	Cambio	Fecha
3.1	En el tipo de certificado de Firma Digital - PERSONA, se agrega el correo electrónico al campo "*emailAddress*" del *subject* por compatibilidad.	15/06/2009
3.2	En el tipo de certificado de Firma Digital - SITIO, se quita el largo de clave 512 y se permite la extensión DNSname para múltiples dominios dentro de SubjectAltName.	03/08/2010
3.3	Se agrega el tipo de certificado Firma Digital – EMPRESA para certificados de persona jurídica junto a la versión 1 de la CP Empresa.	12/04/2011
3.4	En el tipo de certificado de Firma Digital - SITIO, se agrega Autenticación del cliente (1.3.6.1.5.5.7.3.2) para permitir autenticación de TLS.	09/06/2014
3.5	Para todos los tipos de certificado se agrega el algoritmo sha256RSA.	21/04/2015